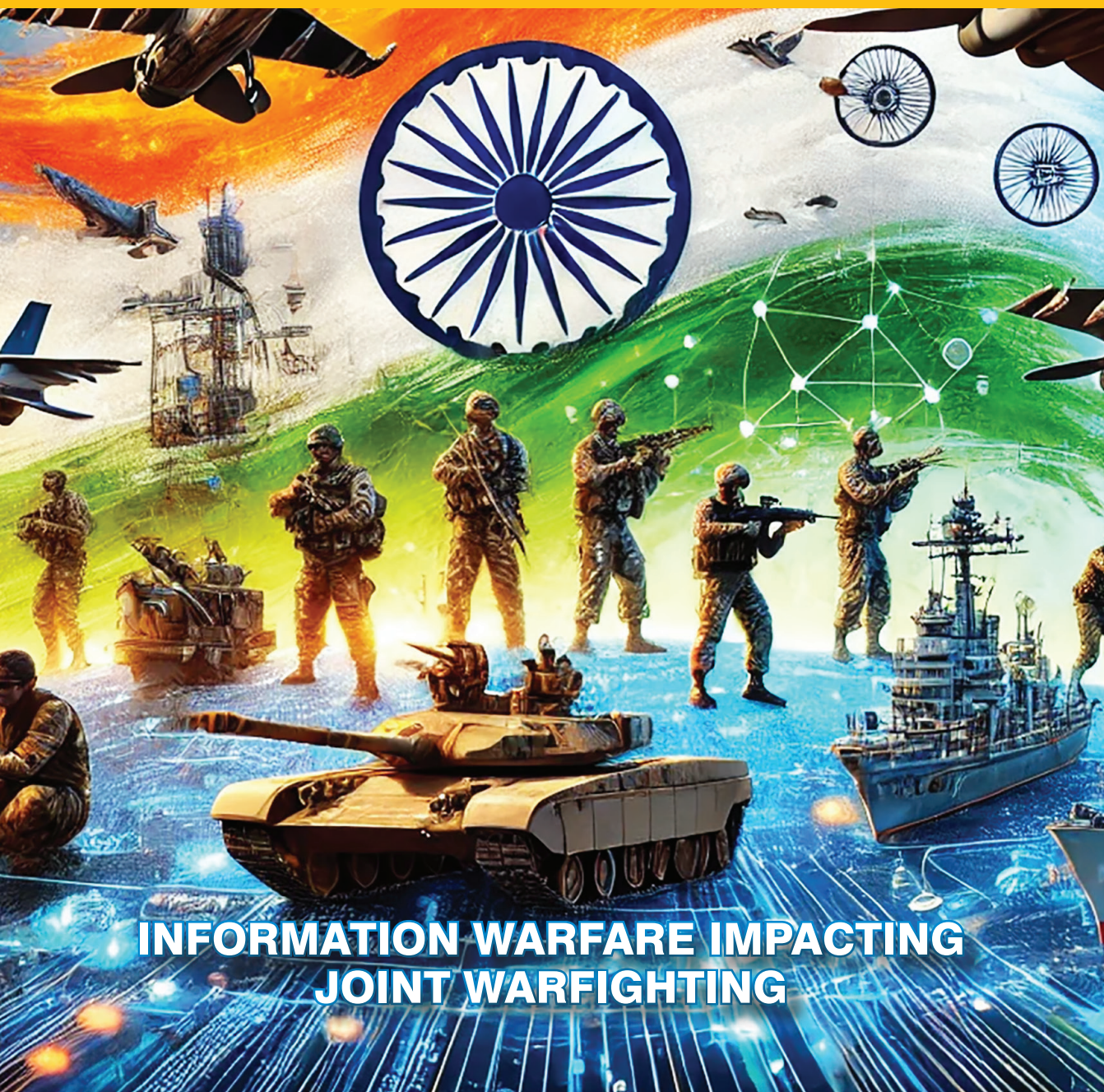
SYNERGY

Journal of the Centre for Joint Warfare Studies (CENJOWS)

VOLUME 4 ISSUE 1 ISSN : 2583-5378 FEBRUARY 2025



INFORMATION WARFARE IMPACTING JOINT WARFIGHTING

SYNERGY

JOURNAL OF THE CENTRE FOR JOINT WARFARE STUDIES

Volume 4 Issue 1 ISSN : 2583-5378 February 2025

CENJOWS
(Established : 2007)
Room No 301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi - 110003 (INDIA)
Telephone Nos : 011-24364881, 24366485
Fax : 011-24366484
Website : www.cenjows.in
E-mail : cenjows@cenjows.in, cenjows@yahoo.com

ABOUT US

CENJOWS was raised in 2007 as an independent think tank, registered under the Societies Registration Act, 1860. This aims to promote Jointness as a synergistic enabler for the growth of Comprehensive National Power and provide alternatives in all dimensions of its applications through focused research and debate.

Year of Publication	:	2025
Frequency	:	Bi-Annual
Language	:	English
Publisher	:	Maj Gen (Dr) Ashok Kumar, VSM (Retd), Director General, CENJOWS 301, B-2 Wing, 3rd Floor Pt. Deendayal Antyodaya Bhawan CGO Complex, Lodhi Road New Delhi-110003
RNI Number	:	DELENG/2022/82424
Editor	:	Maj Gen (Dr) Ashok Kumar, VSM (Retd) (dg@cenjows.in)
Deputy Editor	:	Dr Ulupi Borah, Senior Fellow (ulupi.borah@cenjows.in)

301, B-2 Wing, 3rd Floor
Pt. Deendayal Antyodaya Bhawan, CGO Complex
Lodhi Road
New Delhi-110003

All correspondence may be addressed to:
Editor
Centre for Joint Warfare Studies (CENJOWS)
301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003
Telephone: (91-11) 24366485/Telefax: (91-11) 24366484
e-mail: cenjows@cenjows.in/cenjows@yahoo.com
Website: www.cenjows.in

Price : Rs 750/- INR or US $25

RNI No: DELENG/2022/82424

Print ISSN : 2583-5378
Online ISSN : 2583-536X

INFORMATION WARFARE
IMPACTING JOINT WARFIGHTING

CONTENT

Notes:

- Views expressed in articles are individual opinions of the writers, and not of CENJOWS.
- Contributors to Synergy Journal are requested to visit the website for the theme of the next issue and guidelines.

MESSAGE

Information, in the digital era, is a critical asset and a formidable weapon at the disposal of a nation to further its national interests. Information warfare, encompassing cyber operations, psychological operations, disinformation campaigns, and many more tools alters the very nature of the battlefield. Information Warfare's impact extends beyond the digital realm into the cognitive domain and influences decision-making at all levels.

Information Warfare needs to be integrated into the planning and execution of joint operations of the armed forces to produce desired dividends. This will allow our armed forces, which operate in an extremely complex and contested information environment, to be better equipped.

Information Warfare enhances the ability of a nation to conduct operations across all domains of war disrupting the decision-making processes of the adversary and influencing public perception. Integration of information warfare into joint operations will foster greater coordination and interoperability among the different branches of the armed forces, ensuring a unified and cohesive approach to warfare.

As the lethality of Information Warfare is driven by rapid technological changes, it demands that we continue to adapt and innovate to stay ahead of the curve. We need to invest in development of better

capabilities and ensure that our personnel are trained appropriately to be able to operate in this dynamic environment. The command and control structures of the future need to be robust and resilient while being flexible and responsive to the threats of information warfare. Information warfare needs to be integrated at the national level towards the achievement of the national objectives as any disjointed effort could prove to be counter-productive.

This edition of 'Synergy' themed 'Information Warfare Impacting Joint Warfighting', aims to highlight the significance of Information Warfare and the need for its integration at the highest level. I am certain that this edition will encourage debates on the subject that would contribute towards enhancing the capability of the Indian Armed Forces in the complex domain of Information Warfare.

I must complement 'Team CENJOWS' for taking out this timely apt publication.

Jai Hind!

(Anil Chauhan)
General
Chief of Defence Staff

Lt Gen Johnson P Mathew,
PVSM, UYSM, AVSM, VSM
Chief of Integrated Defence Staff to the
Chairman, Chiefs of Staff Committee
& Chairman CENJOWS

FOREWORD

With the challenges posed by modern warfare today, Information Warfare (IW) has become a significant constituent in shaping the future of joint war fighting. Defence strategists as well as all other stake holders are increasingly interested in IW, a rapidly evolving and yet imprecisely defined battle field. It has surpassed the conventional way of fighting a war with the use of data, misinformation and strategic influence. This issue of Synergy on 'Information Warfare in Joint War Fighting' explores how Indian Armed forces can leverage information superiority to be at an advantage in all aspects of combat as compared to their adversaries.

Since the ancient times, intelligence networks were employed to gain an upper hand in a conflict. Even today, battles fought with precision technology and real-time data have the ability to acquire, control and prove its strategic value. However, the current times demand far more than simple intelligence gathering. This mostly involves the orchestration of cyber operations, electronic warfare, psychological warfare and so on. IW has transformed the whole process of seeing, analysing, decision making, acting and influencing the battlefield. This has also greatly influenced the outcome of the operations.

India has been working under a complex geopolitical environment and therefore, the role of IW is immense. Our adversaries are increasingly depending on misinformation, cyber warfare, hybrid tactics etc. To

deal with such challenges, it is required that our joint forces initiate collaborative approach in the war fighting with special focus on IW. The Synergy Journal issue of February 2025 makes an effort to highlight important issues related to IW including the mitigation measures associated with the challenges of IW. It is imperative that IW capabilities be strengthened and integrated with Command and Control (C2) systems as well.

In addition, cohesive approach remains a core element in synchronising the IW efforts which have been highlighted in this issue. It also discusses about securing information dominance and protecting the networks which the Indian Armed Forces could be utilising.

Influence campaigns targeting a larger public to manipulate their opinion, critical infrastructures attacked through cyber and advanced electronic warfare to play havoc with the communications have been demonstrated by our adversaries. This issue delves into highlighting the lessons learnt from IW practices at a global level and how it is instrumental in guiding India's Information Warfare doctrine.

IW is considered as one of the most important constituents in modern warfare. A proper road map is required to improve these capabilities for collaborative war fighting. The Synergy Journal Issue of February 2025 has shared perspectives to mastering this domain with an intention to simulate the thought process of the stake holders to be ready to protect our national interests with strength and resilience.

I compliment Team CENJOWS for bringing out this issue of Synergy Journal in a professional manner. I am sure that the readers will enjoy going through these well covered research based articles.

Jai Hind!

(J P Mathew)
Lt Gen
CISC

Maj Gen (Dr) Ashok Kumar, VSM (Retd)
Director General CENJOWS

FROM THE DIRECTOR GENERAL'S DESK

The evolving nature of the contemporary war has placed Information Warfare at the forefront of global security landscape. As information is not just an enabler- it has proved to be a battleground itself, decisively influencing outcomes and impacting every facet in the society, which makes it important now more than ever to adapt to these asymmetric methods.

The unconventional forms of warfare are ever-increasing and omnipresent, hence it is upon the military leaders worldwide to recalibrate the coordination of response from joint forces, and to integrate information services across forces to gain strategic superiority. The pressing need to abridge the Observe, Orient, Decide and Act (OODA) loop with our Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) structures cannot be overstated.

As a rising global power, India identifies the information domain as part of its comprehensive defence strategy. Our focus must be on uninterrupted flow of information across services and their constituents, for seamless interoperability to ensure protection of national assets and project power whilst disrupting adversaries effectively.

The Russia-Ukraine war has taught the world how IW can shape engagements, highlighting the need to be prepared for hybrid threats. Our

immediate neighbours also pose persistent challenges, necessitating a proactive and nuanced IW strategy to safeguard national interests and maintain strategic stability in the region.

With the rapid advancements in technology leading to the rise in cyber and electronic warfare- information as a tool can be manipulated to shape perceptions, influence political landscapes, disrupt infrastructure, and misinformation campaigns. Our vision must extend beyond traditional approaches, to stay vigilant and united to uphold the endeavours of national security while building a futuristic defence force which is equipped for sychronised IW campaigns, ready to harness the power of information for the strategic gains.

We are happy to present this Feb 2025 issue of Synergy Journal with the theme of 'Information Warfare Impacting Joint Warfighting' and hope these articles will generate adequate debate for all the stakeholders. I compliment all the authors for penning their thoughts. I also compliment Dr Ulupi Borah who has worked tirelessly to present this document in its current form alongwith other team members of CENJOWS.

Jai Hind!

(Ashok Kumar)
Maj Gen (Retd)
Director General

INFORMATION WARFARE IMPACTING JOINT WARFIGHTING

Lt Col Vidyanand Medhekar

"Know thyself know thy enemy, thousand battles thousand victories."

- Sun Tzu

Abstract

Over time, Information Warfare (IW) has emerged as a separate mode of warfare due to continuously evolving technology and availability of plethora of targets in every spectrum of society as well as organisations. The adaptive nature and facelessness of IW complicates the nature of the problem by commencing war without the crossing of borders or firing a single bullet. The most lethal way of warfighting, 'Joint Warfighting' or 'Multi Domain Operations (MDO)', has also not been spared by the IW, impacting it in every single stage of the battle. The ability of IW to raise the horizon of Grey Zone coupled with asymmetric threats imposes decision dilemmas in political as well as military hierarchy remarkably, impeding the warfighting capability of a nation by exploiting fault lines in society and breaking the cohesion of joint forces. The heavy reliance of joint forces on sensors, 'Command and Control (C2)' elements, communication and network spectrum to execute any mission makes it more vulnerable to IW creating intangibles in fog of war. However, careful orchestration of IW protecting own vulnerabilities at all costs enhances effectiveness of own joint forces manifolds reducing troop requirement to fight and cost of war providing victory with limited or no bloodshed. The paper reinforces the fact that, "IW can be fought only by IW" and if employed by us with complete technological superiority guarding own vulnerabilities, can enhance joint warfighting capability manifolds ensuring a strategic victory. Further the paper also provides a detailed understanding of IW and joint warfighting culminating into the

impact of IW and measures to combat IW especially in Indian scenario as Indian Armed Forces are into process of enhancing joint warfighting capability.

INTRODUCTION

The quote given above highlights the importance of information in warfighting. Today, with increased technological threshold and enhanced means of warfighting, the IW has become a mainstay and gained sizeable portion in the spectrum of warfighting. Blurring the boundaries and providing a certain mean of dislocation of enemy, IW fits into every space time matrix of warfighting. Weaponisation of information is not new to the world, right from 'Mahabharata' where Dronacharya was made to believe the death of Ashwatthama to today's warfighting, IW has always played a pivotal role in victory in any form of war. With evolving modern day technologies and increased reach as well as ability to influence the masses, IW provides an opportunity to win and threatens to checkmate the opponent. Impacting every element of national power, IW has seeped deeper inside in today's politics, military and economics thereby degrading war waging ability of the nation.

IW AND COMPONENTS OF IW

The changing nature of international politics is making intangible and complex form of power more important. Power is passing from the 'capital rich' to the 'information rich'. The rapid advancements in information technologies are creating new problems and vulnerabilities for the country where national and military data have become a national treasure. Today's technology has shifted conflicts from traditional spectrum to non-traditional spectrum, weaponising information and providing a tool of warfighting which is IW.

IW is a complex notion and has many meanings as it has proponents, detractors and observers. IW can be defined as 'actions taken to protect the integrity of one's own information systems from exploitation, corruption or destruction while at the same time exploiting, corrupting or destroying an adversary's information systems and in process achieving an information advantage in the application of force. It is also

includes actions taken to achieve information superiority in support of military strategy by affecting adversary's information and information systems while leveraging and defending our information and information systems'.[1] The IW consists of defensive as well as offensive components[2] and both are required to be employed in coordinated manner simultaneously for successful orchestration of IW.

In an interconnected world, access to quick, accurate, secure information, infrastructure and services is essential to the military to conduct operations. Subsequently, the ability to deny, delay or degrade these to the opponents could potentially prove decisive in war. Equally, the ability to deceive opponents about the true nature of a situation would provide obvious and potentially lethal advantages. So, IW can be said to be using alternate means to achieve goals that previously required the use of serious military force and a lot of bloodshed. In other words, IW is the effort to win wars without or with little fighting by influencing opponent's mindset, C2, sensors and data by using and managing information to pursue a competitive advantage through offensive and defensive efforts[3].

The targets of IW include a nation's government, military, private sector and population making human cognition the ultimate 'Center of Gravity (CoG)'. The IW uses physical, cognitive and information dimensions to carryout activities like network centric operations, electronic warfare, psychological operations, military deception and operations security, all of which are also components of IW. The advancements in technology have enhanced horizon of IW manifolds engulfing civil populace into the conflict to degrade war waging ability of the country by shaping opinions and destabilising Internal Security (IS) of the country.

Therefore it won't be wrong to assume in today's scenario that, "IW is a conflict between two or more states in the information space with the goal of inflicting damage to information system as well as carrying out psychological campaigns against the population of a state in order to destabilize society and the government".[4] Hence, IW falls into the domain of political warfare as it targets various elements of national power. Increasingly, IW is becoming central in conflict and confrontational situations as the human cognition has

become CoG in determining the outcome of conflict or confrontation.

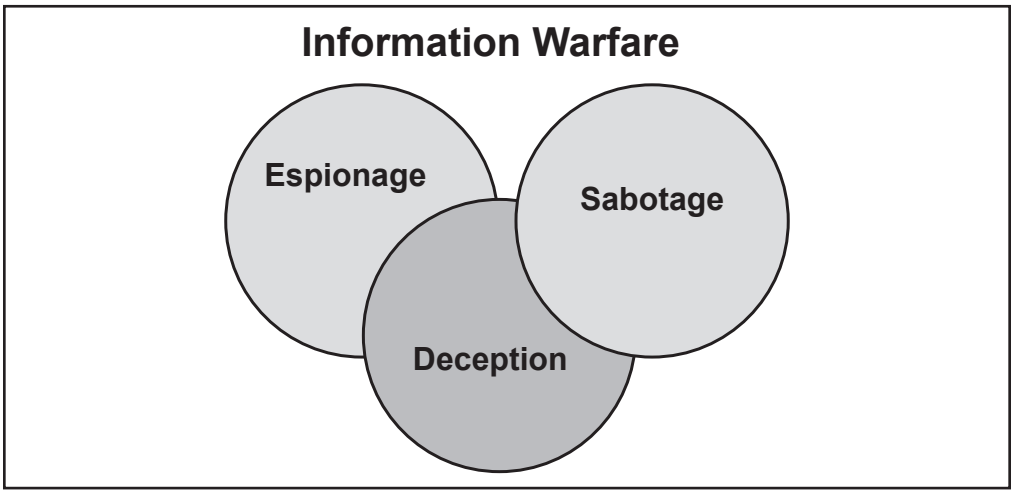
The impact of IW can be understood in detail if we understand its methods of execution. IW plays a crucial role in today's warfighting techniques by shaping the battlefield right before the commencement of hostilities and throughout the war using various non kinetic measures to affect the human cognition of civil as well as military nature, sensors and data involved or related to the conflict. In military domain, IW can be orchestrated using defensive as well as offensive components impacting OODA loop and imposing decision dilemmas[5]. The components of IW are as given below[6]:

- **Command and Control Warfare (C2W).** Involves attacks on opponents ability to generate commands and communication with the services and deployed forces.
- **Intelligence Based Warfare (IBW).** Integration of sensors, emitters and processors into reconnaissance, surveillance, target acquisition and battlefield damage assessment systems.
- **Electronic Warfare.** Techniques that enhance, degrade or intercept flows of electrons or information.
- **Psychological Warfare.** Designed to affect the perception, intentions and orientations of decision makers, commanders and troops.
- **Economic Warfare.** Expressed in one of two forms i.e., information blockade or information imperialism.
- **Cyber Warfare.** The use of information systems to carryout series of attacks and counter attacks between nations is termed as cyber warfare. The goal is to disrupt a country's critical operations and infrastructure to gains access to research, intelligence and data. Cyber warfare is motivated by government or military interests or hacktivism. Hacktivism is a combination of hacking and activism that can be socially or politically motivated.

Recognising the gravity of situation and post assessing IW campaigns waged by adversaries, the Indian Armed Forces have also stepped

up their efforts to orchestrate IW using both offensive and defensive components. In continuation with the process of modernisation and to orchestrate IW in coordinated manner, the Indian Army has established IW branch to combat misinformation and false propaganda being spread through social media for adverse psychological impacts. To keep up with needs of the future battlefield, hybrid warfare and social media reality, the new office of DGIW has been established which is being held by an officer of the rank of Lieutenant General under whom ADGPI and IW branches have been placed for a coordinated response. The ADGPI deals with media projection and has a social media wing. Besides this, a separate cyber unit has also been placed under DGIW as part of 'Reorganisation of the Army HQ'. The new reorganisation provides enhanced offensive and defensive IW capabilities allowing synchronised execution of IW.

IW is relatively cheaper and offers high returns on investment for resource poor nations. The technology to launch attacks is simple and is widely available worldwide. IW systems can be cobbled together from parts available in electronics stores on the streets of any city in the world or can be delivered online. International law is also ambiguous regarding criminality and acts of war on information infrastructure. Besides information hardware, IW produces huge impact in battlefield with lesser human resource requirements to execute missions and also reduces bloodshed. This character of IW bridges technology and force



Source: Author

parity between two countries allowing relatively weak nation to stand against a stronger adversary.

CONCEPT OF JOINT WARFIGHTING AND PRINCIPLES OF JOINT WARFIGHTING AFFECTED BY IW

Enhanced battlefield transparency and kinetic as well as non-kinetic enablers of combat coupled with potential threat of non-state actors and asymmetric warfare have complicated today's battlefield manifolds necessitating rapid technological and doctrinal advancements in traditional warfighting methods. Though advancements in technology have increased the tempo and lethality of operations in every sphere but there exists a need for seamless integration of armed forces to generate maximum combat power in the area of operations. Such a superior combat power can only be generated by synergised application of various elements of armed forces of the country in time and space to deliver decisive and swift victory at lesser cost.

Joint warfare is a military doctrine that places priority on the integration of the various branches of a country's armed forces into the unified command to achieve a unified objective. This concept emphasises on coordination, interoperability and synchronisation across various branches to maximise combat effectiveness. It can also be described as 'team warfare' requiring integrated and synchronised application of all appropriate capabilities and the synergy that results in maximised combat capability for a unified action. Hence practitioners of joint warfare must acknowledge the importance of the inter arm/services processes as well as non-military agencies in military planning.

While the nature of war is immutable, its conduct and methodology continue to evolve following the principles of war. The principles of warfighting are required to be ensured during every stage of planning as well as execution. The delicate balance of forces in joint campaign or operation[7] and its effect are directly proportional to the ability of a practitioner to protect the principles of joint warfighting at all times. However, heavy reliance of joint forces on C2, sensors, data and synchronised application of forces also offer opportunities to IW to sabotage these principles and defeat the practitioner of joint warfighting

in time and space. In order to make joint warfighting more resilient and lethal, there is need to understand impact of IW on principles of joint warfighting. Impact of IW, positive or negative, on some of the major joint warfighting principles is as given below[8]:

- **Maneuverability.** The IW with its components has enhanced intelligence gathering speed and Battle Field Transparency (BFT) shortening OODA loop and increasing maneuverability in decision making as well as movement of troops by avoiding unwanted deployments or lifts increasing speed of operations. On the other hand, the compromised information and deception by enemy will also surely lead to reduction in maneuverability of joint forces impeding speed of operations.
- **Economy of Force.** IW provides a cheap option to strike enemy at every stage of battle and time-space matrix of the enemy with plethora of targets without any bloodshed preserving forces for use of them at somewhere else ensuring economy of force.
- **Unity of Command.** The purpose of unity of command is to ensure unity of efforts under one responsible commander for every objective. IW can be used to maintain as well as destroy this principle with offensive and defensive elements either maintaining or breaking the unity of command.
- **Surprise.** The principle of surprise is to strike swiftly at a time or place where the enemy is unprepared increasing tempo of operations and creating series of opportunities to attacker resulting from sudden collapse of the defender. Surprise is one of the important principles of joint warfighting which has been largely compromised by IW due to enhanced BFT, information sharing and deception abilities hiding true nature of situation.
- **Restraint.** The principle of restraint is to use only the amount of force necessary to influence the adversary. IW largely contributes to this principle due to its ability to reduce requirement of troops to execute any operation ultimately ensuring restraint of force and reducing collateral damage.

- **Legitimacy.** The perception of legitimacy maintains legal and moral authority at both national and international levels. This perception can either be maintained or sabotaged by IW by using various tools available in IW with their ability to reach to masses and shape their opinions.

- **Interoperability.** To ensure seamless and synergised application of joint forces, arms and agencies participating in operations are required to have interoperability amongst themselves and equipments being operated. This interoperability is ensured using seamless communication and timely data sharing which can be protected as well as sabotaged by IW.

- **Unity of Effort.** To ensure maximum combat power at target, integration of combat power of the three services and their activities is a must. Forces being applied should be united in time, space and purpose. The IW with its defensive and offensive capabilities can either ensure timely unification of forces or delay in unification of forces in projection areas providing big target to the opponent and opportunity to destroy forces piece meal.

- **Command and Control (C2).** C2 is very important aspect of joint warfighting which provides it with necessary direction and flexibility to carry out mission and exploit fleeting opportunities to enhance tempo of operations. The nerve centre of joint warfighting can be completely sabotaged or protected using components of IW.

The IW can impact joint warfighting in both ways, either by ensuring successful completion of a mission or a catastrophe. The capabilities of joint forces can be enhanced by IW but same can also be degraded by IW. The effects of IW are varied which are often dependent upon technological threshold of both the parties involved in conflict, targets available and fault lines existing or ready to brew. The principles mentioned above cannot be overlooked while planning or executing MDO or joint operations as it will render entire joint campaign untenable. Hence, the practitioners of joint warfighting must employ all means to safeguard these principles from any negative impact at all times while targeting the weaknesses of an enemy in pursuit of a swift win.

IMPACT OF IW ON JOINT WARFIGHTING AND WAY AHEAD

Though IW has great potential but need for on ground hold of strategic areas and IB for sovereignty of a nation cannot be ruled out. IW cannot replace joint warfighting in any scenario as it is unable to ensure complete destruction of enemy. Though IW has a great ability to influence joint warfighting but it cannot produce results by itself alone since IW relies on human cognition for achieving victory but not physical destruction of human. The need of keeping boots on the ground can never be obviated whatever advances IW makes. So, rather than employing IW alone it would be prudent to infuse IW in joint warfighting or MDO to enhance its capability and ensure victory at a lesser cost and in lesser time.

In the Indian scenario, keeping the geo political situation and threat of two and half front war in mind, the use of IW is a must to counter the shortfall of manpower and to bridge technological gap to pursue own geo political interests as there is no other warfighting technique available which can produce an impact as that of IW with lesser cost. India has also been facing issue of fake propaganda and exploitation of fault lines by adversaries since evolution of communication technology. In such situations, India won its wars due to the resilient mind set of the soldiers and population which can now be targeted by IW in present day scenario disbalancing force equation in subcontinent.

Due to the intense geo political situation and threat of a two and half front war, India needs to ensure fast paced and localised campaigns in future which is only possible with joint warfighting or MDO. Keeping this in mind, suggested warfighting strategies in Indian scenario in the domain of joint warfighting are as given below:

- **Network Centric Warfare (NCW)**. Integrates sensors, shooters and decision makers across services.
- **Effect Based Operations (EBO).** Focuses on achieving specific effects rather than just destroying enemy forces.
- **Rapid Decisive Operations (RDO).** Aims at swift and decisive actions to disrupt enemy operations.

- **Adaptive Planning and Execution (APEX).** Emphasises on flexibility and rapid adaptation.

The strategies mentioned above have a common requirement of enhanced tempo of operations in conduct of operations. Employment of IW in warfighting will not only enhance tempo of operations but also protect own vulnerabilities with minimum troops meeting troop deficit in two and half front war scenario. Further, human cognition can only be won by shaping opinions and building narratives which is only possible by extensive employment of IW. There is no other option available other than IW to target human cognition. Hence, it can be inferred that IW has deep impacts on warfighting techniques and especially joint warfighting or MDO owing to its reliance on C2, sensors data and synergy in application of forces. The following are some of the major impacts of IW on joint warfighting:

- **Tempo of Operations.** IW with its effect on maneuverability, speed, C2, sensors and surprise can enhance or impede tempo of operations. In joint warfighting, tempo of operations is very important as it allows exploitation of fleeting opportunities crippling defences of opponent.

- **Grey Zone.** The ability to sabotage data and deception capabilities of IW increases Grey Zone in spectrum of warfighting imposing decision dilemmas at every level. The created Grey Zone can further be exploited by adversary to wrest initiative from opponent and further impede speed of operations.

- **Global View and Human Cognition.** Any war requires legitimacy from its own countrymen and global forums for its sustenance and to achieve the end state. The ability of IW to affect the human cognition is phenomenal and with its long reach and ability to influence masses can either bring all in support or against. The global support can assist to procure latest military hardware required to counter ever changing battlefield and sustain economy of the country.

- **Synergy.** Offensive component of IW can reduce synergy amongst enemy troops while defensive component as well as BFT enhances own synergy manifolds which in turn contribute to tempo of operations.

- **Simultaneity.** IW due to its huge reach and speed can ensure simultaneity in operations which further contribute to tempo of operations in positive as well as adverse ways.

- **Force Ratio.** IW with its tool has ability to reach to masses and influence them through technical gadgets in seconds and since whole process is highly dependent on machines, it reduces number of troops involved war. This characteristic of IW offsets disadvantage of numerically inferior military. As the IW targets human cognition it produces huge impact over its opponent degrading the ability to fight. IW produces huge impact with lesser force making it more economical and cost effective tool of warfighting. Some of them have been discussed in the following paragraphs:

  - **Reduced Cost of Warfighting.** IW reduces manpower requirements of the country allowing it to use those troops fight somewhere else overwhelming area of operations. Further, the cheap technology available coupled with high tech military IW gadgets provide create huge and bigger impact than ordinance with less bloodshed making IW a cheaper tool of war.

  - **BFT.** The high tech gadgets of IW enhance BFT providing better decision making ability or increase dilemma by sabotaging sensors and reducing BFT which in turn affects the tempo of operations impacting OODA.

  - **Intelligence and Counter Intelligence.** This includes actions of adversary to gather own intelligence including human intelligence, signal intelligence and open source intelligence and detecting as well as countering our intelligence efforts. The modern day technology provides plenty of gadgets to carryout task which are cheap and have very huge impact on joint operations.

Tactics, Techniques and Procedures (TTPs). The availability of much efficient and less manpower intensive technology in IW has offered an opportunity to change TTPs of traditional battle fighting at every level which can enhance tempo of operations and survivability by obviating

certain steps in battlefield procedures by allowing machines to do those risky procedure which needed human to perform them.

With technological advancements, IW is going to be more and more lethal and cost effective which will change tomorrow's battlefield completely. The availability of plethora of targets, cost effective ways, facelessness and adaptiveness are the facets of IW which makes it different from other warfighting tools. Impact of IW is so much that it can tilt balance of power towards the numerically weak but technologically superior military without firing any bullet, capability which no other warfighting technique has in present day scenario. Glimpses of IW and its potential threat have been witnessed by the world in ongoing conflicts wherein lot of deep fakes were used and sensors as well as communication systems were targeted to break the will of soldiers fighting and eliminate high value targets. Keeping this in mind, to meet the parity in forces in case of a two and half front war as well as to bridge technological gap, India will have to infuse IW in its joint warfighting techniques mentioned above for swift and decisive victory at lesser cost.

The effects caused by IW can only be mitigated by IW since human cognition can only be shaped by IW. Further, non-employment of IW will increase the requirements of manpower and cost for fighting manifolds as no other warfighting technique produces effects as that of IW at similar cost. To infuse IW in joint warfighting India has to ensure following during infusion process besides creation of joint structures, Integrated Theatre Commands (ITCs) to enhance joint warfighting capabilities for effective conduct of IW for enhanced joint warfighting abilities:

- **Infusion of IW in Warfighting Doctrine.** To ensure coordinated orchestration of IW in time and space with better effects, IW is required to be included in warfighting Standard Operating Procedures (SOPs) and doctrines with timelines as well as end state. This will not only help in implementation of IW but also provide direction to develop home grown technology required to be focused for upgradation of IW capabilities. Also, inclusion of civil infra and concerned departments in fighting IW will only boost capabilities of armed forces and help to ensure synergy in implementation of IW enhancing effectiveness of IW.

- **Effect Based Development of IW Technology.** Technology evolution is a vast sea of opportunities and is time consuming considering technology availability in India. In order to bridge parity in technological superiority, India will have to focus on developing technology that will counter technology of its adversary in its vicinity rather than looking at all round development as this will seize initiative from adversary providing India much needed time and budget for implementation of technology tying down opponent's resources. So initially the focus of India should be on development of effect based technology and later it can shift to all round technology development.

- **Inclusion of AI and Space Technology in IW.** India is trying to make substantial developments in field of semiconductors, AI and space industries. These technologies will provide tremendous boost to India as adversaries of India are also yet to master them. Already existing edge in space technology and information technology will provide necessary platform for development of home grown technologies and their further infusion in IW. Hence, government of India has to ramp up its efforts to develop the technology in these fields as bridging the gap in these fields is important for India keeping existing platforms in mind. Use of AI and space technology in IW will provide technological edge over the adversary by enhancing lethality of IW and reducing manpower requirements to fight.

- **Inclusion of IW in Training of Armed Forces.** Prepare personnel and organisation to understand, anticipate and counter the evolving tactics of IW. Build resilience against misinformation and train troops in the cognitive, cultural and operational dimensions of IW. Regularly update training programs, integrate new lessons from recent conflicts and develop a flexible doctrine that can address emerging threats in the information domain.

- **Induction of IW as Separate Arm.** India has ramped up its efforts to increase jointness in joint warfighting by introducing of ITCs and CDS but infusion of IW still remains less explored area. Creation of IW branch at Army Headquarter is a welcome step but there is a dire requirement to expand this branch right upto formation levels to

ensure well-coordinated response. The idea revolves around creation of a separate IW arm keeping its importance in today's warfighting in mind which will not only boost IW capabilities including cyber security but also ensure better management of IW assets and much coordinated as well as effective IW capabilities. The IW unit can be allocated to a corps with its sub unit affiliated right upto brigades. The implementation of this step will also enhance cyber security issues of the armed forces keeping the increasing number of cyberattacks in mind by adversaries. As per the article of Hindu published on 30 Oct 2024, India received over 79 million cyberattacks in 2023, ranking it third globally in terms of the number of such incidents which had increased by 15% as compared to previous year.[9] Globally, cyberattacks increased by 76% in first quarter of 2024, with India among the most affected countries. A study of PRAHAR nonprofit organisation (Public Response against Helplessness and Action for Redressal) indicates that cyberattacks on India are projected to rise to a staggering 1 trillion per annum by 2033, reaching 17 trillion by 2047, when the country turns 100.

- **Change in TTPs.** This is a sequential step after development of certain degree of IW capabilities, Indian Armed Forces should change its TTPs allowing smooth induction of IW at every level and obviating requirement of physical presence in certain risky missions.

- **Directive Style of Command.** Armed forces are required to practice directive style of command which will ensure success of operations even in absence of directions from hierarchy. The decision dilemmas created due to IW can be mitigated to a certain extent by practicing directive style of command on ground.

- **Increased Officer Men Interactions.** In the age of deep fakes, false propaganda can only be countered by passing direct orders to men with logical explanations to counter misinformation campaign of enemy and to avoid misunderstandings amongst troops leading to reduced trust of men in their leadership jeopardizing the safety of mission.

- **Enhanced Coordination Between Ministry of Electronics and Information Technology (MeitY), Ministry of External Affairs (MEA) and Ministry of Defence (MoD).** In today's scenario where geo politics is bounded by interests of the country in the complex multi polar world, IW needs to be orchestrated right from the global platform to ensure continued global support to own actions. The parallel channels between MoD, MeitY and MEA will ensure integration of three key ministries in orchestrating IW and help in countering fake propaganda as well as asserting in point of view. The parallel channels are required to be established upto command level through nodal officers of Indian Armed Forces.

- **Enhance Technological Threshold.** India missed industrial revolution but now making every effort to bridge this gap. The better policies launched by government of India and improved ease of doing business ranking have attracted attention of many foreign companies providing much needed technological knowledge. Plus the push through 'Aatmanirbhar Bharat' has also provided much needed platform for home grown defence technology which has been evident from defence export as well as defence equipment production in the country. Yet there exists a requirement to enhance the technological threshold which can only be made possible by constructing more Research and Development (R&D) facilities with more budgetary allocations. This will not only provide home grown technology to armed forces but also ensure complete security of missions by providing robust C2.

IW has impacted significantly to any form of warfare with its abilities to fight much before commencement of hostilities and meeting ends at lesser costs. The dependency of joint forces on sensors, C2 and communication systems including network spectrums exposes joint forces to IW and allows complete manifestation of IW in every stage of battlefield. In initial stages of battle, IW can be employed to shape battlefield and divide opinion of civil population to discredit the leadership of the country and armed forces with fake propaganda. In later stages of battle, IW can be manifested to sabotage sensors, C2, human cognition and data breaking the cohesion of troops and isolating them by broadening Grey Zone.

CONCLUSION

The IW is going to be the mainstay of tomorrow's battlefield due to sheer availability of plethora of targets in every domain, cheap cost and its ability to meet ends with limited resources creating huge impacts without any bloodshed. The facelessness, adaptivity and continuity are the basic nature of IW which make IW more flexible and lethal. The ability of IW to fit into every space time matrix of any form of conflict at any stage is unique making IW an all-time weapon. The continuous evolving technology is making IW more and more lethal which can dislocate enemy without even firing a bullet much before commencement of active hostilities. The reach of IW has increased with advancement in communication sector threatening to involve innocent civilians in conflict undermining their security and destabilizing governments.

The joint warfighting which is highly dependent on synergised application of forces has huge threat from IW as it directly targets various principles of joint warfighting degrading the capability of joint forces. Though IW poses significant threat in the realms of joint warfighting but requirement to orchestrate joint operations or MDO can't be ruled out in any scenarios in Indian context due to the requirements of adversaries of India to control geographical features in region to ensure their own interests. Hence, the requirement to physically hold the area to control it cannot be ruled out as sensors and surveillance devices can be hacked and manipulated. In such intense scenario, the effective and timely orchestration of IW by Indian Armed Forces in conjunction with joint operations will not only enhance the ability of joint forces but also enhance the tempo of operations providing swift and decisive victory in ever changing geo political environment in Indian sub-continent by breaking the will of opponent to fight in fog of war and segmented battlefield. The infusion of IW in joint warfighting will reduce the bloodshed and cost of warfighting reinforcing the fact, 'IW can only be fought by IW'.

"The country that masters emerging technologies, combines them with doctrine, and develops the leadership to take advantage of it...the side that does that best is going to have...advantage at the start of the next war."

General Mark Milley, United States Army
20th Chairman of the Joint Chiefs of Staff

★★★

Lt Col Vidyanand Avinash Medhekar is an alumnus of National Defence Academy and was commissioned in Infantry in 1 NAGA (DRAS) in Jun 2009. The officer has experience of serving in varied active areas including OP SNOWLEOPARD in Eastern Ladakh, OP RAKSHAK in J&K and UNIFIL. He has tenanted instructional appointments at National Defence Academy as instructor CI 'B' and The Infantry School, Mhow as Instructor CI 'A'.

NOTES

1 *Borden, C. A. (1999). WHAT IS INFORMATION WARFARE? Aerospace Power Chronicles. https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf*

2 *DeVries, A. (1997). Information warfare and its impact on national security. In The United States Naval War College. The United States Naval War College.*

3 *Wilson, G. (2022, August 1). Information warfare: what is it, and why should we care? The Cove. Retrieved September 18, 2024, URL: https://cove.army.gov.au/article/information-warfare-what-it-and-why-should-we-care-0*

4 *Ibid*

5 *Griskenas, S. (2023, September 6). Information Warfare: Concepts, impact, and examples. Nord VPN. Retrieved September 17, 2024, URL: https://nordvpn.com/blog/information-warfare*

6 *Damjanovi, D. (2017). Types of information warfare and examples of malicious programs of information warfare. Redalyc.org, 65(4).*

7 *Department of Defense. (2023). Joint warfighting. In Joint Chiefs of Staff. NDU.*

8 *Finnan, J., Gray, L., Perry, J., and Lust, B. (2019, November 18). Wolfe, Montcalm, and the principles of joint operations in the Quebec Campaign of 1759. NDU Press. Retrieved September 20, 2024, URL: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2019421/wolfe-montcalm-and-the-principles-of-joint-operations-in-the-quebec-campaign-of/*

9 *The Hindu Bureau. (2024, October 30). Incidents of cyberattacks on India may reach 17 trillion by 2047: Study. The Hindu. URL: https://www.thehindu.com/sci-tech/technology/incidents-of-cyberattacks-on-india-may-reach-17-trillion-by-2047-study/article68810313.ece*

INFORMATION WARFARE THROUGH ELECTRONIC WARFARE

Air Marshal Daljit Singh, PVSM, AVSM, VSM (Retd)

Abstract

Electromagnetic spectrum (EMS) pervades all operational domains, and it binds them together through networked connectivity. Freedom to operate in an electromagnetic spectrum is crucial to achieve information superiority by the armed forces. With advancements in computerisation, communication and sensor technology, the spread of electromagnetic spectrum employment has increased tremendously in all regimes. Battle of EMS superiority is fought through Electromagnetic Warfare (EW), which directly influences information superiority. IW has a much wider canvas of psychological warfare, command and control warfare and EW. This article exclusively covers the employment of EW as a tool of Information Warfare, as freedom of operation in EMS is crucial for all operational domains.

INTRODUCTION

Information is an important ingredient to plan and take decisions in all fields including civil enterprises, governance and military operations. The process involves collecting and collating relevant data, storing, interpreting, analysing taking decision and disseminating them. Technological advances in sensors, communications, computerisation and digitisation have transformed the information process tremendously. For military operations, the air and space based sensors generate massive multi-spectral data covering a very large swath of geographical area. This requires tremendous computational power, digitisation of data and Artificial Intelligence (AI) embedded algorithms to glean useful

information in a compressed timeframe. Manual analysis of electronic or photographic data would take months to collate. Accurate information derived from multiple sensors would ensure enriched information which is considered essential to plan and execute successful operations. Timely information is crucial to shorten the Observe, Orient, Decide and Act (OODA) loop and remain ahead of the adversary action plan, for successful execution of operations. Freedom to have access to the required information and denying the same to the adversary, has led to a concept of IW, which has been conceived for many decades. Information Warfare, as perceived by many practitioners, encompasses a very large canvas that includes cyber war, Command and Control (C2) war, psychological war and EW. The boundaries amongst these subsets are loosely defined. The IW, as defined in the Indian Air Force (IAF) Doctrine 2022, is, “Actions taken to preserve the integrity of one’s own information system, while at the same time exploiting, corrupting or destroying an adversary’s information system, and in the process, achieving an information advantage for the application of Information Operations (IO) - the offensive and the defensive”.[1] This definition excludes the scope of psychological warfare, which has been quite pervasive in recent conflicts, however, the IAF may have considered it to be beyond their operational domain. This is evident while dwelling on 'No War No Peace (NWNP)' scenario, the IAF Doctrine mentions cyber, electronic and psychological warfare, as inclusive to the IW, with a caveat that all instruments including the government and private media are to contribute towards achievement of information dominance.[2] The Doctrine of the United States Air Force (UASF) defines the IW more comprehensively as, "The military capabilities employed in and through the Information Environment (IE) to deliberately affect adversary human and system behaviour and pre serve friendly freedom of action during cooperation, competition, and conflict."[3] This definition amply covers employment of forces to influence military forces, political leadership and public. The USAF IW concept consists of six principal capabilities - cyberspace operations; electromagnetic spectrum operations (EMSO); information operations, public affairs (PA), intelligence; and weather (WX)[4]. What is amply clear is that electromagnetic spectrum is the glue that integrates all other domains of air, sea, land, cyber and space operations. As all the

military elements are networked to share information for better situational awareness (SA) and shorten OODA loop, it is crucial to maintain EMS superiority that will lead to information superiority. While the term EMSO is prevalent in the Western world as the scope includes electromagnetic spectrum management, the term EW is prevalent in the Indian military and it is defined as the 'Military action employed in the electromagnetic spectrum domain and directed energy to degrade, exploit, reduce or prevent hostile use of EMS and ensure own freedom of operation in the same'. The EW activity is divided into the elements of Electronic Support Measures (ESM), Electronic Protection (EP) and Electronic Attack (EA), this article will discuss the scope of IW execution exclusively through EW.

