Warfare Without Borders: An Era of Asymmetric and Cyber Warfare

Lavpreet Sharma

INTRODUCTION

Wars can be lost and won in the mind and virtual spaces as much as in the physical battlespace.[1] Before launching its full-scale invasion in 2022, Russia executed large-scale cyber attacks on Ukraine's military infrastructure, targeting the Command-and-Control (C2) networks and air defence systems. The "Fox-Blade" malware attack, aimed at disrupting air operations and radar systems, was an early indication of cyber warfare being a key component of modern conflict. As a response, Ukraine swiftly sprang into action to strengthen its cyber security structure. The need of the hour was to maintain operational control using cloud-based systems despite the cyber attacks by Russia. Ukraine not only fortified its cyber defence but also launched an offensive by efficiently pitching drones like the Turkish Bayraktar TB2 in the battlefield to strike Russian ground targets, despite the Russian

Squadron Leader **Lavpreet Sharma** is a serving officer in the Indian Air Force.

1. Doctrine of the Indian Air Force IAP 2000-22, Cyber Warfare, p. 66.

air superiority. In order to counter this miniature (vis-à-vis a conventional fighter aircraft) yet lethal platform, the Russian forces arrayed Electronic Warfare (EW) tactics to disrupt the Ukrainian drone communications and Global Positioning System (GPS) signals. The war has established how combat drones can reap asymmetric advantage against even a technologically superior adversary, thereby proving to be credible force multiplier indeed.

Modern warfare has not even a remote resemblance to the erstwhile conventional battlefields. Gone are the days when militaries used to engage a known enemy within defined geographical dimensions, using orthodox weapons; conflict today intrudes into the economic, cyber, psychological and asymmetric dimensions. Hybrid warfare, an approach that combines conventional and non-conventional methods, has emerged as the foremost mode of conflict in the 21st century. Relevant examples comprise the frequent cyber operations, economic coercion, and maritime militia activities by China in the South China Sea, thus, creating strategic advantages for it without triggering a full-scale war. In view of this modern era of conflicts, the Indian Air Force (IAF) must evolve at a rapid pace; beginning with a thorough strategy to counteract hybrid threats, while ensuring that cyber infrastructure, EW systems and Air Defence (AD) networks remain operationally robust against even the most sophisticated adversaries.

FACETS OF HYBRID WARFARE

Hybrid warfare is a multi-sphere war tactic that encompasses:

(a) **Conventional Warfare**: Deployment of defence forces, to conduct operations on land, air and water. An example is the Indo-Pak War of 1971.

(b) **Cyber Warfare**: This includes hacking, electronic sabotage, and network disruption. Stuxnet, a cyber weapon attributed to Israel and the U.S., was used to sabotage

Iran's nuclear centrifuges, showcasing the effectiveness of cyber operations in modern conflicts.

(c) **Asymmetric Warfare**: The use of guerrilla tactics, proxy militias, and drone warfare. A notable case is of the Houthi rebels in Yemen, who employed low-cost drones to strike on the oil refinery of Saudi Arabia, causing significant economic and military disruption.

(d) **Information Warfare**: Propaganda, disinformation and psychological operations. The 2016 U.S. presidential election interference, attributed to Russian disinformation campaigns on social media, is a prime example of how perception warfare can influence the political landscape.

(e) **Economic Warfare**: Financial disruptions, sanctions and trade restrictions. The U.S.-China trade war illustrates how economic measures are used to weaken adversaries without a direct military conflict.

(f) **Political Warfare**: Espionage, legal manipulation and efforts to destabilise governments. The Cold War era proxy conflicts, where both the U.S. and the Soviet Union engaged in political manoeuvring to install favourable governments, are the classic example.

Cyber warfare and asymmetric warfare are the primary facets of hybrid warfare. They comprise attractive low cost war-waging models with blurred traditional boundaries and an expanded role for perception management. Thus, this article will be focussing on these two critical facets of the modern era warfare.

