# Enhancing Cyber Security and Asymmetric Warfare Capabilities: Strategic Imperative for Air Forces

*Shreyas Gaikwad*

The modern aerospace domain is dynamically transforming each passing day and is characterised by an enormous array of challenges. The escalating numbers of cyber attacks and employment of asymmetric warfare tactics by non-state actors remain of significant concern. The increasing dependence on computer-based systems and communication networks has added to the complexity by introducing composite vulnerabilities, resulting in greater susceptibility to cyber attacks. Such attacks have devastating consequences, extending from compromised security to the loss of sensitive information, and have been evident over and over again. There is a rise of non-state actors, employing asymmetric warfare tactics to exploit weaknesses in traditional military defences. The same involves sub-conventional and non-conventional methods like terrorism, guerrilla warfare and cyber attack in furtherance of their objectives. The use of drones has become a prevalent strategy

Squadron Leader **Shreyas Gaikwad** is a serving officer in the Indian Air Force.

of non-state actors, enabling them to carry out targeted strikes against states, populations and infrastructure, with minimal risk of detection, and with maximum impact.

## INTRODUCTION

The preceding two decades have witnessed a paradigm shift in the characteristics and variety of security threats that are emerging as major concerns for air forces worldwide. The increasing reliance on digital infrastructure has added new vulnerabilities that have compromised operational safety, resulted in the loss of sensitive information or disrupted vital infrastructures.[1] Non-state actors consisting of extremist organisations and hacktivist groups, etc., have exploited these aspects to launch deadly and devastating attacks, disrupting routine, peaceful functioning of the society.

The air forces are required to adopt a preemptive and innovative approach for the mitigation of such rising threats. This requires leveraging cutting-edge technologies such as Artificial Intelligence (AI) and Machine Learning (ML) embedded autonomous solutions to enhance cyber security measures. The employability of such technologies is highly dependent on the development of robust asymmetric warfare capabilities, including special operations forces and precision strike assets. By ensuring the same, air forces can remain adaptable, resilient and effective to face the increasingly complex and dynamic security environment.

The justification for this approach is based on the fact that traditional military strategies are no longer as effective as they were, to counter contemporary threats.[2] The speed and agility

[1] A. George, T. Baskar Shaji, and P. Balaji Srikaanth. "Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors," *Partners Universal International Innovation Journal*, 2.1, 2024, pp. 51-75.

[2] Ciprian Efimov, "The Challenges of Tactical Units Operating in the Grey Zone Hybrid Operational Environment," International Scientific Conference Strategies XXI, Carol I, National Defence University, 2019.

of cyber attacks require a rapid response capability that can only be achieved through the use of advanced technologies. The unconventional nature of asymmetric warfare tactics coerces one to deliberate on the dynamic security scenarios and to develop innovative solutions to counter these threats. The use of cutting-edge technologies can augment response capabilities by enhancing situational awareness, improve decisiveness and augment operational effectiveness. The development of robust asymmetric warfare capabilities shall assist in countering non-state actors effectively, reducing the risk of intimidation and other forms of asymmetric warfare.

## THE CYBER SECURITY CHALLENGE

The importance of cyber security in modern military operations cannot be undermined. With the developing technologies' reliance on digital systems and networks, the risk of cyber attacks is going be an ever increasing concern. A successful cyber attack can have dire consequences like compromising operational security and disrupting command and control systems while putting innocent lives at risk.[3] The potential impact of a cyber attack on an air force's operations is enormous and can include:

- **Compromised Operational Security**: Access to sensitive information such as mission plans, troop movements and tactical communications, allowing adversaries to anticipate and counter planned tactical operations.
- **Disruption of Critical Systems**: Cyber attacks can disable or disrupt critical systems like air traffic control, navigation and communication networks, jeopardising the conduct of safe and effective operations.

[3] Premkumar Chithaluru, Rohit Tanwar, and Sunil Kumar. "Cyber-Attacks and Their Impact on Real Life: What are Real-Life Cyber-Attacks, How do They Affect Real Life and What Should we do About Them?," *Information Security and Optimization*, Chapman and Hall/CRC, 2020, pp. 61-77.