EMS, IW, AND EW RELATIONSHIP

All the ground based and airborne early warning, surveillance, tracking and synthetic aperture radars use some segment of EMS to provide information on hostile ground based and airborne targets. Passive sensors in the EMS regime of acoustic, electro-optical (EO), Infra-red (IR) and Ultraviolet (UV), microwave and radio frequency regimes provide digital photography, electronic order of battle (EOB), terrain layout, weather, communication network layout, communication content and military activity. Space based assets employ Radio Frequency (RF) spectrum copiously for recording information through sensors and downloading them to the ground stations for analysis and for sharing with airborne elements for SA. The satellite communication uplinks, downlinks and sensors can be degraded by EW means, which would result in significant degradation of the adversary information operations. For coordinating and controlling multi-domain operations, EM spectrum is the main 'electronic superhighway' which binds other domains together and ensures timely dissemination of information and facilitates command and control of the fighting force. Freedom of operation in employing EMS for information is ensured by the Electronic Protection (EP) element of EW, which provides resilience, and redundancy for IO. The IO of the adversary is exploited by monitoring the EM activity to map and monitor communication network and other potential targets. This activity is achieved by Electronic Support Measures (ESM) element of EW. The degradation, disruption, deception manipulation and destruction

of the hostile information sources is achieved through the Electronic Attack (EA). The IW and EW are, therefore, intricately linked to maintain information superiority over the adversary. The goal of EW is to achieve EMS superiority, contributing to gaining and maintaining information and decision advantages to achieve the military operational objectives. It is, therefore, important to examine the EMS operational environment and EW applications towards information superiority.

PRESENT EMS OPERATIONAL ENVIRONMENT

Technological developments have led to the EM spectrum being employed at much diverse and wider frequency bands as compared to the past. It is a physical entity characterised by frequency, waveform, power, and time. These EM characteristics are affected by atmospheric and other environmental attenuation considerations. The 'ideal spectrum windows' at different frequency ranges are, therefore, restricted. The EM operational environment has, therefore, become highly congested, especially so as the EM spectrum is being exceedingly employed for civil applications of mobile phone connectivity and internet of things (IoT). The EM spectrum transcends all geographical boundaries and, therefore, the environment is highly contested by the adversaries. The EM spectrum usage is also governed by the international and national policies, prevailing status of technology and each frequency band has unique physical properties, which constraints the employment of electromagnetic spectrum. Cross domain employment and network centric operations have increased the density of EM transmissions which results in electromagnetic interference (EMI) if the frequency distribution is not deconflicted at the planning stage. As the competition between the electronic protection and electronic attack remains dynamic, increased complexity and sophistication have been introduced in the waveform characteristics, employing technologically advanced spread spectrum frequency hopping (FH) techniques and encrypted transmissions, which are difficult to detect and counter. Spread spectrum technique modulates a signal across many carrier frequencies to make transmissions difficult to detect and jam.

EW APPLICATIONS FOR SUPPORTING IW

- **Information Mapping Services.** Information services of the adversaries are detected 'mapped' and geolocated by regularly

monitoring the electromagnetic transmissions of the adversary. Ground based and Airborne Electronic Intelligence (Elint) platforms like dedicated Elint aircraft, Unmanned Aerial Vehicles (UAV), and satellite based Elint sensors are employed to detect, identify and geolocate the adversary non-communication EOB and other active RF sensors. Technical parameters are recorded to create a data base of the 'RF signature' of the emitters, Advanced Elint systems have capability to 'fingerprint' each individual radar of the same type, which also provides deployment history of the radars. In peace, regular monitoring of the EOB provides deployment pattern for strategic planning and 'change detection' is analysed for conclusions. During the transition to war, such missions are launched more frequently and closer to the area of interest, for better assessment of hostile deployment. This facilitates better operational planning and offensive IW strategy. RF Communication Intelligence (Comint) assets are similarly employed to map the communications network and Command and Control (C2) Centres. The present fighters, transport aircraft and helicopters also have integrated Electronic Support Measure (ESM) receivers called Radar Warning Receivers (RWR), capable of recording and geolocating hostile radars, which supplements the data obtained from other Elint resources. The whole process of EOB generation involves compiling the data base of each sensor in terms of Signature, modes of operation, geolocation and operational characteristics. Similarly, communication networks are mapped for technical characteristics, modulations and geolocation. The communication activity and movement provide indication of the force movement or imminence of operation. Weather satellites and aerosonde balloons map the weather information of the target area, which is useful for planning operations with suitable weapons. The information obtained through Elint/Comint provides strategic and tactical awareness that supports present operations and future planning. The ESM receivers onboard fixed wing aircraft provide situational awareness and warn against immediate threat for tactical actions. The technical characteristics of the transmitters help in preparing threat identification data base and effective countermeasures.

- **EW for Offensive IW.** Offensive IW involves actions and activities taken to affect enemy decision-makers by attacking their information and information systems. In today's networked operational environment of all domains, any degradation or disruption in freedom to operate in EMS, adversely affect operational outcome. Electronic attack on C2 Nodes, communication networks, Integrated Air Defence System (IADS) are conducted to degrade situational awareness of the adversary and paralyse the C2 network. For overall EA planning, the entire AD network, including the C2 Nodes, networking topology, sensors overlap, crucial control systems of the weapons deployed, and weapons lethality zones are analysed to ascertain the optimum strategy. This would provide maximum pay off, in ensuring higher mission success rate of the follow-on attack forces. This EA could involve hard kill of C2 Centres with stand-off precision guided munitions, Anti-Radiation Missiles, or soft kill with offensive jamming of radars and communication networks. For each individual AD weapon system consisting of early warning radars, acquisition radars, fire control radars and communication network- the entire chain of control is analysed for planning the attack. Ideally, each link of AD network could be targeted, however, the EA assets would always be at a premium and therefore, the crucial link in the AD chain may be targeted to achieve maximum pay off. Time synchronisation with the attack force is conducted for maximum effect. For example, to degrade an Air Defence weapon system, the early warning, acquisition, and tracking radar vulnerabilities are analysed, additional inputs on, lethal ranges of the weapons, alternate routing profile of the attack force would be analysed to plan the attack strategy that would increase mission success rate by minimising attrition of the force. If attacking acquisition radar is the critical link to trigger missile launches, it would be targeted with higher priority whereas the early warning radar may be avoided by following appropriate flight profile or detection ignored. EA tactics involve degradation, denial, deception disruption and destruction of the hostile AD network. Consideration of selection of the operational tactic and technique would be governed by the most optimum operational plan that would ensure maximum success rate of the attacking forces. Various EA techniques are described in subsequent paragraphs:

- **Degrade/Deny.** Having analysed the adversary EOB and communication networks, EA is planned to degrade the adversary systems by electronically jamming the appropriate sensors. With effective jamming, the information on the position of the attack force, the strength and type of attack force would be degraded, however, there would still be some limited information available on imminence and direction of attack. With active jamming, the adversary would be forced to employ an alternate mode of operation which would degrade the weapon performance. For air operations, standoff jammers are employed to jam surveillance radars from further ranges, escort jammers are employed that accompany the attack force to degrade the acquisition radars. Tracking radars are targeted through airborne self-protection systems. Stand-in jamming is conducted by UAVs or other EW missiles fired ahead of the main package. Simultaneously, communication network is targeted to prevent or delay targeting and control inputs, while satellite communication network may also be targeted depending on the criticality of the mission. The plan is required to be well coordinated and synchronised to degrade the adversary information system for specific time and in a specific area. The main advantage of this soft kill EA is that the jammers could be re-used, re-tasked and reconfigured to meet the operational objectives. The main drawback being that the jamming effect is limited in time and space and the hostile systems would be fully functional when the jamming ceases. The ground and naval elements also employ similar tactics and techniques to degrade hostile military machinery. Recently, the Global Positioning System (GPS) receivers are being degraded by jamming the GPS receivers of UAVs, standoff weapons and time synchronisation of communication networks. Normal GPS receivers are easy to jam as their receiver sensitivity is very high to receive the GPS signals from satellites. This has also resulted in collateral GPS jamming of civil flights which could be hazardous for safe civil flight operations.

- **Deception.** Deception techniques are employed to deceive the adversary decision makers into believing the false targets or information created in the operational scenario, which would divert,

delay or dilute the enemy action. The information system of the hostile force is, therefore deceived into false assessment of the raid. For aerial attacks, the deception is achieved by launching airborne decoys that simulate profile of the attack force and generate similar radar cross section (RCS) ahead of the strike force. This technique was amply employed during the Beka Valley operation by the Israeli Defence Force (IDF) that deployed remotely piloted vehicles (RPV) and during the Gulf Wars the U.S. Forces deployed tactical air Launched Decoys (TALD). Another deception ploy that has been employee since 'Normandy Landing' campaign of World War II, is to conduct diversionary attack to lure away the enemy from the main axis of main attack from a different direction. This deception technique was employed by the IAF during Balakot Air strike in Pakistan, in February 2019. Active deception jamming deceives the tracking radars by generating false target position, which is achieved by capturing the tracking centroid of the radar and moving it away from the actual target, by generating stronger signal. The ground and maritime forces employ deception communication plans and multiple thrust axis to deceive the enemy into believing the false attack thrust. It is important to understand that the EW lessons learnt during past operations are as relevant today, as they were decades back. GPS spoofing has been copiously employed against UAVs and other platforms to falsify the systems of their actual locations. The Iranian Forces had successfully spoofed the GPS receiver of the RQ-170 Sentinel UAV on December 05, 2011, and brought it down in Iranian Territory.[5]

- **Destruction.** The EW action also includes physical destruction of the hostile sensors, weapon systems and C2 Centres either by directed energy or by other physical means. Hunter killer missions were developed during the Vietnam War by which the 'hunter' aircraft equipped with ESM sensor would lead the 'Killer' fighters equipped with bombs/rockets to the Surface to Air Missile (SAM) sites for their physical destruction. As the attrition to these missions increased with induction of infra-red shoulder fired missiles, Anti-Radiation Missiles were developed to destroy the SAM sites from standoff

ranges. The present Anti-Radiation Missiles (ARM) have much larger attack ranges and have sophisticated dual band terminal guidance receivers that ensure successful attack despite the victim radar going 'silent'. The radar operators were so intimidated by the ARMs during the first Gulf War that they used to abandon the site on detecting the ARM launch. The present air to ground precision guided missiles are also employed for DEAD (Destruction of Enemy Air Defence) missions as their terminal guidance systems may use target scene matching algorithms and similar systems to preclude tracking of radar electromagnetic radiations. Dedicated fighter aircraft like F-18G 'Growler' of the US Navy and, J-16 of the Chinese Air Force are equipped with high power jammers and ARMs for this type of mission. Major advantage of the hard kill option is that the sensor is put out of action for much longer period, and it impacts the hostile AD operations. The ARMs are quite expensive, and their employment would be selective.

- **EW for Defensive IW.** Freedom to use EMS for IO is crucial, especially in the networked multiple operational domains environment. Electronic Protective measures ensure robust, resilient EMS operation that should withstand and continue functioning despite hostile electronic attack. The process starts with preventing the adversary from exploiting our electromagnetic transmissions, corrupting, creating confusion, and ambiguity during the process of information analysis. The second aspect known as anti-ECCM ensures resilient and robust network and sensors that continue to operate under active jamming conditions and ensure graceful degradation. Most of the armed forces employ multi-spectral and multi-layered sensors which cannot be simultaneously jammed. Passive sensors remain electronically undetected and have jamming immunity. Networked sensors ensure composite picture despite jamming few of the radars as inputs from alternate sensors are available.

- **Anti-ESM Measures.** To prevent the adversary from detecting and recording our EMS transmissions and collating ELINT/COMINT, the armed forces promulgate Electronic Emission Policies (EEP) to avoid electronic transmission of sensitive systems closer to the border and

only designated training frequencies are specified to avoid exposing the entire operating frequency band of the radars. Similar emission policies are also promulgated for communication systems. Dummy transmitters or phased out airborne and ground based radars could be deployed closer to the border and operated at regular intervals to corrupt and confuse the electronic data being compiled by the adversary. Low Probability of Intercept (LPI) radars is employed to reduce the chances of detection by the adversary systems. Training of sensitive nature is carried out deeper inside our own territory to prevent information on operational tactics and operating scenarios. EW exercises are also conducted well in depth to prevent snooping by adversaries. The communication transmissions are encrypted and employ wider spread spectrum techniques to prevent monitoring of communication contents. The trials of new strategic weapons being developed are carried out deep inside our own territory and the area over the sea is sanitised of any 'snoopers' before clearing the trials.

- **Anti-ECM Measures.** Radars and other electronic sensors incorporate anti-ECM features known as Electronic Counter-Countermeasures (ECCM) during the manufacturing stage itself, to ensure continued operation during active jamming by hostile forces. These measures include frequency agility, wider band frequency operations, low side lobes, employment of IR and optical sensors as alternate sensor to circumvent jamming effect on RF sensors. Employment of passive aircraft detection sensors along with radars prevents total information denial of the airborne threats. The IAF has recently published a requirement to acquire Passive Surveillance System for this purpose. Active Electronically Scanned Array (AESA) transmitter technology is inherently jamming resistant due to electronic scan speeds, selectable radiation patterns and low side lobes. Most of the present radars employ AESA transmitters. V/UHF band radars are being digitised and upgraded to counter airborne stealth design advantage. Dummy transmitters that mimic actual radar transmissions are deployed around important radars sites to divert ARM attacks by generating stronger EMS. Corner reflectors that deflect the radar transmissions are deployed close to the high

power radars to confuse the ARM homing head about the exact source of transmission centroid. Most of the AD weapon stations have GPS spoofers/jammers to degrade precision weapons. Own GPS receivers can be incorporated with advanced receiver antennae that filter out the jamming due to adaptive antenna pattern generation. Communication networks are configured to ensure alternate lines of communication including optical fibre cables and satellite based communications to ensure enough redundancy. Netcentric centres generally have many servers located at different geographical locations to ensure uninterrupted takeover of operations in case one centre gets physically destroyed.

EW OPERATIONAL STATUS OF INDIAN ARMED FORCES

Armed forces all over the world including the Indian Armed Forces have shifted from the platform-centric operations to network-centric operations.[6] The IAF has operationalised Integrated Air Command and Control System, which has all C2 Centres, military and civil radars, SAMs and AWACS. The system provides common air situation picture and is networked with airborne elements. The IA has also deployed similar system called 'Akashteer', which provides filtered Air Situation picture and controls AD weapons. The IN has deployed maritime domain awareness that has networked all naval sea borne elements with C2 Centres. For mapping hostile ME spectrum, the IAF has airborne assets including fixed wing aircraft, UAVs ground based systems and Aerostats for ELINT and COMINT Operations. The Indian Army also employs UAVs and ground based systems for Sigint operations. The Indian Navy (IN) has a fleet of P-8I Poseidon Maritime surveillance aircraft that undertakes maritime surveillance and Intelligence Surveillance and Reconnaissance (ISR) missions. The IN has Sigint systems onboard most of the ships. However, the SIGINT Data analysis has not been fully centralised or automated. The IAF has airborne self-protection jammers, RWRs onboard all fighters and appropriate EW equipment onboard transport and helicopter fleets. The IA and IN airborne assets are also appropriately equipped with EW protection systems. All radars and sensors inducted in the armed forces have embedded ECCM circuits to defend against hostile offensive EW action.

TECHNOLOGICAL DEVELOPMENTS FOR EW

Artificial Intelligence (AI) is being embedded in EW systems for faster Sigint data analysis and dissemination. Netcentric operational capability has reduced the OODA cycle that can also update the jamming techniques of onboard EW systems while airborne. AESA technology has improved the jamming capability of Airborne Self Protection Jammers (ASPJ) and has improved the simultaneous multiple targets jamming capability. Digitisation and advances in computer technology have brought in much more advanced jammers and ARMs. There have been tremendous advances in the communications field that have made the communication systems more resilient and jam resistant. However, technological advances have also been employed to field in much more complex and advanced sensors with better resilience to jamming. This dynamic competition will continue to prevail in future.

PRESENT GAPS AND CHALLENGES IN EW

- Common network for sharing information near real-time, integrated and common network for all the three services is considered essential. This has not been achieved mainly due to the apprehension of secrecy and security.
- Airborne encrypted software defined radios are yet to be standardised for the three services due to which intelligence, airspace control, targeting and situational awareness cannot be fully exploited.
- SIGINT collation resources exist with all three services and other agencies. The data collated from fixed wing aircraft, UAVs and ground bases sensors are analysed in isolation which fails to enrich the quality of data. Data obtained from modern RWRs is quite accurate and substantial. However, it is not integrated with other SIGINT data to improve the data base.
- AI and ML applications are considered essential to analyse the SIGINT Data and to refine active jamming techniques against emerging new threats. The present EW systems lack the AI and ML tools.

- All the airborne self-protection jammers onboard the fighters have been imported from abroad and some of them came embedded in the fighters procured from abroad. DRDO has been attempting to develop the ASPJs for quite some time, without success, due to which the LCA-Mk-I fighter has been inducted without any ASPJ. The indigenous RWRs lack the directional accuracy required of a modern RWR. The Indian Defence industry has not yet achieved the capability to produce the contemporary EW systems. BEL has been manufacturing ground based Sigint systems which are difficult to maintain and operate.

- As the armed forces adapt to netcentric operations, complex communication waveforms with spread spectrum and FH techniques are generated to prevent communication monitoring and to ensure resilience against communication jamming. The armed forces require much more advanced COMINT and COMJAM systems to ensure effective interference against hostile networks. Much more R&D is required in this area.

RECOMMENDATIONS

- HQ IDS may prioritise standardisation of connectivity protocols for all the armed forces and integrate all the services C2 network to ensure faster dissemination of actionable intelligence, situational awareness and airspace management. This would also ensure seamless integration of Theatre Commands in future.

- Standard and interoperable airborne SDRs are essential amongst all the services to ensure connectivity across all airborne elements and C2 centers. This would drastically reduce OODA loop timeframes.

- Indian defence industry and DRDO must collaborate with reputed foreign EW manufacturers and coproduce EW systems, to accelerate technology absorption and work towards acquiring niche technology for EW systems.

- Developers of AMCA, LCA-Mk-II and other future fighters must embed EW systems and integrate them with onboard avionics at the

development stage itself, to ensure the most efficient approach to EW capability. These systems must be upgradable with AI and ML embedded in them.

- Collation and analysis of SIGINT data should be centralised from maximum sources to enrich data inputs. AI and ML applications must be employed for faster data analysis.
- Till now emphasis has been non-communication EW systems. With operationalisation of netcentric concept, the operators and defence industry must work towards development and employment more advanced COMINT and COMJAM systems.
- More research on Smart cognitive EW systems, which adapt to changing hostile EMS environment and counter new threats must be conducted to remain abreast of the current trends in EW research.
- HQ IDS may consider reorganising its structure to integrate cyber, EW and operational planning and ensure well synchronised operational plans for maximum effect.

CONCLUSION

EMS is the common e-way that pervades all other operational domains and binds them together. IW is highly dependent on EMS for operations. Therefore, freedom to operate in the EM spectrum is crucial to ensure operational superiority. EW ensures this freedom of operation in the EMS domain and prevents the hostile forces the same freedom. All elements of EW viz, EMS mapping, offensive and defensive EW contribute towards IW superiority. The armed forces have inducted EW systems, however, the defence industry and DRDO have not kept abreast of development in this field. There is deficiency of modern ASPJs and other EW which can only be plugged in with much more R&D in this field. For faster absorption of EW technology, collaboration with reputed foreign EW defence industry and coproduction will accelerate the process. At the national level all elements of the IW must be enmeshed and synchronised with military operations to achieve information superiority. Standardisation of the SIGINT data and communication network amongst the armed forces

would ensure much better SIGINT data for tactical decisions. Initiative by the present government to stimulate Indian defence industry would pay high dividends in EW operational capability of the Armed Forces in due course of time.

★★★

Air Marshal Daljit Singh, PVSM, AVSM, VSM (Retd) was an Air Officer Commanding-in-Chief of an operational Command. He regularly writes article on defence strategy in various magazines and has been a keynote speaker in many International Seminars on Electronic Warfare and Air Defence.

NOTES

1 *'Doctrine of Indian AirForce, IAP 2000-22 (Indian Air Force Air Headquarters Vayu Bhawan Rafi Marg New Delhi 110106) p- 65*

2 *Ibid page 40*

3 *USAF DOCTRINE PUBLICATION 3-13,"Information in Air Force Operations, USAF February 01, 2023. P-4*

4 *CSAF signed USAF IW Strategy, July 2022.*

5 *Iranians claiming to down US Drone, 04 Dec 2011, BBC News https://www.bbc.com/news/world-middle-east-48700965accessed on Oct 06 2024*

6 *Air Power and Emerging Technologies. KW Publishers Pvt Ltd New Delhi), 2022, Chapter 4, p 67.*

INFORMATION WARFARE ON INDIA: FIGHTING AN INVISIBLE WAR

Maj Vishnu RJ

Abstract

Information Warfare (IW) is emerging as a critical threat to the national security of India especially since it is exploiting the fault lines in a huge and diverse population. It aims to gain an upper hand over the enemy by creating confusion, degrading the societal structure and destroying the resolve of the targeted country. A nation is destabilised using a multitude of techniques including cyber-attacks, misinformation and psychological operations. The complex and multifaceted nature of IW presents a tricky battlefront in which any potent opponent is tempted and confused to act, thereby eschewing a set-piece mechanical response. Social media, news platforms and digital networks are being extensively used to disseminate false narratives, incite social unrest and undermine public trust in national institutions. The disruption of technology has introduced new soldiers for IW in the form of deepfakes, bot armies and other intelligent machines to this digital battlefield. There is an urgent requirement to address this invisible war waged on India to safeguard its sovereignty and democratic values. This study explores the concept of IW along with its effect on the contemporary battlefield to understand its effects on a nation. The study also suggests certain countermeasures and recommendations, especially given a dual front IW by China and Pakistan

INTRODUCTION

Indian epic Mahabharata mentions this famous incident where misinformation was used to deceive Guru Dronacharya into believing his son Ashwatthama was dead instead of the elephant with the same name. This act by Yudhishitra led to the death of Dronacharya and shifted the momentum of the Epic Mahabharata Battle in Pandavas' favour. From ancient strategists like Kautilya and Sun Tzu to modern thinkers like David Petraeus emphasised on the concept of 'Winning a war without fighting'. It involves the use of wisdom, strategy and diplomacy to force the opponent to surrender.[1] The WWI too saw an extensive exploitation of the information domain. Great Britain, then a global communication hub, caused a communication blackout for Germany by cutting off telegraph lines which was the mainstay of military communication. Similarly, the command-and-control structure of Iraq was collapsed by the US-led coalition in the first Gulf War. They deactivated the SPOT satellite system to obscure Saddam Hussein's observations before deploying tactical diversionary manoeuvres by US ground forces. In more recent times, Russia used hybrid warfare in Ukraine to effectively annex Crimea even without firing a shot. IW when used to their full potential can significantly influence the battlefield by deceiving, weakening and degrading the enemy's resolve. These non-violent manoeuvres are more powerful and destructive than conventional military strategies like fire and manoeuvres. However, to influence a foreign audience effectively, one must be well-versed in their language, culture and history. In the twenty-first century, a multitude of technologies are interacting in various planes making IW a decisive tool in modern battlefields particularly for weaker actors due to its accessibility and low cost.

PHILOSOPHICAL PERSPECTIVE OF IW

Information Operations defines IW as the “integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt or usurp the decision-making of adversaries and potential adversaries while protecting our own”.[2]

IW covers a multitude of actions to gain a competitive advantage over the enemy by influencing ideas and perceptions. It involves a constant

integration of information, physical, psychological and cognitive domains on the foundation of data, technology and communication networks. The existing established beliefs and customs are progressively destroyed to exhaust the spirit of a nation. Traditionally, this was made possible through a calculated mix of disinformation, misinformation and propaganda. Along with radio communication came Electronic Warfare (EW) and growing reliance on computers paved the way for cyber warfare within the realms of IW. The integration of cyber, cognitive and space domains is further complicating the effects of IW.

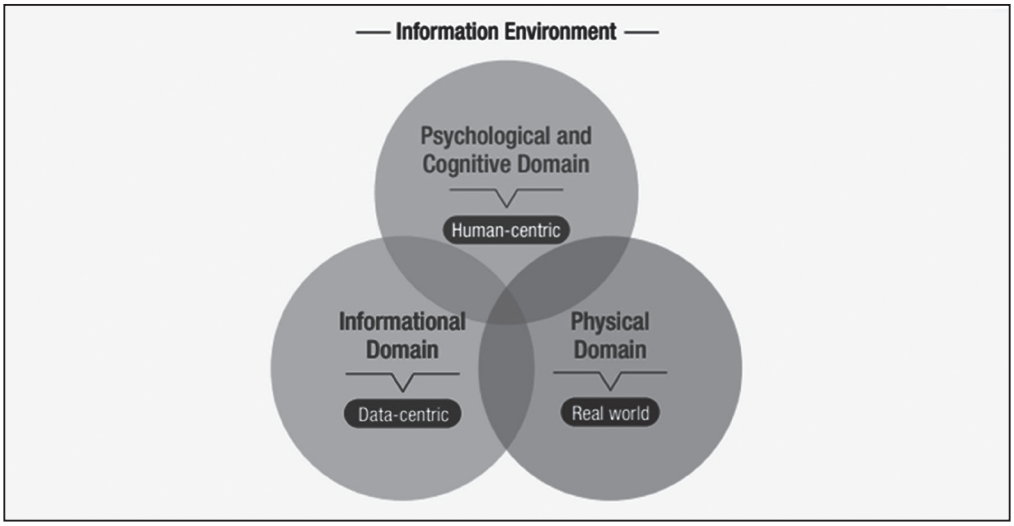


Figure 1: Interactions in the information environment. **Source:** Shinji 2023, 28.[3]

- **Information is Power.** There is a continuous interaction between a person with his working environment and his understanding of an event is influenced by the information available to him along with his personal beliefs. It will be highly empowering for him to have accurate information at the right time as it helps him shape his decisions, influence opinions and drive changes. Thus, sustained misinformation and propaganda can easily obscure the truth and progressively influence the belief system of a person. The impact of IW is often enhanced by shaping the response of an audience through controlled narratives in microtargeted content.[4]

These sensationalised media are subconscious biases leading to reactions rather than thoughtful responses. The COVID-19 pandemic highlighted that information overload can cause confusion and chaos. The world was exposed to too much information which was a combination of correct information, misinformation and disinformation that occurs during a disease outbreak. The WHO defines this as infodemic'.[5]

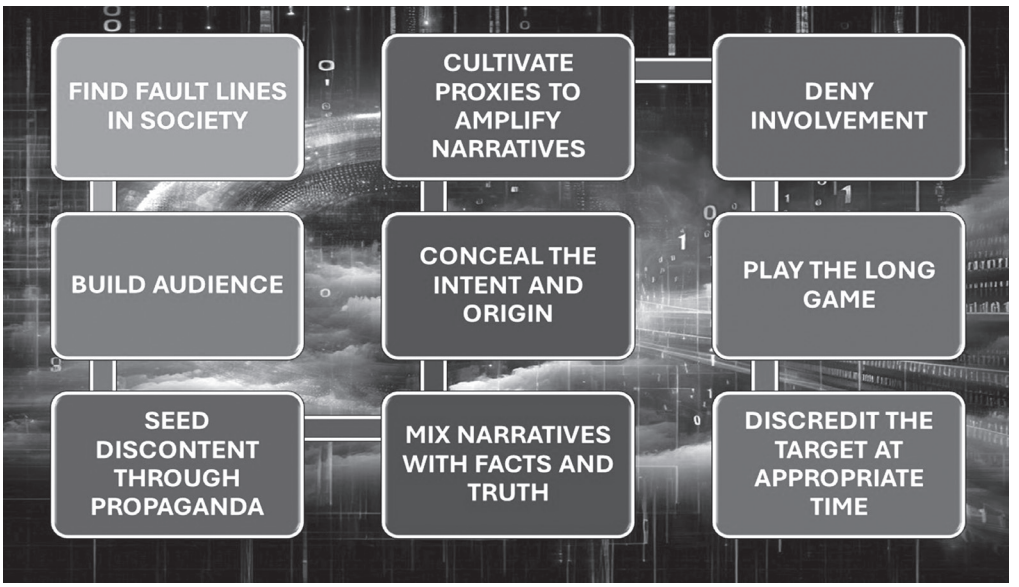


Figure 2: Operation of IW to achieve the result. **Source:** Author

- **IW in the Digital Era.** Disruptive technologies are transforming IW by increasing the speed, influence and impact of information dissemination. It enables IW operations in the complete spectrum of warfighting by integrating multiple domains in both time and space. Even though cyberspace has evolved as a powerful medium for shaping consciousness and social values the nature of influence continues to transform with the evolution of technologies like AI and Big Data. Social media and digital communication are now primary means of global influence and countries are leveraging on them to shape public opinion. Digital tools have increasingly evolved to become more effective, efficient and intelligent. This is increasing the complexity and frequency of IW in the modern battlefield.

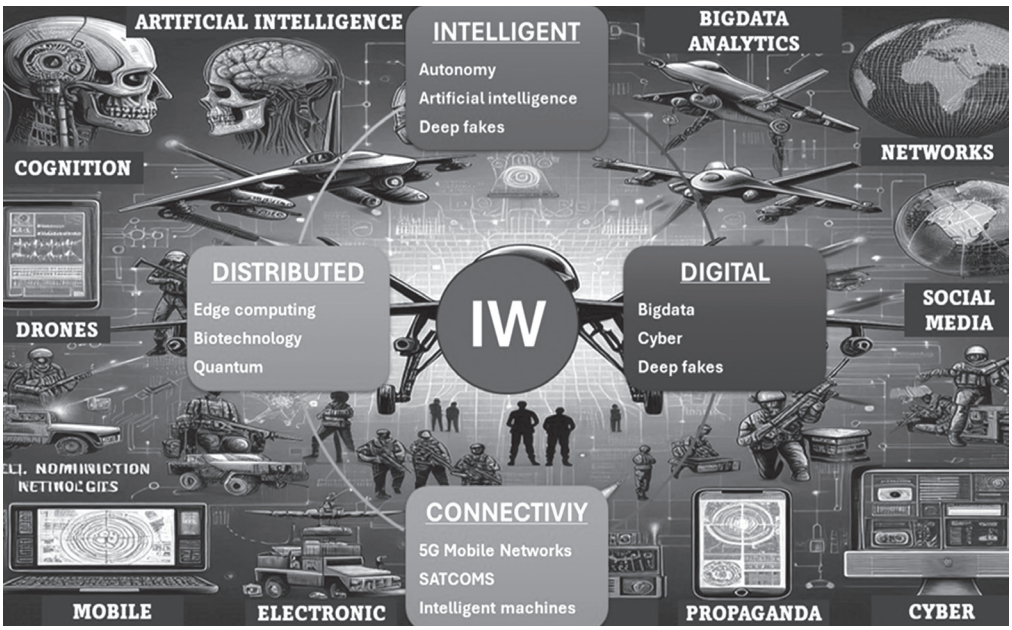


Figure 3: Interpretation of technologies involved in IW. **Source:** Author

- **IW Altering Traditional Warfighting Concepts.** While conventional warfare focuses on fire and manoeuvre, IW emphasises the strategic use of information on the backbone of technology to outmanoeuvre adversaries. This is making it a vital component of modern military strategy. The U.S. Department of Defence has been integrating IW into its operations to counter threats from state and non-state actors.[6] Recently, there has been a rise in computational propaganda and AI-generated content to manipulate public opinion for political activism and public mobilisation. However, the impact of these digital contents varies with each generation highlighting the complexity of new-gen IW. Gen Z favours reliable news sources and uses social media as their main news platform. Even though they view each content sceptically and expose falsehoods by fact-checking information. They are still struggling to identify misinformation. The exposure to false stories on a large scale and huge rate is making them more susceptible to IW. Countries like China and Russia have been leveraging IW to achieve their geopolitical goals without engaging in direct military conflict.[7,8] Big Tech companies like Meta and "X" are significantly influencing

content management on their platform to alter the information as per their interest.

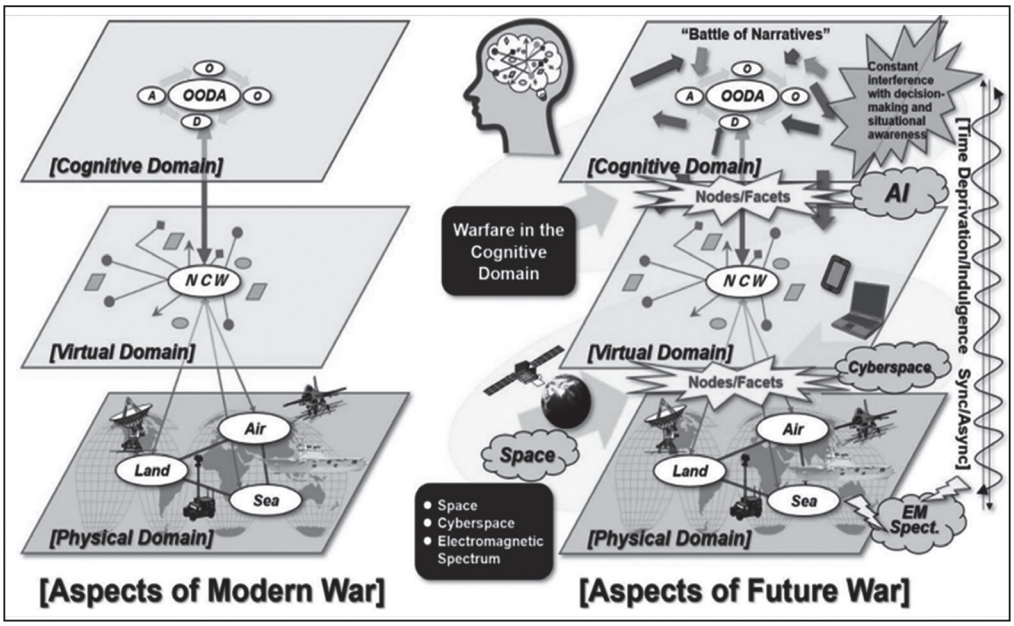


Figure 4: Complexities of the future under the umbrella of IW.
Source: Kazumi 2021.[9]

- **Ethics and IW.** IW has a complex relationship with the 'Just War Theory'. While IW can justify initiating war Jus ad Bellum through narrative building and propaganda, it contradicts the ethical conduct of war Jus in Bello and post-war justice Jus post-Bellum. These operations involve information manipulation, identity theft, infringement of privacy and security breaches thereby lacking ethical justification and morality. It often causes political and social dilemmas in a country by meddling in its internal affairs. Constant exposure to manipulated information can have psychological effects on the countrymen of the targeted nation, including increased anxiety, fear and a sense of helplessness.[10] Information manipulation can harm human psychology and give an unfair advantage to the powerful nation. Balancing national security with individual privacy rights

is a dilemma. Technology is outpacing the existing International conventions. These laws and guidelines lack codes of ethics for IW.

- **Human-Machine Integration and Evolution of CDO.** The lethal blend of humans with disruptive technologies like AI, affective computing, biometrics, neurotechnology and cyber technology is revolutionising global intelligence. Intelligent machines are used to gauge and envisage human behaviour using sentiment analysis and predictive algorithms. Based on these algorithms, the bots create and spread deep fakes, fake news and other misleading content to influence perceptions and behaviours. The recent conflicts amply demonstrate the evolution of traditional IW to CDO which is the ultimate form of IW. CDO is an inclusive multi-dimensional attack and defence strategy involving political, economic, military, diplomatic and public opinion tactics. CDO leverages information and technology by integrating disruptive technologies with IW to target cognition. It begins at the conscious level to affect how people perceive a nation, disrupt societal understanding, control reactions by exploiting psychological vulnerabilities and is referred to as 'Cognitive Hacking'.[11]

- **IW for Effect-Based Operations (EBO).** EBO aims to achieve the end state with minimal force and emphasises strategic effects. It aims to reach definite effects rather than merely destroying enemy forces. This process involves analysing the relationships and influences in the adversary's system to predict their responses and actions. This approach starts by defining the strategic effect and plans backwards to identify necessary tactical actions to achieve this effect. This philosophy enables the tactical intertwining of IW with EBO to achieve the desired 'effect'. Strategic communication is used to shape public opinion to accomplish this end state. Thus, enabling an intersection between EBO and Cognitive Domain Operations (CDO) at the strategic plane by directly targeting cognition.

- **Digital Colonisation (Kwet 2019).**[12] Domination of less powerful regions by powerful nations or corporations using digital technology is often called Digital Colonisation. The powerful tech companies are extracting, exploiting and controlling data from developed countries to

cause economic and social dependency, unlike historical times when colonisation was for exploiting natural resources. The companies like Google, Amazon and Meta dominate the digital landscape and collect vast amounts of data from developing countries.[13] While India is the country with the biggest amount of Facebook users, of the location of Facebook's fifteen data centres, ten are in North America, four in Europe and one in Asia.[14] These countries not only overshadow local cultures and social values leading to a loss of local identity but also set up data centres and infrastructure to benefit their home countries.

IW TECHNIQUES

World nations have taken massive strides to develop techniques and procedures to incorporate IW into the new age of warfighting. Propaganda and Psychological Operations are widely used to manipulate global judgment about a nation through planned radical, economic, military and socio-political activities. These actions are directed towards organisations and individuals of the targeted country to create emotions, attitudes, understanding, beliefs and behaviour.[15] The information revolution revolving around Internet-enabled platforms and technologies effectively degraded the natural resiliency of democratic processes to manipulative IW.[16] This gave way to the cyber-based influence technique based on a continually iterative and time-sensitive process where it is crucial not only to message first but also to maintain a sustained rate.[17] Military Deception is another vital tool that can integrate traditional warfighting tactics with cyber capabilities. It hampers the decision-making of the enemy and forces him to misallocate resources.

OPSEC on the other hand provides a foundation for identifying and protecting critical information by balancing security with operational efficiency to assist military planners in prioritising and safeguarding critical data. This is achieved through information security, information assurance, physical security and operations security.[18] EW shapes the information environment electronically on the backbone of advancements in various disruptive technologies and is often integrated with PSYOP, Military Deception and Computer Network Operations. This integration

helps to create a comprehensive strategy to influence, disrupt, or deceive adversaries.[19] The digitalised IW is also using social media platforms supported by intelligent machines to influence and achieve strategic objectives. Automated bot accounts are launching coordinated campaigns to amplify specific messages to make them appear more credible. During the Russo-Ukraine conflict, Ukraine has effectively managed to gain global sympathy by sharing real-time updates, videos and memes.[20] Perception management on the other hand monopolises on achieving strategic objectives by influencing how people perceive reality. It alters basic human emotions using carefully crafted messages by targeting emotions like fear and anger.

Figure 5: Stages of OPSEC**. Source:** Author

IMPACT OF IW ON NATIONAL SECURITY

IW significantly impacts geopolitics by influencing political processes, destabilising adversaries and shaping the global perception of an event, a conflict or a nation. Russia has been an expert in using IW effectively to undermine the democratic process for various states, especially the US. They used race-related issues to target African Americans through social media, hacking, and disinformation. In 2016, Russian operatives associated with the St. Petersburg-based Internet Research Agency

used social media to conduct an IW campaign designed to spread disinformation and societal division in the US.[21] These tailored messages can alter the socio-political condition of the targeted country by addressing the specific audience to create new fault lines or exploit old ones. During the Russo-Ukraine conflict, Kyiv used a mix of emotion, political interests and even humour to counterattack Moscow online to create a herd effect as users across the world shared Zelensky speeches, satirical Darth Putin quips and videos made by Ukrainian citizens.[22] Russia countered this by employing influence-for-hire firms to target far-right and far-left groups with tailored messages that indirectly supported their narrative which led to declining global support for Ukraine and increasing criticism of Western support for the war. Over the past year, Russia has aimed to weaken Ukraine's resolve and create internal discord by discrediting its civilian and military leaders. Ukraine was portrayed as an unstable nation by amplifying the internal conflicts using social media. The Kremlin's propaganda apparatus established the largest known influence operation on TikTok to disseminate rumours about Ukrainian political corruption.[23] On the other hand, the US and British acting in cooperation, announced details of a purported Russian plot to install a pro-Moscow regime in Kyiv and named a pro-Russia former member of the Ukrainian parliament as Putin's preferred puppet.[24] Strategic competition has evolved from the traditional binary view of peace and war to an extensive continuum of competitions that stays below armed conflict.

Strategic Communications (StratCom) are often used by nations to demonstrate their national goals and interests. It protects one's narrative from hostile foreign narratives to ensure the alignment of political goals with national interests. NATO has built its capacity and capability by creating the first military StratCom doctrine in March 2023. This forms the foundation for organising and conducting these operations in a new era. These operations use concealed actors, methods and goals to disseminate messages rapidly and repetitively to blur the line between reality and fiction through cross-media reinforcement by influencers. The use of familiar topics or seemingly verified evidence creates a mix

of lies and partial truths to shape public judgment. This process is known as “information laundering”.[25]

CHINA-PAK IW ONSLAUGHT ON INDIA

India may encounter concurrent conflicts with both China and Pakistan potentially involving both overt military assistance and covert support between the two nations. IW is a major front where they can collaborate to create division within Indian society and discredit India globally. Beijing is already conducting a large-scale misinformation campaign using multiple social media platforms such as ‘X’, Facebook, Instagram and YouTube against New Delhi by spreading fake news and propaganda online to undermine India’s global reputation. Since 2020, China’s intensified disinformation strategy and Chinese diplomats have assumed a more aggressive posture in supporting and guarding Beijing’s interests against criticism. This broader IW approach is often termed as 'Wolf Warrior Diplomacy'. China’s misinformation factories are manufacturing numerous fake news against India’s G20 presidency, the Manipur conflict, Buddhism & the Dalai Lama and are even spreading lies to fuel tension between India and Canada.[26] China has been making multiple micro-aggressions such as not sending a delegation to the Y20 forum hosted by India, disputing India’s use of the theme 'Vasudhaiva Kutumbakam' and the release of maps claiming Indian territories as Chinese. They have been running false claims about the conflict in Manipur, accusing India of running concentration camps for minorities and suggesting that Northeast Indian states should secede from India.[27]

Pakistan too has been involved in numerous disinformation campaigns by spreading fake news and divisive content against India. Channels and websites from Pakistan, including the Naya Pakistan Group have been posting divisive content on sensitive topics. These websites with over 3.5 million subscribers and 5.5 billion views have been trying to spread discontent in Kashmir, the Indian Army and minority communities. They aimed to undermine the election process in India by highlighting issues like the farmers’ protest and the Citizenship Amendment Act. Kashmir

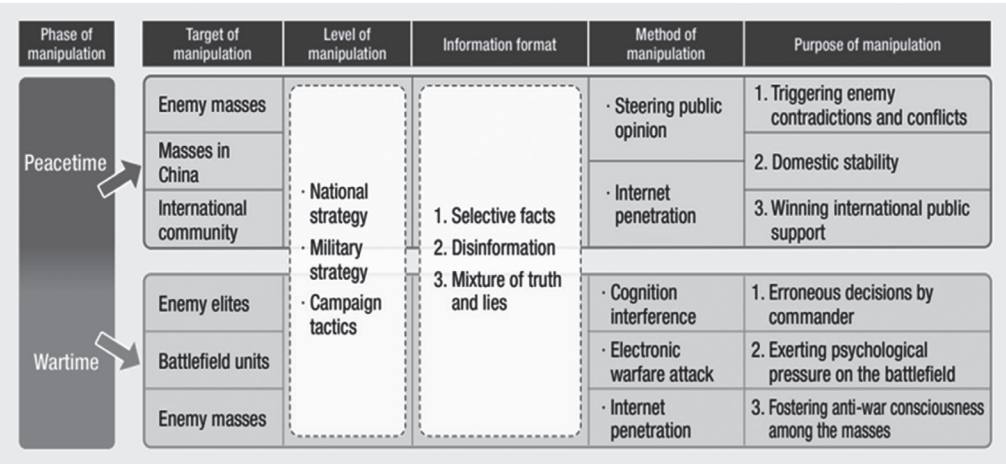


Figure 6: Line of Operations of PLA IW. **Source:** Shinji 2023, 49.[28]

has seen a huge spike in disinformation campaigns especially after the abrogation of Article 370 in 2019. This involves false claims about resource shortages and administrative problems in the region post the abrogation. In 2021, the Ministry of Information and Broadcasting ordered the blocking of twenty YouTube channels and two websites sponsored by Pakistan for spreading anti-India propaganda and fake news.[29]

SOCIO-POLITICAL IMPLICATIONS OF CHINA-PAK IW

- **Political Impact.** They exploit identity politics such as inequality and wealth disparity in India by disguising propaganda as genuine information causing widespread scepticism and cynicism. This causes the population to undermine the government, divert their attention from nation-building and incite political violence. Continuous disinformation will erode public trust in institutions including judiciary, media and scientific communities.
- **Social Impact.** IW exacerbates the social and political divide in society to cause heightened polarisation and social unrest within India. It fosters mistrust and suspicion among diverse groups by exploiting sensitive issues like religion, ethnicity and identity causing anxiety, stress and a sense of helplessness. This undermines the

efforts of the government and other institutions to create inclusive and resilient communities.