ASYMMETRIC WARFARE: DISRUPT, DECEIVE AND DOMINATE

> All warfare is asymmetric because one exploits an enemy's strengths while attacking his weaknesses.
>
> – Sun Tzu

The concept of asymmetric warfare has been around for centuries. An unprecedented Israeli attack nicknamed Operation Grim Beeper, exploiting evolving technology to explode hand-held pagers and walkie-talkies in two separate events across Lebanon and Syria,[2] resulted in 42 killed and thousands of Houthi militants injured.

The security set-up in which we operate nowadays is very fragile when it comes to proactive threat assessment and the number axes of approach that are to be defended. Regional powers are evolving their capabilities for asymmetric warfare by investing in Chemical, Biological, Radiological and Nuclear (CBRN) tactics. This evolving scenario warrants transformational breakthroughs in our perception about the existing military forces and the adaptation of new technologies to take the fight to the enemy.

With the Balakot strikes, the IAF redefined deterrence, proving that the best response to asymmetric threats is an equally asymmetric and decisive use of air power. It was a classic example of asymmetric air power: leveraging precision, intelligence and strategic surprise to neutralise threats beyond conventional engagement zones. Air power significantly shapes the dynamics of modern asymmetric conflicts, facilitating rapid engagement and precision strikes. Its ability to conduct aerial reconnaissance equips military forces with vital intelligence, enabling them to identify and monitor adversarial movements. This intelligence allows conventional forces to adapt their strategies effectively. On the one hand, air power serves as a tool of physical destruction of various centres of gravity of the adversary, while, on the other, it can influence public perception through psychological warfare,

2. "How Israel's 'Operation Grim Beeper' Rattled Global Spy Chiefs", *Financial Times*, December 28, 2024.

thus, playing a decisive role in reshaping the overall dynamics of conflict in asymmetric warfare.[3]

Challenges for Air Power Employment

It may appear that employment of air power in asymmetric warfare would be devoid of major challenges apart from the obvious counter-air operations by the adversary, however, the very nature of hybrid warfare presents numerous challenges that affect operational effectiveness.

Unambiguous target identification is one of the significant challenges. Irregular combatants often blend effortlessly with civilians, thereby complicating the gathering of intelligence and increasing the risk of collateral damage. Logistical limitations too present challenges in remote or hostile environments, limiting air power's reach and effectiveness. Counter-measures such as EW or anti-aircraft systems, challenge the traditional operational approaches of air power. Hence, the ever-evolving asymmetric warfare demands adaptive strategies.

Mitigating the Novel Challenges

Operations in asymmetric warfare warrant continuous transformation of tactics, accentuating the need for flexible air assets that can operate across various environments and against non-conventional adversaries. This adaptability can significantly modify the balance of power[4]. A crucial lesson learnt from the employment of air power in asymmetric conflicts is the necessity of target identification, precision strike and minimum collateral damage. This sensitivity not only preserves civilian lives but also aims to maintain local support. Successful engagements in

3. "The Role of Air Power in Asymmetric Warfare Dynamics", July 24, Edition hosted on https://totalmilitaryinsight.com
4. Ibid.

asymmetric conflicts highlight that synergy between air and land forces optimises overall effectiveness, ensuring that air power plays a cohesive role in strategic objectives.

The IAF needs to integrate the following asymmetric strategies to enhance operational effectiveness:

(a) **Swarm Unmanned Aerial Vehicle (UAV) Tactics**: Low-cost drone swarms can overwhelm enemy air defences, disrupt radar systems and conduct precision strikes without risking human pilots.

(b) **Electronic and Cyber Warfare Integration:** Jamming enemy communications, disrupting satellite-based navigation and launching cyber attacks on adversary C2 networks can degrade an opponent's ability to conduct coordinated air operations.