- **Diplomatic Issues.** Coordinated disinformation narratives are launched by these nations to diplomatically isolate India by portraying her negatively in global fora. The aim is to cause a rift between India and its allies by creating suspicion about India's intentions. Indian diplomats will face difficulties in garnering support on agendas like terrorism and regional security on global forums like the UN.
- **National Security Concerns.** Coordinated IW can disrupt essential services, damage the economy and expose sensitive information to endanger operational stability and threaten national security. Advanced AI technologies especially language models have enhanced China's ability to conduct sophisticated IW. The deepfake videos are undermining governance and public confidence by creating realistic but fake videos of politicians and celebrities. This is often termed as 'infocalypse'.[30]

WORK-IN-PROGRESS FOR INDIA AND ARMED FORCES

With the disruption in technology and social media, information is being highlighted as an important joint function in military operations leading to greater advocacy and integration of information into military plans. The major lessons for India are as given below:

- **Bolstering Cybersecurity.** The digital era necessitates an enhanced use of cyber assets to cope with the speed of technology. The critical networks, infrastructure and systems are thus vulnerable to cyber-attacks and their protection will be crucial for fighting against IW. They can be protected by enhancing the security of digital infrastructure and implementing robust cybersecurity measures.

BOLSTERING CYBERSECURITY	
Government Networks	Conducting frequent security audits and vulnerability assessments. Implement strong encryption protocols using Multi-Factor Authentication. Role-based access controls to limit access to sensitive information.
Security of Critical Infrastructure	Ensure system resilience and swift recovery by implementing redundancy. Updating incident response plans and fostering public-private collaboration for threat intelligence sharing and best practices.
Security of Private Sector Systems	Conduct regular cybersecurity training, deploy endpoint security solutions and implement data loss prevention. Deploy comprehensive endpoint security solutions to safeguard devices connected to the network.
General Cybersecurity Measures	Regular software update and segment networks to protect against vulnerabilities and contain malware spread. Utilise advanced threat detection systems, such as intrusion detection systems (IDS) and intrusion prevention systems (IPS).
Futureproofing	2FA add an extra layer of security to prevent unauthorized access. RPKI secures internet routing by verifying IP addresses. IPv6 addresses modern security features like IPsec, ensuring long-term internet growth and secure communications.

Figure 7: Measures to bolster cyber security. **Source**: Ratiu 2024[31] Clark 2023[32]

- **Promoting Media Literacy.**The major component of the IW setup is the cognitive and psychological domain. Humans are both the target as well as the resource in this scenario. The humans operating in this setup must critically evaluate the information and understand it before giving a suitable response. Thus, educating the public on this aspect is crucial in this digital age. Key aspects are given in Figure 8.

PROMOTING MEDIA LITERACY	
Media Literacy Programs	Incorporate media literacy into school curriculums to teach students how to analyse and evaluate information from an early age. Conduct community workshops and seminars to educate adults on recognising disinformation.
Identifying Disinformation	Promote the use of fact-checking websites and tools to verify the accuracy of information. Encourage individuals to critically evaluate the information they encounter by assessing the evidence provided and identifying potential biases.
Understanding Information Sources	Educate individuals on evaluating the authority and reliability of various sources. Government must promote transparency in media by advocating for clear authorship and accountability for published content.
Making Informed Decisions	Advocate for comparing multiple sources to gain a comprehensive understanding of a topic and use logical reasoning skills to evaluate the validity of arguments and evidence.
Reducing Impact of False Narratives	Initiate awareness campaigns to highlight the dangers of disinformation and the importance of media literacy. They must encourage discussions to build collective understanding and resilience against false narratives.
Building a Resilient Society	Collaboration between educational institutions, government bodies and media organizations to improve media literacy. Emphasis must be given for continuous learning.

Figure 8: Media Literacy. **Source:** Compiled by the author

- **Collaborative International Efforts.** India must advocate and facilitate agreements to simplify secure intelligence exchange between allied nations. Sensitive information must be shared over

established protocols while ensuring data protection and privacy. Joint intelligence centres must be set up with trusted allies for real-time information sharing on emerging threats. This will facilitate the quick identification of IW threats and their mitigation. Alliances like QUAD must collaborate to find transformative solutions for combating IW threats and share best practices to foster global cybersecurity guidelines.

- **Investing in Technology and Innovation.** The government must invest in home-grown advanced technologies and innovations to enhance the ability to detect and counter IW. AI-enabled algorithms can be effectively used to monitor and analyse data by detecting patterns of various IW techniques. These intelligent platforms can facilitate real-time alert systems to enable rapid coordinated responses. Cheap open-source secure cybersecurity tools must be created and made available to the common man to protect his data. Pilot programs to evaluate these technologies in real-world scenarios to gain valuable insights should be implemented and refine the approach before large-scale deployment.
- **Joint Inter-Service Network.** Indian Armed Forces could collaborate with the private technology companies to build a robust network setup which is both cyber and EMP-hardened. These networks must possess adequate redundancy and survivability to function in all environments. It must consider a proactive approach based on the Chinese Net Force model[33] that is more offensive rather than the existing more defensive 'CERT' concept to respond to cyber-attacks.
- **Building and Retaining a National Force for IW.** Immediate response is vital in IW to prevent considerable damage and maintain national harmony. Indian Armed forces must build a dedicated national force with strong IW capability to enhance the global standing as a formidable force. It must take cues from the recently established Cyber Command while laying the foundation for this new force. This force must be facilitated on the foundations of a strong legal and ethical framework, homegrown technologies, international collaboration

and a trained workforce.[34] An evolutionary approach must be taken that can start with the integration of the current IO resources from the three Services into a newly formed IO Command Headquarters. Additional specialist units could be raised subsequently in a phased manner to gradually boost its capabilities.[35]

Building and Retaining a National Force for IW	
Cyber Espionage	Gather intelligence on potential threats by infiltrating adversaries networks.
Disinformation Campaigns	Craft and disseminate false information to mislead adversaries and disrupt their operations.
Strategic Planning	Developing and executing offensive IW strategies to weaken adversaries.
Threat Detection	Identifying and monitoring cyber threats, misinformation and espionage activities.
Counter Intelligence	Preventing and neutralizing espionage efforts by foreign entities aimed at compromising national security.
Incident Response	Coordinating rapid responses to cyber-attacks and misinformation campaigns to mitigate their impact.
Analysis and Reporting	Providing detailed analysis and reports on IW threats and trends to help decision-making.
Collaboration	Working with other national and international agencies to share intelligence.
Training and Development	Educating and training personnel in IW tactics, techniques, and procedures to enhance overall capabilities.
Oversight and Accountability	Monitor intelligence activities to ensure that they adhere to legal standards and respect civil liberties. Implement internal policies and directives that provide guidelines and procedures for its operations.

Figure 9: Measures to Build a National Force for IW. **Source:** Author

- **Incorporation of IW Concepts in Military Training.** Incorporating IW into military training is crucial for preparing the armed forces for the digital battlefield. This comprehensive training must include dedicated courses on cyber defence, offensive cyber operations and information strategies. It should also include war games, simulations and joint exercises using cyber ranges and the latest IW tools.[36]
- **Whole-of-Government Approach.** The whole-of-government approach includes collaborative efforts across various tools of governance including military, intelligence, academia, civilian agencies and law enforcement. This strategy emphasises inter-agency collaboration, robust information sharing and unified strategies including establishing legal standards, fostering public-private partnerships and engaging in international cooperation.[37] Dedicated funds must be arranged through long-term legislative appropriations

and diversified sources like grants and public-private partnerships. The government must establish partnerships formalised through agreements like MOUs and joint ventures with tech companies and cybersecurity firms. IW strategies must be assessed through regular review of performance matrices and insights must be communicated for necessary alterations by the government.

CONCLUSION

Information had evolved to become both a weapon and a battleground. The new age of digital battlefields is necessitating innovative cognitive combat tactics. IW along with other domains of warfighting had embraced the nuances of disruptive technologies, generational changes, cognitive developments, etc to achieve this effect. This new age IW revolves around the concept of altering the perception of a population through cognitive shaping to achieve political goals. It should be understood that this invisible war is not just a matter of national security but also protection of democratic principles. The study has emphasised the multifaceted and disrupting nature of IW. Adversaries are exploiting digital platforms, social media, deep fakes, bot armies, etc to spread false narratives, incite social unrest and erode trust in national institutions. Effective countermeasures must be developed by India based on the understanding of these newage IW tactics. To safeguard its sovereignty and democratic values, India must develop homegrown disruptive technologies, improve cyber resilience and promote media literacy. This must include digital literacy, strengthen digital infrastructure and foster international cooperation. Combat stages in this approach involve monitoring web-connected devices, mapping information spaces and evolving rapid responses. India must form dynamic and proactive future strategies based on vigilance, rapid response and multinational cooperation. This will ensure the societal cohesion and the integrity of the democratic processes in the digital age.

★★★

Maj Vishnu RJ is an alumnus of the Defence Services Staff Collage, Wellington, the National Defence Academy, Khadakwasla and Sainik School Kazhakootam. He is a serving officer in the Regiment of Artillery and is currently posted as an Instructor Cl 'A' at School of Artillery, Deolali.

NOTES

1 *Amanda Penn, Subdue the Enemy Without Fighting: 5 Rules (Sun Tzu), SHORTFORM, 15 November 2019, Accessed: 28 August 2024, URL: Subdue the Enemy Without Fighting: 5 Rules (Sun Tzu) | Shortform Books.*

2 *Brunetti-Lihach Nick, Information Warfare Past, Present, and Future, Real Clear Defense, 14 November 2018, Accessed: 28 August 2014, URL: Information Warfare Past, Present, and Future | RealClearDefense.*

3 *Shinji Yamaguchi, et al, China's Quest for Control of the Cognitive Domain and Gray Zone Situations, National Institute for Defense Studies, Japan,2023,28.*

4 *Gavin Wright, Microtargeting, TechTarget, September 2023, Accessed: 28 August 2014, URL: What is microtargeting? | Definition from TechTarget.*

5 *Sarah Gibbens, A guide to overcoming COVID-19 misinformation, National Geographic, 22 October 2020, Accessed: 28 August 2014, URL: The 'infodemic' of COVID-19 misinformation, explained (nationalgeographic.com).*

6 *Roger C. Molander, Andrew Riddile, Peter A. Wilson, Strategic Information Warfare: A New Face of War, RAND, Research Published 1996, RAND, Accessed: 28 August 2024, URL: Strategic Information Warfare: A New Face of War | RAND.*

7 *Christopher H. Chin, et al, When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force, National Defense University Press,04 May 2023, Accessed: 28 August 2024, URL:When Dragons Watch Bears: Information Warfare Trends and Implications for the Joint Force > National Defense University Press > News Article View (ndu.edu).*

8 *Brunetti-Lihach Nick, Information Warfare Past, Present, and Future, The Strategy Bridge, 14 November 2018, Accessed: 28 August 2024, URL: Information Warfare Past, Present, and Future (thestrategybridge.org).*

9 *Kazumi Naganuma, Warfare in the Cognitive Domain: Narrative, Emotionality, and Temporality, NIDS, 30 March 2021, Japan.*

10 *Ramjee Divya and Jensen Benjamin, Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs, Center for Strategic and International Studies (CSIS), 20 December 2023, Accessed: 28 August 2024, URL: Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs (csis.org).*

11 *Baruchin Rotem, How Modern Hackers Exploit Human Psychology With Cognitive Hacking, Cyabra, 05 August 2024, Accessed: 28 August 2024, URL: Everything You Need To Know About Cognitive Hacking (cyabra.com).*

[12] *Kwet Michael, Digital colonialism is threatening the Global South, Al Jazeera, 13 March 2019, Accessed: 28 August 2024, URL: Digital colonialism is threatening the Global South | Science and Technology | Al Jazeera.*

[13] *Jindal Divyanshu, The War On Conscience: India In The Age Of Cognitive Warfare, India Foundation, 2023, 07.*

[14] *Hicks Jacqueline, 'Digital colonialism': why some countries want to take control of their people's data from Big Tech, The Conversation,26 September 2019, Accessed: 28 August 2024, URL: 'Digital colonialism': why some countries want to take control of their people's data from Big Tech (theconversation.com).*

[15] *Congressional Research Service, Defense Primer: Information Operations (congress.gov), Updated 18 December 2018, 01.*

[16] *Whyte Christopher, Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare, Journal of Cybersecurity, 14 September 2020, Accessed: 28 August 2024, URL: Cyber conflict or democracy "hacked"? How cyber operations enhance information warfare | Journal of Cybersecurity | Oxford Academic (oup.com)*

[17] *Collins Liam and Cook Chaveso, PSYOP, Cyber, and Info War: Combating the New Age IED, Modern War Institute At West Point, 04 June 2021, Accessed: 28 August 2024, URL: PSYOP, Cyber, and Info War: Combating the New Age IED - Modern War Institute (westpoint.edu).*

[18] *C. A. Theohary, Defense Primer: Information Operations, Congressional Research Service,18 December 2018, Updated: 28 August 2024, URL: Defense Primer: Information Operations (congress.gov), 01.*

[19] *C. A. Theohary, Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues, Congressional Research Service, 17 March 2009, Accessed: 28 August 2024, URL: Information Operations, Cyberwarfare, and Cybersecurity: Capabilities and Related Policy Issues (congress.gov), 28.*

[20] *Daniel Johnson, The real reason Ukraine's information war is so successful, Task & Purpose, 29 March 2022, Accessed: 28 August 2024, URL: The real reason why Ukraine's information war is so successful (taskandpurpose.com).*

[21] *The Select Committee On Intelligence, United States Senate on Russian active measures campaigns and interference in the 2016 U.S. Election, Report Of The Select Committee On Intelligence, Volume 2, 2016, Accessed: 28 August 2024, URL: Report_Volume2.pdf (senate.gov).*

[22] *Ramjee Divya and Jensen Benjamin, Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs, Center for Strategic and International Studies, 20 December 2023, Accessed: 28 August 2024, URL: Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs (csis.org).*

[23] *The Digital Forensic Research Lab, Undermining Ukraine: How Russia widened its global information war in 2023, Atlantic Council, 29 February 2024, Accessed: 28 August 2024, URL: Undermining Ukraine: How Russia widened its global information war in 2023 - Atlantic Council.*

[24] *Boot Max, Why the U.S. Ramped Up Its Information War With Russia, Council on Foreign Relations, 10 February 2022, Accessed: 28 August 2024, URL: Why the U.S. Ramped Up Its Information War With Russia | Council on Foreign Relations (cfr.org).*

[25] *Arjomand Noah, Information Laundering and Globalized Media — Part I: The Problem, Center For International Media Assistance, 20 August 2019, Accessed: 28 August 2024, URL: Center for International Media Assistance (ned.org).*

[26] *Sagar Pradip R., How China has unleashed a misinformation war on India, India Today, 18 October 2023, Accessed: 28 August 2024, URL: How China has unleashed a misinformation war on India - India Today.*

[27] *Shinji, China's Quest for Control of the Cognitive Domain and Gray Zone Situations,33.*

[28] *Shinji, China's Quest for Control of the Cognitive Domain and Gray Zone Situations,49.*

[29] *PIB, India dismantles Pakistani coordinated disinformation operation, PIB, 21 December 2021, Accessed: 28 August 2024, URL: Press Release:Press Information Bureau (pib.gov.in).*

[30] *Huminski Joshua, Deep Fakes: The Coming Infocalypse, Diplomatic Courier, 29 August 2020, Accessed: 28 August 2024, URL: Deep Fakes: The Coming Infocalypse (diplomaticourier.com).*

[31] *Ratiu Ramona, Securing the Future: Enhancing Cybersecurity in 2024 and Beyond, ISACA, 12 February 2024, Accessed 02 September 2024, URL:Securing the Future: Enhancing Cybersecurity in 2024 and Beyond (isaca.org)*

[32] *Clark Anthony, 3 Strategies for Ensuring the Security of Your Digital Infrastructure, ARIN, 27 October 2023, Accessed 02 September 2024, URL:3 Strategies for Ensuring the Security of Your Digital Infrastructure - American Registry for Internet Numbers (arin.net).*

[33] *Wuthnow Joel, China's New Info Warriors: The Information Support Force Emerges, Texas National Security Review, 24 June 2024, Accessed on: 05 September 2024, URL: China's New Info Warriors: The Information Support Force Emerges - War on the Rocks.*

[34] *Blannin Patrick, The Good Operation: Notes on a Whole-of-Government approach to National Security, Modern War Institute at Westpoint, 05 April 1028, Accessed: 05 September 2014, URL:The Good Operation: Notes on a Whole-of-Government approach to National Security - Modern War Institute (westpoint.edu).*

[35] *Panwar, Grey Zone Operations In The Infospace Dimension: Imperatives For India.*

[36] *Kick Jason, Cyber Exercise Book, Germany, MITRE, 11.*

[37] *Statements and Releases, Addressing the Collective Challenges of our Time: Implementing the U.S. Strategy to Prevent Conflict and Promote Stability, The White House, 01 April 2022, Accessed on: 05 September 2024, URL: Addressing the Collective Challenges of our Time: Implementing the U.S. Strategy to Prevent Conflict and Promote Stability | The White House.*

TECHNOLOGICAL ADVANCEMENTS IN ELECTRONIC WARFARE AND ITS EFFICACY IN RUSSIA-UKRAINE CONFLICT

Maj Gen AK Srivastava, VSM (Retd)

Abstract

Electronic Warfare (EW) is an important aspect of contemporary military operations and it has rapidly evolved, keeping pace with technological advancements. In modern military operations, full electromagnetic spectrum dominance is imperative for success. Russia-Ukraine war is the latest conflict which the world is witnessing, wherein most sophisticated Electronic Warfare systems have been used. Russia possesses well developed EW systems since long which they have been constantly upgrading. On the other hand, Ukraine did not have matching levels of EW systems. In spite of their superiority, Russian forces were not successful in achieving electromagnetic dominance at least in the initial phases of the conflict. However, they were able to consolidate their EW efforts and increase the effectiveness after the conflict became more static and a war of attrition. Ukraine, with the support from US and NATO (North Atlantic Treaty Organisation) countries, was able to fight back on the EW front. They were able to protect their communication and radars to a great extent and were also able to carry out jamming and disruption of Russian systems.

The article gives a glimpse of the advancements in EW domain over a period of time and carry out a critical analysis of EW operations in Russian-Ukraine conflict. Some useful lessons learnt have been drawn, which will be useful for gearing up our EW systems for electromagnetically dense battlefield environment.

INTRODUCTION

EW is defined as the military actions taken to prevent or reduce enemy's effective use of radiated electromagnetic (EM) energy and actions taken to ensure our own effective use of radiated electromagnetic energy. The information environment in which military operations are conducted is getting extremely complex due to electromagnetic spectrum. There is growing need for the armed forces to have unrestricted access to the electromagnetic environment which provides opportunities and throws challenges for electronic warfare in support of military operations. Within the information operations domain, EW is an element of information warfare.

Electronic Warfare, a sub set of Information Warfare (IW) is the most vital part of IW on the battlefield where it is employed as a weapon. The Electronic Warfare has evolved over a period of time starting from the WWI to the modern day battle environment. As the usage of electromagnetic spectrum has been growing, the Electronic Warfare is also growing to cover new bands of spectrum like Millimetric Wave, Terahertz, Infrared (IR), Optical band and associated technologies. Electromagnetic warfare can be applied from air, sea, land, or space by manned and un-manned systems, and can target communication, radar, infrared or other military and civilian assets. In this article, the developments in the field of EW, its growing importance in the concurrent warfare and an assessment of deployment and effect of Electronic Warfare in Russia-Ukraine war have been reviewed.

THE CONCEPT OF ELECTRONIC WARFARE [1]

The ever increasing proportion of specialisation, complexity and performance of modern weapon systems is directly due to electronics. The basic principle of Electronic Warfare if to exploit adversary's electromagnetic transmissions to gain operational intelligence and apply countermeasures to deny the use of electromagnetic spectrum to the enemy. Simultaneously, take measures to protect one's own unimpeded

use of the same spectrum. The three basic elements of Electronic Warfare are as shown in Figure 1 below.

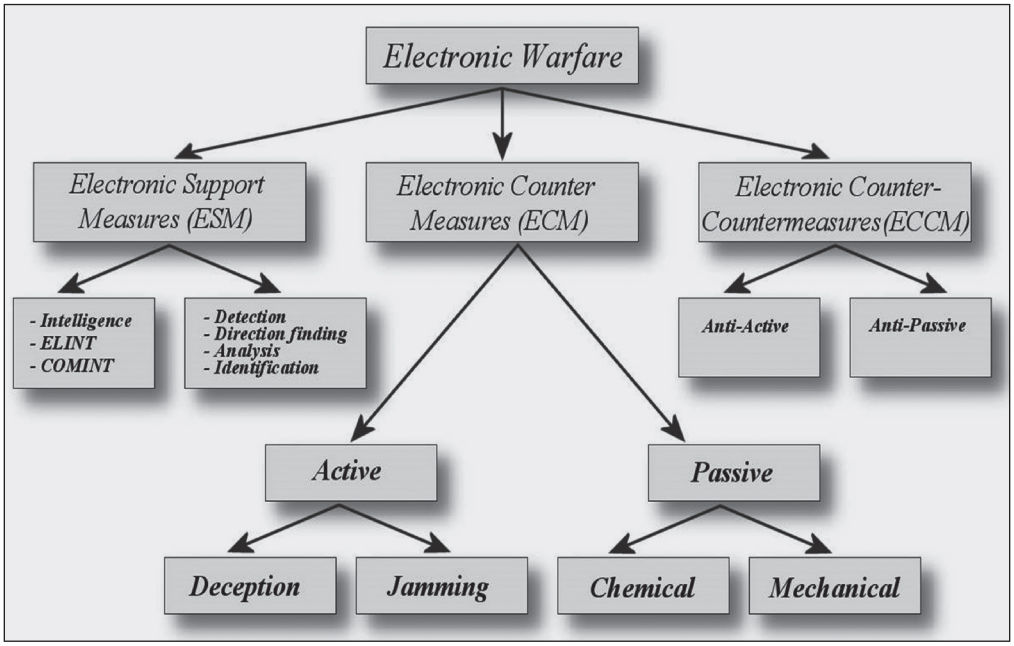


Figure 1 : Elements of Electronic Warfare.[2] **Source:** Christian Wolff, "Types of Electronic Warfare", Radartutorial.edu. https://www.radartutorial.eu/16.eccm/ja05.en.html

Electronic Support Measure (ESM). Part of EW which implies actions taken to search, intercept, locate and identify sources of radiated EM energy for purpose of exploiting it in support of military operations

Electronic Counter Measures (ECM). It involves actions taken to prevent or reduce the enemy's effective use of the EM spectrum. ECM can be either active or passive. Active Measures of ECM includes Jamming and Deception.

Electronic Counter Counter Measure (ECCM). Measures taken to protect one's own electronic systems against enemy ESM & ECM and enhancing the efficacy of own ESM system.

EVOLUTION OF ELECTRONIC WARFARE AS A CRITICAL DOMAIN [3]

Electronic Warfare techniques have evolved over a period of time starting from WWI to exploit the opportunities and vulnerabilities thrown up by the electromagnetic spectrum. During WWI, the electromagnetic spectrum was not very busy. The newly invented radios were used for communications, coordination of operations and for directing fire. Radio receivers were used to monitor enemy's communications and rudimentary direction finding equipment were used to locate the enemy positions. The communications jamming emerged at the same time, but was not widely employed as it was preventing own use of those radio frequencies. Also, the warfare happened slowly and the enemy could evade jamming in various ways.

The use of more sophisticated EW systems started during WWII. Airborne radars and jammers came up and advanced technologies enabled jamming and communicating on different frequencies. The fluid nature of warfare gave definite operational advantage to troops by intercepting, jamming and exploiting enemy's electronic systems. RAF and U.S. bombers made use of metallic chaff which were dispensed to confuse German AD radars. Jamming was also done of German VHF ground to air communications used to guide their fighter aircrafts towards the targets.

During the intense Cold War period in the 1950s and beyond, the competition to develop military arsenals accelerated and so was the case of electronic warfare equipment. Owing to technological advancements, more sophisticated EW systems with higher power, wider frequency ranges, and complex waveforms were developed. The systems were made small to fit into aircrafts and ships. As part of electronic protection measures, stealth aircrafts and ships with drastically reduced RF, IR, acoustic, and visual signatures were developed.

Electronic Warfare is an important aspect of contemporary military operations and it has rapidly evolved, keeping pace with technological advancements. In modern military operations, full EM spectrum dominance is imperative for success. This has led to a competition

amongst the major militaries to lay overwhelming emphasis on the development of next-gen sensors, communications, countermeasures, and counter-countermeasures.

TECHNOLOGICAL IMPERATIVES: KEY TO EW SUCCESS [4]

New technological advancements are constantly augmenting the EW capabilities and ensuring success of EW missions. Some key technologies which are vital for EW equipment include highly sensitive digital receivers, efficient and automated signal analysers and enhanced feature extraction techniques. Spread spectrum techniques and their countermeasures, stealth technologies and addressing dense electromagnetic spectrum are vital for modern EW systems.

Digital beamforming and adaptive technologies have improved the range of the systems and enable interference rejection, super resolution and power management. Antenna technology like Active Electronically Scanned Array (AESA) and compact T/R modules have enabled the development of scalable AESA radars. Multi band and multi-mode RF front ends have helped in the development of software defined radios and configuring of communication & EW functions in a single hardware.

The future technologies like nanoelectronics, with Carbon Nanotube (CNT) will make the EW systems compact and scalable. A single CNT can carry out all functions of components required in a receiver. The nano receivers under development are heading towards universal RF processor which will configure different radio bands from a vast grid of nano cells, each earmarked for a single frequency slot. It will be possible to reconfigure the system to achieve the functionality of a different radio. Many more such technologies are under development.

ELECTRONIC WARFARE IN RUSSIA-UKRAINE CONFLICT

Russia-Ukraine war is the latest conflict which the world is witnessing, wherein most sophisticated Electronic Warfare systems have been used. Russia possesses well developed EW systems since long which they have been constantly upgrading. Since Ukraine was a part of

USSR earlier, they also possess some old Russian EW knowledge and systems. However, as the war progressed, they received considerable support from the US and NATO countries and gave a stiff fight in the EW domain.

Commenting on EW in this conflict, the commander of the USSF's Space Delta 3 Col Nicole Petrucci said during an event, "What we have seen in the Ukraine-Russia conflict is more EW than we have ever seen before".[5]

Russia and Ukraine have been jamming each other's electronic systems. Ukraine has employed electronic warfare to strengthen its air defence against Russian missiles and drones. Russia, on the other hand has been carrying out jamming and interference of signals to disrupt global positioning system satellites that are being employed by Ukraine for guided aerial and artillery munitions.

Russia is known to have a total of five EW brigades, out of which, three brigades are deployed against Ukraine. Ukraine is using many radios and electronic equipment supplied by NATO. Russian EW operators already have experience in dealing with these radios based on their operations in Syria. Therefore, they are able to jam radio sets being operated by Ukraine.

The most powerful and actionable tool in EW is ECM which includes jamming. For example, the Russian R-330Zh Zhitel can jam satellite communications, GPS and cellular networks. Russian forces also resorted to deception as part of ECM in that they used RB-341V Leer-3 system to break into cellular network of eastern Ukraine and passing fake orders to troops during the insurgency period of 2014 to 2022. The range of Leer-3 for jamming VHF and UHF frequencies is extended by using repeaters mounted on Orlan-10 drones.

ESM, is used for detection, monitoring, direction finding and analysis of enemy's transmissions. The process identifies the vulnerabilities in the targeted transmissions from radios, radars and other electronic devices for exploitation. Using their ESM capabilities, most ECM systems using Direction Finding equipment can find the coordinates of enemy radio

and cellphone transmissions which can be used to direct fire and destroy these targets.

Russian exclusive ESM system Moskva-1 is a precision HF/VHF receiver that can detect the reflections of commercial TV and radio signals from targets like ships and aircrafts and find their coordinates. Thus, this passive receiver can track targets and pass on the data to suitable weapon systems for carrying out neutralisation.[6]

RUSSIAN EW CAPABILITIES

Russia has well-organised and equipped EW units and formations since long, which are well trained and battle hardened. Their five EW brigades are deployed with five Russian military districts, which were West, South, North, Central and East districts. These EW brigades support regional EW operations that include jamming of enemy surveillance radars and satellite communications over long ranges. These brigades are equipped with heavier EW equipment like Krasukha-2, Krasukha-4, Leer-3, Moskva-1, and Murmansk-BN systems. Besides, each Russian Army Maneuver Brigade has one EW Company on its orbat which have lighter equipment like R-330Zh Zhitel and carry out EW support within about 50 km range.

Table 1 below gives out the details of major EW equipment held with Russian Army.

S. No.	EW SYSTEM	PURPOSE	YR FIELDED	DESCRIPTION
1	1RL257 Krasukha-4	Targets X-band and KU-band radars, on aircraft, drones, missiles, and low-orbit satellites	2014	Based on two KamAZ-6350 trucks, one a command post and the other fitted with sensors
2	1L269 Krasukha-2	Targets S-band radars, particularly on airborne platforms. Often used paired with the Krasukha-4	2011	Also based on two KamAZ-6350 trucks
3	RB-341V Leer-3	Disrupts VHF and UHF communications, including cellular communications and military radios, over hundreds of kilometres	2015	Consists of a truck-based command post that works with Orlan-10 drones to extend its range

S. No.	EW SYSTEM	PURPOSE	YR FIELDED	DESCRIPTION
4	RH-330Zh Zhitel	Jammer; can shut down GPS and satellite communications over a radius of tens of kilometers	2011	Consists of a truck command post and four telescopic-mast phased-array antennas
5	Murmansk-BN	Long-range detection and jamming of HF military radios	2020	Russian sources claim it can jam communications thousands of kilometers away
6	R-934B	VHF/UHF jammer that targets wireless and wired communications	1996	Consists of either a truck or a tracked vehicle and a towed 16-kilowatt generator
7	SPN-2, 3, 4	X- or K u-band jammers that target airborne radars and air-to-surface guidance-control radars	(not available)	Consists of a combat-control vehicle and an antenna vehicle
8	Repellent-1	Antidrone system	2016	Weighs more than 20 tonnes
9	Moéskva-1	Precision HF/VHF receiver for passive coherent location of enemy ships and planes	2015	Published sources cite a range of up to 400 kilometers

Table 1: Major Russian EW Equipment [7,8]

ECCM is meant to protect electronic systems from ESM and ECM. With highly sophisticated sensors and jammers having been developed, ECCM has become extremely important aspect of EW for survivability on the battlefield. ECCM encompasses technologies and methods to shield electromagnetic systems from being detected or jammed. Some of the ECCM techniques include frequency hopping and spread spectrum techniques that are resistant to jamming. One example during the Russia- Ukraine war is use of US supplied SINCGARS radios by Ukraine which have anti jamming measures.

INITIAL LACK OF IMPACT OF RUSSIAN EW

Russia is known to have well equipped EW units and formations with highly skilled and experienced personnel. Therefore, it was expected that Russian forces, with their overwhelming proportion of EW resources, would dominate the electromagnetic spectrum right from the beginning.

Russia had earlier invaded the Crimean Peninsula in Feb 2014, a part of Ukraine and captured it. Since then, Russians have been using EW as a vital part of their operations in no war-no peace situation, also called 'Grey Zone' warfare in the Donbas region. Russians used Leer-3 EW vehicles along with Orlan-10 drones to jam Ukrainian communications. They were also breaking into the local mobile-phone networks and sending publicity material. Ukrainian radios were detected, geo located and targeted.

However, in the major escalation, when the Russian invasion commenced in February 2022, it was observed that the Russian EW was not effective. Ukrainian forces were not facing the levels of jamming which they had experienced in Donbas. The effect of drones and ground based EW operations was also not visible. Russian forces did carry out physical destruction of some radio stations and TV towers, however, Ukrainian leadership remained in communication with other counties.

REASONS FOR THE FAILURE OF RUSSIAN EW[9]

There were some inherent differences in the operational conditions prevailing during the Russian invasion of Ukraine as compared to Donbas region. The key factors are summarised in the seceding paragraphs.

- **Slow Progress of Russian Offensive due to Lack of Air Superiority.** The Stinger shoulder-fired missiles provided by NATO to Ukraine inflicted heavy attrition on Russian helicopters and jets. So when Russian troops crossed the border, the desired levels of air superiority was not available, making their progress slow and thereby they faced constraints in use of drone based EW equipment. On 03 Mar 2022, the UK's Ministry of Defence said the Russian advance on Kyiv has been delayed by "staunch Ukrainian resistance, mechanical breakdown and congestion".[10]

- **Lack of Manoeuvre Space.** There were difficulties in moving forward due to lack of manoeuvre space and Ukrainian resistance. Also, there were problems in deploying ground based EW equipment due to lack of deployment areas for jammers in predominantly urban environment.

- **Inability to Effectively Employ Russian Drones.** Russian forces could not send their drones at far distances due to limited range and vulnerability of control signals in Ka and Ku bands. Russians resorted to advance along multiple axes with Ukrainian forces interspersed between Russian columns and jamming by Ukrainians was effective due to close ranges.

- **Dense Electromagnetic Environment**. Dense population in the areas of operations led to dense electromagnetic environment. With civilian cellphone networks transmissions and military communications getting mixed up, it was difficult for Russian systems to identify military transmitters.

- **Use of NATO Single-Channel Ground and Airborne Radio System, or SINCGARS by Ukraine Forces**. Ukrainian Forces had some Single Channel Ground and Airborne Radio System (SINCGARS) radios and were trained in its operation, but the numbers were very limited. However, after the invasion by Russian forces, large number of these radios were provided by NATO to Ukraine. Their earlier radios were made in Russia and they had some vulnerabilities which were known to Russians, and hence could be exploited. SINCGARS have in-built high grade encryption and frequency hopping features which make them jam resistant.

  There were certain videos released showing Russian armoured convoys stuck along the roads near indicating that there were problems of logistics back up delaying the move. The effect was felt on the move of other elements also including EW equipment. Also, the Russian forces remained on the move, due to which they could not set up heavy systems like the Krasukha-4.

CONSOLIDATION OF RUSSIAN EW EFFORTS[11]

Russian forces slowly consolidated their EW efforts and started becoming more effective. Excalibur artillery shells, which were received by Ukraine from the US in March 2022 had GPS navigation system which were

Figure 2 : Russian Jammer Krasukha 4. **Source :** https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

highly accurate. By March 2023, they suddenly started missing their targets due to jamming of GPS signals. Similarly, Joint Direct Attack Munitions (JDAM) guided aerial bombs and Guided Multiple Launch Rocket System GMLRS long-range missiles, which are used with U.S-made High Mobility Artillery Rocket Systems (HIMARS) started missing the targets. Jamming was also being carried out of the control signals of Ukrainian drones, making them crash.

The operational situation in Ukraine has considerably changed and Russia forces are at an advantage now. Russia has consolidated its positions in Ukraine's South and East. Ukraine has suffered heavy attrition in men and weapons. With consolidation of positions, the front lines are better defined and the Russian logistics support has also improved considerably. Russian forces are now using their EW systems for directing indirect weapons. The Russian aim of capturing Kyiv in a quick operation did not materialize and the conflict has changed to a

war of attrition, which provides opportunities to Russian forces to use EW advantageously. Russian forces are no longer spread over multiple lines in built up areas and they are able to find Ukrainian positions and direct fire at them.

Russia has overwhelming superiority in EW resources as compared to Ukraine with three EW brigades deployed in this conflict. The Russian EW operators have gained enough experience with SINCGARS radios and are able to detect the emissions with Leer-3 and Orlan-10 drones. Though due to high grade encryption and frequency hopping, it may be difficult to intercept and exploit, it is possible to detect the transmissions and carry out its geolocation. The well-defined front lines enable Russian EW units to target Ukrainian military units based on the detected transmissions.

Russians had found it difficult to use their powerful EW system, Krasukha-4 during advance towards Kyiv. Now in the Donbas region, EW brigades are effectively using the Krasukha-4 to jam the radars and communication links on Ukrainian drones, thus degrading their surveillance.

Russian forces have also carried out re-organisation of their forces to suit the present conflict. The manoeuvre brigades with an strength of two thousand have been reorganised into battalion tactical groups (BTGs) with each having one section of maneuver brigade's EW company for close support. The GTGs are using short range jammers like the R-330Zh Zhitel to jam the control signals of Ukrainian drones ranging from Bayraktar TB2s to DJI Mavics. R-934B VHF and SPR-2 VHF/UHF jammers are being used to degrade communications. Russian EW is fully exploiting the loopholes when Ukrainian units use older radios and cellphones.

UKRAINE'S FIGHT BACK[12]

Ukraine has also augmented its EW resources to counter the Russian electronic attacks. They have successfully employed US supplied counter-drone systems and have downed large number of Russian

Figure 3 : Russian Leer-3 EW System with Orlan-10 Drone for Range Extension. **Source :** https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

drones by jamming of GPS and control signals. They have also been reported to have used high power microwave to damage electronic components in drones and disable them.

They are also using the EW systems provided by the US to jam the communication systems of the Russians with considerable success. The Russian forces do not have very advanced radios like SINCGARS in all their units and often use mobile phones and unencrypted radios for communications which are susceptible to jamming and DF. Russia's latest radio, the 'Azart' sixth-generation SDR, developed by Russia's NPO Angstrem are being introduced in service, but, so far, their numbers are small.

Well defined front lines are also helping Ukrainian EW as it is more convinient to carry out location fixing without ambiguity. Ukraine's EW

have worked on the vulnerabilities of Russian high power systems as it is easy to detect their transmissions. Ukrainian EW is now detecting transmissions from Leer-3 and Krasukha-4 and making them targets.

Ukraine is in the process of developing indigenous EW System. One Ukrainian company, Infozahyst is engaged in developing such equipment. In a modest beginning, two of their equipment have already been introduced in service. These are 'Plastun-RP3000' man-portable direction finder, and truck-mounted version, the Khortytsia-M. Many more equipment are under development.

UKRAINE'S KURSK OFFENSIVE SUPPORTED BY ELECTRONIC WARFARE AND DRONES[13]

Ukraine launched a surprise offensive on 06 Aug 2024 advancing into Russian territory and threatening the city of Kursk. During this offensive, Ukrainian forces planned and executed EW operation very meticulously and effectively. According to Russian military Telegram channel Troika (Three), the Ukrainians forces disabled Russian reconnaissance drones, denying intelligence to the enemy using new interceptor FPVs. Thereafter, avoiding enemy observation, short-range jammers were moved forward to advance positions which were already fed with data from ESM activities carried out in preparation to this offensive.

STARLINK EFFECT[14]

In February 2022, American company SpaceX activated their Starlink satellite internet service in Ukraine to replace internet and communication networks destroyed by Russians during the conflict. Since then, Starlink is being used by Ukrainian government, military and civilians. The Starlink internet has provided a significant benefit to Ukraine's military units, enabling them to share real-time drone inputs, and provide communications where cellphone services have been disrupted. The network has been very useful in guiding Ukraine's drone attacks on Russian targets, thus providing considerable boost to Ukraine's operational efficiency.

Starlink operates a large constellation of thousands of low-earth orbit satellites. It uses narrow beams of the Ku and Ka bands, and the antennas are very small due to higher frequencies which are steered to reject unwanted signals. Thus, they are difficult to jam. The data over the network is encrypted making it highly secure.[15]

RECOMMENDATIONS

- The analysis of EW operations in Russia Ukraine conflict brings out that EW has to be planned as part of overall operational plans and not in isolation. Movement and deployment of EW resources and logistics support have to be facilitated by commanders to harness its full potential. Russian forces found it difficult to extend the ranges of jammers through drones due to lack of air superiority in the intended areas of operations.
- Conventional EW equipment, especially the jammers are high power equipment which are bulky and often carried on heavy mobile vehicles. Taking them close to the enemy lines in the battlefield is fret with the risk of being a target. Hence, there is a need to lay proper emphasis on light weight equipment operating from alternate platforms to work in echelons.
- EW is a weapon of war and EW planning must be fully dovetailed and synchronised with the overall operational plan. It should not be employed in isolation.
- Jamming of enemy's electronic devices is extremely resource heavy. Also, all the systems cannot be jammed all the time. There should be proper prioritisation of targets as per the operational conditions.
- Anti-jamming measures like frequency hopping and spread spectrum techniques are a must for the radios for operational deployment.

- Incorporation of encryption in devices is highly essential as it provides protection against monitoring by ESM devices and also denies information regarding the type of network. Thus it makes it difficult for the enemy to prioritise the targets.
- The vulnerability of GPS signals from the enemy jammers puts a big question mark on GPS based navigation and guidance systems. This calls for having option of working in GPS denied environment. There should be alternative systems like inertial navigation, and advancements like quantum technology based inertial navigation require due consideration.
- Open-source intelligence is critical, including social media posts. Russian soldiers are being targeted when they violate rules and use their cell phones.
- Ukrainian political leaders used social media to communicate directly with their people.
- There should always be provision for alternate means of communications available during the operations. For example, Starlink proved to be a great enabler for Ukraine during a crisis situation.
- Perhaps the biggest lesson from Ukraine for EW is that winning the airwaves does not equal winning the war.

CONCLUSION

Although Russia possesses well developed EW systems since long time which they have been constantly upgrading. But Russian forces were not successful in achieving electromagnetic dominance in the battlefield at least in the initial phases of the conflict. This happened due to various reasons like lack of air superiority, slow progress of battle which led not difficulties in movement and deployment of heavy EW equipment. However, they were able to consolidate their EW efforts and increase the effectiveness after the conflict became more static and a war of attrition.

Ukraine, with the support from US and NATO countries, was able to fight back on the EW front. They were able to protect their communication and radars to a great extent and were also able to carry out jamming and disruption of Russian systems.

The employment of EW in this conflict has thrown up many important lessons which have been closely watched by the leading militaries of the world. It is hoped that the lessons learnt will guide the nations including India to be better prepared for an intense battle in the electromagnetic spectrum.

★★★

Maj Gen Ashok Kumar Srivastava, VSM (Retd) has commanded a Signal Regiment in the sensitive Akhnur Sector of J&K, along the Line of Control. After retirement from service, the General Officer has worked with the corporate sector, wherein he headed technological ventures related to Communications, Surveillance Devices, Command & Control solutions and GISArmy and Spectrum Management for the three services.

NOTES

1 *Nimish Gupta, "A Perspective on Electronic Warfare (EW)", USI Publication, available at https://www.usiofindia.org/publication-journal/a-perspective-on-electronic-warfare-ew.html*

2 *Christian Wolff, "Types of Electronic Warfare", Radartutorial.edu. https://www.radartutorial.eu/16.eccm/ja05.en.html*

3 *Mario LaMarche, "The History of Electronic Warfare: An Overview of Electronic Warfare Part 1", Mercury Systems Inc, Blog, 04 Sep 2018 available at https://www.mrcy.com/company/blogs/history-electronic-warfare-overview-electronic-warfare-part-1*

4 *Rajesh Uppal, "Mastering the Electromagnetic Battlefield: Electronic Warfare technology Trends and Market Dynamics", IDST, 30 March 2024. https://idstch.com/technology/electronics/mastering-the-electromagnetic-battlefield-electronic-warfare-technology-trends-and-market-dynamics/*

5 *Chris Gordon, "'More EW Than We Have Ever Seen Before' in Ukraine, Space Force Official Says", Air & Space Forces Magazine, 24 April 2024. https://www.airandspaceforces.com/ew-ukraine-space-force-training-electronic-warfare-leader-says/*

[6] *Bryan Clark, "The Fall and Rise of Russian Electronic Warfare", IEEE Spectrum, 30 Jul 2022. https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare*

[7] *Jonas Kjellén, "Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces", FOI September 2018. https://dl.icdst.org/pdfs/files3/906f2544ddd693eb1118881a5baff0a3.pdf*

[8] *Richard Scott, "From the JED Archives: Tuning In, Turning On: Russia Brings Radio Electronic Combat to the Fore", Journal of Electronic Dominance, December 2020. https://www.jedonline.com/2022/03/22/from-the-jed-archives-tuning-in-turning-on-russia-brings-radio-electronic-combat-to-the-fore/#:~:text=In%20the%20Swedish%20Defence%20Research,to%20that%20of%20other%20combat*

[9] *Mark Cazalet, "Silent Struggle: Accounts from the Frontlines of Ukraine's Electronic War", European Security & Defence Article, 21 Sep 2023. https://euro-sd.com/2023/09/articles/33980/silent-struggle-accounts-from-the-frontlines-of-ukraines-electronic-war/#:~:text=At%20the%20start%20of%20the,fragging%20their%20own%20side's%20communications*

[10] *Nigel Walker, "Conflict in Ukraine: A timeline", Research Briefing, House of Commons, 16 Sep 2024. https://researchbriefings.files.parliament.uk/documents/CBP-9847/CBP-9847.pdf*

[11] *Oleksandr Tartachnyi, "The Invisible War: Inside the electronic warfare arms race that could shape course of war in Ukraine", The Kyiv Independent, 12 Mar 2024. https://kyivindependent.com/the-invisible-war-inside-the-electronic-warfare-arms-race-that-could-shape-course-of-the-war/*

[12] *Mark Cazalet, "Silent Struggle: Accounts from the Frontlines of Ukraine's Electronic War", European Security & Defence Article, 21 Sep 2023. https://euro-sd.com/2023/09/articles/33980/silent-struggle-accounts-from-the-frontlines-of-ukraines-electronic-war/*

[13] *David Hambling, "Ukraine's Kursk Offensive Blitzed Russia With Electronic Warfare And Drones", Forbes, 09 Aug 2024. https://www.forbes.com/sites/davidhambling/2024/08/09/ukraines-kursk-offensive-blitzed-russia-with-electronic-warfare-and-drones/*

[14] *Nick Paton Walsh, "Ukraine relies on Starlink for its drone war", CNN, 26 Mar 2024. https://edition.cnn.com/2024/03/25/europe/ukraine-starlink-drones-russia-intl-cmd/index.html*

[15] *News Article, "How is Starlink Ukraine's strategic tool in the face of Russian invasion ", The Economic Times, 15 Feb 2024. https://economictimes.indiatimes.com/news/defence/how-is-starlink-ukraines-strategic-tool-in-the-face-of-russian-invasion/articleshow/107710900.cms*

CYBERWARFARE IN RUSSIA UKRAINE WAR LESSONS FOR INDIA

Flt Lt Shobhit Mehta & Gp Capt Umang Kumar

Abstract

Russia invaded Ukraine on 24 February 2022, however the inevitable happening could have been predicted post the War in Donbas 2014. This 10-year-long ongoing struggle is a major testament to the importance of Cyber Space in the battlefield arena. Ukraine neglected its importance for the initial 8 years and was finally paralysed after the ViaSat compromise by the Russian hacktivists. This reactive approach cost Ukraine billions of dollars due to multiple cyber-attacks namely Operation Armageddon, Operation Snake, Ukraine Power Grid attack, and the famous ViaSat attack. It was finally on 26 February 2022, when Mykhailo Fedorov, Minister of Digital Transformation pioneered the formation of the IT Army of Ukraine.[1] The step was very reactive; however, the Ukrainian IT Army has subjugated Russian hacktivists by launching five major cyber-attacks in 2024 only, thus proving that the power of cyberspace lies not in the quantity of minds but the quality. The paper takes us through major cyber-attacks from both fronts and brings out the vital lesson i.e. Self-Reliance. The paper houses two terms at the core, i.e., Cyber Warfare and Information Warfare. Both the terms are closely interlinked as Cyber Warfare provides a platform for large information warfare campaigns. It would not be wrong to comment that Elon Musk has been the knight in shining armor for Ukraine as all forms of military and commercial communication in Ukraine depend entirely on Starlink, a subsidiary of SpaceX. The population of Ukraine is 3.5 times of Israel, still what makes Israel tempestuous is the self-

confidence. Self-confidence comes from self-reliance, bringing extreme sovereignty to decision-making. Today, Ukrainian decision-making is bound to be affected not only by the interests of the West but also by private players like SpaceX. Through the course of the paper, it could be learnt how regulated OSINT, extreme self-reliance, focused Psy-Ops and an armored cyberspace could become the most lethal form of deterrence in this modern warfare.

INTRODUCTION

Cyberwarfare is no longer an alien term in today's geopolitical scenario. It is a tool for highly disruptive Information Warfare (IW) campaigns. Although it is tough to differentiate between cyber-warfare and IW, IW covers propaganda, psyops, and influence campaigns while cyber warfare encompasses DDoS attacks, deploying malware, Zero-day exploits, etc. Countries have recognised cyber-warfare as an important dimension of warfighting with superpowers slicing a huge percentage of defence budget into the same. 46 percent of global digital transactions happen in India. India being the second most populous country plays a significant role in cyberspace and can be a decisive factor in PSYOPs. Recently, a prudent move by the Union Government to train 5000 cyber commandos in the next five years while strengthening the I4C wing of the Ministry of Home Affairs speaks about the potential of cyberwarfare. The paper briefly discusses the various cyber-attacks undertaken by both Russia and Ukraine and bring out important lessons for India.

BACKGROUND OF THE CYBER WAR

Cyberwarfare has been an important confrontation component in the ongoing Russia-Ukraine Conflict since the invasion of Russia on February 24, 2022. After the end of the Cold War, it was the fourth time Russia used military power against its neighbour. However, it was the seventh time Russia used cyberwarfare as a part of a larger campaign that encompasses economic disruption, propaganda, cyber sabotage, DDoS attacks, MiTM attacks, and cyber espionage. Although the physical invasion into the Ukrainian territory happened in 2022, the first cyber-

attack dates back to 2013 with major Russian weapon Uroboros being in sensation since 2005.

The Russia-Ukraine War has been widely covered in various Global broadcasts. Social Media has been a boon and a bane depending on which front exploits it logically and in a regulated manner. The existing evidence on the war has been collected via Open Source. The timelines of cyberattacks during the ongoing Russia-Ukraine are discussed in the following paragraphs:

- **Operation Armageddon**. The operation has been active since mid-2013. Russia opposed the Ukrainian inclination towards the EU. Extensive phishing emails lured the victim to open a malicious attachment. Cybercriminals exploited previously obtained confidential documents to entice Ukrainian targets into downloading malicious payloads from a remotely compromised Control server. The final payload was some form of RAT (Remote Administration Tool) that caused Cyber Espionage.[2] Additionally, the early campaign has also included malware which redirects traffic by disrupting the DNS servers used by the victim machines. The modus operandi involved targeted phishing emails, self-extracting archives, and disruption of Critical Information Infrastructure. More than 5000 cyber attacks were launched against around 1500 Ukrainian entities including the Ministry of Foreign Affairs. It is a perfect example of Russia's broader hybrid warfare strategy combining conventional military tactics with cyber operations.

- **Operation Snake.** The cyberespionage 'toolkit' called Snake or Ouroboros(Serpent in Greek mythology) attacked classified Ukrainian systems like the famous Pentagon plaguing. Post massive Kiev protests due to Mr. Yanukovych's unexpected inclination towards Russia in 2014, 14 cases of Snake were registered with a total of 32 in Ukraine itself since 2010 out of 56 worldwide.[3] Snake gives full remote access to the compromised systems leading to siphoning data from local computers to

remote servers. The attacks were linked with the Moscow time zone and compromised computers of the Ukrainian PMO and at least 10 Ukrainian embassies making highly sensitive diplomatic information available to the perpetrators of the attack. Snake has been recognised as a far more precise weapon than Stuxnet and is an extremely targeted piece of malware that initially infected 84 prominent public websites that were regularly visited by top officials of public and private enterprises. During the initial stage of the attack, users who visited the compromised websites were asked to update their Shockwave player software. Information was collected from thousands of individuals who consented to this request. During the secondary stage of infection, users with IP addresses linked to government entities were targeted with an initial malware called 'wipbot'.[4] This software enabled Snake operatives to assess the rank of infected individuals within the government hierarchy. Finally, a highly targeted malware attack was launched onto the computers of identified higher officials. The modus operandi involved the covert operation of the toolkit enabling it to remain undetected. Snake became active only when the system connected to the internet. It acted as an intermediary point in a network of compromised devices, to exfiltrate data. The attack targeted government networks, critical infrastructure, and private enterprises. The FSB's deployment of Snake signals a long-term strategy to gather critical military intelligence.

- **Interference in Ukrainian Parliamentary Elections (2014).** CyberBerkut, a pro-Russian hacktivist group having ties with Fancy Bear (GRU hacker group) compromised the Ukrainian Central Election system, four days before the national vote.[5] Within 24 hours, the compromised data was uploaded to the internet depicting the success of the operation. The Malware delineated a false result onto the internet, post which DDoS attacks hung the Election Commission website. Ukrainian cybersecurity personnel were able to remove the malware 40 minutes before the election results went live, preventing it from releasing erroneous results.[6]

The modus operandi involved propaganda to discredit the legitimacy of the elections and project Ukraine as a failed state. The Kremlin claimed Ukraine to be controlled by 'fascists' and 'neo-Nazi sympathisers'. The scaling of the attack involved citizens in Crimea and certain areas of Donetsk and Luhansk losing their ability to participate in elections. Widespread misinformation campaigns undermined public faith in the integrity of the voting process.

- **Ukraine Power Grid Hack.** On December 23, 2015, there was an unscheduled power outage in Ukrainian power companies affecting 2.5 lakh personnel.[7] Further technical analysis revealed the presence of BlackEnergy (BE) malware in the computer systems of power companies. In the event mainly three power distribution companies (Oblenergos) were impacted. The cyber-attack at each company was exercised within 30 minutes. Remote operation of breakers was conducted either by remote Industrial Control System (ICS) via VPN or by existing Remote Administration Tool (RAT) at the operating system level.[8] For both possibilities, it is pertinent that actors were able to acquire legitimate credentials via suspected social engineering. KillDisk malware was executed after a cyberattack that corrupted the master boot record of the infected system. The firmware of serial to Ethernet devices was also corrupted. The modus operandi involved complete control of SCADA systems through phishing emails, thus causing remote shutdowns. Unlike data theft attacks, this was aimed at actual physical disruption leading to temporary blackouts affecting roughly 230,000 consumers.[9]

- **2017 Cyber Attacks on Ukraine.** On 27 June 2017, Colonel Maksym Shapoval, a Ukrainian intelligence officer was assassinated in a car bomb in the capital city of Kiev.[10] Post the assassination, the largest known hacker attack in world history was launched. The cyberattack was carried out using the NotPetya virus which used EternalBlue exploits. Soon after NotPetya was executed, the computer underwent a forced

restart as the Masterfile Table of the hard drive was executed, which further displayed the text that files had been encrypted and access could only be granted in exchange for Bitcoins.[11] Also, the Server Message Block protocol in Windows got exploited thus infecting local computers connected to the same network. During the attack, the servers at Ukraine's Chernobyl Nuclear Power Plant and Ukrainian Railways were affected thus handicapping an entire nation. Within 24 hours, the attack was halted and on technical investigation, it was found that the attack was initiated from MeDoc update which is a tax accounting software with over 4 lakh downloads. Servers at the State Savings Bank of Ukraine and Boryspil International Airport were also compromised.[12] Although there is no evidence of a direct connection between the killing of Colonel Shapoval and the NotPetya virus attack, the same couldn't be a mere coincidence. Colonel Shapoval was a senior Ukrainian Security Service (SBU) official and head of a key counterintelligence unit involved in uncovering Russian spies. The incident reflected the Russian Hybrid warfare strategy combining Psyops with Electronic invasion. The modus operandi involved utilising the EternalBlue vulnerability. It was clearly an example of Hybrid Warfare. Scaling of the attack involved targeting over 80 Ukrainian entities, including financial institutions and government agencies. The attack quickly expanded globally, impacting organisations in Europe and the United States. 10% of Ukrainian computers were impacted. The attack resulted in significant operational disruptions and worldwide financial losses exceeding $10 billion.[13]

- **2022 Cyber attacks on Ukraine.** On 14 January 2022, a cyber-attack occurred on 70 government websites including Foreign Affairs and Defence Ministry.[14] Before this on 13 January, Microsoft Threat Intelligence Centre (MSTIC) identified Whispergate carrying out cyber sabotage on various public, private, and non-governmental organisations. Later on 19 January 2022, the Russian hacktivist group Primitive Bear tried to attack a top

Western public entity in Ukraine. A significant distributed denial-of-service (DDoS) attack struck the websites of Ukraine's defence ministry, army, and two major banks, PrivatBank and Oschadbank, on February 15, 2022.[15] This cyberattack compromised the online presence of these key institutions. Various mobile apps and ATMs of various banks were also compromised. Russian Main Intelligence Directorate (GRU) was suspected behind the attack since there was high traffic flow from GRU-based IT infrastructure towards Ukrainian IP addresses. On 23 February 2022, a wiper malware attack was identified on computers belonging to defence, aviation, IT, and banking sectors in Ukraine. On 24 February 2024, thousands of ViaSat modems went offline after hackers targeted a VPN installation in Turin thus pushing wiper malware into multiple KA-SAT broadband modems of ViaSat. This disrupted Ukrainian networks since they used ViaSat's network for communication. Internet services too were crippled in Ukraine post the attack.[16] On March 9, 2022, the Quad9 recursive resolver, which blocks malware, thwarted 4.6 million cyberattacks targeting devices in Ukraine and Poland.[17] A surge in phishing and malware activities was detected as the majority of blocked DNS requests originated from Ukraine. Since 1.4 million Ukrainian refugees were present in Poland, figures for Poland were also elevated. In the ViaSat Modem hack, a VPN appliance misconfiguration was exploited to gain unauthorised entry into the ViaSat network's management segment. The cyberattack utilised a wiper malware called 'AcidRain', which erased data on targeted devices. The attack impacted thousands of modems and resulted in the shipment of approximately 30,000 new modems. Further upgraded version 'AcidPour' was released to have an even greater impact.[18]

- **Attack on Starlink in Ukraine.** After the disruption of ViaSat Networks, on 26 February 2022 Minister Mykhailo Fedorov, requested Elon Musk for Starlink assistance in Ukraine.[19] The response was swift and positive. Within two days, the first shipment of Starlink terminals arrived. Unlike conventional

satellite internet, Starlink used fragmented networking using narrow beams of Ku and Ka bands. Starlink is the lifeline of military and business communication in Ukraine which uses a high degree of defence-in-depth concept.[20] However, there were many videos of careful dismantling of the Starlink terminal. Russian hacktivists got Starlink terminals from the dark web and used the OSINT to first dismantle the terminal and finally place a Modchip in the PCB which provided them access into the highly secure layers of Starlink communication, thus interfering with the available bandwidth. Ukraine has reported degradation in Starlink connectivity over time.[21] The operational approach relied heavily on open-source intelligence (OSINT) and sophisticated electronic warfare systems. As Russian military operations escalated, interruptions became more common and intense, especially in the vicinity of Kharkiv, leading to major communication breakdowns among Ukrainian military units. This is a perfect example of Russian Hybrid Warfare.

- **Ukrainian Attack on Planet**. In mid-January 2024 Ukrainian hacktivists sabotaged 2 petabytes of data and compromised 280 servers at Planet which is a state space hydro-meteorology Research Centre that aided the Russian military in analysing satellite imaging.[22] The damage was the US $10. Further, a Russian Arctic outpost on the Bolshevik Island was cut off from Russian communication networks. The attack involved extensive reconnaissance of the facility's operations, security measures, and personnel. Ukraine attacked deep into Russian territory and was a major confidence booster and resulted in increased Western aid as the world witnessed Ukraine's ability to strike back.[23]

- **HUR Attack on Bureaucrats.** On February 4, 2024, hackers from the Main Directorate of Intelligence of Ukraine's Defence Ministry (HUR) compromised a digital document management platform called 'bureaucrats'.[24] This infiltration revealed multiple confidential files belonging to high-level Russian officials, especially Russian Minister Timur Ivanov. Additionally, the HUR hackers disrupted

Russian military technology for modifying commercial DJI drones, effectively disabling the servers operating Russia's 'friend or foe' recognition system.[25] The attack method involved Advanced Persistent Threat (APT) techniques.

- **Attack on Moskollector.** In April HUR targeted Interregional Transit Telecom (MTT) disarraying critical configuration files leading to network disruptions in Moscow and St. Petersburg. Further Sewage Monitoring and Control System of Moscow was disrupted after 87,000 sensors of communication giant Moskollector were shut down.[26]

- **DDoS Attack on Russian Aerospace .** In early June 2024, HUR launched a DDoS attack on various government websites like the Ministry of Justice, Defence, Finance, IT and Communication, Industry and Energy, etc. Website of United Aircraft Company (UAC), was rendered inaccessible for an extended period.[27] On June 12, 2024, hackers from Ukraine disrupted the online systems of several Russian airports, including Yuzhno-Sakhalinsk, Saratov's Gagarin Airport, etc. causing delays for flights primarily bound for Sochi, Moscow, etc. Before this incident, HUR compromised the official website server of the Stavropol Region's State Duma, inserting the message 'Hold on, we will liberate you!'. Subsequently, HUR along with the BO Team hacker group attacked Russian municipal web resources, disabling two hypervisors and multiple communication devices.[28]

- **Attack on Russian Banking Establishment.** On July 23, 2024, Ukraine's Ministry of Defence Main Intelligence Directorate launched an operation to identify financial institutions that were funding military operations against Ukraine.[29] Subsequently, cyber attack was launched disabling customers of several major Russian banks to access cash from ATMs. The databases of numerous prominent banks, including RSHB Bank, iBank, Alfa-Bank, Raiffeisen Bank, Tinkoff Bank etc. were compromised, followed by service interruptions at multiple large Russian

telecommunications and internet service providers, such as Tele2, Beeline, MegaFon, and Rostelecom.[30]

UNMASKING RUSSIA'S CYBER ONSLAUGHT : AN ANALYSIS

Various cyber warfare tactics were employed by Russia including DDoS attacks, phishing attacks, and malware deployment across various Ukrainian Critical Information Infrastructure. The attacks however lacked planning, coordination, and quality. Despite being a well-established superpower, Russia was unable to tone down its adversary's morale in the initial days of invasion. Although Russian planning was a combined effort by both military units and pro-Russian hacking groups highlighting the importance of public-private partnership in times of distress, still the quality was not up to the mark. The ViaSat's KA-SAT satellite attack caused considerable disruption, however, could not provide the required tactical advantage thus causing a disconnect between cyber actions and military outcomes.[31] The research paper brought out a series of cyber-attacks launched by Ukraine since January 2024. This shows the inability of Russia to adapt to the changing warfare arena and its trivial attitude towards Ukraine considering it a weak adversary. The major issue with the Russian forces was the unchecked use of social media by military personnel thus revealing information about their movements and deployment. Also, the Russian forces relied on poorly secured communication systems including consumer-grade technology and Ukrainian telecom infrastructure. Even the disciplined units relied on poorly secured systems and had no choice but to share data over insecure channels. There are shreds of evidence that Russian investment toward ensuring an armored communication channel never saw the light of day due to prevailing corruption within the Russian procurement channel.[32]

ANALYSING UKRAINE'S CYBER STRIKES

Initially, Ukraine was ignorant to the power of cyberwarfare and faced many hostilities since its communication resources were compromised by Russian forces. In any war, timely communication is a highly decisive factor. Despite initial hostilities, what happened next is an inspiring case study for generations to come. Ukraine swiftly adapted to cyberwarfare,

exploited OSINT to its peak and gathered critical information about Russian movement and deployment. Within two days Starlink terminals were imported and communication facilities were restored. The HUR carried out significant operations, exposing classified Russian files and disrupting essential services within Russia.[33] Ukraine's cyber potential is evident from the fact that it was able to penetrate into Russian networks and extract classified information. Ukraine also employed robust EW techniques to intercept unsecured transmissions. This has enabled them to acquire real-time intelligence on Russian troop movements and locations, providing a strategic edge despite their numerical disadvantage in combat.[34] Ukraine not only fostered its cyber potential in times of distress but also operated successfully which is highly commendable. As Ukraine persists in its cyber campaign against Russia, it encounters several policy challenges. Furthermore, Ukraine could consistently engage in combating narrative warfare, a strategy Russia has employed since and even before February 24, 2022.

INDIA'S TAKEAWAYS FROM THE CRISIS

Russia-Ukraine war taught us many lessons on adaptability, resilience, emotional intelligence, indigenisation, geopolitical relationships, and most importantly grit. Some of the key lessons can be summarised as follows:

- **Strengthening the Communication Infrastructure.** Ukraine was entirely dependent on ViaSat Communications based in Carlsbad, California for its military and commercial communication. After the satellite modems got compromised, Ukraine was left crippled. Communication is the most important factor in today's digital-dominant arena. Even during the 2014 invasion of Russia into the Crimean Peninsula, it was the communication infrastructure that was disrupted and OFC lines were cut down thus amputating the Crimean Peninsula. It is a matter of pride that both the internet service giants of India, i.e., Airtel and Jio are India-based and thus have an emotional connection with maintaining resilience to any cyberattack on the Indian subcontinent, unlike ViaSat which

chose to withdraw the service to avoid further security breach thus affecting their services in other nations as well. It is of utmost importance that Indian Government works in close coordination with these internet giants and sensitise the decision makers on strengthening their physical and cyber security of servers. It is of utmost importance that every employee instills a soldierly attitude. In a similar vein, Reliance Industries has launched a commendable initiative. Rather than hiring random individuals without background checks to protect high-value industrial servers, the company has established a specialised security division called Reliance Global Corporate Security (GCS).[35] The Agnipath scheme is a fresh induction in the military set-up of the nation. The aim has always been a leaner and younger army, however, critics can argue about the non-secure future of recruits. India could draw lessons from nations where military service is compulsory and appreciate their quality of human resources. New Delhi is not providing an insecure future and definitely not imposing compulsory military service, rather bringing down the average age of armed forces and helping individuals instill ramrod posture by giving on-field practical exposure, unlike online platforms educating on how to get up early in the morning and stay motivated. Even after 4 years of engagement, the lessons learnt are going to stay forever with the recruits. Corporate giants like TATA Group, Bharti Airtel, Mahindra Group, Adani Group, etc. should definitely draw motivation from Reliance and ponder upon developing their own credible security arm for safeguarding high-value industrial assets employing the ones who gave their youth to the nation.

- **Investment into Cognitive Warfare.** Cognitive warfare represents the non-traditional conflict that employs psychological and information-centric strategies to affect the subconscious thus manipulating thoughts, convictions, and sentiments of individuals, groups, and countries.[36] One method of conducting cognitive warfare is the use of Software Defined Radios (SDR) for dynamic audio messaging. The first step in the project will be to develop

an SDR for handling wide-bandwidth signals and handling data in real-time. Then specialised software must be developed to embed subliminal messages in audio streams. The SDR will then be placed in areas to continuously sniff enemy frequencies. Machine learning will pick up on trends and psychological loopholes. These habits and weaknesses will be analysed, and subliminal messages will be created and, via Digital Signal Processing, delivered to the enemy via audio streams in a way that conscious perception can't hear. SDR will be programmed to change frequencies and modulation schemes and track the alteration of enemy behaviour and morale to provide feedback that can help tailor future subliminal messaging attacks.

- **Investment in Hardware and Software Testing Labs and Skilled Force.** The creation and implementation of hardware and software testing facilities play a vital role in improving the quality, dependability, and efficiency of tech products. These facilities provide environments for thorough product evaluation, ensuring compliance with industry norms and user expectations. The establishment of testing facilities incorporates a number of steps, including identifying the technologies and hardware required, hiring skilled staff, and putting certified testing procedures into place. Physical product evaluation and software-integrated testing need to be carried out in efficient testing facilities. To find flaws and guarantee smooth cross-platform operations, software testing uses a variety of approaches, such as unit, integration, and system tests. Despite growing recognition of the importance of these testing facilities', India continues to face infrastructure challenges and a lack of skilled professionals in this field.[37] Investment in specialised training programs needs to be focused. As per the NASSCOM report, India will need over 1 million skilled software testing professionals by 2025.

- **Self Reliance.** The 2017 Cyber Attack on Ukraine taught us that India cannot afford any zero-day exploit and this is only possible if it goes for Make in India followed by extensive testing. Western

military aid is crucial for Ukraine's hardware supplies, while approximately 30 percent of Russia's defence manufacturing relies on components sourced from abroad.[38] A prudent move by Indian Defence Forces to discard Chinese cameras is a major step to prevent any cyber espionage by foreign agents. The example of PCB tampering and Modchip has been discussed. In this arena of the 'Internet of Things' where everything is connected via the internet to everything needs to be prevented from leaving digital footprints. Segregating from the internet is impossible, the only thing possible is going for products that are Made in India ranging from an earphone to automobiles that can tap the conversation via Android Play. India also quite behind in terms of an indigenous mobile company that is widely accepted and thus is a point of concern.

- **Evolution of Centralised Cybersecurity Framework.** Several ministries and agencies oversee cybersecurity in India, with the Ministry of Electronics and Information Technology (MeitY) developing cybersecurity policies, the Ministry of Home Affairs (MHA) handling cybercrime investigations and national security matters, the National Technical Research Organisation (NTRO) gathering technical intelligence, and the National Critical Information Infrastructure Protection Centre (NCIIPC) safeguarding critical infrastructure. Unlike Israel, where the Israel National Cyber Directorate (INCD) functions as a centralised authority for cybersecurity under the Prime Minister's office, India lacks a unified command structure. The INCD effectively coordinates national efforts and combines military and civilian resources. In contrast, India's decentralised approach may result in multiple agencies responding independently during a national emergency, without a single authority coordinating their actions. If given the authority to issue directives and manage responses during cybersecurity emergencies, the National Security Council Secretariat (NSCS) could potentially serve as the single point of contact (SPOC).

- **Need for Clearer Guidelines on Setting Offensive Posture.** India always had a defensive approach toward cybersecurity. The formation of institutions like CERT-In which focuses on incident response and mitigation is a testament to this. The country did not have clear policies to initiate cyber offensives. The introduction of the Joint Doctrine for Cyberspace Operations in June 2024 was a major shift in India's cybersecurity stance, recognising the need for incorporating offensive capabilities.[39] It provided frameworks for better cross-service collaboration but lacked clear guidelines for putting offensives into practice.

- **Need for a Robust and Ethical Framework.** India recently introduced its Joint Doctrine for Cyberspace Operations. The step clearly reflects the cyber awareness of the nation, however lacks clearer guidelines and accountability measures while carrying out an offensive cyber-attack. This incertitude will prevent a focused offensive posture. The UN Charter discusses the principles of state sovereignty and non-intervention which draw a very hazy picture regarding the legality of cyber operations.[40] For example, offensive cyber actions could be considered breaches of sovereignty, raising legal issues regarding escalation.[41] A well-defined legal framework would help in establishing accountability protocols for personnel engaged in offensive operations. This will ensure that actions align with both national and international laws.

- **Regulations on OSINT.** Starlink has been providing military and commercial communication in Ukraine after the ViaSat Modem Hack.[42] However, hacktivists have been able to penetrate the highly secure firewall systems of Starlink with the help of Modchip which is placed after careful dismantling of the terminal. There were many videos on dismantling the Starlink terminal on YouTube primarily from the West. It is an exemplar of acting against the interests merely for minuscule gains. It is of paramount importance to apprise Indian-based tech giants to share minimum resource data on an open platform. Ukraine exploited videos and selfies uploaded by Russian soldiers to target their positions, prompting

Moscow to implement legislation prohibiting smartphones on the battlefield. Additionally, Kyiv and its supporters utilised open-source information to shape narratives against Moscow. Consequently, it is crucial to emphasise the controlled use of open-source data.

- **Exploiting the Primitive Yet Powerful Psyops.** India is the second most populous country in the world. With the advent of the IT revolution and YouTube shows the huge pool of talent that India holds. YouTube CEO mentioned that creators should be recognised as 'next-generation studios' for the way they are refining entertainment and India is the fastest-growing market for video-sharing platforms and is leading in many global trends in terms of the creator economy all over the world. From fitness to entertainment to education to vlogs to webinars to gaming, in every sphere of India Youtubers are ruling. This can be a major tool for India while exercising PSYOPs as part of cyberwarfare. Indian Government should work in close coordination with these next-generation studios and shape public opinions as per the interest of the nation. PSYOPs have been the most powerful tool for ages. All the freedom fighters exercised this form of warfare. With the advent of the cyber dimension, the outreach has increased manifolds.

- **Strengthening the Narrative Warfare.** The battle for narrative dominance is a psychological effort to influence public sentiment domestically and internationally. Skillfully constructed narratives can garner support for military actions, justify policies, and persuade undecided groups. In the current digital landscape, managing information flow is crucial. Countries must proactively shape their narratives to thwart adversaries' attempts to manipulate public perception. A cohesive messaging strategy strengthens a country's narrative and undermines opposing viewpoints, necessitating a dedicated psychological operations structure across various command levels. India could establish a psychological operations unit at the theatre command level to effectively handle narrative warfare. Probably Command Cyber

Operations and Support Wings (CCOSW) can be tasked with the same. The unit can initially give exposure to the military lifestyle to journalists and media houses and in turn, get the soldiers trained on media management and narrative warfare. Israel and the US are perfect examples of the same. "Hasbara," a term in Hebrew meaning "explanation," describes Israel's efforts in public diplomacy.[43] These initiatives aim to influence global perceptions and narratives about the nation, especially its policies and actions. Israel's narrative warfare includes the distribution of government-approved military narratives and Search Engine Optimisation which boosts favorable content and diminishes negative information. Another example to quote is the 77th Brigade of the U.S. Army which concentrates on combating misinformation and conducting information operations within conventional military activities. The best way to emerge as a leader in narrative warfare is to play a game on two fronts. To shape the narrative of the world towards India it is essential to checkmate major social media platforms like Meta, Twitter, and YouTube which are all US-based and India has hardly any control over their information optimisation algorithms. Filtering the narration through the psychological operations unit could be significant in this aspect. To shape the narrative within India and India towards the world, lessons from China could be learnt which has banned Western social networking sites and has achieved self-reliance in narrative warfare as well. WeChat is a substitute for Meta, Sina Weibo is a substitute for Twitter and Youku is a substitute for YouTube. New Delhi too could develop its very own narrative warfare DCs and launch apps that will ensure control of information flow, rapid dissemination of state narratives, monitoring of real public sentiment, and counteracting foreign narratives.

- **Dedicated Task Force for Strengthening HUMINT Around Indian Borders.** Sashastra Seema Bal (SSB), post-1962 Chinese invasion was actively involved in strengthening national unity among border populations and nurturing loyalty to India,

especially in remote areas that felt disconnected from the central government.[44] The paramilitary force exercised the HUMINT potential of local villagers thus bolstering intelligence and early warning systems for military units.[45] A similar concept can be revived and a dedicated task force functioning under Command Cyber Operations and Support Wings (CCOSW) under each command can be formulated that will work in close liaison with IB and R&AW, thus further strengthening inter-agency ties.

- **Raising Cyber Territorial Army.** In the realm of Information Technology (IT) and cybersecurity, India has established itself as a global leader, demonstrating the exceptional skills of its workforce. The IT industry accounts for roughly 7.5% of India's GDP, with projected revenues of $254 billion for FY 2024. India is home to more than 70,000 recognised startups and approximately 107 unicorns.[46] The nation has also made considerable progress in cybersecurity, implementing measures to strengthen digital security frameworks and address cyber threats. The government should create a platform for these passionate techies to serve the nation. The PSYOPs unit proposed above can collaborate with Internshala or LinkedIn and recruit individuals fit to serve the nation as part of the Cyber Territorial Army, which can be separate to that of the Territorial Army's existing initiatives like that with the CyberPeace Foundation, in organising hackathon. This will motivate non-uniformed civilians from leading private and other sectors to join the armed forces and the output will surely be better post donning the uniform.

- **Nurturing a Strong Cyber Wing.** Ukraine followed a very reactive approach when it came to cyberwarfare. Following the Russian invasion, Mykhailo Fedorov, who serves as both the Minister of Digital Transformation and First Vice Prime Minister of Ukraine, declared the establishment of the IT Army of Ukraine on February 26, 2022. Since 2014, Ukraine has been under constant cyber-attack. A proactive decision could have saved Ukraine from such attacks well in advance. The recent initiative by Union Government

on training 5000 Cyber commandos in the next 5 years is a commendable step towards securing information and cyberspace.

- **Revisiting Past Memorandums and Treaties.** Various memorandums and treaties are signed over time, however, with changing governments the practical execution of the agreements becomes questionable. As was the case with Ukraine which gave up nuclear arms in the 1994 Budapest Memorandum in exchange for favourable commitments from various nations including Russia. India needs to visit past memorandums and thoroughly evaluate the trustworthiness guaranteed. Even the UN Security Council didn't take any major step towards the Russia-Ukraine conflict highlighting the inability of international bodies when superpowers are involved. On paper, many agreements have been signed like General Security of Military Information Agreement (GSOMIA), Logistics Exchange Memorandum of Agreement (LEMOA), Communications Compatibility and Security Agreement (COMCASA), Basic Exchange and Cooperation Agreement (BECA) and Bilateral Defence Cooperation Agreements.[47] New Delhi needs to ensure that these agreements are exercised once in 6 months and thoroughly discussed in joint exercises and lessons learned are incorporated and necessary changes are made in the agreement, or else every time new government comes, new agreements will keep getting piled up without making any sense.

- **High Adaptability.** A paper published in the 'Carnegie Endowment for International Peace' mentions that cyber-attacks do not serve as decisive strategic tools. Instead, they function in an auxiliary capacity, complementing broader warfare efforts in primary combat zones. Offensive cyber operations during an armed conflict are not strategically decisive but rather play a supporting role in major theatre wars. Although it was evident that Russia had far more cyber op capabilities than Ukraine and Ukraine saw a lot of such attacks since 2014, however still as of today, Ukraine is standing strong against the mighty Russians and this teaches the biggest lesson of 'High Adaptability'. Ukraine always

dealt with such attacks with an open mind and embraced evolving technical solutions despite the conventional battlefield marches. One such example is requesting Elon Musk for Starlink services in Ukraine overnight on X.

- **Placements, Hackathons, and Internships (Israel's Elite Secret Cyber Unit 8200).** A cybersecurity council comprising both government and private sector representatives should be established in India. This body should be empowered to conduct investigations, convene meetings, and propose specific cybersecurity measures. India also needs to expand international cooperation and engage further with international organisations like the US, Interpol, and the Global Forum on Cyber Expertise. India is home to the brightest minds in the world studying in top tech institutions like IIT. Indian Government should engage in Campus Placements attracting the top minds to work with CERT-In rather than Google, Facebook, or other Tech Giants. Also, Cyber Wing should keep track of Hackathon champions and motivate them to work for the nation by giving internships. Internships are the best means to introduce young sharp minds to this way of life where money takes a backseat and something higher drives them to work for the nation. Israel's elite secret cyber unit 8200 is the mastermind behind the recent pager attack which consists of mostly Gen Z. Now it's India's turn to channel the massive potential of the Indian Generation Zoomers.

CONCLUSION

The world only respects the one, who is powerful and independent. There is no place for the weak. The crux of the paper boils down to just one word: Atmanirbharata. The word is the key to Global dominance and becoming a world leader. The Government of India has taken various initiatives to ensure an armoured cyberspace. Some of the key milestones in this direction have been the introduction of the National Cyber Security Policy 2013, the formation of the National Critical Information Infrastructure Protection Centre (NCIIPC) under section 70A

of the IT Act 2000 (amended in 2008), the formation of Indian Computer Response Team and in turn introduction of Cyber Swachhta Kendra by Cert In in 2017. Personal Data Protection Bill was introduced in the year 2023 which focused on concurrence-based Data Collection by businesses. Ministry of Home Affairs introduced The Cyber Coordination Centre to ensure coordination between various law enforcement and cyber security agencies. In 2018, the Defence Cyber Agency (DCyA) was established. In June 2024, India introduced its Joint Doctrine for Cyberspace Operations, under the leadership of the Chief of Defence Staff. Although this doctrine marks a significant advancement in bolstering India's cyber capabilities and fostering inter-service cooperation, the issue of a disjointed governance framework remains unresolved. Additionally, the doctrine requires the inclusion of appropriate legal guidelines for initiating offensive cyber attacks. The government has largely invested in developing indigenous Software Defined Radios (SDRs) bringing together the Defence Electronics Applications Laboratory (DEAL), IIT Kanpur and DRDO.[48] This process needs to be expedited, and concurrent research should be initiated on software development for real-time analysis of adversary communications, taking into account the Software Development Institute (SDI). Israel follows an aggressive approach and eliminates targets in advance to maintain regional supremacy. The Stuxnet attack showcases the offensive stance of both the US and Israel. India should work on similar lines but first, decide the rules of engagement for global awareness. India must actively work towards strengthening the narrative warfare. By promoting narratives that distort reality, Russia aims to attract global attention in its favor. As one of the most populous nations, India should actively work towards safeguarding itself from the projection of distorted reality. To boost the cyberculture in the country, basic cyber hygiene should be introduced as an independent subject in schools and young minds should be educated on the potential of the cyber world. Ethical hacking and cyber security can be made an independent engineering discipline with universities working in close coordination with DCyA, CERT-In, TCS, NCCC, etc. towards providing internships and handpicking exceptional talent. Additional Security Operation Centres should be established across

the Nation to ensure real-time threat monitoring and incident response. India could also ponder over incentivising cybersecurity start-ups and providing funding to top research institutions working towards filling gaps in the cyber-ecosystem. Thus, building a ramrod and credible security arm, boosting local tech innovation, identifying nascent talent via hackathons and internships, incentivising cyber startups, fostering public-private partnerships, and educating on correct cyber posture can help sketch a resilient digital future of India.

★★★

Flt Lt Shobhit Mehta is a serving officer in the Indian Air Force and is an Engineering graduate from IIIT Ranchi. He is an alumnus of AFTC Bangalore.

Gp Capt Umang Kumar is a serving officer in the Indian Air Force. He is an alumnus of AFTC Bangalore and did his M Tech in Computer Science from IIT Bombay.