(c) **Defensive Asymmetry**: While offensive asymmetry is crucial, defensive measures are equally important. Camouflaging assets, deploying decoy systems, and using Artificial Intelligence (AI)-driven deception techniques can mislead adversaries as well as protect critical infrastructure. Counter unmanned aerial systems have been acquired to mitigate enemy drone attacks.

(d) **Special Operations and Cyber-Aided ISR**: Cyber Intelligence, Surveillance, Reconnaissance (ISR) enabled special forces' operations can provide real-time battlefield intelligence, allowing for precision strikes against high-value targets.

The IAF must defend its networks just as aggressively as it does its airspace. Cyber intrusions can cripple air operations before a single missile is fired. As brought out earlier, the understanding of the cyber space, its associated vulnerabilities and ways to exploit them, need special emphasis.

CYBER SPACE: OMNIPRESENT ELEMENT OF HYBRID WARFARE

> Iran has been accused of conducting cyber espionage operations targeting US Air Force bases in the Middle East, seeking intelligence on drone operations and air defence networks.
>
> Taiwan has reported cyber attacks on its air defence systems, believed to be part of China's broader information warfare strategy.
>
> Israel's Cyber Directorate actively countered Hamas and Hezbollah militant groups using AI-driven detection and offensive cyber operations.

These headlines from contemporary news websites across the world unequivocally point towards the ever-evolving cyber warfare and the challenges pertaining to cyber security. Cyber warfare has brought a paradigm shift in the fundamental character of war, aptly making it the fifth domain of warfare (land, sea, air and space being the other four domains), thereby *necessitating a review of doctrines and operational concepts*.

The IAF is employing the Operational Data Link (ODL) to enable seamless network-centric operations through integration of all combat systems on this ODL[5]. With the ODL configured, all our platforms, the 4.5 Gen Tejas and Rafale, 5th Gen manned Advanced Medium Combat Aircraft (AMCA), unmanned Autonomous Unmanned Research Aircraft (AURA) ISR systems and surface-based weapon systems would use ODL for data exchange from the Integrated Air Command and Control system (IAACS), between platforms and C2 centres to increase situational awareness, reduce sensor-to-shooter time and, thereby, enhance the efficacy of operations. A future war in our context will have a pronounced cyber threat due to this aspect of networking.

5. Air Marshal Ramesh Rai, VM (Retd), "Combining Cyber with Air Force Operations".

Cyber Warfare: Vulnerabilities and Methods of Capability Enhancement

National Cyber Security Gaps:

(a) **Dependence on Foreign Technology**: Reliance on imported defence software and hardware increases the risks of backdoor infiltration. Foreign vendors may discontinue support, leaving critical infrastructure with unpatched vulnerabilities.

(b) **Fragmented Cyber Policies**: Lack of coordination among the military, intelligence and government agencies may lead to conflicting cyber policies, causing confusion and weak enforcement.

(c) **Emerging Cyber Espionage Threats**: State sponsored hacking groups from China and Pakistan increasingly target Indian networks. The major *modus operandi* comprises email-based phishing attacks and planting malware through unpatched software.

IAF Specific Cyber Threats

(a) **IAF Network (AFNET) Security**: Though encrypted, the AFNET faces threats from zero-day vulnerabilities which are software/hardware/firmware flaws that are unknown even to the vendor and, thus, remain unpatched.

(b) **IACCS Infrastructure Weaknesses**: The IACCS is the critical hub for managing air operations, real-time surveillance and decision-making in the IAF. A cyber attack on the IACCS could paralyse AD and thereby, severely impact national security.

(c) **Drones and UAVs**: Enemy EW systems could hack or jam UAVs, leading to real-time intelligence leaks and, subsequently, may hijack them or force then to crash.