NOTES

1 *D. Goodin, "After Ukraine recruits an "IT Army," dozens of Russian sites go dark," 1 March 2022. [Online]. Available: https://arstechnica.com/information-technology/2022/02/after-ukraine-recruits-an-it-army-dozens-of-russian-sites-go-dark/. [Accessed 26 September 2024].*

2 *B. Prince, "'Operation Armageddon' Cyber Espionage Campaign Aimed at Ukraine: Lookingglass," Security Week, 28 April 2015. [Online]. Available: https://www.securityweek.com/operation-armageddon-cyber-espionage-campaign-aimed-ukraine-lookingglass/. [Accessed 26 September 2024].*

3 *L. Ciolacu, "'Game-Changing' Snake Malware Used in Espionage on Ukraine," 2014 March 11. [Online]. Available: https://www.bitdefender.com/en-us/blog/hotforsecurity/game-changing-snake-malware-used-in-espionage-on-ukraine. [Accessed 01 Jan 2025].*

4 *S. Jones, "Russia-linked cyber attack on Ukraine PM's office," CNBC, 08 August 2014. [Online]. Available: https://www.cnbc.com/2014/08/08/russia-linked-cyber-attack-on-ukraine-pms-office.html. [Accessed 21 September 2024].*

5 *M. Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," The Christian Science Monitor, 18 June 2014. [Online]. Available: https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers. [Accessed 29 September 2024].*

[6] *Ibid*

[7] *"Cyber-Attack Against Ukrainian Critical Infrastructure," 20 July 2021. [Online]. Available: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. [Accessed 01 Jan 2025].*

[8] *Ibid*

[9] *Ibid*

[10] *A. Luhn, "Ukrainian military intelligence officer killed by car bomb in Kiev," The Guardian, 27 June 2017. [Online]. Available: https://www.theguardian.com/world/2017/jun/27/ukraine-colonel-maksim-shapoval-killed-car-bomb-kiev. [Accessed 23 September 2024].*

[11] *Ibid*

[12] *J. Wolff, "How the NotPetya attack is reshaping cyber insurance," 01 Dec 2021. [Online]. Available: https://www.brookings.edu/articles/how-the-notpetya-attack-is-reshaping-cyber-insurance/. [Accessed 01 Jan 2025]*

[13] *Ibid*

[14] *D. Jones, "Viasat network cyberattack linked to newly discovered Russian wiper," Cyber Security Dive, 2022 April 2022. [Online]. Available: https://www.cybersecuritydive.com/news/viasat-network-cyberattack-linked-to-newly-discovered-russian-wiper/621421/. [Accessed 24 September 2024].*

[15] *Ibid*

[16] *Ibid*

[17] *"Cyberattacks on Ukraine Increase Tenfold," 28 Mar 2022. [Online]. Available: https://evgenverzun.com/cyberattacks-on-ukraine-increase-tenfold/. [Accessed 01 Jan 2025].*

[18] *Ibid*

[19] *M. Burgess, "The Hacking of Starlink Terminals Has Begun," Wired, 10 August 2022. [Online]. Available: https://www.wired.com/story/starlink-internet-dish-hack/. [Accessed 22 September 2024].*

[20] *Ibid*

[21] *Ibid*

[22] *B. Toulas, "Ukraine: Hack wiped 2 petabytes of data from Russian research center," 26 Jan 2024. [Online]. Available: https://www.bleepingcomputer.com/news/security/ukraine-hack-wiped-2-petabytes-of-data-from-russian-research-center/. [Accessed 01 January 2025].*

[23] *Ibid*

[24] *Kyiv Post, (2024), "HUR Hacks Russian Defense Ministry, Gets Access to Classified Documents", URL: https://www.kyivpost.com/post/28979*

[25] *The New Voice of Ukraine, (2024), "Ukrainian cyber specialists disrupt Russia's drone control system in successful operation", URL: https://english.nv.ua/nation/cyber-specialists-of-the-hur-attacked-the-russian-drone-control-system-50391154.html*

[26] *"Ukrainian Hackers Launch Cyberattacks on Subsidiary of Major Russian Telecom," 28 April 2024. [Online]. Available: https://www.kyivpost.com/post/31798. [Accessed 01 Jan 2025]*

[27] *M. Fornusek, "Ukrainian cyberattack 'paralyzed' work of Russian ministries, companies, source said," 05 June 2024. [Online]. Available: https://kyivindependent.com/ukrainian-cyberattack-paralyzes-work-of-russian-ministries-companies-source-said/. [Accessed 01 Jan 2025].*

[28] *Ibid*

[29] *P. Paganini, "Ukraine's cyber operation shut down the ATM services of major Russian banks," 27 July 2024. [Online]. Available: https://securityaffairs.com/166214/cyber-warfare-2/atm-services-russian-banks-hacked.html. [Accessed 01 Jan 2025]*

[30] *Ibid*

[31] *OCCRP, "A Most Reliable Ally: How Corruption in the Russian Military Could Save Ukraine," 13 April 2022. [Online]. Available: https://www.occrp.org/en/feature/a-most-reliable-ally-how-corruption-in-the-russian-military-could-save-ukraine. [Accessed 05 December 2024].*

[32] *Ibid*

[33] *K. Denisova, "The Kyiv Independent," 04 March 2024. [Online]. Available: https://kyivindependent.com/military-intelligence-claims-cyberattack-on-russian-defense-ministry-gave-access-to-classified-documents/. [Accessed 05 December 2024].*

[34] *S. Magnuson, "Daily Fight for Ukraine Spectrum Superiority Puts Electronic Warfare Front, Center," 03 August 2024. [Online]. Available: https://www.nationaldefensemagazine.org/articles/2024/3/8/daily-fight-for-ukraine-spectrum-superiority-puts-electronic-warfare-front-center. [Accessed 01 December 2024].*

[35] *"Global Corporate Security," [Online]. Available: https://rgsscareers.ril.com/. [Accessed 02 December 2024].*

[36] *S. Yu, "Cognitive Warfare: A Psychological Strategy to Manipulate Public Opinion," [Online]. Available: https://www.igi-global.com/chapter/cognitive-warfare/332283. [Accessed 03 December 2024].*

[37] *"Software Testing: Trends Shaping the Industry-May 2022," [Online]. Available: https://www.nasscom.in/knowledge-center/publications/software-testing-trends-shaping-industry-may-2022. [Accessed 29 November 2024].*

[38] *"Russia's War Machine Runs on Western Parts," 22 February 2024. [Online]. Available: https://foreignpolicy.com/2024/02/22/russia-sanctions-weapons-ukraine-war-military-semiconductors/. [Accessed 02 December 2024].*

[39] *G. s. Ananya Raj Kakoti, "The new cyberspace doctrine's impact on India's security," 09 July 2024. [Online]. Available: https://www.hindustantimes.com/ht-insight/future-tech/the-new-cyberspace-doctrine-s-impact-on-indias-security-101720517961470.html. [Accessed 03 December 2024].*

[40] *"Sovereignty," [Online]. Available: https://cyberlaw.ccdcoe.org/wiki/Sovereignty. [Accessed 04 December 2024].*

[41] *Ibid*

[42] *Z. H. Z. K. Wang Peiwen, "Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security," [Online]. Available: https://interpret.csis.org/translations/starlink-militarization-challenges-and-responses-to-space-intelligence-and-information-security/. [Accessed 04 December 2024].*

[43] *"The art of deception: How Israel uses 'hasbara' to whitewash its crimes," [Online]. Available: https://www.trtworld.com/magazine/the-art-of-deception-how-israel-uses-hasbara-to-whitewash-its-crimes-12766404. [Accessed 01 December 2024].*

[44] *A. Chakravorty, "Explained: Why was the Sashastra Seema Bal force created?," 17 Feb 2016. [Online]. Available: https://indianexpress.com/article/explained/sashastra-seema-bal-ssb-news/. [Accessed 01 Jan 2025].*

[45] *A. Sharma, "Know Your Paramilitary | Part 5: SSB — India's Watchful Protectors at The Nepal And Bhutan Borders," 15 April 2022. [Online]. Available: https://www.news18.com/news/india/know-your-paramilitary-part-5-ssb-indias-watchful-protectors-at-the-nepal-and-bhutan-borders-4986169.html. [Accessed 28 November 2024].*

[46] *S. Sun, "IT industry in India - statistics & facts," 12 June 2024. [Online]. Available: https://www.statista.com/topics/2256/it-industry-in-india/#topicOverview. [Accessed 05 December 2024].*

[47] *"Indo-US Military Agreements," [Online]. Available: https://byjus.com/free-ias-prep/militaries-us-india-share-facilities/. [Accessed 01 December 2024].*

[48] *"Application of Software Defined Radio (SDR) in the Indian Defence Sector," 21 December 2023. [Online]. Available: https://www.hsc.com/resources/blog/software-defined-radio-applications-defense/. [Accessed 04 December 2024].*

ARTIFICIAL INTELLIGENCE AND INFORMATION WARFARE: A DANGEROUS WEDLOCK

Col Gaurav Soni & Mr Dhruv Swarnakar

Abstract

This paper aims to understand the newfound and potentially menacing relation between Artificial Intelligence (AI) and Information Warfare (IW). It previews as to how AI could fundamentally change IW making it highly incisive and accurate. While control of information and spread of disinformation shall continue to remain the central theme of IW, in the times of tomorrow, artificially generated disinformation campaigns will exponentially enhance the speed, intensity and most importantly the accuracy of such operations. It reads into the known global instances of AI powered IW to include a case study of the recently concluded Taiwan Elections. It not only covers as to how AI is creating new content at unprecedented speeds but also how it sparks a viral chain of distribution reaching billions of users at an incredible pace. The paper covers as to how AI takes course corrective measures towards the information content by continuous feedback and refinement making the information campaign an assured success. A unique aspect discussed in the paper is how AI is able to weave the data into making the human mind believe the information by factoring-in a touch of authenticity. Aspects like Truthiness, Cognitive Fluency Bias, Hashtag Creations, AI Engagement, AI Simulation, Generative Adversarial Network (GAN), Social Media Analytics, Sockpuppet accounts, Click Farms etc have been elaborated in the paper. The paper throws light on global instances of AI powered IW campaign levying special focus on China's

demonstration of offensive and defensive IW campaigns. Towards its conclusion, it aims to recommend suggestions at the concept level especially applicable to democratic countries likes India in order to battle the rising 'Monster Duo' of AI and IW.

INTRODUCTION

On March 16, 2022, through a video message, Ukraine's defiant President Vladimir Zelensky asked his forces to lay down their arms in the ongoing Russia-Ukraine conflict. It took no time for the video to be circulated to millions of users across the world, and soon enough, global strategists were set to wonder whether the conflict was coming to an end. It took more than 24 hours of restorative actions at the hands of Ukraine to convince its own army and the world that the video was 'deepfake' and was artificially crafted and inseminated in social media. So much so was the impact that some of the news channels had begun running the story that Zelensky had fled Kyiv. Even prominent new channels like 'Ukraine 24' found their website's homepage defaced with hackers having inserted the fake video in the opening webpage. Immediate rebuttal came in from President Zelensky himself who negated release of any such video through Facebook. While Russian social media such as Vkontake, continued to toss the video repeatedly as far and wide as possible, majority of the speedy restoration actions were undertaken by western social media giants like Youtube, Twitter and Meta which reacted favourably by quickly removing the video. Meta's security head Nathaniel Gleicher, Twitter representative Trenton Kennedy and YouTube's Ivy Choi did not lose any time in calling the video 'synthetic' and in 'violation of their policies'.[1] While a supportive Social Media, as in the instant case, could arrest the alleged 'deepfake' video in time, an adversarial information campaign duly powered by Artificial Intelligence(AI) could have changed the outcome of the conflict. It may have to believed that the brewing concoction of AI with far reaching and powerful social media is heralding a change in the design and conduct of modern wars and this, if tapped, has a potential to bring about incalculable damage to the adversary.

This paper aims to understand the newfound and menacing relationship between AI and Information Warfare (IW). It previews how AI could fundamentally change IW, making it highly incisive and accurate. It reads into the global instances of AI-powered IW and briefly covers China's progress in the domain. Towards its conclusion, it aims to recommend enactments at the concept level, especially applicable to democratic countries like India, to battle the rising 'Monster Duo' of AI and IW.

IS DISINFORMATION ENOUGH FOR INFORMATION WARFARE?

The Media-(Dis)information-Security document Defence-Education-Enhancement-Programme (DEEP) of NATO identifies gaining of information advantage over adversary as the key objective of information operations. In doing so, it outlines that, own information-space needs to be protected while destroying and disrupting adversary's information and its flow.[2] Use of information as a tool to warfare is not a novel concept and adequate instances of its application can be drawn out even from the earliest battles and epics known to mankind. Since then, the concept of IW has undergone numerous changes in the manner in which own information-space is protected and that of the adversary denied. Considerable evolution did take place post the World Wars, in a manner that its application could now be through newly evolved domains such as Electromagnetic, Economic, and Cyberspace. However, the generation of content, its speed of generation and application, trial and testing, validation, intensity of effort and accuracy of IW targeting remained limited in scope and execution. Fast forwarding today, and specially so in the last decade, the character of information operations is once again undergoing a metamorphosis. Though the domains of application of IW may remain unchanged but the manner in which information will be synthesised and applied is set to undergo an overhaul with the manifesting of Large Language Models (LLM). One such example is the Open AI's Chat GPT. While control of information and spread of disinformation shall continue to remain the central theme of disinformation, in the times of tomorrow, artificially generated disinformation campaigns will exponentially enhance the speed, intensity and most importantly the accuracy of such operations.[3] A case study of operations of a Chinese

Origin Information Technology (IT) Cell called 'Storm 1376' also known as 'Spamouflage' or 'Dragonbridge', in the Taiwanese General Elections elaborates on how AI can execute a coordinated, expeditious and highly accurate IW campaign.

AI-POWERED IW CAMPAIGN ON TAIWAN ELECTIONS: A CASE STUDY

In January 2024, Taiwan conducted its 16th presidential elections. The election remained narrowly contested between the Democratic Progressive Party (DPP), headed by its candidate William Lai, and the Kuomintang (KMT) party led by Yu-ih, with the third party being the Taiwan People's Party (TPP), run by Ko Wen-je. While DPP and TPP have a democratic approach, KMT is believed to be enjoying China's backing. A report released by Microsoft Threat Intelligence published on Microsoft's Official website brought out that beginning in November 2023, China-based Group 'Storm 1376' artificially generated thousands of memes denigrating images of DPP and TPP in the forthcoming elections.[4] In December 2023, a deepfake video of a woman claiming to be the mistress of DPP candidate William Lai was pumped into social media and made viral by AI tools through Search Engine Optimisation (SEO). Also, emerged in December the 'Spring Breeze Files', which alleged that William Lai was an informant acting against Taiwan.[5] These files were artificially amplified on social media like Twitter, Facebook and Japan's social media app 'Line'. Sensational hashtags were artificially generated using crawling software, which could feel the pulse, diction and vocabulary of the voter. These artificially generated hashtags exponentially increased the speed and spread of the viral files. In January itself, a series of videos titled 'Secret History of Tsai-Ing Wen' wherein artificial anchors virtually read out a 300-page document alleging a number of frauds on the then president Tsai-Ing Wen to include falsified academic credentials, finances and personal life.[6] These videos were artificially generated using 'Capcut opensource AI software' designed by China-owned firm ByteDance, which is also the parent company of Tik-Tok.[7] One of the most remarkable AI-generated IW campaigns emerged right on the day of the election when an AI audio recording depicting

Foxconn's head, Terry Gou, was seen backing the KMT candidate Hou Yu-ih. It is imperative to understand that Foxconn is the most revered private company in Taiwan and is responsible for its semiconductor prowess.

The campaign, as above, is not only related to the 'Creation of Disinformation' but has far more to do with its distribution, marketing, feedback-based improvement and precise and timely delivery to the targeted audience. Some of the advanced processes which were seen to be manifesting in the campaign are discussed as follows:

- **Creation of Content - Deepfake Videos**. An AI model or software is created based on complex algorithms called Variational Autoencoders (VAEs) or Generative Adversarial Network (GAN). Once the software or the model is ready, a very large set of images, videos and voiceovers of the target individual is then imported onto the model.[8] This large dataset is used to train the model to the desired degree of accuracy. Desire propaganda scripts is then inserted in a manner as if the target individual himself is delivering the script. Chinese software like Capcut can facilitate its editing in a smooth manner by providing unique features like chroma key (green screen), keyframe animation and motion tracking, which refine an AI-generated deepfake video. Keyframe Animation, for instance, gives a much finer control over the target object's movement and allows for smooth transitions, while Motion Tracking helps synchronisation of the movements.

- **Creation of Distribution Media - Virtual Accounts Using Virtual Phone Numbers.** Almost all social media platforms now necessitate linking of the account with a personal mobile number. An AI-based web engine can create bots which are 24 x 7 active on the internet, creating virtual phone numbers. Alternatively, apps like 'Call Hippo' can be used to generate virtual phone numbers. These phone numbers can then be used to create virtual email accounts and, consequently, social media accounts. Once such an account is created, bots pretending to be human

entities can be designed to be part of large-scale fake Whatsapp groups, Telegram Groups or any closed group on the internet. Activities of a normal, legitimate group, like Casual Chats, Display Profiles, etc, are artificially undertaken by these member bots. In a process called 'AI Engagement' or 'AI Simulation', the bots can even be trained to like, comment or share chats, thus earning the trust of other human members. At the opportune time thereafter, the bots pump deepfake videos and falsified information on these groups as part of coordinated IW campaign.[9]

- **Social Media Analytics - Understanding Public Sentiment**. Firstly, a large data set is extracted with the help of member bots from groups on social media. This is integrated with various data analytics AI software like Microsoft Power BI, IBM Watson, Sprout Social, Tableau AI, etc. Data which is analysed includes comments, reviews on products, likes, dislikes, watch times, repeat watching frequency, sharing patterns, etc. Even emojis and the undertone in the language of comments are analysed. Bots can even incite discussions and artificially generate pointed questions to know and better understand the minds of human participants.[10] Such analysis gives out some key outputs like the potential favourable or non-favourable target audience, key issues of contention and issues which can be sensational in nature. Even individual target personnel can be identified.

- **Hashtag Creation - Setting a Chain Reaction**. A hashtag first indexes a post and then incorporates it as part of a much larger audience. Thus, it is not merely a private group agenda but allows the subject to attract participation from an audience spread across the globe. AI can create sensational hashtags by first undertaking social media analysis and understanding of common public sensations and then undertaking Natural Language Processing (NLP) to create the most apt hashtags. Some of the most commonly available AI hashtag generating software like 'Ahref' and 'Hootsuite' can craft hashtags that can propel a subject exponentially and thus hog the attention space.[11] Once artificially

pushed to the extent of being 'Trending', it thrusts itself into the mind space of a considerably large section of society. Such can be the negative impact of hashtags that, on one occasion, the #Pizzagate, resulted in the spreading of false rumours of child trafficking, public mobilisation, and even firing incidents in the US.[12]

- **Optimisation, Refinement and Testing**. AI tools undertake an iterative process to closely monitor their actions during all of the processes as above to continuously identify problem areas, undertake remedial actions and thus artificially correct and refine the processes. Unlike human processing, which entails considerable processing and decision delays, AI-based refinement procedures enhance targeting accuracy multi-folds in near real-time.[13]

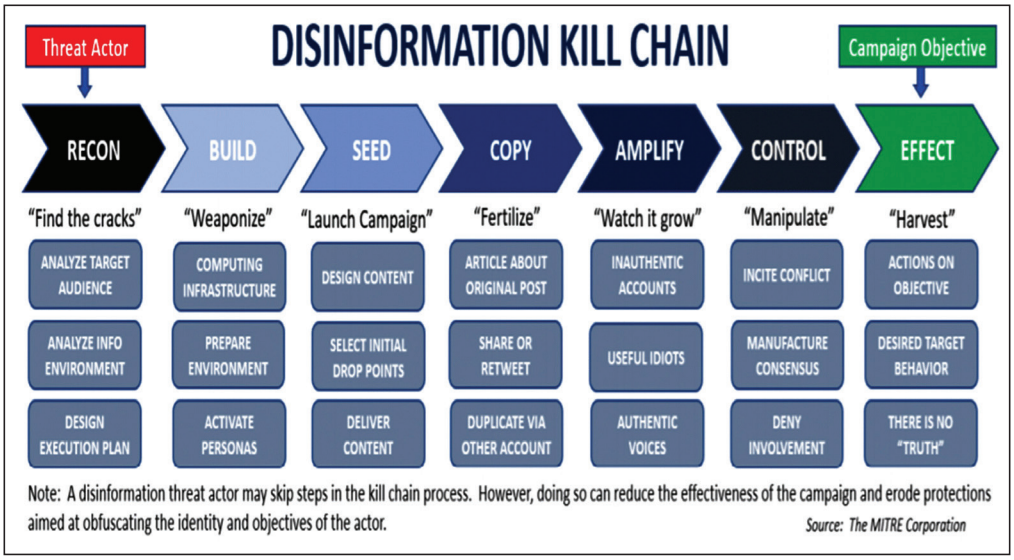


Figure 1: Disinformation Kill Chain Adopted in IW. **Source:** The Mitre Corporation

Unlike earlier elections where conventional IW was a standard tool for meddling with election outcomes, the 16th Taiwanese elections saw a never before well-coordinated AI-powered IW campaign at the hands of adversaries. In this campaign, the focus shifted from the mere creation

of disinformation to the processes through which this disinformation was executed, making it highly precise and effective. Such a shift in the IW is best understood in the language of business management. In business, the Product Concept applies to the generation of quality and cost-effective products. On the contrary, the Marketing Concept targets the market and aims to integrate profitability with manufacturing by suitably modifying production, processes, delivery and communication.[14] Before the onset of AI, information campaigns were largely focused on the product, i.e. Disinformation. However, with the coming of AI, IW does not just focus on Disinformation but its quick generation, mass distribution, targeted approach and feedback-based iterative modifications applicable both to the product, i.e. disinformation and the process in a highly automated, sharp, incisive and ruthless manner. The advantages of incorporating AI in IW are not limited only to the creation of the product i.e. Disinformation and processes enhancements. In fact, the most remarkable advantage is its ability to package the Disinformation in a manner most trustable by human minds. This is discussed in subsequent paras.

Tinkering the 'How' of What We Believe. AI-generated IW manipulates two of the many fundamental qualities of human thought. First is Cognitive Fluency Bias wherein humans tend to believe what is easy to process or 'be understood' by them[15] and second is Factor of Truthiness, which tends to accord authenticity to a well-presented, convincing and gripping visual, text or speech. Given the vast data set available to AI models and its ability to modify them and selectively embed them with evidence, AI can produce information that is highly polished and well presented in a considerably short time. Given the constraints of time in a strained scenario, human-made presentations can appear to be 'messy', 'disorganised' and even 'delayed when pitched against outputs of AI. Since AI presentations would be easy to process, Cognitive Fluency Bias causes human minds to believe them more vis-à-vis human-made presentations. Further, the 'Factor of Truthiness' invokes authenticity in AI presentations, which is not likely to undergo scrutiny by human 'gut feeling' as it is well crafted and seemingly duly evidenced.[16] Thus, AI-generated content can not only be fake but also be so engineered

that it even aims to tinker with the human subconscious, which is the key element in crafting our initial beliefs and proclivities. Once such beliefs are instated, they are reinforced using 'filter bubbles', which, in essence, are a set of contents shown over and over to a user based on his initial choices and inclinations. Similar to the concept of YouTube recommendations, which display videos similar to users' earlier choices, such filter bubbles over a period of time, build a tunnelled vision and a belief system that is resilient and defiant even if conflicting arguments are logical and duly supported by evidence.[17] Action based on beliefs and not based on objective facts. Once the belief system is concretised, humans tend to act according to belief and not based on objective facts or even visual reality. Defined very popularly by the term Post Truth and adopted by the Oxford Dictionary in 2016 as its word-of-the-year, in this phenomenon, individuals prioritise their firmly instilled beliefs even if they face contrarian real evidence. Decisions and Actions that follow are drawn from these beliefs.[18]

RECENT USAGES OF AI IN IW: GLOBAL SCAN

Some of the recent cases of aggressive uses of AI-integrated IW undertaken by nations across the world are briefly discussed in subsequent paras.

- Moldova, which is a neighbouring state to Ukraine, has been adopting a pro-west stance in the Russia-Ukraine conflict. In a deepfake video, Maia Sandu, the west-friendly President of Moldova, was seen backing a Russia-friendly political party and was shown to propose her resignation.[19]

- In June 2024, Tech firm Open AI alleged that Israel's AI firm STOIC may have launched an AI campaign in India in an attempt to meddle with Indian elections. It was alleged that the AI campaign called Zero Zeno praised the Congress Party and undertook an anti-BJP stance. One of the typical modus operandi of STOIC is to create fictional persons and generate artificial biographies to garner voters' attention.[20]

- AI-powered 'Shallowfake' videos can artificially slow down or increase the speed of video. In May 2019, US House of Representatives Speaker Nancy Pelosi's video was 'Shallowfaked', making her speech appear drowsy and drunk. Such videos can significantly dent the reputation of the target individual.[21]

- Venezuela's government used the services of the private company 'Synthesia' to generate pro-government AI-generated news through news channels which never existed and were artificially created.[22]

- Political parties explore new ways to build emotional connections as part of their voter outreach. In Indonesia, an AI app launched by a presidential candidate enabled users to artificially create a joint selfie with the leader, thus building a personal connection.

- Another form of large-scale AI-powered IW is the generation of 'Robocalls' faking the voice of popular personalities. In the run-up to primary elections in the US New Hampshire, people received a large number of phone calls from robots impersonating US President Joe Biden.[23]

CHINA'S CONCEPTUAL PURSUITS AND GIANT LEAPS IN AI-ENABLED IW: A BRIEF OVERVIEW

Control of Information Space has remained an approach at the heart of China's Strategic pursuits. Chinese Defence White Paper of 2004 modified China's erstwhile approach of 'local wars under modern, high-tech conditions' to 'local wars under informationised conditions', which was further modified to 'Winning Local Wars under conditions of informationisation'.[24] By 2015, China had further tweaked its military strategy to 'winning informationised local wars'. This was also the time when the PLA Strategic Support Force (PLASSF) had begun to take shape, and concepts of 'Integrated Network-Electronic Warfare (INEW)' were introduced.

As LLM models such as Chat GPT have enabled generative AI solutions offering automated content creation and processing, China has made constant efforts to maintain an incisive edge in the domain. At the grassroots level, its Academy of Military Sciences, PLA Academy of Electronic Technologies, Military Strategy Research Centre and the Academy of Xian for Politics have undertaken research studies and have developed themselves into pockets of excellence. China's Military Strategy of 'Intelligentised Warfare' is a four-pronged approach achieved through information-processing, quick decision-making, cognitive warfare and use of swarms. To execute these, China has identified that AI must form the core of Intelligentised Warfare.[25]

At the concept level itself, China has not shied away from accepting AI as a driving tool to Modern Warfare. In 2017, PLA's 'New Generation AI Development Plan' categorised AI as a strategic Initiative and identified the need for a Whole-of-Nation approach in the domain. In 2019, President Xi Jinping, while addressing the Collective Study Session of CCP's Politburo, identified the need to guide public opinion by using AI in IW domains of news collection, its production, distribution, and timely feedback and suggested creation of AI Editorial Departments.[26] In May 2021, he further identified the need to create an opinion of the external public favourable to China. During the 'Internet Civilisation Conference' conducted in 2022, Ye Zhenzhen, a CCP secretary, expressed that big data and AI help understand citizens better and can contribute towards China's leadership. He referred to the development of projects focussed on cognitive computing in order to guide public opinion and even public values and called them 'national weapons in the digital era'.

CHINA'S OFFENSIVE APPLICATION OF AI

- In August 2023, a forest fire engulfed the areas of Maui in Hawaii, USA, after which Storm 1376 flooded the internet with AI-generated files, memes and articles blaming the US government for testing a 'Weather Bomb' leading to the fire incident. Interesting to note is that the flames were artificially shown to be engulfing cities and suburban towns to cause outrage in the local populace with an aim to create an outrage in the public.[27]

- Soon enough, in November, after a train derailment in Kentucky, Storm 1376 artificially drew similarities of the incident with Pearl Harbour or the 9/11 Terrorist Attack and called it a US government vendetta.[28]

- The Microsoft Threat Intelligence Report released in 2024 highlighted that a large number of 'Sockpuppet' accounts operating on social media are linked to the Chinese Communist Party. Sockpuppet accounts are virtual accounts wherein bots may pretend to act as citizens of the country and participate in actual political discussions, thus swaying common public thoughts.

- In August 2023, Chinese Storm 1376 undertook a powered IW campaign pointed towards nuclear water discharge into the Pacific Ocean by Japan and attributed this act to US-Japan making attempts towards Water Hegemony. Realistic-looking Twitter accounts, captivating AI memes and visuals were used to garner public attention.[29]

- In the run-up to American elections, several deepfake videos emerged depicting US President Joe Biden giving out 'transphobic' viewpoints in an attempt to undermine his popularity in the transgender community.

- Meta, the parent company of Instagram and Facebook, revealed that over 8000 fake Chinese accounts were deleted, which may have been originally based either in China or in China's 'Click Farms' in Brazil and Vietnam.[30] Earlier, a Click Farm typically employed a large number of persons to click on online content, feigning large traffic flow and thus enhancing popularity statistics. With AI now in the offing, Click Farms are now easily being 'cultured' and upscaled by employing artificial bots.

- China does not fall short of running an IW campaign, even at individual levels. Chinese immigrants who are now US citizens are targeted by AI bots sending out countless messages and flooding their social media accounts. Jiyayang Fan, a Chinese-US citizen,

received a barrage of AI-generated demeaning messages calling her a traitor and homophobic.[31] Even an AI-generated hashtag, #TraitorJiayangFan, was first made to trend with the help of AI tools and then retweeted between 12,000 users.

CHINA'S DEFENSIVE APPLICATION OF AI

China's internet firewall and CCP's absolute control of the in-house narrative are well known. Despite these guards in place, China has maintained an active defensive AI-powered IW campaign under:

- **Search Engine Optimisation (SEO).** China's surveillance bots maintain a constant vigil over search queries. When searched for sensitive topics like 'Uyghur' or 'Xinjiang', Chinese state media showing positive news rank best in SEO results thus returning as the top pages on Google or Bing.
- **Astroturfing Marketing.** Astroturfing Marketing is a business term wherein inauthentic messages are subtly pushed to make them appear authentic. China undertakes large-scale coordinated campaigns posting AI-generated posts supporting CCP's policy in the form of fake people's interviews depicting wide grassroots acceptance.[32]
- **Drowning Conversations.** A large quantum of artificially generated messages and articles are created to drown out anti-China conversations on the internet.
- **Multi-Channel Networks (MCN) of Social Influencers.** While YouTube is banned in China, some Youtubers are permitted and contracted out using a MCN agreement with the CCP. These are popular influencers, often women, who bring the best picture forward and are allowed to be monetised on YouTube. Comments generated on their videos are artificially reposted for increased visibility through AI models. On the other hand, non-MCN channels are not allowed to be monetised, thus drawing away the inspiration to create even neutral content.[33]

- The Chinese government has created a large number of surveillance chatbots that trap an online query or discussion on Tienmann Square and prevent the display of any information on the subject.
- China has also outsourced UK-based firm Synthesia, which has artificially created a Western media news channel 'Wolf News' singing praises for CCP. This was primarily targeting the in-house Chinese population towards strengthening their belief in the CCP.

The application of AI by China for powering the new generation of IW needs a detailed study and can only be covered as a brief overview in this paper. It should, however, be understood that, having identified the burgeoning role of AI in future IW, China, incited by its desire to control the global narrative, will continue to hone its AI prowess.

GLOBAL EFFORTS TO COUNTER AI-POWERED IW

Given its propensity and accuracy, IW powered by AI can considerably undermine governments, regulatory mechanisms and belief systems of a large mass of people. The threat posed by AI-powered IW has drawn the attention of governments across the globe.

- The European Union (EU) is amongst the forerunners in countering IW powered by AI. In 2019, the EU's Rapid Alert System was launched, which was aimed to enable common situational awareness by sharing information and jointly mitigating disinformation between stakeholder countries. EU has legislated that media platforms are required to give assurance on curbing Disinformation on Election proactively. Very soon, it is likely that legislation will require social media platforms to identify deepfake content and 'label' them prior to circulation. EU's AI model Project InVID is an intelligent Web Crawler which undertakes video fragmentation, annotation detection, video forensic investigation, contextual analysis and web intelligence analysis for filtering out authentic content to be provided to news media. This content can then be handed over to responsible media houses and journalists

for publishing on their news platforms. It also introduces a User Generated Content (UGC) Verification App, which can identify and authenticate a valid user who can then post authentic data only on the web.[34]

- Social media firms have also evolved their own mechanisms to thwart IW campaigns. Google has developed a Convolutional Neural Network (CNN) called EfficientNets, which can analyse fake images on the web. Microsoft has developed 'Video Authenticator' to give a percentage basis veracity to a video. Microsoft has also initiated Project Origin partnering with Radio Canada, BBC and The New York Times, which aims to verify online content by attaching digital certificates to files which can be plugged in with the user's browser extension. Wall Street Journal and Associated Press have also come together towards Trusted News Initiative with a plan to create similar labelling or certification of online content. This plug-in, called Newsguard, can be installed with various online browsers.
- China has been moving towards criminalisation of deepfakes as the Cyberspace Administration of China has called it a threat to China's security and social stability.
- Necessary changes in the legislation of democratic governments are a much-desired reform to battle IW. Singapore, in 2021, passed a Foreign Interference Countermeasure Act, which allows its bureaucrats to take suo motto cognisance of Foreign Interference and thus undertake suitable countermeasures.
- The US is unequivocal about its prioritisation of AI. The 2023 National Defence Authorisation Act (NDAA) brought in a $20 billion hike in spending on AI. Further, the US Third Offset Strategy (TOS), which is a highly tech-oriented innovative programme, has identified AI to be the number one on the list of priorities. In 2018, the US announced the formation of the Jt AI Centre (JAIC) to progress AI as a tool for future warfare. In 2019, the US Department of Defence proposed its 'Defend Forward' Strategy, which aimed to disrupt malicious IW away from the US mainland.

DoD's DARPA has also undertaken the Media Forensics (MediFor) for large scale threat detection and Semantic Forensics (SemaFor) large-scale characterisation of flagged content in order to reach its originator.[35] In 2020, JAIC adopted IW as one of the key objectives of its AI campaign. By 2022, JAIC was merged with the Chief Digital & AI Office (CDAO), which is not only limited to the military but adopts a whole-of-government approach for data analytics and AI strategy. One of the most remarkable steps has been the raising of the Global Engagement Center (GEC), which is a US Government body operating under the Bureau of Public Affairs, with an objective to counter foreign disinformation campaigns by undertaking inter-agency coordination. One of the main objectives of the GEC is also to collaborate globally with like-minded nations towards such initiatives. In its Special Report on China's IW campaign released in 2023, the GEC identified that China's Information Manipulation is a 'challenge to the integrity of global information space'.[36]

KEY CHALLENGES: BATTLING AI POWERED IW

A report published by Davos has identified disinformation facilitated by AI as the most grave short-term threat to mankind. In the ever-evolving technological scenario, battling AI-based IW can be immensely challenging. Some of the key characteristics that give AI-powered IW a definite edge in the 'cat and mouse' game are discussed in subsequent paras.

- **Accessibility and Affordability.** Modern Open Source AI tools, despite being new in the market, are remarkably cheap and accessible, thus lowering the entry barrier for most users.[37] Softwares like DeepFaceLab allow the creation of Deepfake videos at almost no cost. This allows for large-scale participation and a humongous generation of data available to the target audience. Even if a counter-campaign is run, it is likely to be overwhelmed by the sheer propensity of data.

- **Policy Structure - Very Large Online Platforms (VLOP).** Some of the biggest VLOPs, such as Google, Facebook, and Twitter,

came together to sign an understanding wherein they assured the prevention of the usage of AI tools from interfering in elections. However, some platforms like Telegram, having end-to-end encryption, have refrained from such understandings and thus are not bound to check or control AI-generated deepfake data. It is, therefore, that Telegram remained one of the most extensively used services for the flow of AI-powered IW during the Russia-Ukraine conflict.[38]

- **Undermining Trust in Truth.** Excessive flooding of information of a variety puts the information consumer in a situation of dilemma as to what to believe and what not. This allows for a window of opportunity even to a mischief-maker as he can brand any information on the internet as AI-generated, thus whisking it away as mere propaganda. Such a window, popularly termed as Liar's Dividend, allows even a real culprit to capitalise on the dilemma so created and deny even real evidence.[39]

- **The Streisand Effect.** In most cases, the first response of the government is to ban or remove content from social media to prevent its proliferation. However, psychologists believe that it gives rise to what is known as the Streisand Effect which, on the contrary, intrigues the common public and further motivates them to consume the content.[40] An official rebuttal by an authentic source may provide a better alternative.

- **Freedom of Press and Freedom of Expression.** Especially applicable in democratic countries like the US and India, AI-powered IW finds adequate windows of operation under the protection of freedom of the press or that of expression.

SUGGESTED COUNTERMEASURES BY DEMOCRACIES: AI-POWERED IW

Very Large Online Platforms (VLOPs) are the prime movers of the mass population. There is a need to draw operating guidelines and regulations necessitating these platforms to inform the government and public at large on foreign IW campaigns. Adequate transparency norms have to be instituted. Detection, deepfake labelling and responsibility for verification of authentic information before the public's consumption has to be mandated upon the VLOPs.

There is a need for a clinical approach in the identification of foreign IW campaigns. Foreign agencies instigating such vendettas have to be brought under regulation or duly censored before the public's consumption. There is also a need to develop advanced AI software and tools that can detect and counter malicious IW campaigns. Web browser plugins or government-developed apps hosted on official websites should be developed to detect such discrepancies.

The concept of Cognitive Innoculation entails that suitable pre-emptive warning be given to the public en masse about the possible intent and approach of the adversary's IW campaign. This can remarkably reduce the extent of impairment likely to be caused by a malicious IW campaign.[41] Such warnings will have to be predictive in nature and will, therefore, have to use AI-based apps or software to detect anomalies and subsequently inform the public.

A quick rebuttal in the form of a correct narrative has to be built up. However, given the speed and intensity of AI-powered offensive IW, such rebuttals will have to be artificially generated and processed for wider consumption. Stronger regulations carefully crafted to be able to delineate freedom of expression from intentful anti-national IW

campaigns are the most important steps towards preserving security while also retaining the democratic character.

A battle in the information space needs an integrated approach. Such integration is at two levels. Firstly is the global collaboration of countries and agencies, which need to combine vigilance with response for an accurate and quick response in arresting the disinformation campaign. The second is integration at the national level. Specialised and empowered mission-based agencies adopting a whole of government approach towards data integration and analytics, detection and mitigation of IW campaigns will have to be raised to address disinformation drives.

CONCLUSION

The modern world security calculus is set to undergo an unprecedented tumult with the coming of new-age IW campaigns powered by AI. With its astute abilities to remain in control of information battlespace, AI can lead to large-scale population mobilisation, thus leading to a state of disharmony and perpetual distrust even amongst unsuspecting players. In particular, are the vulnerable democratic nations where the will of the people sets the national agendas. With nations like China, which not only limit IW to the military but apply a whole-of-society approach in times irrespective of conflict and peace, it is this will of the people and their natural belief system which shall be at the centre of the AI-powered IW campaign of the future. Battling IW powered by the ever-evolving and maturing AI will, therefore, have to be at the core of all efforts of responsible governments.

★★★

Col Gaurav Soni is presently posted as Directing Staff in the Junior Command Wing, Army War College. The officer is from Artillery, has served in Srilanka and has commanded his regiment along the Indian borders. The Officer is a PhD in Defence and Strategic Studies and is a PG Diploma in AÍ and Machine Learning.

Mr Dhruv Swarnakar is pursuing research in Mechatronics at Manipal Institute of Technology, Udupi. His areas of interests include Mechatronics and Robotics. With keen interests in Weapon Technology and AI, he actively follows defence upgrades across the globe. He is a research member for projects undertaking designing of Bionic Arm for handicapped persons. He has also made significant contributions towards research for Disaster Management and Weather Forecasting using Machine Learning Algorithms.

NOTES

[1] *Simonite, Tom. 2022. "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be WIRED." March 17, 2022. https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/.*

[2] *DEEP. n.d. "What Is Information Warfare?" Accessed September 12, 2024. www.nato.int/nato_static_fl2014 /assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf.*

[3] *Hunter, Lance , Craig Albert, Josh Rutland, Kristen Topping, and Christopher Hennigan.. 2024. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." Defense & Security Analysis 40 (2): 235–69. https://doi.org/10.1080/14751798.2024.2321736.*

[4] *"China Tests US Fault-Lines and Ramps AI Content to Boost Its Geopolitical Interests - Microsoft On the Issues." n.d. Accessed September 18, 2024. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/.*

[5] *"China Tests US-Fault-Lines and Ramps AI Content to Boost Its Geopolitical Interests - Microsoft On the Issues." n.d. Accessed on September 18, 2024. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/.*

[6] *Tsai Yung-yao, Jonathan Chin. 2024. "China Is Posting Fake Videos of President: Sources - Taipei Times." Accessed on September 13, 2024. www.Taipeitimes.Com/News/Front/Archives/2024/01/11/2003811930.*

[7] *Chi Hui Lin. 2024. "How China Is Using AI-News Anchors to Deliver Its Propaganda | Artificial Intelligence (AI) | The Guardian." Https://Www.Theguardian.Com/Technology/Article/2024/May/18/How-China-Is-Using-Ai-News-Anchors-to-Deliver-Its-Propaganda. 2024. Accessed on 14 September, 2024. www.theguardian.com/ technology/ article/2024/may/19*

[8] *Zendran, Michał, and A Rusiecki. 2021. "Science Direct-NC-ND-License https://Creativecommons.Org/Licenses/by-Nc-Nd Peer-Review under Responsibility of the Scientific-Committee of KES International. Swapping Face-Images with Generative Neural Networks for deepfake Technology-Experimental Study." Accessed on 13 September, 2024. https://doi.org/10.1016/j.procs.2021.08.086.*

[9] *Rajvardhan Oak. 2024. "Friend-or-Faux : How Bots Pose Challenges in Social-Media Spaces." Accessed on 09 September, 2024. www.Timesofindia.Indiatimes.Com/Blogs/Cyber-Chronicles/Friend-or-Faux-How-Bots-Pose-Challenges-in-Social-Media-Spaces/. January 17, 2024.*

[10] *Ibid*

[11] *"70 Best Social Media Hashtag AI Tools - 2024." n.d. Accessed September 18, 2024. https://topai.tools/s/social-media-hashtag-.*

[12] *Mark Fisher. 2016. "Pizzagate: From Rumor-to-Hashtag to Gunfire in D.C." December 6, 2016. Accessed on 02 September, 2024. www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06.*

[13] *Hunter, Lance , Craig Albert, Josh Rutland, Kristen Topping, and Christopher Hennigan.. 2024. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." Defense & Security Analysis 40 (2): 235–69. Accessed on 07 September, 2024. https://doi.org/10.1080/14751798.2024.2321736.*

[14] *Philip Kotler. 2000. "THE MARKETING CONCEPT." 2000. Accessed on 07 September, 2024. https://www2.nau.edu/~rgm/ha400/class/professional/concept/Article-Mkt-Con.html.*

[15] *Kliegr, Tomas, Bahník, and Fürnkranz. 2021. "A Review of Possible-Effects of Cognitive-Biases on Interpretation of Rule Based Machine Learning Models." Accessed on 08 September, 2024. Artificial Intelligence 295 (June):103458. https://doi.org/10.1016.*

[16] *Mallory Schlossberg. 2014. "One Of The Best-Moments On 'Colbert Report' Was When He Coined 'Truthiness' In 2005 | Business Insider India." December 19, 2014. Accessed on 11 September, 2024. https://www.businessinsider.in/one-of-the-best-moments-on-colbert-report-was-when-he-coined-truthiness-in-2005/articleshow/45568420.cms.*

[17] *Rhodes, Samuel. 2022. "Filter Bubbles, Echo Chambers, & Fake-News: How Social-Media Conditions Individuals to Be Less Critical of Political-Misinformation." Political Communication 39 (1): 1–22. Accessed on 19 September, 2024. https://doi.org/10.1080/10584609.2021.1910887.*

[18] *Lewandowsky, Stephan. 2019. "The Post Truth World, Misinformation, & Information Literacy: A Perspective From Cognitive-Science." Informed Societies, February, 69–88. Accessed on 06 September, 2024. https://doi.org/10.29085/9781783303922.006.*

[19] *Madalin Necsutu. 2023. "Moldova Dismisses Deep fake Video Targeting President-Sandu | Balkan Insight." December 29, 2023. Accessed on 12 September, 2024. www.balkaninsight.com/2023/12/29/moldova-dismisses-deepfake-video-targeting-president-sandu/.*

[20] *ET Online. 2024. "STOIC-Hits-India with 'Zero Zeno': Israeli Firm Tries to Disrupt Lok-Sabha Elections; Pushed Anti-BJP, pro-Congress Content - The Economic Times." June 1, 2024. Accessed on 06 September, 2024. https://economictimes.indiatimes.com/news/elections/lok-sabha/india/stoic-hits-india-with-zero-zeno-israeli-firm-tries-to-disrupt-lok-sabha-elections-pushed-anti-bjp-pro-congress-content/articleshow/110611373.cms?from=mdr.*

[21] *Kalev Leetaru. 2019. "The Real Danger Today Is Shallow Fakes And Selective Editing Not Deep Fakes." August 26, 2019. https://www.forbes.com/sites/kalevleetaru/2019/08/26/the-real-danger-today-is-shallow-fakes-and-selective-editing-not-deep-fakes/.*

[22] *Jeronimo Gonzalez. 2023. "AI Avatars Are Being Used to Spread Pro-Venezuela Propaganda |Semafor." February 21, 2023. https://www.semafor.com/article/02/21/2023/venezuela-uses-ai-avatars-to-disseminate-propaganda.*

[23] *Casey Tolan, Donie O'Sullivan, and Jeff Winter. 2024. "How a Biden AI Robocall in New Hampshire Allegedly Links Back to a Texas Strip Mall | CNN Politics." February 8, 2024. https://edition.cnn.com/2024/02/07/politics/biden-robocall-texas-strip-mall-invs/index.html.*

[24] *Bath, P. 2021. "China's Military Space Strategy | Vivekananda International Foundation." VIF. Accessed on 10 September, 2024. https://www.vifindia.org/article/2021/june/15/china-s-military-space-strategy*

[25] *Hunter, Lance , Craig Albert, Josh Rutland, Kristen Topping, and Christopher Hennigan.. 2024. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." Defense & Security Analysis 40 (2): 235–69. Accessed on 09 September, 2024. https://doi.org/10.1080/14751798.2024.2321736.*

[26] *Nathan Beauchamp, Mustafaga, and Bill Marcellino. 2023. "The U.S. Is not Ready for AI Fuelled Disinformation-But China Is TIME." October 5, 2023. Accessed on 06 September, 2024. https://time.com/6320638/ai-disinformation-china/.*

[27] *"China Tests US-Fault-Lines and Ramps AI Content to Boost Its Geopolitical Interests - Microsoft On the Issues." n.d. Accessed September 18, 2024. https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/.*

[28] *Ibid*

[29] *Ibid*

[30] *"The United States Isn't Ready for the New Age of AI Fuelled Disinformation | RAND." 2023. August 5, 2023. Accessed on 02 September, 2024. www.rand.org/pubs/commentary/2023/10/*

the-united-states-isnt-ready-for-the-new-age-of-ai.html.

[31] *Koh Ewe. 2024. "Microsoft China Uses AI to Sow Disinformation & Discord Around-the-World TIME." April 5, 2024. Accessed on 06 September, 2024. https://time.com/6963787/china-influence-operations-artificial-intelligence-cyber-threats-microsoft/.*

[32] *Rosa Lazarotto, Barbara, and Barbara-da-Rosa. 2023. "The Grass Isn't Always Greener on the Other Side: The Use of Digital-Astroturfing to Spread Disinformation and the Erosion of the Rule of Law." LSU Law Journal for Social Justice & Policy 3:9.*

[33] *Zhao Chenchen. 2022. "China Tightens Multi-Channel Networks Regulations - CGTN." March 18, 2022. www.news.cgtn.com / news/ 2022-03-18/ China-tightens-multi-channel-network-regulations-18tS8nOaUpy/index.html.*

[34] *"EU AI-Act-2024 Regulations & Handling of Deepfakes - BioID." n.d. Accessed September 19, 2024. www.bioid.com/2024/06/03/eu-ai-act-deepfake-regulations/.*

[35] *Wil Corvey. n.d. "Semantic Forensics." Accessed September 19, 2024. www.darpa.mil/program/semantic-forensics.*

[36] *Gec. n.d. "How the PRC Seeks to Reshape the Global Information Environment." Accessed September 19, 2024. www.state.gov/how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment.*

[37] *Hunter, Lance , Craig Albert, Josh Rutland, Kristen Topping, and Christopher Hennigan.. 2024. "Artificial Intelligence and Information Warfare in Major Power States: How the US, China, and Russia Are Using Artificial Intelligence in Their Information Warfare and Influence Operations." Defense & Security Analysis 40 (2): 235–69. Accessed September 18, 2024. https://doi.org/10.1080/14751798.2024.2321736.*

[38] *Ibid*

[39] *ibid*

[40] *Jansen, Sue C., Brian M., and Barbra Streisand. 2015. "The Streisand Effect and Censorship Backfire." International Journal of Communication 9:656–71. Accessed on 16 September, 2024. http://ijoc.org.*

[41] *Pilditch, Toby D., Jon R., Jens Madsen, and Sander Van Der Linden. 2022. "Psychological Inoculation Can Reduce Susceptibility to Misinformation in Large Rational Agent Networks." Royal Society Open Science 9 (8). Accessed on 17 September, 2024. https://doi.org/10.1098/RSOS.211953.*

119-134

ARTIFICIAL INTELLIGENCE DISRUPTION IN INFORMATION WARFARE AND INFLUENCE OPERATIONS

Gp Capt R K Dogra

"There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know, we don't know. But there are also unknown unknowns. There are things we don't know, we don't know."

- Donald Rumsfeld

Abstract

In this new age of hybrid warfare, nations have resorted to the use of Information Warfare (IW) as an unconventional method to impose their National Will on an adversary with high anonymity and without violating international laws on sovereignty. Information security as part of the National Security Strategy is an important step towards waging the war in info space, the fifth dimension of Warfare. Information warfare has lately transformed into Information Warfare and Influence Operations (IWIO) in the comprehensive international security scenario. IWIO is witnessing rapid changes due to the emergence of disruptive technologies, especially the ones affecting cyber and digital spaces. Artificial Intelligence (AI) is one such disruptive technology that has used incursions in the internet to become a permanent fixture in the daily lives of all humans. AI not only augments the offensive capabilities of non-state, malicious actors in the digital space but also weakens

the defensive networks of our society against information manipulation. This realisation is increasingly pushing international institutions and their member states to question the harmful effects of AI, particularly in the present geopolitics, marked by a resurgence of information warfare. AI thus has a huge capability to influence IWIO. This paper will study how AI is disrupting the IWIO domain, how large state actors like the US, Russia, and China are using AI for IWIO and how India should respond to the use of AI in IWIO.

INTRODUCTION

IWIO are essentially intended to position your message across or to prevent your adversary from doing so in your domain. IWIO is not just about developing a coherent and convincing storyline but also involves a multitude of Psy Ops like confusing, distracting, dividing and demoralising the adversary. Influence can be mostly exerted using information.[1] However, technologies in the cyber world have enabled nations and non-state actors to influence specific audiences in more intrusive ways that may steal, destroy, inject, compromise or change information by having hidden access to information systems and networks. AI is one such technology that has the potential to incapacitate an adversary's information grid by intruding into its physical and cognitive worlds.

Many government officials, military leaders, and researchers acknowledge the evolution of information war into IWIO.[2] It has become a double-edged sword, equally important for the powerful states as well as technically poor states, non-state actors, and individual experts in software. The importance of IWIO to international security can be judged by the fact that it can shape global and domestic narratives that affect stability within states, international alliances, and the survivability of governments and leaders. As per the military and security pundits, 'Information superiority could be the single most decisive factor in present and future warfare'. IWIO is evolving at a rapid pace due to transformations in the technologies that have occurred in recent years that influence the IWIO domain. AI developments have a significant impact on IWIO because they not only enhance the speed and effectiveness

of IWIO operations but also shape the specific IWIO tactics that can be employed.[3]

This astounding growth of AI is well acknowledged by the world with the public release of ChatGPT and is further supported by facts indicating how AI is increasingly becoming an integral part of government and public sector infrastructure. Along with the rapid digitalisation of government organisations and private businesses, the expansion of AI is seen in all spheres of life, enhancing opportunities and productivity for individuals and businesses all around the globe. AI represents an exciting new domain in technology with the potential to revolutionise access to data, information and interactions with the world. However, this increasing exposure to AI has also brought more risks of exploitation and manipulation. AI has functional weaknesses and, due to its novel nature, highlights the urgency of addressing its exploitation within an established and legalised framework. This paper will present IWIO in the broader context of information warfare. The second part of the paper gives a comprehensive analysis of the marriage of AI and information and researches the significant risks this relation poses to any country's security and sovereignty. The third part of the paper presents how countries like the US, China and Russia are using AI in the IWIO domain. The fourth segment of the paper deals with suggested countermeasures that may help detect or reduce the role of AI in IWIO. In the final segment, AI and IWIO will be discussed in the security context of India.

CONCEPT OF INFORMATION WARFARE

By definition[4], the core weapon and target in IW is 'information'. It is the product that has to be manipulated to the advantage of those trying to influence events. The means of achieving this influence are multiple. Sympathisers of IW can attempt to directly change the data or to deprive adversaries of access to it. The methodology used in data or information collection, storage, and dissemination can be compromised. Using more subtle techniques, the way the data is interpreted can be changed by altering the context in which it is viewed. Thus, the range of activities in the context of information warfare is

unlimited. However, the first thing to be established is the nature of information itself.

INFORMATION AND IWIO

IW is a complex phenomenon, and a plethora of definitions exist for this term. Academicians and researchers have explained IW as 'the deliberate manipulation or use of information by one party on an adversary to influence the choices and decisions the adversary makes for military or strategic gain'. Whilst detailed, this definition signifies the fundamental elements of IW, namely the intentional and targeted aim to influence an adversary's decision-making process through information. With the ever-expanding impact of technology on wars and the extent of usage of information as an element of war, information warfare has stepped up as information operations, and these operations can fall within the realms of psychological operations, operations security, military deception, and electronic warfare. The meaning of IWIO can be well explained by Lin's definition, which is the "deliberate use of information (whether true or false) by one party on an adversary to confuse, mislead, and ultimately to influence the choices and decisions that the adversary makes".[5]

ALL WATCHED OVER BY MACHINES OF LOVING GRACE

By Richard Brautigan 1967

I like to think
(and the sooner the better!)

of a cybernetic meadow where mammals and computers live together in mutually programming harmony like pure water touching clear sky.

I like to think
(right now, please!)

of a cybernetic forest
filled with pines and electronics where deer stroll peacefully past computers as if they were flowers with spinning blossoms.

I like to think (it has to be!)
of a cybernetic ecology where we are free of our labors and joined back to nature, returned to our mammal brothers and sisters, and all watched over

by machines of loving grace.

ROLE OF AI IN INFORMATION WARFARE

As we transcend into the era of digitalisation, we encounter a definite shift in the way we manage the complex systems that govern our administrations, enterprises, and personal lives. Undoubtedly, AI has become a crucial element in this evolution. Global access to the internet was at first driven by an independent vision;[6] there are now serious and multiple concerns regarding the increasing incursion of AI into our world. It is now established that this technology is becoming a permanent fixture in our daily lives, as indicated by the availability of freely accessible tools such as image generators and conversational agents like chatbots. It is shocking to witness the rapid growth of AI Large Language Models (LLMs), such as OpenAI's ChatGPT, Meta's Llama and Google's Bard. Trained on an enormous collection of open-source data collected from the internet and containing many billions of parameters, the capability of LLMs to generate coherent, well-structured, and persuasive sentences resembling human writing has alarmed experts. Consider the term cognitive fluency bias, an extensive subject in academic AI research in recent times. Cognitive fluency[7] bias - when people mistakenly equate polished presentation for authenticity - can mislead. This bias is deeply rooted, often influencing one's perceptions and decisions without their conscious knowledge. Cognitive fluency bias is especially prone to 'truthiness', truthiness is 'how smart, sophisticated people use unrelated information to decide whether something is true or not'. Truthiness illustrates how high-quality presentation whether through well-crafted text or compelling visuals can make statements appear more truthful. In Newman's words, 'when things feel easy to process, they feel trustworthy'.

Malevolent minds can exploit AI-generated content to take advantage of cognitive fluency bias and truthiness, thereby highly influencing people's intuitive thinking. These 'gut feelings'-the cognitive mechanisms for rapid and mostly accurate decision-making are rooted in the brain's evolved heuristics for judgments. This logical presentation style of AI-generated content projects a feeling of intelligence and aligns with the heuristic to accept certain statements at face value without extensive scrutiny to

differentiate factual data from fiction. This use of AI for disseminating false information that bypasses mindful scrutiny is worrisome, more so because AI language models can be used to prepare fictional or fake messages intentionally targeting large segments of the population. These AI-generated, repetitive messages cause it to appear more reliable, a phenomenon called the 'illusory-truth effect'.

This realisation of illusory truth or fabricated realism is prompting international institutions and their member states to caution the countries against the harmful effects of AI[8], especially in a geopolitical context marked by the increased use of information warfare. AI gives an edge to the offensive capabilities of states and malicious private actors engaged in cyber and information warfare. Armed with tools and technology to generate false information, AI can contribute hugely to the intensification of information fog. While safeguards exist to restrict these tools from accessing requests that are considered to be unsafe and malicious, there are loopholes in their moderation. It is possible to 'jailbreak' ChatGPT, which means bypassing the restrictions and safeguards imposed by OpenAI. Indeed, the AI tools being developed and deployed by these malign actors hold adequate potential to offer narratives tailored to match specific cultural and linguistic contexts, targeting diverse sociological and ethnic groups to ensure better responses. With the help of AI, thus, it becomes possible to produce low-cost, high-quality propaganda narratives, doing away with the need to hire humans who are domain experts.

The ability of ChatGPT to code in different programming languages helps in the creation of online sites and networks of automated accounts (botnets), which in turn can be directed to intensify the formulated narratives, a phenomenon known as astroturfing. This practice is likely to attract malicious activities from state and private actors in two different ways. It can significantly increase the creation of botnets, which will be active on social networks, more importantly when social platforms such as Metaverse and Twitter are doing massive layoffs of those who were engaged in moderation tasks. Secondly, cybercriminal operations, such as phishing, will increase, enabled by ChatGPT, which may help in the

rapid generation of fake emails with a convincing level of realism capable of bypassing traditional anti-spam filters.

EMPLOYMENT OF AI IN IWIO BY THE US, CHINA AND RUSSIA

THE US

In the preceding paragraphs, we have seen how AI can enhance IWIO by increasing the pace of IWIO operations and how it can be applied to a wide range of IWIO applications. Three major powers of the world, the US, China, and Russia[9] are applying AI in their IWIO strategies and tactics in unique and actively impactful ways.

The United States, though late in waking up to the advantages of AI in the IWIO domain, is applying AI in its overall defensive IWIO strategy through numerous techniques. The US is utilising AI in many governmental and military areas in identifying and countering IWIO threats spread online and over social media. The US is deploying specific AI applications to identify particular texts, themes, images, and videos that are part of foreign governments' and non-state actors' IWIO operations. The objective is to contain threats that have plans to spread misinformation and propaganda, intensify polarisation and division within the population, and may cause discontent with the elected government.

US plans to use AI to scan through large amounts of data to identify misinformation, propaganda, and intentionally divisive content that is intended to sow discord among domestic and friendly overseas groups. Emphasis is also being placed on using AI technology to counter AI-driven deepfake technology that could be misused by adversaries for IWIO operations directed at the US and organisations like NATO. Additionally, AI is being used to protect critical infrastructure from cyber-attacks. Machine Learning programmes are being deployed to sift through large amounts of data for any indication of possible attacks and thereafter generate AI programmes to defend against Cyber-attacks.

CHINA

China incorporates Mao's notion of the People's War, which consists of employing overwhelming Cyber-attacks combined with online disinformation. IWIO has to be the central component of China's military strategy, given that China secretly acknowledges that it cannot match US military spending. There are confirmed reports that China has employed IW simulation training for over a decade, and IW units specialised in psychological warfare are embedded within its security structure. Furthermore, it is important to note that operations in Cyber-space are an important component of China's IW strategy. An interconnected network of Chinese online influencers who reinforce Chinese narratives in IWIO-targeted countries is an example of this cyber force.

China plans to utilise emerging new technologies like AI in a wide variety of sectors and regions, including 'disruption through trade wars, information manipulation in cyberspace, and military integration of disruptive technologies'. To achieve its goals, China created the Strategic Support Force (SSF) in 2015. China is reportedly using AI under its cognitive warfare tactics to attempt to manipulate public opinion in Taiwan regarding its plans for reunification. This is being done in part through AI-powered programmes and bots that target Taiwanese citizens through the spread of misinformation and propaganda on social media. China has also mounted significant international IWIO operations ranging from AI bots generating misleading content on social media to altered videos depicting the treatment of Uyghurs in China.

RUSSIA

Russia is currently lagging behind the United States and China in terms of incorporating AI technology into its digital security infrastructure. The recent Russia-Ukraine war, however, has forced Russian think tanks to aggressively use AI as war tactics. Russia has demonstrated a concerted effort to further develop its already advanced IWIO tactics with the help of AI technologies.[10] Russia's internet-sponsored propaganda manufacturing facilities are now equipped with AI-powered deepfake

technology that can create more realistic false narratives by constructing fake images and even video clips.

Russia exploits information ecosystems by interjecting dis/misinformation (partially attained through cyber-attacks) and fake news stories that a majority of those exposed to, believed true at the time. Russia's perspective of IWIO covers a wide space of technology, where jamming electronic communication and limiting access to the electromagnetic spectrum, cyber-espionage, and Distributed Denial of Services (DDoS) attacks are no different from (and work in tandem with) using trolls and bots to spread dis/misinformation, establishing pro-Russian media outlets, or supporting local sympathisers to propagate favourable messages.

COUNTERMEASURES FOR MITIGATING AI RISKS IN IWIO

Monitoring the Information Environment

Recognising the severity of the threat of AI in the IWIO domain calls for enhancing capabilities to monitor, analyse, characterise, evaluate, predict, and visualise the information environment. This guidance aligns with the Observe and Orient stages of the Observe-Orient-Decide-Act (OODA)[11] loop. The observation here represents the important first step in the early detection of degradation attempts and issuing of warnings about potential disinformation campaigns. Orientation involves understanding the complex interplay between cognitive biases and the information produced by AI language models. Observation and orientation together lay the foundation for informed decision-making and planning effective action against suspected malign players.

One such example of information-sharing initiatives is the European External Action Service's Rapid Alert System (launched in 2019), which highlights the importance of international collaboration in addressing disinformation threats. Host of pacts between participating countries of various organisations like QUAD, BRICS, AUKUS, etc, can formulate guidelines and policies to monitor and share activities related to IWIO attempts from non-state actors.

Issuance of Advanced Warnings

The important task of issuing timely warnings constitutes an important countermeasure against malign information operations. It is observed that preemptive warnings about possible disinformation attacks significantly reduce the risk of people getting influenced by these attacks. The warnings alert audiences about potential attempts to misinform them, which in turn leads to critical evaluation of the information being encountered. When there is a preemptive warning, the cognitive bias of perceived truthfulness is attenuated to scepticism, forcing the audience to think more.

In the process of issuing effective warnings, attention should be given to not only exposing false narratives but also endorsing true ones. There is a need to continuously adapt to the rapidly evolving information environment. This is possible if there is the ability to promptly detect and respond to emerging disinformation campaigns. Leveraging AI and machine learning technologies can assist these efforts by monitoring the information environment, identifying threats, and swiftly issuing relevant warnings.

Partner Information Operations

In the face of pervasive AI-driven threats, developing partnerships, planning and conducting collaborative operations have become more crucial. By sharing partner nations' capabilities, countries can significantly strengthen their capability against disinformation and subversion attempts. This partnered approach recognises the complex and dynamic nature of the information environment. A core objective should be to enhance partner nations' ability to execute successful information operations independently. Equipping these forces with the knowledge, strategies and tools to operate effectively within the information environment will not only counteract disinformation but will also raise global awareness about the nuances of IWIO.

The Concept of Cyber Teammate

The cyber teammate[12] is a concept application of AI technology for cyber defence and countering information attacks. It is software-based, and it provides a unique and otherwise lacking sense of the environment to the cyber warriors. With the availability of ML algorithms, excellent computing speeds and availability of data, the cyber teammate will build its logic of cyberspace and will support the cyber teams by giving them a clear perspective and understanding of the conflict. A cyber teammate will essentially collect data across open sources, translate and synthesise it in short paragraphs, provide a status update and isolate the tactical and technical information relevant for combat. It would also have the capability to identify the effect of data (information) on/of cultural influence through social media by automating part of the translation process and simulating more credible inputs by process of exploration to conclude better on the impact of inflammatory posts. The cyber teammate will be deployed passively; as and when it assesses mischievous massive amounts of open written text, it will be able to detect changes in tone or style and link together differences in the text to further generate a warning or caution.

FORMING LEGAL REGULATIONS

REAIM Summit

Advances in AI and consequent misuse have sparked increasing calls for setting up regulatory oversight. Raising the slogan 'Responsible AI for Safer Tomorrow', 80 countries across the world participated in the first REAIM[13] summit in the year 2023, and 61 endorsed the non-binding agreement, including major nations like the US, UK, China, Japan, Australia etc. The first meeting of the REAIM took place in Hague in 2023. Following the summit, the US launched its 'Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy'. The UN has also called for initiating a legally binding treaty by 2026 to ban the use of Lethal Autonomous Weapon Systems (LAWS).

EU AI Act

Another notable example of these emerging regulations for AI is the proposed EU AI Act[14], a landmark legislative effort poised to shape the future of AI governance in Europe. The Act's risk-based framework segregates AI systems into four categories: prohibited, high-risk, limited-risk, and minimal-risk. Each category is subject to varying degrees of regulatory scrutiny and compliance requirements. This structured approach reflects a conscientious effort to harmonise AI advancement with public safety and ethical standards.

US Blueprint for an AI Bill of Rights

White House has also come up with 'Blueprint for an AI Bill of Rights', which talks about five principles that should guide the design, use, and deployment of automated systems to protect the American public in the age of artificial intelligence. The 'Blueprint for an AI Bill of Rights'[15] is a guide for a society that protects all people from these threats—and uses technologies in ways that reinforce the US public's highest values. From principles to practice, the bill is a handbook for anyone seeking to incorporate these protections into policy and practice, including detailed steps toward actualising these principles in the technological design process. These principles help provide guidance whenever automated systems can meaningfully impact the public's rights, opportunities, or access to critical needs.

Likewise, NITI Aayog in India has also issued regular directions for responsible use of AI by companies in India. Research is also going on to explore the use of AI in countering AI-generated misinformation or data.[16] Some of these concepts are AI Firewalls, Guardrails, Watermarking and content detection.

VULNERABILITY OF INDIA TO AI AND IWIO

India is undoubtedly one of the fastest-growing markets for social media users. However, due to a lack of awareness, laws and mechanisms to check the spread of rumours, fake news and manipulated videos, it is

easy to manipulate the Indian population. Pakistani state-run agencies are increasingly using cyberspace for the collection of sensitive information and the spreading of misinformation. At the same time, Chinese intrusion into the lifestyle of Indians is unprecedented. From malicious hardware infused cheap mobiles to data-gathering apps of Chinese origin, the Indian public has at present no safeguard against the Chinese hidden information war. India is the biggest user of smartphones in the world. These mere statistics make Indian citizens prone to misuse of AI by state and non-state actors. With smartphones aggressively advertising the use of AI, the danger is even further growing. To add to the woes is the monopoly of apps and social media giants who are sending sensitive data and even selling it for their gains. Indian citizens, its soldiers and their families are at the greatest risk of this misuse of AI by Chinese and Pakistani agents.

RECOMMENDATIONS FOR INDIAN SECURITY LANDSCAPE

Through programmes such as Satyamav Jayate, Pradhan Mantri Gramin Digital Saksharta Abhiyan, and National Digital Literacy Mission, India has taken preventive measures to counter disinformation and increase digital literacy.[17] One of the best examples of this was during the COVID-19 pandemic, wherein the government established a WhatsApp chatbot and a fact-checking unit under the Press Information Bureau. However, the government needs to revamp the information and broadcasting network to reach the last man in explaining the good and bad of AI. This can be done through schools, panchayats and social media advertisements.

On the IW front, the Indian Army created the position of Director General Information Warfare two years ago to monitor propaganda from China and Pakistan. These initiatives, however, are primarily serving as fact-checks and not addressing the larger objective of dominating the 'war of narratives'. Technologically superior and coherent efforts are required to win this propaganda warfare. IW sections set up at the unit level must educate troops regularly on identifying and scrutinising malicious AI-enabled information warfare.

Countering the anti-India narratives can be effective only in the short term. The Government of India will need to adopt a coordinated and Whole of Nation approach involving all ministries in need of the hour to combat the IWIO that targets the Indian minds, especially the youth, to generate communal discord and discontent against the government.

The Ministry of Defence must invest aggressively in technologies that can identify and counter the AI in IWIO intended for its forces. In this regard, it must convince the Government of India to force social media giants like Metaverse and Twitter to set fact-checking and filter AI-polluted information aimed towards India. Lastly, Government of India must formulate tough laws for foreign firms found involved in fabricating disinformation, deep-fakes and exploiting online social space to incite people to destabilise the chosen government or influence leadership. As covered earlier, India should become part of larger world forces making efforts to counter the malicious use of AI.

CONCLUSION

The rapid advancement of AI, its intrusion and its expanding role in modern societies are unstoppable and undeniable. The article was a detailed exploration of AI's complex nature, revealing the risks it pose in the realm of information warfare. This risk is actually real and not hypothetical; it presents a tangible threat in our current digital world, where AI technologies such as Bing Chat and ChatGPT are all the time more intertwined with the internet and easily accessible gigantic pools of open data.

The accessible nature of AI also means that current vulnerabilities in AI systems could be exploited by a wide group of malevolent forces, ranging from radical terrorist networks to antagonistic state actors. Such exploitation could potentially disrupt societal structures and skew public perception, a risk that is amplified considering AI's increasing integration across multiple sectors, including government and private enterprises. Regulatory frameworks like the EU AI Act represent positive steps towards safer management of AI. Yet, they still lack a holistic approach to

covering the full spectrum of risks associated with AI, especially against sophisticated adversarial AI tactics. The risk associated with the use of AI in IWIO necessitates a regulatory method that not only channels and controls AI development but also facilitates its harmonious integration and evolution in the face of external threats, while maintaining balance with our complex socio-technological landscapes and human right.

★★★

Gp Capt R K Dogra is serving Aeronautical Engineering officer of IAF. He specialises in aircraft technology, especially the MRO functions. He has served as Chief Engineering Officer of an important base in EAC. He is currently working with LRDE, DRDO and writes on technology and defence related subjects.

NOTES

1 *Pascal Brangetto, Matthijs A. Veenendaal: Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations, 2016 8th International Conference on Cyber Conflict Cyber Power.*

2 *Lance Y. Hunter, Craig D. Albert, Josh Rutland, Kristen Topping & Christopher Hennigan (05 Mar 2024): Artificial intelligence and information warfare in major power states: how the US, China, and Russia are using artificial intelligence in their information warfare and influence operations, Defense & Security Analysis, DOI: 10.1080/14751798.2024.2321736*

3 *Ibid*

4 *Hutchinson, W., and M. Warren. "Principles of Information Warfare." Journal of Information Warfare 1, no. 1 (2001): 1–6. https://www.jstor.org/stable/26485918.*

5 *Lance Y. Hunter (p-6)*

6 *Dusan Bozalka: Information warfare in the age of Artificial Intelligence*

7 *Russel Hanson, Adam R Grissom, Christopher A Mouton: The Future of Indo-Pacific Information Warfare- Challenges and Prospects for the rise of AI (RAND Corporation, 2024)*

8 *Ibid*

9 *Lance Y. Hunter (p-14)*

10 *Lance Y. Hunter (p-22)*

[11] *Russel Hanson (p-5)*

[12] *Guyonneau, Rudy, and Arnaud Le Dez. "Artificial Intelligence in Digital Warfare: Introducing the Concept of the Cyberteammate." The Cyber Defense Review 4, no. 2 (2019): 103–16. https://www.jstor.org/stable/26843895.*

[13] *Prasad, Ashika S . "AI in Warfare: The REAIM Summit and India's Approach – CENJOWS." Cenjows.in, October 15, 2024. https://cenjows.in/ai-in-warfare-the-reaim-summit-and-indias-approach/.*

[14] *Lax, Edwin. "AI Pollution: The Future Threats of Information Warfare." Trendsresearch.org, 2024. https://trendsresearch.org/insight/ai-pollution-the-future-threats-of-information-warfare/?srsltid=AfmBOooaFzjvhv17FTGqrYOqlgXsXusTJ29FJq5vbYysN2VySIfA31OY*

[15] *Whitehouse Website (www.whitehouse.gov), The Blueprint for an AI Bill of Rights*

[16] *Rahul Kapoor, Theresa T Kalathil: AI Regulation In India: Current State and Future Perspectives, Morgon Lewis (Jan 2024)*

[17] *Young Voices. "India's Two-Front Information War." orfonline.org, May 10, 2023. https://www.orfonline.org/expert-speak/indias-two-front-information-war.*

DEEPFAKE – MISINFORMATION, PROPAGANDA AND INFORMATION WARFARE

Wg Cdr Anand R Navaratna

Abstract

Since World War II, the ill effects and benefits of misinformation and propaganda in the face of war is well documented and, researched. By leveraging Artificial Intelligence (AI) and Military Intelligence (MI), deepfakes enable creation of hyper-realistic synthetic media, posing unique challenges to confidentiality, integrity and accessibility of military information systems. The paper explores historical examples of misinformation such as World War II, the Cold War and evaluates as to how deepfake has transformed psychological operations, deception strategies and non kinetic warfare. The paper highlights the plausible opportunity through military training, strong command structure, digital awareness and regulation of technology. The paper highlights the need to develop dual use capability viz., offensive and defensive. The challenges to adaptation of this technology is deliberated. With strong ecosystem, the military can effectively develop India specific solutions to achieve digital supremacy in joint information warfare.

INTRODUCTION

The migration from information to misinformation is historically docketed and well-researched. The reference to the use of misinformation to win a war is also an established truth from time immemorial. Misinformation spread is usually attributed to either winning through overselling the preferred narrative or psychologically rallying a popular narrative to gain popularity and fame. In the context of using propaganda for

winning a war, there cannot be a better narrative than the Second World War. If propaganda and misinformation are the ways to spread narrative, deepfakes have emerged as a popular means to undertake such propagation with the evolution of technology. This paper defines deepfake as a technology and considers a few examples as a case study. In the subsequent sections, we also analyse how deep fakes emerge as powerful 'misinformation tools'.

PROPAGANDA AND MISINFORMATION IN WORLD WAR II

The World War II provided an exemplary narrative of how print and radio were used to sell the popular narratives of the Governments of the day. A dedicated minister and a dedicated ministry of propaganda under the German Army altered the narrative of war. Further, these were used as tools to rally support for the Government, demoralise the enemy and tilt the favour in support of the German Army. If Germany used these to disseminate misinformation, the Allies used media to portray their great victories and undertake mass recruitment for their Armies. In the previous research lessons from World War II established that propaganda and misinformation can:

- **Mobilise Citizens.** Governments used radio, print, and movies to appeal emotionally and mobilise the citizens. Films like 'Why We Fight' of 1942 were used to imbibe a sense of patriotism and duty towards the nation.[1] Posters with 'I Want you' were also great for soldier recruitment (Fig 1). The Office of War Information controlled and crafted the news that did not undermine unity

Fig 1 : US Army Enlistment Poster. **Source:** USA National Achieve Catalog, https://catalog.archives.gov/id/513533

and righteousness. The main aim of this initiative was to bolster morale and encourage enlistment.[2]

- **Control of Information.** The governments held tight to unfavourable news about the war. They censored the information suitable for the Government and its war effort as it's depicted in Fig 2. The British Ministry of Information managed the press and even encouraged self-censorship amongst journalists.[3] The image of the country and soldiers' goodwill were weighed over

Fig 2 : 1945 German Propaganda Poster. **Source:** US Holocaust Memorial Museum, https://encyclopedia.ushmm.org/content/en/photo/1945-nazi-propaganda-poster

the facts and ethics on the ground. Under Joseph Goebbels, there was an effort to build the Nazi narrative surrounding Hitler, war glorification and victories of Germans.[4]

- **Enemy Bashing.** The press emerged as an effective platform to build a narrative. It was a channel to undertake enemy bashing. The barbaric acts of the enemy were graphically presented.

Further, the Nazis used media to depict Jews and other minorities as a threat to societal well-being resulting in widespread anti-semitic sentiments within the boundaries of their own country.[5]

THE COLD WAR ERA

Misinformation and propaganda contributed immensely to war efforts even after World War II, from the widespread coverage of the Nuremberg Trials to the emergence of the USSR as a potential threat to the American Dream, which received widespread coverage, building a narrative and helped to galvanise popular public sentiments. The Cuban Missile Crisis, the American Lunar mission, the USSR Sputnik mission, nuclear tests and the Warsaw-NATO narrative were a few of the instances that helped build upon the narrative aiding Information Warfare in the 'no war' scenario also. The evolution of media in terms of 'coloured print' and 'better printing technology' helped scale up the news. The population's access to news and interest in worldly affairs grew exponentially. The misinformation and propaganda surrounding the 'USA-USSR' cold war captured the imagination of a generation of citizens leading up to the disintegration of the USSR and the emergence of Russia.

POST COLD WAR ERA

The use of misinformation, propaganda and over selling of incidents did continue even after the Cold War era. The Gulf War was one such use case. A captured American solider was rescued and this incident was used to boost the morale through sensationalisation of news.[6] The color TV had emerged and it captured the imagination of people. The Kosovo War, Afghanistan invasion and search of NATO for weapons of mass destruction narrative was played in front of the world by a galaxy of news channels. The countries as per their local narrative tried to build up the event. Further with emergence of .com boom, the blogs and online news portals played their analysis, narrative and propaganda. With .com boom, the terrorists started using these sites for recruitment. ISIS and Syrian civil war saw widespread utility of these sources. In no time the Facebook and Twitter had emerged. These social sites were

used to decimate biased narrative using doctored images or videos to influence public opinion.[7] Also, Ukraine conflict saw increased use of digital platforms in spread of misinformation.[8]

In recent times, with technology, scale and reach, the missing parameter in the spread of misinformation and propaganda was 'authenticity and trust'. AI and its computing power today can establish these. Some cases exist where the computed or constructed images/ videos appear more genuine than the original content. Further, the ability to portray as an imposter has an exponential effect. Here, an imposter can digitally disguise himself or herself as a political figure, military leader or terrorist. Technology provides the ability to make the fake narrative as accurate as possible.

DEEPFAKE

Deepfake combines two words, 'deep', which is taken from a deep learning technique, and 'fake', which means non-real. It is an artificial intelligence capability built using machine learning algorithms to create synthetic media representing something or someone. The outcome can be just a voice or a video with voice. Technology has evolved so much that it becomes challenging for general citizens to discern real from fake. The misinformation created has a profound impact as it can alter public opinion, distort reality, and instil fear and unrest. Though the image, voice or video creation follows a complicated technology, the result is easy to distribute. The authenticity of deepfake aided by digital distribution like social media, WhatsApp or YouTube can escalate public sentiment in no time. The scale and time to reach a large sect of people is lightning fast. Thus, this technology can bolster misinformation and propaganda. It is an ideal weapon and catalyst in Information Warfare (IW).

DEEPFAKE TECHNOLOGY

Deepfake is built around the use of deep learning algorithms. The most popular one is Generative Adversarial Networks (GANs). The intent of this paper is not to dwell deep into the technology itself; it will be interesting to comprehend the sophistication of technology used in the

creation of synthetic data. GANs override the technology called 'neural networks'. These are called neural networks, as in function, the working is akin to human neurons. The GANs consist of two components: the generator and the discriminator. As the name suggests, the generator is responsible for generating final video audio or synthetic data.

On the other hand, discriminator extracts feature online of actual images of the person in question. This duo of generator-discriminators competes to provide better synthetic output while extracting features of authentic images or videos.[9] With time, the discriminator is trained to extract features surrounding the person of interest, while the generator is trained to generate quality data. As GANs are based on neural networks, the ability to continually learn and improve is this technology's most significant contribution and feature.

The training dataset constitutes a collection of images and videos of the target. The encoders –decoders are used to extract features through this large dataset. The encoder compresses the input data while the decoder reconstructs it. Thus, the knowledge these encoders-decoders gain can transfer facial features, expressions, and voices from one individual to another and from one context to another. Once the features are mature, the training of neural networks can be interoperable and used in different contexts or narration without much effort. Thus, this technology also improves adaptability. An individual with malicious intention can recreate the features suiting a new context using knowledge of trained data of different contexts.

FEATURES OF DEEPFAKE

In the context of IW, deep fakes bring the following features to the table:

- **Face Swapping.** In the simplest form, one's face can be superimposed onto someone else's body. The technology provides seamless integration into the body and provides facial movements and expressions, making it difficult for viewers to discern. The illusion makes viewers believe the act performed by an individual is genuine.

- **Voice Synthesis.** By training the speech of the target individual, modulation, tone, pitch, and cadence can be altered to suit the act. Thus, an individual's realistic audio or voice can be generated. The algorithms are so mature that voice can be generated for speech or text. These voice notes are widely circulated over social media to spread misinformation.
- **Text to Video.** There is ongoing work with significant progress around using text descriptions to create a video. This is possible by using natural language processing capabilities with visual generation tools. Thus, a new video can be generated quickly using textual input.

CHARACTERISTICS OF DEEPFAKE

A few of the notable characteristics of deep fake which are relevant in the context of information warfare are:

- **Credible.** The algorithm and creation of deepfake are computationally daunting but effective in quality. The synthetic image audio or video appears to be expected to the viewer. Thus, the target illusion is credible in quality.
- **Scale.** Deepfake illusion, once generated, can be circulated like a regular multimedia file or attachment for distribution. Though generation of deepfake is a professional task, there are no particular requirements to replay the file. Thus, scaling deepfakes for wider reach is easy.
- **Speed.** The generation of deepfake is aided by the quality and computational power of the computer. However, the speed at which it can spread misinformation is high. Also, this becomes a regulating challenge once a deepfake is in circulation.
- **Ubiquitous.** With increased front-end and easy-to-use software, anybody with access can create a realistic synthetic outcome. Thus, the technology is becoming increasingly ubiquitous. Also, the encoder-decoder learning can be adopted interoperable to

different context and scenario for creation of synthetic video/ image or voice.

USE CASE OF DEEPFAKE

In one of the famous applications of deepfake, US House Speaker Nancy Pelosi appeared to be slurring her words, undermining her credibility in 2019. This sparked discussion about the ethical use and regulation of deepfake to prevent misinformation and influence political discourse. In the entertainment industry, there have been instances of videos being created that featured celebrities in compromising situations. This has the potential to cause harm and emotional distress. As per a study, only 30% of respondents could accurately identify a deepfake video.[10] This advanced technology, aided by a lack of awareness, leads to the potential manipulation of public perceptions. The repercussions do not just stop here. As per a 2020 study, people exposed to deep fake videos, in general, are found to question the authenticity of all media, leading to generalised scepticism that could erode trust in legitimate news outlets.[11] Further, individuals exposed to emotionally charged deepfake content were more likely to alter their opinion on political issues.[12]

INFORMATION WARFARE APPLICATIONS OF DEEPFAKE

Technological development has a direct implication on the country's military. Arguably, misinformation and propaganda do not involve the military in general or soldiers in particular. However, the use of deepfake is not limited to the spread of misinformation and propaganda itself. The Confidentiality, Integrity and Accessiability (CIA) triad, called in the context of information security, can be potentially breached using deepfake. Once done, the sensitive information can be extracted for operational benefit and to train the deepfake models for more considerable military gains. The potential military applications of deepfake are:

- **Psychological Warfare.** Deepfake can be used to influence and affect the morale of the troops. The misinformation can be about troop deployment, pay and pensions, social fabric, family values, or political issues. These videos, images, or voice notes can be

circulated on social media or extensive messaging services, which are beyond the control of services to regulate. Also, this misleading information can be directed towards service personnel and their family members only, which can create greater panic and confusion. The well known and most recent example of this scenario was witnessed in Russia-Ukrainian war. In February 2022, a deepfake video of Ukraine President Volodymyr Zelensky was circulated, wherein it appeared that he is appealing to the Ukrainian forces to surrender to Russian military.[13] This led to mass condemnation of President within Ukraine. There were claims of Ukrainian forces also using deepfake videos of Russian President Vladimir Putin as a tool for pys-ops. The intercept reported a leaked document from Pentagon, showed that Department of Defense, USA has conducted advanced tests on offensive use of deepfakes and issued tenders for its use as part of psychological warfare in aid to special operations.[14]

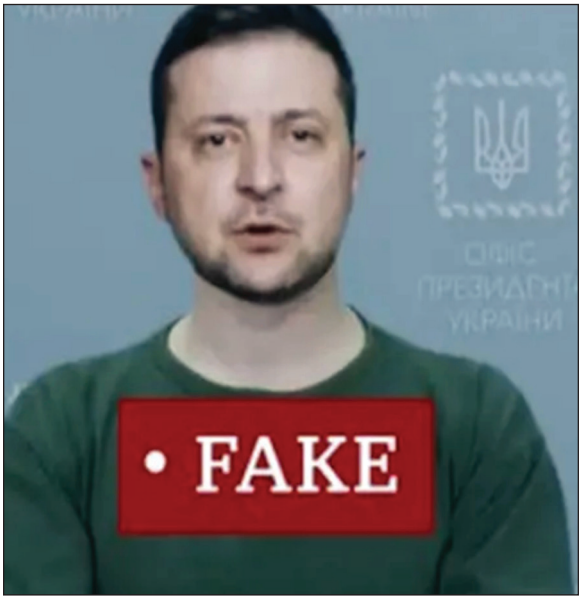


Fig 3 : Deepfake video of Ukrainian President. **Source:** https://theintercept.com/2023/03/06/pentagon-socom-deepfake-propaganda/

- **Deception Operations.** The enemy can spread misinformation on aspects surrounding the professional competence of the corps and regiment. Aspects like 'territory captured', 'low serviceability', 'standard of soldiers and equipment' and 'pay and allowances' are a few deceptive messages that the enemy can directly affect the morale and reputation of the military. Also, family members can be targeted using suitable old methods of honey trapping, financial fraud and death news combined with deepfake narratives surrounding the life of military personnel in the family. Effective use of deepfake voice notes allows the military leadership's voice and commands to be replicated. Further, in operational communication, ATC commands can be replicated using deepfake technology to jam the medium of communication, thereby causing deception and confusion. In 2024, Russian media circulated deep fake videos in which a military general dealing with intelligence was shown to be admitting to Ukraine, being the one behind the Islamic terror attack in Moscow. This led to uproar in both Russia and within Ukraine. The BBC Verify reportedly undertook a detailed analysis of the video using advanced forensic technology and established

Fig 4 : Deepfake interview of Ukrainian Official. **Source:** Moscow attack: debunking the false claim, https://www.bbc.com/news/world-europe-68657383

that the video is edited using two Ukrainian TV broadcast which used to make a video.

Further, Northwestern University carried out a project, wherein a deceased terrorist (Mohammad al-Adnani) of Islamic State, was trained to say the same words as Syrian President Bashar al-Assad. The development involved two prong process, wherein the voice of trainer (Syrian President) was used to train a subject (Mohammad al-Adnani, who is dead) as part of their Terrorism Reduction with AI deepfakes (TREAD) initiative.[15] Another known case of short term and tactical deception was reported by Ukrainian Intelligence agency, wherein they reportedly intercepted a deepfake call between Prime Minister Denys Shmyhal and CEO of Turkish drone manufacturer Baykar having a conversation of cancelling drone supply orders.[16] This created considerable confusion in the minds of soldiers and drone manufacturers alike.

Fig 5 : Russian Special Services tried to use deepfake technology to contact the management of Baykar on behalf of the Prime Minister of Ukraine. A frame from the DI`s video. **Source**:https://mil.in.ua/en/news/ukrainian-intelligence-intercepted-the-russian-provocation-against-baykar-ceo-haluk-bayraktar/

- **Data Exploitation.** The data surrounding the life and operations of military personnel and their family can be recreated as audio, video and images. The data to train these models can be obtained from social media posts or other sources. These data, as per the requirement of the enemy, can be doctored to create confusion, deception, commit financial fraud or cause damage to the reputation of an individual. Doctored videos of honey trapping, disclosing service information and acts violating service norms can harm an individual's life and career. The service reputation is also affected. Thus, the existing service norms surrounding data of military personnel are at most premium and must be guarded. Simple off the shelf AI image-voice generation tools are used to spread misinformation and rake-up sentiments. A simple search of Gaza war provides AI generated images posted by individuals which are sensitive in nature.

Fig 6 : AI generated images of Gaza War. **Source:** https://petapixel.com/2023/11/07/adobe-stock-is-selling-ai-generated-images-of-the-israel-hamas-conflict/

There are projects reportedly undertaken to train deepfake modes based on the enemy commander's voice intercepts. These models are then trained to use synthetic voice as per mission tactical requirements. With gigabytes of data, creation of deepfake voice, video or image is not challenging. Political figures, military leaders, media influencers

and business houses are vulnerable. The digital foot print available is utilised for training the models on high end hardware of military grade.[17] Deliberate attempts to manipulate the training data of artificial intelligence and Machine Learning (ML) models to corrupt their behavior and elicit skewed, biased or harmful outputs cannot be ruled out. This approach is termed as 'data poisoning'.

- **No War No Peace (NWNP) Applications.** The capability of deepfake models can be interchangeably used. The models can be further trained with new data to make them mature. Deepfake can be used as an offensive and defensive application on the enemies during NWNP. During peace times, data extraction, model training, improvement in model accuracy, and individual target profiling can be undertaken. During war or hostile situations, a deepfake narrative can be used to carry out an offensive against enemy military personnel for operational benefit. Academic study have shown the ability of AI and deepfake to alter geo data. In military applications, by use of altered geo map, image or coordinates, a sense of deception and confusion can be imbibed leading to collateral damage. Live data related to transportation, logistic movement, ship movement or target information can be intercepted and manipulated to produce artificial or synthetic maps. Drone warfare is expected to bear the brunt of the technology. This technology is termed as 'deepfake geography'.[18]

- **Non-Kinetic, Non-Contact Warfare (NKNC).** This grey zone of application can be effectively used as per requirement. Deepfake, along with cyber warfare, can be used to affect enemy morale, spread confusion and induce chaos without the use of kinetic energy or without any kind of physical contact. Deepfakes, as per operational requirements, can be used to gain tactical advantage. However, the ethical usage of deepfake needs deliberation and policy backing. A case of use of deepfake image used by Russia to demonstrate, deployment of troop by USA against it was circulated to heighten tension between nations. These approaches are apt example of NKNC warfare.