Enhancement of Cyber Warfare Capabilities

IAF views cyber operations as an integral part of all military operations. We are continuously working to upgrade these capabilities at all times.[6]" Our conventional war-fighting capability needs to be enmeshed with the cyber domain in both defensive and offensive sense. While certain tools are already being implemented, there is a need to further enhance cyber security by including the following strategies:

(a) **Zero Trust Architecture (ZTA) Implementation**: The IAF must adopt a zero trust approach, ensuring that every device, user and application is continuously verified before being granted access. Adopting the ZTA means assuming that no one, either inside or outside the network, is to be trusted even by default. Access controls, authentication, and authorisation must be verified continuously. This approach limits the risk of insider threats and helps protect sensitive data.

(b) **Artificial Intelligence Based Threat Detection**: Artificial Intelligence (AI) and Machine Learning (ML) can be used to boost cyber security by identifying anomalies in real-time, predicting cyber threats and automating responses to attacks. Nations with strong AI-enabled cyber capabilities can detect and counteract cyber threats faster, maintaining operational readiness.

(c) **Red Teaming and Cyber Resilience Exercises**: Regular cyber security drills, penetration testing, and red teaming exercises can help the IAF identify vulnerabilities and improve the defensive posture. These exercises should simulate real-world cyber threats, including electronic warfare scenarios.

6. Air Chief Marshal Vivek Ram Chaudhari, PVSM AVSM VM ADC (Retd), in an exclusive interview with the Editor-in-Chief of *SP's Aviation*.

(d) **Securing the Supply Chain**: Stronger vetting of defence contractors, end-to-end encryption and block-chain technology for supply chain integrity can mitigate the risks of compromised components.

(e) **Strengthening Network Security:**

(i) **Firewalls and Intrusion Detection Systems (IDS):** Implement robust firewalls and Intrusion Detection/ Prevention Systems (IDPS) to detect and prevent unauthorised access to sensitive systems/networks.

(ii) **Network Segmentation:** Isolate critical systems and networks from less sensitive ones to limit the potential spread of cyber attacks. For instance, air defence systems, communication networks, and weapon systems should be on separate networks to prevent cross-contamination in case of a breach. Migration of critical operations systems to the Red Network is one such initiative that has been implemented in the IAF recently.

(f) **Data Encryption and Integrity:**

(i) **End-to-End Encryption:** Use strong encryption protocols for communication and data storage to protect sensitive information such as operational plans, intelligence, and weapon systems data.

(ii) **Integrity Verification:** Regularly verify the integrity of critical data to detect any unauthorised modification. Implement techniques like checksums, hashes, or digital signatures for critical files and communications.

(iii) **Secure File Transfers:** Refrain from transmitting sensitive data over non-secure open networks. Inculcate the practice of using secure methods like Secure File Transfer Protocol (SFTP) and Virtual Private Networks (VPNs).

(iv) **Collaboration with National and International Cyber Security Agencies:** The IAF should work in partnership with the Computer Emergency Response Team—India (CERT-IN) and National Critical Information Infrastructure Protection Centre (NCIIPC) to exchange intelligence of, and counter-measures against, emerging cyber threats.

CONCLUSION

"***In an era of hybrid warfare, the battle is often won before it is fought***." This era stresses on a paradigm shift in how air forces perceive security challenges and strategise counter-measures. Unlike conventional military engagements where boundaries and assets are clearly defined, modern hybrid warfare is shaped by the indiscernible forces of cyber intrusion, economic coercion and asymmetric disruptions. Gearing up for this hybrid battlespace is no longer an elective choice—it is a strategic imperative for national security.

The IAF must implement an exhaustive cyber security strategy that encompasses modern technologies, incident management, personnel training, perpetuation of an exclusive department of researchers, and alliances with national and international partners to stay ahead of evolving cyber threats. The capability of the IAF to identify potential sources of threats through artificial intelligence and, subsequently, neutralise them by robust hybrid warfare strategies (kinetic and non-kinetic), will outline its operational effectiveness. Hybrid warfare is no longer a futuristic concept; it is an ever-evolving reality. The air force that adapts to it swiftly will not only emerge victorious but will also shape future warfare.