- **Simulation and Training.** As the deepfakes are designed based on data and patterns, this technology can effectively train our troops and conduct simulated drills surrounding the operational, social and financial facets of our troops. This will help develop awareness and build confidence. USA, reportedly uses a Ghost Machine hardware for effective cloning of voice, video and images. These are then used on a high-end hardware to produce deepfake outcomes to train the special forces on scenarios of deception and deepfake. This provides the soldiers an edge to understand aspect of both offensive and defensive use of deepfake. Projects like Terrorism Reduction with AI Deepfakes (TREAD), are effective environment simulators to provide troops exposure and also train cyber troops for offensive operations.

REGULATION AND FRAMEWORK

Due to the breadth and potential harm to society, there has been an increase in demand for regulation of deepfake technology. Some have called for self-regulation, while most countries want to invoke dedicated regulation with a focus on deepfake. Some of the countries in which a thought process towards this has begun are:

- **United States of America.** Since the speaker of the house incident, the call for regulation and accountability of deepfake has increased. The proposed act is expected to reveal when deepfakes are used, especially in political advertising and spreading misinformation.[19] The state of California has laws against harm, defraud or deception in the context of revenge porn and election-related materials.

- **European Union.** The Digital Services Act is a larger umbrella that mandates misinformation and increases transparency in the context of the digital use of data. Also, the Union is mulling over a proposal to bring in an Artificial Intelligence Act to curb and regulate AI and its applications.[20]

- **United Kingdom.** The UK proposes a law to regulate all aspects

surrounding misinformation, privacy infringement and safety through the Online Safety Bill.[21]

- **India.** A few instances of deepfake have enabled the Government of India to consider a dedicated bill along with the Information Technology Act 2000, the Personal Data Protection Bill and Bharatiya Nyaya Samhita. The Government has set up a study committee to look into the impact of AI and emerging technology, including deepfake, and make suitable recommendations.

In the context of military applications, the challenge in regulation increases. The ability to use this technology both for offensive and defensive means needs ethical and legal backing. However, this aspect needs legal scrutiny and multi-country cooperation. The ability to have multilateral legal cooperation is the need of the hour. The application developer, user, and final distributor can be housed in different countries. Thus, culpability can be cross-border. Thus, the situation is challenging.

CHALLENGES TO DEEPFAKE ADAPTATION

- **Technology is Evolving.** Better algorithms, higher computational powers and better training data make the adaptation of this technology difficult. Micromanagement and standardised adoption cannot be easy. Determination of right algorithms and right dataset for training is a continuous and ongoing task.

- **Organisation Structure.** Deepfake forms part of NKNC scenario. This calls for all three services to bring change in doctrine. Placing this vertical under existing structure may pose a challenge. Also, as its non-contact and non-kinetic, there is no need to take physical arms, ammunition or delivery vehicle any way close to physical border; at same time NKNC may lead to sudden escalation and full-fledged conflict. Centralisation of decision and decentralisation of action may not be a full proof solution. Thus, command and control of this niche area will be challenging. Placing this aspect under a tri-services command can be studied. Incorporating, this along with EW, IW and Cyber

may be a natural choice in ethos; however, in spirit deepfake being characterised by deception - confusion - misinformation - propaganda, can be part of counter intelligence organisation too. Deepfake requires adaptation of sophisticated technology. The dual nature of deepfake application viz., offensive and defensive makes the choice at organisational level more complex, as our services have demarcated offensive and defensive elements at organisational command and control level. Thus, the choice for command and control is neither easy nor natural.

- **Skilled Deepfake Experts.** Military leadership around the world have acknowledged the need to face cyber threats and space threats. The skilled manpower required for offensive and defensive use of deepfake needs skilled human resource. Thus, nurturing a cadre within the existing cyber-space force or formation of dedicated unit needs deliberations. AI and ML at fundamental level are curated and ecosystem is built at national level. Defence forces who are focusing on AI/ ML applications in defence can consider development of strong workforce who is trained on deepfake creation and deployment. The essential aspect is to not only build AI/ ML experts but challenge is to have AI/ ML experts with operational orientation. This brings in the aspect of capability building in our training institutes. High end hardware, dataset specific to our offensive/ defensive use case and profiling of our adversary becomes key enablers.

- **Regulation v/s Development.** It is well-established research that over-regulation leads to a lack of development. Some even view regulation as an impediment to innovation. Deepfake sometimes can have beneficial effects, especially in a military context. In the domains of training and simulation, deepfakes can have great value. However, whether we should use deepfake for development is a question.

- **Judicial Issues.** Like the internet and all associated things, this technology needs multi-country participation. In the interest of personal data, security, and ethics, the judicial requirements

differ from those for spreading misinformation and propaganda. Further, each country has its laws, thus making the situation challenging and non-standard.

- **Ethical Constraints.** The offensive application of deepfake for military application may undergo ethical scrutiny.

- **Application v/s Data.** Applications with ease to make deepfake videos are available on the internet and in stores. However, for military applications, the dataset required for training of these algorithms cannot be generic. Thus as service and for effective joint fighting, there is a greater need to develop this dataset. Further, the capability to build application both to detect deepfake and to generate one has to be built. Off the shelf, applications developed by commercial entities may not in entirety support our purpose or may not be effective for military application. Thus, our services will need to have larger gestation period to build an effective war fighting capability.

- **CIA Triad Infringement.** It will be challenging for policymakers, regulators and the judiciary to protect the information security triad. Technologies like deepfake have a high potential to infringe on the triad and redefine it. Thus, the protection of data, especially operational data, becomes challenging. Capability to detect deepfake narratives built by enemy is key to ensure this. Thus training, equipment requirement, effective command and control aided by skill of service personnel will help in inhibiting such infringement. Also increasing digital literacy of service personnel and their families will ensure a strong data protection.

- **Public Awareness.** Owing to the reach of technology and its effect, it is imperative for nations to undertake public awareness campaigns. The enemy military may not target our military or our personnel directly but can release synthetic videos that have effect on citizens in general. The ability to discriminate real from fake and further knowledge to refrain from spreading such misinformation can go a long way in curbing the menace of deep

fake. This task is challenging owing to public participation and the educational level of various countries.

- **International Cooperation.** Given the global reach of this technology, multilateral cooperation in practicing best practices, sharing sound training values through joint exercises between services, with civil administration, paramilitary and other national military can ensure global cooperation. This will also help in seeking help in times of need. A digital coalition or consortium for coordination between militaries can be established. India being a professional and one of the largest militaries can contribute towards this at scale.

CONCLUSION

Deepfake technology has emerged as a potent tool with relevance in modern military with ability to redefine the dynamics of information warfare especially in domain of grey and NKNC. Its ability to manipulate perceptions, spread targeted misinformation and execute sophisticated deception presents significant operational risks to troop morale. Time is right for militaries to proactively incorporate deepfake in their doctrine. Enhanced training of personnel in deepfake detection and generation will make the IW approach more robust. Militaries through skill development, policy backing, ecosystem building and international cooperation can build a global digital consortium in with India can take the lead. Its ability to simulate realistic training scenarios and rabid deployment ability can prove to be force multiplier. At the same time the challenge of incorporating this technology at organisational level to ensure sound command and control would not be easy. The technology itself is developing with a need for India specific dataset and algorithm to keep out adversaries. Thus, to maintain a strategic edge, the advantages of deepfake must be adopted to supplement national defence objectives while mitigating its risks in evolving digital battle field.

★★★

Wg Cdr Anand R Navaratna is serving as Aeronautical Engineer in IAF. He has done his M Tech in Artificial Intelligence and is perusing his PhD in Digital Transformation from IIT Jodhpur.

NOTES

[1] *Jowett, Garth S., and Victoria O'Donnell. 2018. "Propaganda and Persuasion". Thousand Oaks: SAGE Publications.*

[2] *Browne, Patrick. 2020. "The United States and World War II: A History". New York: Oxford University Press.*

[3] *Harris, Sam. 2018. "Propaganda and the Public Sphere in World War II". Chicago: University of Chicago Press.*

[4] *Welch, David. 2019. "Nazi Propaganda and the Second World War". London: Bloomsbury.*

[5] *Beller, Steven. 2019. "Anti-Semitism in Nazi Germany". London: Routledge.*

[6] *Lindsey, Brian. 2015. "Media and War: The Jessica Lynch Incident." "Media, War & Conflict" 8 (3): 264-278.*

[7] *Cohen, David. 2021. "Understanding the Threat of Deepfakes." "Media Studies Journal" 15 (2): 88-102.*

[8] *Mitchell, John. 2022. "Digital Warfare and Information Manipulation: The Ukraine Conflict." "International Journal of Digital Media" 18 (4): 125-142.*

[9] *Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., ... & Courville, A. (2014). "Generative adversarial nets." "Advances in Neural Information Processing Systems", 27.*

[10] *Cohen, Adam. 2020. "The Role of Social Media in the Syrian Civil War." "Journal of Conflict Studies" 10 (1): 45-67.*

[11] *Jane Wakefield, (2022), "Deepfake Presidents used in Russia-Ukraine War", BBC News, URL: https://www.bbc.com/news/technology-60780142*

[12] *Sam Biddle, (2023), "US Special Forces want to use deepfake for Psy Ops", The Intercept, URL: https://theintercept.com/2023/03/06/pentagon-socom-deepfake-propaganda/*

[13] *Daniel L. Byman, (2023), "Deepfakes and International conflict, Brookings Foreign Policy", Brookings, URL: https://www.brookings.edu/wp-content/uploads/2023/01/FP_20230105_deepfakes_international_conflict.pdf*

[14] *Militarnyi, (2022), "Ukrainian intelligence intercepted the Russian provocation against Baykar CEO Haluk Bayraktar", URL: https://mil.in.ua/en/news/ukrainian-intelligence-intercepted-the-russian-provocation-against-baykar-ceo-haluk-bayraktar/*

[15] *Sam Skove, (2024), " How Army special operators use deepfakes and drones to train for information warfare", Defence One, URL: https://www.defenseone.com/technology/2024/04/how-army-special-operators-use-deepfakes-and-drones-train-information-warfare/395852/*

[16] *Zhao, B., Zhang, S., Xu, C., Sun, Y., & Deng, C. (2021). Deep fake geography? When geospatial data encounter Artificial Intelligence. Cartography and Geographic Information Science, 48(4), 338–352. https://doi.org/10.1080/15230406.2021.1910075*

[17] *Chesney, Robert, and Danielle Keats Citron. 2019. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." "California Law Review" 107 (5): 1753-1820.*

[18] *Mitchell, John. 2022. "Digital Warfare and Information Manipulation: The Ukraine Conflict." "International Journal of Digital Media" 18 (4): 125-142.*

[19] *HR 5586,(2023), "USA Congress", URL: https://www.congress.gov/bill/118th-congress/house-bill/5586/text*

[20] *European Parliament (2023), EU AI Act: first regulation on artificial intelligence, URL: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence*

[21] *Ministry of Justice and Laura Farris, (2024), "Government cracks down on 'deepfakes' creation", Government of UK, URL: https://www.gov.uk/government/news/government-cracks-down-on-deepfakes-creation*

155-171

CONVERGENCE OF SPACE WARFARE AND INFORMATION WARFARE FOR COUNTERING A2/AD OPERATIONS

Gp Capt (Dr) Dinesh Kumar Pandey (Retd)

Abstract

With the progress of contemporary military skills Anti Access/Area Denial (A2/AD) operations keep evolving over time. A2/AD approaches will maintain their influence on the future of battlefields and regulate the ways nations apply their power and tackle security threats. For military strategists and commanders to address the challenges introduced by these fast-paced advancements comprehensively they need deep insights into today's A2/AD landscape. By combining Information Warfare (IW) with space strategies military forces can efficiently respond to A2/AD behaviours improving their operational resilience. Military forces will be able to navigate A2/AD operations smoothly by being knowledgeable about emerging technologies with respect to IW. The study focuses on how IW with space warfare may act as formidable mission for soft as well as hard kills, to accomplish the military objectives.

INTRODUCTION

Modern warfare is not reliving in the battle field alone, but it is also fought in cyberspace. The Russia-Ukraine and Israel-Hamas are other examples of cognitive warfare in information domains which has a close tie with perception strategy. Through social media, the public has been able to interact mostly with warfare in informing the population about propaganda, as well as providing responses to fake news. Handling the

issue of whether the material published on the web is genuine or not is still significant, but here virality might be of even greater value than the content, as far as the search for support is concerned.[1]

Information in the form of resource and weapon is central to contemporary conflicts. It is a dimensionally condensed war that is also temporally compressed in terms of time and space. The 'management' of information in direction of optimal utilisation for the purpose of achievement of military objectives is key determining factor. The IW is the utilisation of information and communication technology to influence the information process and hence impair an opponent.[2]

In military operations, IW means all actions that are taken for the purpose of denying, exploiting, depreciating, or destroying the information, and thus the functioning of the opponent. It also covers defending ourselves from those acts and using own military information functions. Cyberwarfare, electronic warfare and cyber-attack are part and participle of IW. When the activities of counter forces exist in space, cyber and the electromagnetic domain, the response will be soft kill of the intended targets. Expanding the concept of warfighting domains to incorporate space and cyberspace has greatly added to its scope, and conduct of information operations.[3]

BRIEF HISTORY OF IW

Using information as one of the key weapons is not an innovation, but military missions indicate noticeable and emergent problems in information operations. Data is pervasive, but aggravates the C2C interaction. IW is information, deception, cyber actions, and public activities, while conventional forces rely on air supremacy, force and mobility. Conventional warfare refers to the use of firepower both individual and team fired systems within a tightly knit fire control network, to rapidly destroy enemy formations and fire control nodes. Air power has a splendid record in fighting, but it shows a consistent failure in the attempts to adequately harness the information environment as a strategic, operational, and tactical weapon.

If warfare is governed by the strategy and missions, which is then governed by intelligence, it is the business of the military to anticipate and counter probable contingencies. From the media point of view, the reduction on the Iraqi route of death, which is a strategic mileage in Iraq that was highly attacked and destroyed during the First Gulf War, are thought of as taken a determinant in lessening the coalition attacks.[4]

The falsification, or 'hiding' of the events at the battlefield has become a characteristic feature of war since ancient times. For this reason, the First World War may be viewed as one of the key moments in the use of information operations. For the first time it used electronic warfare by intercepting the wireless communication. The inputs, like during the start of the war Great Britain cut all cables from Germany and they had none at all. It is known that such a strategic decision in informational confrontation was exactly used in intercepting the Zimmerman telegram.[5]

To effectively counter A2/AD operations, information warfare and space warfare must come hand in hand to enhance the mission productivity.[6] The following are a few examples of contemporary wars:

In the 2014 Ukrainian conflict, Russia disrupted Ukraine's satellite communications to hinder command and control. Russia combined space-based Intelligence, Surveillance, and Reconnaissance (ISR) with cyber-attacks were carried out to disrupt Ukraine's command and control, during the Russia-Ukraine conflict (2014).[7]

Russia's 2015 cyber-attack on Ukraine's power grid demonstrated the potential for information warfare to disrupt critical infrastructure.[8] In the 2018 Syrian conflict, Russian forces employed electronic warfare to disrupt coalition communications. ISIS effectively used social media for psychological operations, recruiting, and propaganda. The US used space-based ISR assets to track ISIS movements in Iraq and Syria.[9]

In US-China Conflict (2020), The US used space-based assets to detect and disrupt Chinese anti-ship missile systems. During Israeli-Hamas Conflict (2021), Israel used space-based ISR and cyber capabilities to disrupt Hamas's command and control.[10]

To prevent the use of Ukrainian drones and direct coordinate strikes on Russian targets, Russia was also able to interfere with GPS in Ukraine. Number of satellites are employed for a variety of purposes, including navigation and mapping. To disrupt the Ukrainian operations, GPS satellite signals are being targeted by Russian forces from ground stations. On February 24, 2022, the Russia-Ukraine conflict commenced, but jamming was already underway. In the course of their operations in Crimea, which was previously part of Ukraine, the Russians employed GPS interference. A2/AD operations are equally affected with such threats.[11]

ANTI-ACCESS/AREA DENIAL

A2/AD is a concept that is intended to achieve a goal of denying adversaries, a particular geographical region while at the same time making it easier to exploit vulnerabilities in regard to operations within the region. A2/AD is relevant in the air, ground and at sea environments or any fusion of these environments.[12]

Current and potential future adversaries are purposefully designing A2/AD envelopes to keep the enemy forces from approaching key tactical areas. A2/AD is also a combination of sensors, antiship, antiaircraft and ground defences and a long-range fire which are deployed and established by one country to make sure that the aggressor does not advance for the fight. The positions that these zones have are very strategic because they can change the balance of power in a region after.[13]

For Examples: China is building A2/AD zones to deny US forces access to Taiwan and the South China sea. Russia is developing A2/AD zones in the Kaliningrad, Crimea, the Kola Peninsula, and the Kuril Islands to deny the sea lanes necessary for entry.[14]

TARGETING A2/AD FROM SPACE

It was observed that the extent of A2/AD zones' weakness was their command-and-control nodes, which operated as a unique point of

failure, due to disruptive vulnerabilities to Network Centric Operations and communications. However, the US has potential strategies such as precision guided technology for a brief low-cost decapitation initiative targeted at these nodes, that could counter these weaknesses and store the balance. The offence-defence ratio has been squarely seated on the offence for decades. As technology in networks, Artificial Intelligence (AI), and space is advancing, it is having the effect of making these zones more perilous by restoring the upper hand to defence.[15]

Space is an important force multiplier in the area of warfare by providing essential needs for operation that include intelligence, surveillance reconnaissance, communication, navigation, and cyber operations. Tactical assets located in space enable militaries to gain information superiority, provide safe and efficient command and control, and coordinate operations across space and cyberspace, land, maritime, and air on a global scale. However, with the rising use of space for information operations, there are vast weaknesses that expose fundamental infrastructure, and therefore there is a need for precocious defence of such crucial resources. More so, with the improvements in countries and their integration of space-based technologies into their military doctrines, the importance of space in support of the facilitation of information superiority will rise progressively taking its place as one among the main battle grounds in future conflicts.

IW is an essential element of an integrated system of informational assets and informational power. Today, space / info as a domain of warfare has transformed the overall warfare and has provided unprecedented power projection and influence over an opponent. There are variety of applications for the integration of the space and information domains that improves operations, providing instances of the effectiveness of each domain.

THE ROLE OF SPACE IN CONTEMPORARY IW

The space as a strategic domain for military operation, which offers such importance functions as communication, navigation, and intelligence.

Securing physical control and domination of space instruments can enhance significantly a state's military effectiveness. For example, the American GPS supports precise locality and aiming in military operations around the world. In the same manner, reconnaissance satellites deliver timely information that is so valuable in formulation of strategies.

The number of cases of disruption to the communications, navigation, and missile systems of space assets during the Gulf War in 1991 were observed. To a large extent United States benefited from satellite communications and GPS to organise multi-contingency successive sophisticated strategies and accurately co-ordinate the tactical layouts. This method also illustrated the influence of space capabilities within evolving warfare systems.[16]

INFORMATION WARFARE: SHAPING PERCEPTIONS AND INFLUENCING OUTCOMES

Information war is the intentional manipulation, disruption or control of information systems in an effort to affect target adversaries. Cyber operations, psychological operations and electronic warfare can be narrowed down within this strategy. The purpose is altering perceptions, sapphire, and gaining tactical advantages without actually going toe to toe.[17]

At the same time, the conflict between Russia and Ukraine gives evidence of the significance of the informational aspect as the type of war. Among them are highly sophisticated cyber warfare and disinformation as the weapons that have been applied to mobilise public opinions in order to incite unrest. Various elements of IW, with relevant examples are appended below.[18]

- **Cyber-attacks.** Cyber-attacks designate a conventional method of information warfare, in which adversaries use malware, viruses, or misleading software to either stop, harm, or illegally exploit information systems. Discovered in 2010, the Stuxnet worm greatly damaged the centrifuges at Iran's nuclear facilities.

- **Disinformation Campaigns.** Disinformation is characterised by the relentless supply of the public with false or fake news with an aim of modifying their attitudes or eliminating social integration. The case of Russia's part in the 2016 United States Presidential election is still relevant. In order to have an effect on the election results, Russian operatives put out both issues that divide and misleading information through social media.
- **PSYOPs.** Information psychological operations' aim is to change the targeted audiences' general mood, plans, and behaviour patterns. The fliers dropped by the US military over the Iraqi troops during Gulf War encouraged them to surrender and was able to guarantee them good treatment. In demoralisation of Iraqi forces and leading to many large surrenders, the method used did succeed.
- **Electronic Warfare.** In warfare, good communication is beneficial, yet it can sometimes create a vulnerability. In 2007, the Israeli Air Force used electronic jamming to break down Syrian radar defences, permitting Israeli jets to complete a strike on a suspected nuclear reactor without alerting anyone.
- **Social Media Manipulation.** Using social media for propaganda dissemination or the shaping of public beliefs is a new variation on information warfare. More than just exposing the Facebook data collection from millions of users, the Cambridge Analytica case revealed that it had used that data to impact voter behaviour during the 2016 U.S. Presidential Election.[19]
- **Economic Disruption.** One can target economic systems in information warfare. In response to the film 'The Interview', North Korea's cyber-attack on Sony Pictures in 2014 served two purposes: to inflict economic damage and to intimidate other organisations.[20]

Like other systems, to develop and set A2/AD zones, requires ISR components apart from the strike systems even in offence as well as defence. ISR systems are used to search for outgoing threats that can

attack by Defensive Strike Systems. Preventing actions against attack systems has a goal to slow down build-up against US force in enemy structures, supplies and focal points. Bait and deception operations that epitomise efficiencies of A2/AD bubbles, rise guarantor's ground sparring probability. Along with such an approach, the use of these techniques jointly with the technologies that make defence a more powerful kind of warfare, will indicate the extent of the impact at the strategic level in the following years. The first and central tactful aim of the defender is not to beat the United States in a conflict but to get to a point that the cost for every extra user erodes the political gain than the cost per user to United States.

The primary strategic goal of the defender is to uphold, not to outperform the United States in battle, but to raise the costs to the United States until the likely political gain lessens compared to the loss.

A2/AD practises are about using weaponry, sensors, and strategies to obstruct an adversary's entrance or operations in a specific geographic area.

Electronic warfare operational end-to-end capabilities are long-range precision weapons designed for limiting the movements of the enemy forces to a certain extent, or denying the opponent forces to a definite geographical area. Various missile systems, electronic warfare capabilities, air defence networks & long-range precision weapons all are used to challenge the mobility of potential opponents.

Engaging IW it is shown that military forces can effectively counter, limit, deceive or nullify the operations of their adversaries in the A2/AD contexts.

INTEGRATION OF IW WITH SPACE WARFARE AGAINST A2/AD

The space and IW feed off of the synergy that exist between the two and enhances the abilities of the military capabilities. Objects placed in space lie at the basis of information operations, providing people around the globe with internet connections and real-time information transfer. In addition to its other functions, IW is also responsible for protecting the

operational capabilities of space assets from threats that are digital and electronic, thus lending some reassurance about the future of space.

One of the clear examples of synergy in space is the application of ASAT weapons that is anti-satellites weapons. China, in 2007 criticised all tests in this regard and at the same time conducted a live ASAT test demonstrating off how it could wipe out satellites in orbit.[21] It threw light on the vulnerability of space assets and the need for strong IW just to protect those assets. Imposition of cyber defence and electronic countermeasure remain significant, critical for a militarns forces to effectively safeguard space assets while maintaining tactical advantage and dominance.

IW, when integrated effectively, enhances both operational effectiveness and survivability through the following mechanisms:

- **Disruption of C4ISR Networks**. The systems focused on A2/AD operations greatly depend on C4ISR networks—command, control, communications, computers, intelligence, surveillance, and reconnaissance—for both targeting and coordination. By employing Electronic Warfare (EW) and cyber operations, military forces can unleash the full disruptive potential of IW, effectively disrupting or degrading these networks:[22]
    - **Electronic Jamming and Spoofing.** Interfering with enemy radar and communication systems to stop the organisation of missile defence manoeuvres or diminish sensor precision.
    - **Cyberattacks on Data Networks.** Gaining access to or incapacitating principal information networks can confuse the early warning systems of the enemy or misrepresent their command-and-control functions.
    - **Deception Operations.** Militaries are able to misguide their opposition about the locations or goals of their forces, minimising the ramifications of A2/AD targeting, by introducing false information into their information framework.

- **Example.** Blending advanced EW systems including the U.S. EA-18G Growler and others reveals the promise of shielding sensor and radar assets necessary for A2/AD tactics.[23]

- **Denial of Situational Awareness**. Denying the enemy to have accurate situational awareness for decision making, is a crucial part of countering A2/AD strategies. The IW has the potential to do so. For the purpose of achieving this goal, IW might follow different approaches, which may include both cyber and kinetic operations on monitoring infrastructure, use of decoys or fake targets and the monitoring of activities in the electromagnetic spectrum.

  - **Cyber and Kinetic Attacks on Surveillance Assets.** By making adversary satellites unusable (soft kill) or destroying (hard kill) them, as well as the disabling or destruction of drones and ground-based sensors (radar) facilities on earth, one can impair the detection and engagement abilities of incoming forces.[24]

  - **Use of Decoys and False Targets.** Saturating an adversary's sensors with physical or digital decoys enables a push for them to thinly distribute their resources or to target fraudulent targets. During the Gulf War, the coalition military resorted to quite an elaborate camouflage – fake formations such as inflatable tanks and radio chatter to limit the enemy's ability to achieve A2/AD advantages.[25]

  - **Electromagnetic Spectrum Management.** Adjusting the spectrum to achieve electromagnetic silence or to deceive signatures can obscure information on military actions for the adversary.[26]

  - **Example.** In the Gulf War the actual operations of the coalition also decreased the A2/AD control of Iraq with decoys and fakes including inflatable tanks and false radio traffic.

- **Influence Operations and Psychological Warfare.** Psychological operations can be directed at the decision making of the adversary's leadership, as well as the will of the adversary's forces.
    - **Psychological Operations (PSYOPs).** The job of propaganda, misinformation, and disinformation is to sow confusion, cast doubt, or obstruct the movement of opponents in their decisions. The misunderstanding of hazards may result in a misuse of resources.[27]
    - **Cyber and Social Media Operations.** By using web platforms to disseminate disinformation and to create doubt about how truly effective A2/AD defences are. Making political and military leadership a target could require a rethink of the A2/AD assets.
    - **Perception Management.** Engaging in covert information operations that quietly modify an enemy's perspective of the operational environment and thus slow their decision-making and reduce confidence in their A2/AD systems. For example, the utilisation of Russian IW tactics of a hybrid kind in Crimea led to improved coordination among Ukrainian forces and shaped international narratives in ways that advanced the delay of international responses.
- **Achieving Benefits of Cyber Superiority for Improved Command and Control.** The friendly forces gain superiority of the cyber domain, enhance their own operations in the operational area under A2/AD conditions. This involves:
    - **Securing Communication Networks.** Affording friendly forces unhindered access to continue manoeuvre and not to be interrupted or intercepted in certain parts of the battlespace requiring unambiguous command and control.
    - **Cyber-physical Integration.** Combining this information in real time at a faster rate than the adversary utilising

advanced AI and machine learning techniques to counter active A2/AD threats on the battlefield.

- **Resilient Networked Warfare.** Introducing mesh or regional, multiplexed networks of 'last mile' communication hopscotching, and prognosticated sensory nodes or taps that can operate autonomously or redundantly in the occurrence of aggressor cyber or EW surges.

- **Offensive Cyber Warfare and Kinetic Integration.** Offensive cyber operations can be synchronised with kinetic strikes to disable or degrade A2/AD capabilities:
  - **Pre-emptive Cyberattacks on Key Nodes.** Military forces can succeed by locating and penetrating this system's cyber support structures; the A2/AD systems' operation will be hindered as a result. This may refer to blunting air defence command structures, logistics structures or power sources for A2/AD systems.
  - **Integration with Precision Strikes.** Equally, cyber operations can mute the A2/AD command centres and radars which gives the precision targets for kinetic attack and deny the other side any airborne or missile response.
  - **Example.** In 2007, the cooperation between physical and cyber was shown during Israel's Operation Orchard in Syria when the silent breach of Syrian air defences is said to have been accompanied by cyber sabotage that allowed the Israeli aircraft to attack a suspected nuclear site.[28]

- **Net-Centric Warfare and Decision Superiority.** IW supports NCW, where a faster decision cycle defeats A2/AD systems of the adverse party.[29] This is achieved by:
  - **Shared Battlespace Awareness.** Connecting all sensors and shooters in different domains such as air, maritime, space and cyberspace to generate operative picture on a common VTC.

- **OODA Loop Acceleration.** Far from deploying A2/AD systems as a separate mode of warfare, by accelerating the OODA loop friendly forces disrupt the decision-making cycle of the adversary and strike before the adversary can respond.
- **Multi-Domain Operations (MDO).** Inclining towards a synchronised actions approach across different domains (space, cyber, and kinetic) to saturate and outrun A2/AD systems.[30]
- **Example.** The United States and NATO have aimed to improve the multi-domain command and control to acquire decision advantage and overcome A2/AD bubble, which provides forces nonlinear opportunities.

To develop a robust line of defence against the varied threats from IW, different approaches may be exploited subject to availability of resources and feasibility of mission.

WAY AHEAD

Convergence of space warfare and IW is the need of the hour for the successful conduct of the countering A2/AD operations. Considering lessons learnt from the history of air warfare, formulation of conducive standard operating procedures for exploiting available resources merits consideration.

- **Doctrine and Strategy.** Developing a comprehensive and integrated doctrine to address IW and space warfare is essential for the accomplishment of missions to counter A2/AD operations. An explicit command-and-control structure is vital for such operations.
- **Capacity Building.** The conduct of the exercises and training for all joint operations, particularly joint exercises in space and IW, plays a pivotal role. These training sessions will make crew to

feel part of the strategy. The use of space-based assets to carry out space-based ISR capabilities also necessitates advanced satellite communications systems, ensuring a more secure and well-equipped systems. Availability of anti-satellite missile defence systems is of paramount importance.

- **Cyberwarfare.** The cyberwarfare capabilities may be enhanced to continue information warfare. It is necessary to develop an AI environment for information operations that can be used in automated data analysis, identify potential threats for correct decision-making, develop EW capabilities for uninterrupted operations, maintain good cybersecurity practices, provide an anti-satellite missile defence system and conduct regular vulnerability assessments.

- **Convergence.** Ensure that information warfare and space systems are seamlessly integrated to achieve the contemplated results successfully. There should be standards and a common data architecture to conduct information warfare and joint space exercises.

CONCLUSION

The integration of space operations and IW specifies a major change in military strategies. Militaries are better able to complete their tactical objectives more efficiently by maximising the specific traits of space warfare as well as IW, in their efforts relating to power projection and control. As technological progress continues, the collaboration between space and IW will become ever more important in the development of future warfare.

IW is a potent and effective tool against A2/AD strategies and its applications span from the tactical level through operational; and even up to the strategic level of war. By attacking the information system of the adversary, Jamming's deception, control of own and denial of adversary’s network, physical destruction of key enemy nodes, and

co-ordination of cyber operations with physical attacks, military forces could combat efficiently in redundant A2/AD zones. Such operations depend on specific cyber, electronic, and psychological features of warfare recognised by them and to gain informational advantage over adversaries and focus on their vulnerabilities. The armed forces and combatant commands must better organise and prepare themselves to act in the information domain.

★★★

Gp Capt (Dr) Dinesh Kumar Pandey (Retd) was a Group Captain in IAF. He had served in the IAF for more than three decades. He has an experience of more than 2500 Air combats. He was the Director Air Staff Inspections and retired as Director, Joint Control and Analysis Centre. He has written research papers for journals and websites. Presently he is a Senior Fellow at the Centre for Air Power Studies (CAPS).

NOTES

1 *Benjamin Jensen and Divya Ramjee, "Beyond Bullets and Bombs: The Rising Tide of Information War in International Affairs", December 20, 2023, https://www.csis.org/analysis/beyond-bullets-and-bombs-rising-tide-information-war-international-affairs. Accessed on September 3, 2024.*

2 *Col Andrew Borden, "What is Information Warfare?", Air University, 1998, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Chronicles/borden.pdf. Accessed on September 5, 2024.*

3 *"Decoding Anti-Access/Area Denial (A2/AD) Strategy", Military Sphere, June 10, 2024, https://militarysphere. com/anti-access-area-denial-a2-ad/. Accessed on September 4, 2024.*

4 *Nick Brunetti-Lihach, "Information Warfare Past, Present, and Future", The RealClear Defense, November 14, 2018, https://www.realcleardefense.com/articles/2018/11/14/information_warfare_past_present_ and_future_113955.html. Accessed on August 28, 2024.*

5 *Gordon Corera, "How Britain Pioneered cable-cutting in World War One," BBC, December 15, 2017, http://www.bbc.com/news/world-europe-4236755. Accessed on April 3, 2018.*

6 *Dorothy Sherwood, "Integrating space into Information Warfare", US Cyber Command, January 16, 2024, https://www.cybercom.mil/Media/News/Article/3647026/integrating-space-into-information-warfare/. Accessed on October 3, 2024.*

[7] *Alexander Salt and Maya Sobchuk, "Russian Cyber-Operations in Ukraine and the Implications for NATO", August 2021, https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato. Accessed on October 24, 2024.*

[8] *"Cyberattack on Ukraine grid: here's how it worked and perhaps why it was done", The Conversation, January 18, 2016, https://theconversation.com/cyberattack-on-ukraine-grid-heres-how-it-worked-and-perhaps-why-it-was-done-52802. Accessed on October 24, 2024.*

[9] *Anna Varfolomeeva, "Signalling strength: Russia's real Syria success is electronic warfare against the US", May 1, 2018, https://thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/. Accessed on October 24,2024.*

[10] *Robert Ashley, John M. Bednarek, "Gaza Conflict 2021 Assessment: Observations and Lessons", JINSA, https://jinsa.org/wp-content/uploads/2021 /10/ Gaza-Assessment.v8.pdf. Accessed on October 6, 2024.*

[11] *Elizabeth Howell, "How Russia's GPS satellite signal jamming works, and what we can do about it", SPACE, April 14, 2022, https://www.space.com/gps-signal-jamming-explainer-russia-ukraine-invasion. Accessed on October 24,2024.*

[12] *Douglas Barrie, "Anti-access/area denial: bursting the 'no-go' bubble?", Institute for Strategic Studies (IISS), https://www.iiss.org/ar-BH/online-analysis/military-balance/2019/04/anti-access-area-denial-russia-and-crimea/. Accessed on September 6, 2024.*

[13] *Alex Vershinin, "The Challenge of Dis-Integrating A2/AD Zone: How Emerging Technologies Are Shifting the Balance Back to the Defense", National Defense University Press, March 31, 2020, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106488/the-challenge-of-dis-integrating-a2ad-zone-how-emerging-technologies-are-shifti/. Accessed on September 6, 2024.*

[14] *Jon Lake, "China's Stealthy Area Denial", Asian Military Review, March 14, 2023, https://www.asianmilitaryreview.com/2023/03/chinas-stealthy-area-denial/. Accessed on September 3, 2024.*

[15] *Ibid (Alex).*

[16] *Frank Gallegos, "After the Gulf War: Balancing Spacepower's Development", September 18, 1997, https://apps.dtic.mil/sti/pdfs/ADA329263.pdf. Accessed on September 3, 2024.*

[17] *Alcazar and Thomas, "A Role for Land Warfare Forces in Overcoming A2/AD", Military Review, Nov-Dec 2013, https://www.armyupress.army.mil/Portals/7/military-eview/Archives/English/MilitaryReview_20131231_art014.pdf. Accessed on September 6. 2024.*

[18] *Margaret Rouse, "Information Warfare", Techopedia, January 4, 2017, https://www.techopedia.com/definition/29777/information-warfare. Accessed on September 3, 2024.*

[19] *Ibid (Techopedia).*

[20] *Ibid (Techopedia).*

[21] *Carin Zissis, "China's Anti-Satellite Test", Council on foreign Relations, February 22, 2007, https://www.cfr.org/backgrounder/chinas-anti-satellite-test. Accessed on September 4, 2024.*

[22] *Ibid (Alcazar).*

[23] *Stefano D'Urso, "Let's Talk About The Digital Evolution Of Electronic Warfare", The Aviationists, October 26, 2020, https://theaviationist.com/2020/10/26/lets-talk-about-the-digital-evolution-of-electronic-warfare/. Accessed on September 3, 2024.*

[24] *Ibid (Alex).*

[25] *"Decoys: The Art of Disguise", L.A. Times Archives, February 11, 1991, https://www.latimes.com/archives/la-xpm-1991-02-11-mn-839-story.html. Accessed on September 1, 2024.*

[26] *Ibid (Alex).*

[27] *MG Yevtodyeva, "Development of the Chinese A2/AD System in the Context of US–China Relations", Springer Link, September 29, 2022, https://link.springer.com/article/10.1134/S1019331622120048. Accessed on September 9. 2024.*

[28] *Mohan B. Gazula, "Cyber Warfare Conflict Analysis and Case Studies", MIT, May 2017, https://cams.mit.edu/wp-content/uploads/2017-10.pdf. Accessed on September 3,2024.*

[29] *Alberts, Garstka & Stein, "Network Centric Warfare: Developing and Leveraging Information Superiority", NCW, February 2000, http://www.dodccrp.org/files/Alberts_NCW.pdf. Accessed on September 9,2024.*

[30] *Shaun Cannon, "The Alliance's Transition to Multi-Domain Operations", JAPCC, Edition 37, 2024, https://www.japcc.org/wp-content/uploads/JAPCC_J37_screen.pdf. Accessed on September 3, 2024.*

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/.*

STRATEGIC COMMUNICATION AND THE MILITARY

Lt Col Akshat Upadhyay

Abstract

In contemporary warfare, Strategic Communication (SC) serves as a critical force multiplier, shaping perceptions and influencing behaviours across domestic and international audiences. This article explores its role in Information Warfare (IW), examining how SC can enhance military operations and shape the information environment. The paper emphasises the importance of managing the information effects of kinetic actions, highlighting the necessity of countering adversary narratives and controlling perceptions. Additionally, the analysis delves into the use of influence machines and their potential to undermine a nation's resolve. To adapt to this evolving landscape, the paper proposes a comprehensive approach for militaries, suggesting the need to leverage cutting-edge technology, prioritise authenticity, credibility and transparency, and deepen understanding of target audiences. Crucially, the author advocates empowering SC institutions to ensure coordinated and effective messaging. This approach underscores the importance of SC in achieving national security objectives and maintaining an advantage in the cognitive domain.

INTRODUCTION

Nuclear deterrence relies on communicating capability and credibility. In nuclear deterrence literature, this framework is known as the three Cs.[1] It denotes a nation's strength and its willingness to use the weapon.

However, without clear communication, even the most powerful weapons may not deter. During the Cold War, the US and Soviet Union struggled with this, relying on assumptions and strategic culture to interpret each other's actions.[2] To deter an enemy without the benefit of direct dialogue, Thomas Schelling proposed the 'Schelling point,' a game-theoretic solution where people converge on a predictable outcome based on shared expectations and understanding.[3] The high point of this way of communication was the Cuban missile crisis of 1962 where actions and counter-actions signalled intent, both to escalate and later, de-escalate.[4] The advent of modern communication technologies, especially with the Silicon revolution of the 1960s led to more effective ways of getting one's message across. The end of the Cold War, relative democratisation of these technologies and proliferation of security threats led to militaries attempting to utilise information in a manner that furthered their aims - in conventional and sub-conventional operations. The current milieu, that features a combination of great power competition (GPC), generative artificial intelligence (AI), social media platforms and lone wolf actors within the same operational continuum requires militaries to strategically communicate messages to a wide and diffused swathe of audience including friends, foe and neutrals. Not only this, communication also precedes, works in tandem and succeeds kinetic operations, and at times, may preclude kinetic operations in the achievement of a political goal.

WHAT IS STRATEGIC COMMUNICATION?

There are numerous terms used across organisations that are understood to be interchangeable and sometime synonymous to each other. These are Strategic Communication (SC), Information Operations (IO) and Information Warfare (IW). Not only this, there are multiple sub-categories within these terms too. It is therefore important that a certain taxonomy be established for clarity. While there are differing views on what exactly SC is, for the purpose of this paper, it is defined as "orchestrated use of communication - encompassing words, actions, imagery and symbols - to inform and influence key audiences in ways that advance national interests and objectives."[5] Here, inform and influence are two major

aspects of SC and there are different standard operating procedures (SOPs) and agencies to deal with them. However, as in most countries including India, there is no overarching authority to orchestrate the actions of these agencies in pursuit of common national objectives. Therefore, the roles of these agencies overlap resulting sometimes in 'information fratricide' where communication actions by one agency works at cross-purposes to the others.

INFORMATION AS A WEAPON: HISTORICAL EXAMPLES

While SC is an umbrella term and has been coined as recently as 2002[6], information operations, or the use of information to influence adversaries, has been in effect since ages. The Athenians used disinformation during a campaign against Xerxes to dissuade the Persians from working with certain Greek allies at Salamis. They achieved this by sending messages that created distrust in the loyalty of their allies.[7] Operation Fortitude was a military deception operation that tricked Germany into believing that the Allied invasion of Europe would occur in either the Pas de Calais or Norway, instead of Normandy. This was achieved by the creation of a Ghost Army or officially, the 23rd Headquarters Special Troops.[8] Using inflatable tanks, sound trucks, fake radio transmissions and scripts, an environment was created which capitalised on the Germans' own appreciation of where the Allies were likely to land in France. During the 1999 Kosovo conflict, the US deployed psychological operations (PSYOPS) units as part of Operation Noble Anvil to combat Serbian propaganda about the conflict. These units distributed leaflets, broadcast radio and occupied television spots to inform the Serbs about atrocities committed by their government, which was being led by Slobodan Milosevic.[9] These messages countered the narratives being spread by the Serbian government by sharing factual information about the war, including the "campaign of mass murder, systematic rape, and forced evacuation."[10]

INFORM AND INFLUENCE

One of the most comprehensive lexicon of SC has been devised the US military. Before defining the terms used by them and attempting a

degree of interlinking, it is important that the difference between 'inform' and 'influence' is clearly enunciated. For sake of clarity, each SC aspect will be dissected based on the focus, goal, methods and challenges framework. Inform refers to the act of conveying factual information to an audience without the explicit intent to shape their opinions or behaviours. The focus of inform is to provide objective information to audiences aimed at neutral reporting and transparency. This achieves the goal of increasing awareness and understanding of events, policies or perspectives. The methods used for informing are press releases, media engagements, official statements, fact sheets and reports. The challenges, and this issue will become clearer with a case study, of using this aspect of SC are that information, even when presented neutrally, inevitably shapes perceptions and can influence opinions and, the line between informing and influencing blurs when reporting on events with pre-determined strategic objectives.

Influence, on the other hand, represents a more deliberate effort to shape the attitudes, opinions and behaviours of target audiences to achieve specific objectives. Unlike informing, influencing acknowledges an intentionality that goes beyond mere information dissemination. The focus of influence is to shape the attitudes, opinions and behaviours of target audiences to align with desired objectives. The goal is to generate support, change perceptions or encourage specific actions. The methods used here are a little more abstract as compared to the inform aspect. These are persuasive communication, narrative crafting and framing, psychological techniques and leveraging social influence principles. The challenges include maintaining credibility and ethical considerations, especially when targeting foreign audiences and distinguishing between the information effects of kinetic operations and solely communication actions.

HIERARCHICAL ORDERING OF SC CONCEPTS

Though there is no strict hierarchical ordering of the various terms that comprise SC, this author through a perusal of multiple primary and secondary documents related to SC, IO and IW, has come out with

a relational tree. A majority of this ordering is influenced by the US military since they have devised the most comprehensive definitions and activities under SC. In a number of countries, some activities are folded under a single agency while in others they do not exist. At the top is SC, which represents the totality of a government's words and deeds to advance its interests. The next tier comprises IO and IW. While the former is a coordinated process within the DoD that aligns with and supports strategic communication goals, the latter can be viewed as a broader concept, encompassing both offensive and defensive use of information to achieve objectives during crisis or conflict. Activities under IO are Military Information Support Operations (MISO)[11], Military Deception (MILDEC)[12] and Operational Security (OPSEC).[13] These form the third layer. MISO, also referred to as PSYOPS, focuses on influencing foreign audiences' perceptions and behaviours through planned communication and shapes the information environment. MILDEC involves deliberately misleading adversaries through feints, disinformation and other tactics to shape their perceptions and actions. OPSEC aims to protect sensitive information from enemy exploitation, ensuring the integrity and effectiveness of IO and other operations. Cyber Warfare (CW) and Electronic Warfare (EW) form part of both IO and IW and refer respectively to manipulating information systems and the electromagnetic (EM) spectrum and form part of the fourth layer, along with Public Affairs (PA). PA is centered around providing information to various audiences, both domestic and international, about the goals, policies and activities of the government and this term is very US specific. This includes disseminating factual information about military operations, responding to press inquiries, and communicating about humanitarian efforts.[14] There is, however, still significant contestation in placing PA directly under SC or under IO. This represents the ongoing debate regarding the level of integration between PA and IO, with some arguing for closer coordination and others emphasising separation to maintain PA's credibility. At the fifth and last layer are computer network operations (CNO) which are a subset of CW. For the sake of this article, only the broader inform and influence parts will be covered.

CASE STUDY: US MARINE AMPHIBIOUS LANDINGS DURING GULF WAR I: BLURRING BOUNDARIES BETWEEN INFORM AND INFLUENCE

It is generally assumed that inform and influence aspects of SC are separate from each other, with the former falling under the ambit of public information or public affairs, and the latter in the realm of psychological operations or propaganda. However, recent case studies show that this may not entirely be true. In the process, the delicate boundary between these two components is often breached. During the First Gulf War, as part of the 'Two Corps' concept devised by General Norman Schwarzkopf, a 'Left Hook' comprising three armoured divisions, a mechanised infantry division and an armoured cavalry regiment was to lead the main assault to liberate Kuwait from Iraqi control. However, the success of the assault hinged on the willingness of the Iraqis to believe that the main assault was coming either from the south of the Kuwaiti border and/ or from the 5th Marine Expeditionary Battalion (MEB) afloat in the Persian Gulf, to the east.[15] The US Army's Public Affairs Department's stated aim, at least one of them, is "counter[…] misinformation and disinformation".[16] However, Public Affairs officers were involved in briefing members of the press, issuing press releases and facilitating the coverage of the Marines' preparation for the assault, in a classic case of disinformation despite their mandate being the exact opposite. The overall effect was the tying up of Iraqi troops to cater for this 'ghost' Army and the Left Hook decimated the remaining Iraqi force. This is a classic case of the inform and influence elements combining together to fulfil a politico-military objective, but does raise questions regarding the future credibility of such public-facing organisations.

RELATION BETWEEN SC AND THE MILITARY: A BROAD ARGUMENT

Contemporary warfare has evolved in its character as well as nature. In addition to the three traditional domains of land, maritime and air, new domains such as cyber, space, information, EM spectrum and cognitive have been created and are being contested. The modern battlefield has expanded into a 'battlespace' while the cognitive effects of war are

being directly felt, instead of being mediated through kinetic actions. SC therefore serves as a critical force multiplier for the military, capable of amplifying the effectiveness of traditional military operations while also providing distinct advantages in the increasingly important realms of information warfare and shaping of the international environment.

It is difficult for militaries to segregate inform and influence operations from one another since the intention is to impact and affect the minds of relevant audiences. These may range from the domestic, international and adversary. However, SC as a whole is meant to achieve national objectives of a particular country and inform and influence are two of the major ways to achieve the same. The words themselves evoke subjective judgments with the former appearing to be more positive than the latter, but it needs to be clarified that influence is not propaganda or deception. These latter two form part of military operations, though are generally used in the shorter term, when the objective is to sow discord among enemy ranks or disrupt their decision-making processes. Influence is a far more nuanced approach that seeks to build positive long term relationships that may be leveraged in future.

SC can be used by militaries in four effective ways. These are:

- **Countering Propaganda of the Adversary.** Militaries must be equipped to identify and counter adversary propaganda and disinformation campaigns that seek to undermine their operations, sow discord among allies and erode public support. SC for this may take the form of carefully crafted factual narratives and press releases, among other actions. Often, in this type of SC, the timing rather than the content of the counter is more important. Any propaganda of the adversary takes advantage of pre-existing faultlines (social, economic, political, cultural, religious or others) and identifies a trigger event or catalyst to disseminate divisive propaganda. It is extremely essential that this propaganda is identified and immediately countered. Rather than waiting to craft a wholesome fault-proof counter, the aim should be to get the counter-narrative out at the earliest, with a promise to deliver

supplementary proofs or facts in a later time frame. This helps fill the 'information void' which needs to be filled by own military or agency rather than the adversary.

- **Shaping the Operational Environment.** For militaries operating on their own soil, especially in counter-insurgency/counter-terrorism (CI/CT) areas, winning 'hearts and minds' becomes the primary objective - both in fulfilment of the larger political goal and at the tactical level by facilitating kinetic operations. An effective SC must, at all times, remember the primacy of the national aim. This will help in centering narratives and actions.

- **Enhancing Morale and Cohesion.** Internally, SC can play a vital role in enhancing morale and cohesion within the ranks, communicating strategic objectives clearly and ensuring that personnel of the Armed Forces understand and support the mission. With the proliferation or the infiltration of social media platforms and their 'surveillance capitalism'[17] models, the dangers of internal vitiation remain high. An effective SC can preclude this.

- **Establishing and Maintaining Deterrence.** SC is a potent tool for advancing national interests, deterring adversaries and shaping the international environment in a manner favourable to national security objectives. For advancing national interests, SC helps in shaping perceptions and narratives, building partnerships and countering adversarial propaganda. On the other hand, deterring adversaries includes communicating red lines and costs of aggression, exposing and exploiting vulnerabilities of adversaries and maintaining information superiority.

  SC is generally understood as advancing military objectives, pre-, during and post-operations. However, an under-appreciated aspect of SC is the information effects of kinetic actions which may intervene or interfere in the conduct of SC.

INFORMATION EFFECTS OF KINETIC ACTIONS

Kinetic actions, by their very nature, carry significant information effects. In fact, one of the main objectives of warfare is targeting the Cognitive

Centres of the Adversary (CCA), which can be understood as a subset of the conventional notion of Centre of Gravity (CoG). CCA focuses on the mental and psychological aspects of an adversary's power where SC can be used for targeting the enemy's beliefs, perceptions and decision-making processes through kinetic actions. "A bullet still sends a message"[18] means that the conduct of military operations, choice of targets and even the treatment of civilians send powerful messages to both target audiences and the broader international community. The case of Hamas atrocities on 07 October 2023 and their impact on the broader psyche of Israel and the international community is a classic example.[19] Militaries must, therefore, actively manage the information effects of their kinetic operations, anticipating potential misperceptions, countering adversary narratives and ensuring their actions align with their strategic messaging. As a result, it is necessary to include SC and information operations personnel during planning for operations.

INFLUENCE MACHINES

Recent conflicts have highlighted the tactical advantage bestowed on militaries using niche and emerging technologies. Major advances in AI have resulted in a convergence of data-dominant technologies and IO. By definition, an 'Influence Machine' is a system capable of shaping target audiences' perceptions through rapid and effective mimicry of human empathy, surpassing the speed and scale of traditional influence methods.[20] It has three key capabilities: algorithmic content generation, personalised targeting and firehose dissemination. The last term implies using automated systems and bot networks to spread propaganda and disinformation rapidly and widely across multiple online platforms, overwhelming audiences with a constant stream of biased information. One analyst calls the use of influence machines in warfare as a "strategic defeat mechanism"[21] since they can undermine a nation's will to fight and erode public support for government policies, effectively achieving victory without resorting to traditional military force. In a manner of do it yourself (DIY) warfare[22], influence machines can be exploited by non-state actors and individuals to create oversized adverse effects on states. These have the potential to bypass militaries and directly

target the CCA, making the task of SC more challenging. Traditional approaches may not be suited to tackle this threat, especially since they exploit the inherent openness and reliance on public opinion that characterise democratic systems. In fact, the use of influence machines is one of the best examples that demonstrates the changing and evolving nature of warfare, where information dominance and the ability to shape narratives have become crucial determinants of success, with a capacity to surpass traditional military might.

STRATEGIC COMMUNICATION AND THE FUTURE OF TRUTH

In the age of disinformation, deepfakes and AI-generated content, the very nature of truth is under siege. Plato's concept of the "noble lie"[23] raises the unsettling possibility that deception, even with benevolent intentions, could be wielded in SC. This notion is further complicated by Marshall McLuhan's idea that "the medium is the message,"[24] suggesting that the technology used to convey information shapes our perception of truth. Richard Rorty's work, which challenges the idea of objective truth and emphasises the social construction of knowledge, further complicates the matter, suggesting that truth is not something to be discovered but rather something that is created through dialogue and consensus,[25] while Neil Postman's insights warn of the potential for technology to blur the lines between truth and falsehood.[26] These combined perspectives paint a stark reality that the military faces unprecedented challenges in discerning and communicating truth. In this environment, SC must prioritise authenticity and transparency, while constantly adapting to the evolving information landscape. Failure to do so risks undermining the credibility of the military and jeopardising its ability to achieve its strategic objectives.

LIMITS OF STRATEGIC COMMUNICATION

Introduction of new actors and methods powered by niche technologies have also exposed weaknesses in the way SC has been used in the recent past. One of the biggest issues of SC is that of attribution and credibility, especially with operations in the cyber or special forces domain. No SC campaign can directly attribute these efforts to the

state carrying out these operations, however, the same also needs to be conveyed to the adversary in certain terms. Additionally, this also creates a 'firewall' effect - where foreign audiences start questioning the veracity of SC themes and narratives if they feel that the government is unwilling to share details of certain operations to its own citizens. The second is the crafting of compelling and powerful narratives. Militaries are notoriously incapable in this task since this requires specific skillsets not considered part of a conventional military tasking. The third and the most important issue is that SC is a probabilistic undertaking. There is never any guarantee that a particular SC will succeed or fail, and there are no metrics to measure its effectiveness. There are tools which can resort to engagements and sentiment analysis, but these are all manifestations of a larger campaign or may be organically generated. The success of SC is in the achievement of a stated aim or goal and one always wonders what the contribution of SC at the end was.

RECOMMENDATIONS

In view of the challenges described above, following recommendations are suggested:

- **Adoption of Technology.** Just as non-state actors, private companies and individuals are using SC for their aims and objectives, militaries must also do the same. There is a need for continuous research and development (R&D) in AI - either in-house or as part of a collaboration with academia and/or industry. Influence machines need to be defeated by influence machines of our own, while technology needs to be leveraged for crafting and disseminating our own narratives.
- **Prioritise Authenticity, Credibility and Transparency.** Focusing on accurate and verifiable information is essential to build credibility and trust with target audiences. Here SC campaigns by militaries must not only focus on projecting strengths but also acknowledging untoward incidents and that too promptly. Again, the issue of 'information void' is paramount

and the actor filling it first has a leg up in the 24–48 hour information cycle. A military's SC must therefore cater for both positive and negative events and their fallouts.

- **Deepening Understanding of Target Audience.** An effective SC requires understanding of not only domestic but foreign audiences in detail. This requires investments in cultural intelligence and leveraging tools for target audience analysis.

- **Empowering SC and Enhancing Coordination.** SC institutions within the military need to be strengthened and their status elevated to that paralleling military operations and intelligence. Domain expertise should be cultivated in-house as quickly as possible and at times, external agencies should also be roped in. Breaking down silos between different government agencies involved in SC is crucial to ensure a coordinated and unified approach.

CONCLUSION

The evolving nature and character of warfare necessitates that militaries view strategic communication as a core competency with a recognition that every military action, interaction and information contributes to narratives that shape perceptions and influence behaviours. This requires a shift from compartmentalisation of SC to integrating it into all levels of military planning and execution, ensuring every soldier understands their role in shaping the narrative. Militaries must establish a unified command structure for SC, ensuring coherent messaging across all channels, both domestically and internationally, to build and maintain credibility in a complex information environment. Adapting to the dynamic and contested nature of the information age requires agility and sophisticated strategies to counter misinformation and maintain a competitive edge in the cognitive domain, all while upholding ethical considerations of transparency, accountability and respect for truth.

★★★

Lt Col Akshat Upadhyay is currently serving with HQ IDS. He has a Bachelors in Electronics and Telecommunication, Masters in History as well as Political Science and an MPhil in Defence and Strategic Studies. He has authored numerous peer-reviewed papers as well as op-eds and articles in prestigious national and international publications on the issues of home-grown radicalisation, lone wolf terrorism, social media mobilisation, IW and emerging and niche technologies. His first book on India's Coercive Diplomacy against Pakistan (KW Publishers) has been well received and his second book on Absorption of Disruptive Technologies in the Indian Armed Forces is being published. He was also a Research Fellow At MP-IDSA where he wrote extensively on disruptive technologies, non-contact warfare and semiconductors.

NOTES

1 *Matthew P Anderson, "NATO Nuclear Deterrence: The Warsaw Summit and Beyond," Connections QJ 15, no 4 (2016): 5-30.*

2 *Jack L Snyder, The Soviet Strategic Culture: Implications for Limited Nuclear Operations (Santa Monica: RAND, 1977), https://www.rand.org/content/dam/rand/pubs/reports/2005/R2154.pdf.*

3 *Elaine Scarry, "The Extortionist's Doctrine," Boston Review, 26 September 24. https://www.bostonreview.net/articles/the-extortionists-doctrine.*

4 *Graham Allison and Philip Zelikow, The Essence of Decision: Explaining the Cuban Missile Crisis (Hoboken: Pearson PTR, 1999), 34-40.*

5 *Author's own definition.*

6 *James P Farwell, Persuasion and Power: The Art of Strategic Communication (Georgetown: Georgetown University Press, 2012), 10.*

7 *Garth S Jowett and Victoria O'Donell, Propaganda and Persuasion (Washington DC: Sage Publications, 2011), 40-56.*

8 *Taylor Downing, "D-Day deception Operation Fortitude: The World War Two army that didn't exist," BBC, 01 June 2024. https://www.bbc.com/culture/article/20240531-d-day-deception-operation-fortitude-the-world-war-two-army-that-didnt-exist.*

9 *Robin Brown, "Information Operations, Public Diplomacy & Spin: The United States & the Politics of Perception Management," Journal of Information Warfare, Vol 1, no 3 (2002): 40-50.*

10 *Farwell, Persuasion and Power: The Art of Strategic Communication, 16.*

[11] *US Joint Chiefs of Staff, Joint Staff, Military Information Support Operations, Joint Publication 3-13.2, https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading Room/Joint_Staff/Military_Information_Support_Operations.pdf.*

[12] *US Joint Chiefs of Staff, Joint Staff, Military Deception, Joint Publication 3-13.4, https://jfsc.ndu.edu/Portals/72/Documents/JC2IOS/Additional_Reading/1C3-JP_3-13-4_MILDEC.pdf*

[13] *US Joint Chiefs of Staff, Joint Staff, Joint Doctrine for Operations Security, Joint Publication 3-54, https://apps.dtic.mil/sti/tr/pdf/ADA357528.pdf.*

[14] *US Army, Army Public Affairs, Army Public Affairs: Telling the Army Story, https://www.army.mil/publicaffairs.*

[15] *Donald P Wright, "Deceiving Iraq in Operation Desert Storm," in Weaving the Tangled Web: Military Deception in Large Scale Combat Operations ed Christopher Rein, (Fort Leavenworth: Army University Press, 2018), 215-230.*

[16] *US Army, Army Public Affairs, Army Public Affairs: Telling the Army Story, https://www.army.mil/publicaffairs.*

[17] *Sam DiBella, "Book Review: The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power by Shoshana Zuboff," review of The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, by Shoshana Zuboff, London School of Economics Blog, November 4, 2019.*

[18] *Robert Westport, "A bullet still sends a message…," Project on Asymmetric Narrative Approaches, Medium Blog, 21 March 2016. https://medium.com/project-on-asymmetric-narrative-approaches/a-bullet-still-sends-a-message-8612c40dbe78.*

[19] *Roger Cohen, "In a World Changed by Oct. 7, Hatred Is Winning," The New York Times, 07 October 2024. https://www.nytimes.com/2024/10/07/world/middleeast/israel-palestinians-war.html*

[20] *Major Christopher Telley, "The Influence Machine: Automated Information Operations as a Strategic Defeat Mechanism," The Land Warfare Papers, The Institute of Land Warfare, no 121, October 2018. https://www.ausa.org/sites/default/files/publications/LWP-121-The-Influence-Machine-Automated-Information-Operations-as-a-Strategic-Defeat-Mechanism.pdf*

[21] *Ibid.*

[22] *Akshat Upadhyay, "Do-It-Yourself (DIY) Warfare: A New Warfighting Paradigm," Strategic Analysis, Volume 48, no 1, 2024, 15-32.*

[23] *David Lay Williams, "Plato's Noble Lie: From Kallipolis to Magnesia," History of Political Thought, Vol 34 no 3 (2013): 363-392.*

[24] *Kenneth R Allan, "Marshall McLuhan and the Counterenvironment: "The Medium Is the Massage"," Art Journal, Volume 73, no 4 (2014): 22-45.*

[25] *Richard Rorty, "Is Truth a Goal of Enquiry? Davidson vs Wright," The Philosophical Quarterly, Vol 45, no 180 (1995): 281-300.*

[26] *Neil Postman, "Propaganda," ETC: A Review of General Semantics, Vol 36, no 2 (1979):128-133.*

199-211

ATMANIRBHAR BHARAT: TOWARDS BUILDING A CREDIBLE DEFENCE AGAINST IEW

Gp Capt Kancherla Arun Kumar

"Faith is of no avail in absence of strength. Faith and Strength, both are essential to accomplish any great work."

- Sardar Vallabh Bhai Patel

Abstract

Modern weapon systems predominantly have embedded Information and Communication Technology (ICT) devices. Today network centric operations are a norm considering the usage of smart weapons systems, autonomous systems and remotely operated / controlled system. In the present situation, majority of military acquisitions have been from global manufacturers. These systems are susceptible to IEW attacks and pose a serious concern for the national security. The geopolitical situation is dynamic and the coalitions and collaborations are not permanent. It is all a 'marriage of convenience'. Cooperations and collaborations are promoted by many developed countries purely to further their geopolitical aspirations. Inequality, in any sphere, between the two partners tilts the balance more in favour of the technologically developed nation. The other partner would be at the mercy of the developed nation in absence of credible negotiating instruments. Bharat has today realized its potential and strives to maintain its strategic independence and hence wants to be self-reliant and self-

sufficient as far as possible. Defence industry is one such area where the government has initiated many steps to have greater self-reliance. The initiatives aim to give greater autonomy to the nation in terms of both hardware and software. Atmanirbharta in the field of design and development of electronic equipment would play a major role in building a credible defence against IEW attacks.

INTRODUCTION

It is once in a long time that one would come across news like 'Pager Attack'. The recent event where more than 3000 pagers blew up injuring or killing the owners of the pagers. The pager attack was followed immediately with an 'Walkie-Talkie attack' where personal communicators exploded killing many people. News reports and studies suggest that most of the victims were Hezbollah members and the pager attack and the Walkie-Talkie attack was planned and triggered by Israeli intelligence agencies. It is too early to arrive at conclusions. However, the incident does highlight some important aspects of Information Warfare. It is believed that the Hezbollah was using these low tech 'pagers' and 'walkie-talkies' to guard against cyber-attacks on the sophisticated communication equipment which can be traced and intercepted. However, even these so called 'low tech' equipment were not immune to IW attacks. The whole incident presented an excellent case study for research scholars, intelligence agencies and other law enforcing agencies. There are lot of lessons to be learnt from this incident.

Another recent event that garnered interest was the Microsoft Windows systems crash worldwide owing to a glitch during the software update by 'Crowd Strike Holdings Incorporation', a cybersecurity firm. The so-called security update resulted in shutting down of many essential services across the world. Some of the major services affected by the crash were banking services, airline services, hospitals & healthcare services etc.

Stuxnet Computer Worm was in news a few years back as a malware that was supposedly developed to attack Iran’s nuclear facilities. It is believed that it has since mutated and spread to other industrial and

energy-producing facilities. Such malwares are a big threat to critical production / industrial facilities that use Supervisory Control and Data Acquisition (SCADA) systems or the Programmable Logic Controllers (PLCs) for controlling, monitoring, and analyzing industrial devices and processes. PLCs and SCADA systems play a critical role in modern industrial automation.

For those in the field of Information Warfare (IW), these events bring forth aspects needing further focus. While the first and third events are considered to be an act of aggression by parties in conflict, the second event is an example of how internal players can cause major breaches in the systems. The incidents also indicate that the threat can be through either hardware or software or through both. One of the most glaring facts is that in all the three cases the victim parties were dependent on external sources for the hardware and the software.

RELEVANCE OF THESE EVENTS FOR BHARAT AND ATMANIRBHARTA

Though our country holds rich heritage and fathomless knowledge in our ancient texts, the foreign invasions and foreign rule has pushed back the country from a prosperous country to a third world country by the end of foreign rule. Since independence the country has grown and improved its economic status. The industry has grown and the manufacturing sector is catching up the pace with the developed countries. However, there is a lot to be done in the field of technology, especially when it comes to development of indigenous components for critical systems. Some glaring examples that point at the roadblocks in our technological growth are absence of development in core technologies like Semiconductor chip design, miniature / microelectronic components etc. which are basic building blocks of the computer & control systems that are the brains of the smart systems. Any electronic gadget that is assembled in our country has some critical components that are imported as the country lacks depth in design and development of such critical components.

In absence of some indigenous core technologies, our R&D organisation and private industry depends predominantly on foreign technology giants for supply of these core components. In most of the cases, the foreign players have non-disclosure agreements and restrictive clauses which inhibit greater insight into the technology used. Governments of the most of the developed countries control the Intellectual Property Rights (IPR) of the critical technology and discourage Transfer of Technology (ToT) of such technology.

Urgent operational requirements necessitate development or acquisition of weapon systems, the R&D organisations and their private suppliers are forced to integrate these systems at the cost of greater insight into the systems. In such cases trust predominantly plays a major role in finalizing the deals / contracts. There are some safeguards that have been introduced in the Defence Acquisition Procedures 2020 (DAP 2020, Chapter VIII, Acquisition of Systems Products and ICT Systems). However, these safeguards are predominantly based on the trust factor where the supplier / vendor provides the requisite certificates (as per Appendix B to Chapter VIII of DAP).[1] It is necessary to understand that these safeguards may not be sufficient from strategic point of view. As long as we are dependent on external agencies for critical core technologies, we are vulnerable to external pressures and threats.

While speaking at the Cyber Security Conclave held by the Cyber Security Association of India, Dr. VK Saraswat, ex-DRDO head and member of the Niti Ayog, aptly highlighted that 'security begins with a trustworthy hardware'.[2]

STRATEGIC INDEPENDENCE & AUTONOMY

The current geopolitical situation is fluid and there are lot of groupings. There are many so called friendly nations that have friendly relations even with those countries that have difference of opinion with Bharat. For example, Bharat and the United States of America have an enabling agreement Communications Compatibility and Security Agreement (COMCASA) which facilitates interoperability between militaries and

sale of high-end technology. The US government shares this high technology with NATO members including Pakistan as 'global partner'. There is difference of opinions between the US and People's Republic of China. However, China and Pakistan have friendly relations. This is a good example of 'marriage of convenience', which indicates that there are no permanent friends or permanent adversaries. This uncertainty raises questions regarding certain trust based agreements and commitments by the concerned parties.[3]

Apart from the nation states, non-state actors (NSAs) too have an impact on the dynamics of the world. These NSAs, like NGOs, multinational companies, terrorist and religious groups, hackers etc. influence the economies of nations and their future course of action. There are instances where nation states have indirectly supported the NSAs to counter their adversaries.

This poses a major question regarding the degree of trust that exists between the Nations in the volatile, uncertain, complex and ambiguous (VUCA) World.

Bharat has, since independence, believed in non-alignment with the power blocs of erstwhile cold war era. The grouping still continues post the Cold War. However, the grouping in the present situation is more fluid and is governed by economic interests of different players. However, Bharat aspires strategic independence and autonomy to ensure that it has the right to choose a path that would be the best in interest of the Nation. The success of this particular approach necessitates greater self-dependence i.e., 'Atmanirbharta' on many fronts.

One such major front is development of indigenous core technologies for ICT devices that are predominantly used across the spectrum.

SUPPLY CHAIN

A preliminary study of the first incident described above discusses the possibility of introduction of the explosive material and malicious codes into the pagers or the personal communicators somewhere enroute from

the manufacturer to the consumer. The supply chain was meticulously studied, identified, and compromised. The execution of the attack was controlled by the Israeli agencies through the malicious code. This points towards the need for a robust and secure supply chain for the products or the components being imported.

Supply chain disruptions could also happen due obsolescence of some products or components. Technology growth and changes in the last few decades follows the Moore's Law. This pace of growth results in faster rate of obsolescence of modern equipment as the industry adapts to the newer technology for performance enhancement and economic reasons. In such a scenario, there might be situations where alternate sources of these products or components are explored. These sources could be second hand equipment or substitutes developed by a lesser known third party. How far these sources are vulnerable to compromise, by vested parties, is a question that one needs to ask before procuring products or components from them. This increases the risk factor in terms of IEW attacks or cyber attacks.

Strategic grouping and geopolitical scenarios might also cause disruptions in supply chain of critical products or components. Sanctions by source countries might restrain the OEMs from supplying the products and components during critical stages to put pressure on the government to tow their views or line. In absence of support from the OEMs, there might be situations where regular updates (essentially for software) are not available and one is forced to operate with outdated systems with vulnerabilities that are publicized on open sources like internet. In case of hardware, as discussed above, a third-party supplier is explored to provide the product thus creating weak links in the supply chain.

COMPLEXITY OF SYSTEMS

State-of-art weapon systems consist of systems of systems and their architecture is complex in nature. Different embedded systems are used in integration and manufacturing of complex weapon systems. These

systems are used for operations and maintenance of the systems. Each system comprises of thousands of electronic components. Further, these systems come with custom made firmware and software. Any vendor would not like to share the software code for obvious reasons; therefore, 100 percent security evaluations of such systems is extremely difficult. Exploits like logic bombs and trojan horses are extremely stealthy and difficult to identify and neutralize.

Further, there are systems that require regular updates to cover vulnerabilities, or for health monitoring etc. There are systems which necessitate connecting the unit to internet for patch updates or for live health monitoring from remote locations. Such requirements increase the risk factor.

Penetrative testing by experts may help in identifying some of the vulnerabilities but it is very difficult to identify exploits like the logic bombs. Another relevant question that arises is the need for resources to carry out complete system analysis after each update. Over and above such risks, the risk of inadvertent damage to systems is possible as was seen in the case of 'Crowd Strike' security services. As mentioned earlier, there are some safeguards in DAP 2020 for acquisition of such systems, but these safeguards depend on 'trust' and reputation of the OEMs.

The three incidents described at the beginning of the paper reiterate the need for strengthening self-reliance in both software and hardware. The vulnerabilities exist in both software and hardware.[4] Further, with advent of Artificial Intelligence (AI) and it’s usage in advance weapon system poses a major challenge in terms of assessing cyber security aspects of the systems.

NEED OF THE HOUR

From above we can come up with the following major issues that pose challenges to Bharat:

- Bharat predominantly depends on imports for complex weapon systems.

- Most of the modern weapon systems are system-of-systems integrated using processors and computing devices. This means that the systems comprise of customized computing and software/ firmware. OEMs are not forthcoming in sharing the technology behind the systems.
- Bharat aspires to attain strategic independence and hence is balancing its relationship with the different power centers of the world. This balance comes at a cost – 'Trust Deficit'.
- Dynamics of the geopolitical situation in the World poses multiple challenges and impact supply chains. Having a credible supply chain is not guaranteed.
- Complexity of the latest weapon systems makes it very difficult to carry out a comprehensive cyber safety assessment of the system.

All these issues, in one way or other, can be related to IW. These issues create vulnerabilities for Bharat and there is a need to address them as comprehensively as possible. In the present scenario, defensive IW solutions can be considered to be more of tactical nature. The major efforts are directed at neutralizing the attack vectors by building multi-layered protection.

However, there is a need to focus on strategic solutions to counter threats that may not directly appear to be factors in IW. The cases mentioned here are some of the examples that indicate towards some methods which highlight ingenuity of human mind and use of unthinkable tactics to disable systems of adversaries or even cause physical damage to the systems.

IW is not a normal convention form of warfare. The threat from such warfare exists throughout, at all times, irrespective of visible geopolitical relationships. These tactics can be used even by so called 'friendly' partners as negotiation instruments to gain favourable policy decisions in their favour. Manipulation of industrial facilities, economic activities

(like banking, airlines etc.) can be resorted to by parties with vested interests at any time without declaring any direct conflict with the nation. Declaring such acts as intentional action is difficult to prove.

This brings into focus the need for greater self-reliance on design, development and manufacturing of critical components of processors, control units and other ICT devices that are vulnerable to IW. Controlled design, development and manufacturing of such devices with better mechanism to monitor and oversee the activities would ensure better security in the fast developing digital and cyber domain. A robust industry would also give Bharat an opportunity to transform into a major exporter.

ENDS, WAYS AND MEANS – TARGET ATMANIRBHARTA

Having said that, it is necessary to understand that achieving strategic independence and Atmanirbharta is not an easy journey. It involves different stages starting with establishment of strategic intent, formulation of strategy, implementation of the strategy and then evaluating the strategy. This is in iterative process where feedback from each stage is given to the earlier stages to facilitate mid-course path corrections if required or change of strategy in some cases. Dynamic interactions between the nation states and other players would mean that there would be constant need for re-visiting the strategies and effecting course corrections where required.

Government of Bharat has taken many policy decisions in direction of attaining self-reliance. Some of the prominent decisions for Defence are:

- 'Make in India' thrust – encourage FDI through steps like increasing the investment limit to 76 percent, tax incentives etc.
- Revision of Defence Procurement Procedures (DPP) giving rise to the DAP 2020. This has been refined further over time to introduce clauses from time to time. DAP 2020 introduced concepts like strategic partnership to enhance participation of Indian industry. Higher priority has been given to Indigenous systems over global acquisition.

- Establishment of dedicated Defence Corridors in UP and Tamil Nadu to encourage private defence industry.
- Innovation for Defence Excellence (iDEX), an operational framework of the Defence Innovation Organisation (DIO). DIO is a Special Purpose Vehicle (SPV) under the aegis of the Department of Defence Production, MoD. There are many initiatives like having iDEX challenges to encourage MSMEs and start-ups to participate in the innovation drive etc.

The above are but some of the many policy decisions taken by the Government to encourage indigenization and innovation in the field of Defence Equipment. Further, the government has also introduced some reforms like reorganisation of the erstwhile ordinance factories. Review and reorganisation of the Defence R&D Organisation is in progress.

TARGET SEMICONDUCTOR DEVICES – A MAJOR STEP IN ENHANCING IEW DEFENCE

India Semiconductor Mission (ISM) was launched, in 2021, by Ministry of Electronics and Information Technology (MeITY). It aims to establish a strong semiconductor ecosystem in the country. it is a specialized and independent business division within the Digital India Corporation that aims to build a vibrant semiconductor and display ecosystem to enable India's emergence as a global hub for electronics manufacturing and design.

As a part of the initiative, ISM has conducted seminars, webinars, workshops, exhibition and conferences in name of SEMICON India. The first SEMICON was held in 2022. The last SEMICON was held in September 2024. The conference had discussions on various aspects like training, supply chain management, latest manufacturing technology etc. Industry-academia interactions during the conferences also contribute towards better synergy.

Organisations like Electronics Sector Skills Council of India (ESSCI) have been conducting workshops and training sessions for Semiconductor manufacturing.

MeITY had earlier introduced a Design Linked Incentive (DLI) scheme for fostering semiconductor design companies. This is akin to the Production Linked Incentive (PLI). Another scheme which encouraged manufacturing of specified electronic goods is the Scheme for Promotion and Manufacturing of Electronic Components and Semiconductors (SPECS).[5]

SOFTWARE AND FORENSICS

Bharat has been recognized for its prowess in software development. However, there is a lot to be desired for addressing IEW issues that have been discussed. Programming for military systems requires specific skills. Skill development is necessary in such areas.

C-DAC developed the Bharat Operating System Solutions (BOSS). Similarly, a start-up incubated by IIT Madras has developed Bharat OS. These kinds of initiatives would facilitate customization of software for the indigenously developed hardware. There is a need to coordinating agency that would bring together various software development agencies and contribute towards indigenization. Today there are multiple startups having talent and capabilities. There is a need to tap these startups in contributing towards 'Atmanirbharta'. Different challenges being hosted under iDEX is a crucial step in this direction.

The Indian Armed Forces too have been working towards autonomy in the software being used for various systems in the Armed Forces. IAF has specific agency for indigenous software development required for advanced weapon systems. The institute is not only involved in software development but also involved in activities like testing and evaluation of software.

Cyber forensics is another area which would contribute immensely towards understanding various exploits and threats. Institutes like National Forensic Science University (NFSU) and Rashtriya Raksha University (RRU) have been recognized as institutes of national importance and are being empowered to work in cyber security and cyber forensics fields.

A major step taken in this direction is setting up of Defense Cyber Agency (DCA), which is a tri-service agency for providing direction on cyber security aspects. Preparation of cyber strategy, doctrine and policies for the Armed Forces and coordination with other cyber security agencies.[6] One of its primary responsibilities includes policy on eliminating the use of foreign hardware and software in the Indian Armed Forces. Coordination between the Cyber Security Division of MeitY, Cyber and Information Security (C&IS) division of MHA etc. would reap dividends in achieving autonomy in field of Cyber Security.

CONCLUSION

Today as we are moving away from conventional warfare to a multidimensional warfare scenario. Independent or Joint, both types of operations are graduating into Network Centric Operations. Smart Weapon systems, autonomous systems and remotely controlled systems are all part of an effective Combat situation. Embedded ICT devices of such systems are targets for IEW attacks. Susceptibility of such targets to IEW attacks increases multifold if the user does not know the system well. This happens in most of the cases where the systems are imported and ToT is not part of the acquisition contract. Lack of in-depth knowledge hampers building of credible defence against such attacks. Indigenous systems would facilitate better understanding and control of the devices. The degree of threat decreases multifold if the system is indigenous. It also ensures a healthy supply chain and flexibility for scaling up the production as and when required. An indigenous design, development and manufacturing capability would facilitate better monitoring of the complete process. This would enable better governmental control of technology and also ensure that Bharat defends itself from IEW threats that arise due to dependence on technology and components on others This would also strengthen Bharat to resort to offensive IEW tactics, if and when required, in defense of its national interest and security. Atmanirbharta strengthens the national desire to be strategically

independent. This enhances the national power and contribute to overall growth of the nation.

★★★

Gp Capt Kancherla Arun Kumar is a commissioned officer in the Aeronautical Engineering branch of IAF. He has a Bachelor's Degree in Computer Science and Engineering (BE Comp Sc & Engg.). He has a master's degree in Quality Management (MSQM) from BITS Pilani and HRM (MA HRM) from Jamia Millia Islamia. He is a Fellow of the Institution of Engineers (FIE), India and a Member of the Aeronautical Society of India (MAeSI). He is also an alumnus of the College of Defense Management, Secunderabad. During the course of his service, the officer has gained vast experience in maintenance of ISR equipment. He also has expertise in project management and defence acquisition.

NOTES

1 *Defence Acquistion Procedures 2020, Ministry of Defence, Bharat*

2 *Dr. VK Saraswat; Cyber Security (talk during the Cyber Security Conclave, Vigyan Bhavan, New Delhi, 2019)*

3 *Lt. Gen Anil Ahuja (Retd.); Prospects of India – US Defence Cooperation (National Security Vol.IV Issue II, Apr-June 2022, pp 125-138, Vivekananda International Foundation)*

4 *B Poornima; Cyber Preparedness of the Indian Armed Forces (Journal of Asian Security and International Affairs,IO(3)301-324, 2023)*

5 *Giri Hallur, P Ashok; Semiconductor Sankalp: A Vision for India's Tech Dominance (Intelligent Computing and Control for Engineering and Business Systems 2023, IEEE)*

6 *Arindrajit Basi, India's International Cyber Operations: Tracing National Doctrine and Capabilities (United Nations Institute for Disarmament Research, 2022)*

Bibliography

1 *India's Place in the World, Policy Watch Volume XII, Issue 5, May 2023, New Delhi*

2 *Non-state Actors Playing Greater Roles in Governance and International Affairs, Memorandum, National Intelligence council, US, 5 Jul 2023.*

3 *Pranay Kotasthane, Arjun Gargeyas; Harnessing Trade Policy to Build India's Semiconductor Industry, Hinrich Foundation, Advancing Sustainable Global trade, May 2022*

ADVISORY BOARD & EXECUTIVE COUNCIL
CENJOWS

Printed and published by Maj Gen (Dr) Ashok Kumar, VSM (Retd) on behalf of Centre for Joint Warfare Studies (CENJOWS), 301, B-2 Wing, 3rd Floor, Pt Deendayal Antyodaya Bhawan, CGO Complex, Lodhi Road, New Delhi-110003, and Print at Xtreme Office Aids (P) Ltd. Plot No.11, Basement Bhanot Building, Shopping Complex, Nangal Raya, New Delhi-110046

Editor : **Maj Gen (Dr) Ashok Kumar, VSM (Retd)**

CENJOWS

CENTRE FOR JOINT WARFARE STUDIES

(Web site: https://www.cenjows.in - Email: cenjows@cenjows.in / cenjows@yahoo.com)

APPLICATION FOR MEMBERSHIP FOR INDIVIDUALS/ORGANISATIONS
(EFFECTIVE WEF 01 SEP 24)

(TO BE SUBMITTED ONLINE ONLY, ONLY APPLICABLE DETAILS AS PER CATEGORY TO BE FILLED)

To,
The Director General
Centre for Joint Warfare Studies (CENJOWS)
301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi-110003

Dear Sir,

1. Please register me as a **Life☐/Annual☐** member of the Centre for Joint Warfare Studies (CENJOWS).

2. I undertake to abide by the Rules and Bye Laws of the Institution.

3. **Life Membership/ Annual Membership (Individuals).**

Common to All.

(i) Name in full (in Capitals)……
(ii) **Address:-**
Office/Unit……
……
Pin Code …… Phone No …….... Mobile No. ……..
Email ……
(iii) **Permanent/Residential Address**
……
Pin Code …… Phone No …….... Mobile No. ……..
Email ……

(b) **Additional Inputs (in case of Serving/Retired Defence Personnel)**

(i) Parent Service Army/Navy/Air Force/Civil Services ……
(ii) Personal Number…….…… (iii) Rank/ Designation……..……

(iv) Name in full (in Capitals) …… ……..
(v) Decorations ……..... (vi) Appointment ……..……
(vii) Date of Commission ……
(viii) Date of superannuation……
(ix) Date of Seniority (if different form date of Commission) ……..
(x) Date when qualified in DSSC/TSOC ……...

(c) Areas of expertise or interest:-
(i) ……..……..……
(ii) ……..

(d) Any other information that may be of interest to the CENJOWS (including important exposures):-
……
……

(e) Name of College and University where Studying (in case of students) ……
……..

(f) The current membership rates for Individuals are as under:-

(i) Life membership:-
(aa) Serving/Retired Officers (For 20 years) - Rs 2,500/-
Note: 50% discount will be given to the following categories:-
(aaa) Officers qualifying in DSSC /TSOC if apply prior to completion of the course. All service HQs will be intimated for this provision.
(aab) Officers applying within two years of commissioned service.
(aac) Officers applying within two years of superannuation.
(ab) Civilians (For 15 years) - Rs 15,000/-

(ii) (aa) Annual Membership (For one year) - Rs 1000/-
(ab) For University/ College Students (For one year)- Rs 500/-

(iii) Institutional Membership (For 15 years):-
(aa) Non Corporates Membership - Rs 30,000/-
(ab) Corporates Membership - Rs 50,000/-

(g) Proof of my identity (Copy of passport/Voter ID Card/Adhaar Card) is attached for approval of membership **(JPG/ PNG Format).**

(h) Two stamp sized photographs for Life membership card (Individuals) **(JPG/ PNG Format)**.

(j) Payment by NEFT/ Digital as per details given below:-

Name of Organisation	: CENJOWS
Bank Name	: CANARA BANK
Branch Address	: **KASHMIR HOUSE**, NEW DELHI-110011
IFSC Code	: CNRB0019122
A/c Type	: SAVING
A/c No.	: 91222160000046

(Please attach the proof of payment)

4. **Institutional Membership (Institutions/ Organisations)**
(Provision of Lifetime Membership only)

(a) The particulars of our Institution/ Organisation are given below:-

(i) Name of the Institution/ Organisation ……

(ii) Nature of Activity/ Scope of Work ……

(b) Address:-

……..……..……

……

Pin Code ……. Phone No ……..... Email……..……

(c) Name of Head of the Institution ……....

Phone No **……** Mobile No ……....Email ….....

(d) Name of Administrative Officer (for Correspondence purposes) ……..

……..……

Phone No …… Mobile No …… Email ……..…

(e) Areas of expertise or interest:-

(i) ……..……

(ii) ……

(iii) ……..

(f) The current membership rate for Institutional Membership are (For 15 years):-

(aa)	Non Corporates Membership	-	Rs 30,000/-
(ab)	Corporates Membership	-	Rs 50,000/-

(g) Payment by NEFT/ Digital as per details given below:-

Name of Organisation	: CENJOWS
Bank Name	: CANARA BANK
Branch Address	: **KASHMIR HOUSE**, NEW DELHI-110011
IFSC Code	: CNRB0019122
A/c Type	: SAVING
A/c No.	: 91222160000046

(Please attach the proof of payment)

(h) Two membership cards will be issued to the Institution/Organisation.

5. I Certify that the details forwarded above are correct. I shall follow the amended rules and regulation as intimated.

Place : **……** Yours faithfully,

Date : **……...**

FOR OFFICE USE ONLY

Identity Card/Document No: **……..** To be verified by Secretary (Secretary to speak on telephone to confirm the credentials).

New Delhi

Date …….. Secretary, CENJOWS

Accepted/Rejected

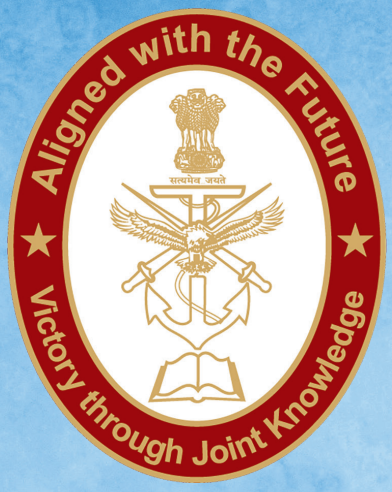
Membership Number **…….**
(Interaction to be held with DG, CENJOWS for Institutional Life Time Memberships)

Place: New Delhi

Date: …….. Director General CENJOWS

Synergy Journal Release by CDS on 03 Oct 24

Synergy Journal Release by CISC on 22 May 24



CENJOWS

(Established : 2007)
Room No.301, B-2 Wing, 3rd Floor
Pt Deendayal Antyodaya Bhawan
CGO Complex, Lodhi Road
New Delhi – 110003 (INDIA)
Telephone Nos : 011-24364881, 24366485
Fax : 011-24366484
Website : www.cenjows.in
E-mail : cenjows@cenjows.in, cenjows@yahoo.com

Connect

https://www.cenjows.in https://www.youtube.com@cenjowshqids7833 https://x.com/CENJOWS
https://podcasters.spotify.com/pot/show/cenjows https://podcasters.spotify.com/pot/show/cenjows
https://www.linkedin.com/comany/centreforjointwarfarestudies https://www.instagram.com/cenjowsindia/?hl=en