- **Loss of Sensitive Information**: Theft of sensitive information, including classified data, personnel records and intelligence reports through cyber attacks can be used by adversaries to gain strategic advantage.
- **Reduced Situational Awareness**: Loss of operational plans and supplementary information can compromise the overall ability to gather and analyse critical information, reducing situational awareness and making it more difficult to make informed decisions. The loss of the planned element of surprise will complicate the conduct of future operations.

To mitigate these risks, air forces must prioritise cyber security and implement robust measures to protect their systems and networks from cyber threats, mainly by ensuring:

- Implementation of robust network defences like firewalls and advanced intrusion detection systems.
- Carrying out regular security audits and vulnerability assessments.
- Ensuring a well-trained cyber incident response team is available at hand and developing incident response plans to quickly respond to, and contain, cyber-based threats on the *modus operandi* and situations faced.
- Collaborating with other agencies and industries to share threat intelligence and best practices to ensure overall capacity-building as a nation.

By abiding by a list of proactive measures and a comprehensive approach to cyber security, air forces can reduce the risk of cyber attacks and protect their critical systems and operations from disruption or disablement. The following aspects mandate consideration to address the above issues.

## Artificial Intelligence Driven Threat Detection

The development of Artificial Intelligence (AI)-based threat detection systems can prove noteworthy in handling cyber risks. AI systems can employ different aspects like machine learning, neural networks, natural language processing and other such algorithms to assess vast amounts of data in real-time to recognise potential threats and anomalies that indicate cyber threats.[4] Implementation of Al-powered threat detection can significantly reduce the risk of network-based intrusions and improve incident response times. It has been established that Al-based detection systems can spot and react to threats up to 10 times faster than other traditional security systems.[5] This can help in taking proactive measures to prevent or alleviate the impact of cyber attacks, and protect critical systems and operations from functional breakdown or interruption. AI-based threat detection systems can help reduce the burden of tasks for the cyber security staff, allowing them to focus on more intricate and high-priority threats in a more resourceful way.

## Incident Response Systems

The capacity to respond quickly and effectively to an active threat is the main function of the incident response systems. These systems are designed to minimise damage and downtime by implementing a structured approach to respond to threats and control cyber-based incidents.[6] Incident response systems must comprise procedures for identifying, containing and eliminating

[4] Seshagirirao Lekkala, Raghavaiah Avula, and Priyanka Gurijala. "Big Data and AI/ML in Threat Detection: A New Era of Cybersecurity," *Journal of Artificial Intelligence and Big Data*, 2.1, 2022, pp. 32-48.

[5] C. Gowdham, et al., *Deep Learning Architectures for Automated Threat Detection and Mitigation in Modern Cyber Security Systems* (2024).

[6] Sureshkumar Somanathan, "A Study on Integrated Approaches in Cybersecurity Incident Response: A Project Management Perspective," *Webology (ISSN: 1735-188X)* 18.5 (2021).

threats, as well as restoring affected systems and services swiftly. Induction of a response system automated for automatic handling of situations will significantly reduce the impact of a cyber attack and quickly restore normal operations. Advanced incident response systems can also help to identify areas for improvement and provide valuable lessons about the patterns of threats, to help refine the cyber security posture and improve overall resilience to evolving cyber threats.

### Cyber Security Information Sharing

"*The fight is only as good as the intelligence and information available at hand is*." Information sharing agreements with other nations and organisations can be a significant step in improving collective cyber security management. Cyber security information sharing includes the exchange of threat intelligence, best practices and lessons learnt which can help to stay ahead of emerging threats, and improve overall response mechanisms.[7] By sharing information of cyber threats and susceptibility, militaries can gain vital insights into the tactics, techniques and procedures employed by adversaries, allowing them to develop more resilient counter measures. Cyber security information sharing agreements can nurture relationships and cooperation between nations, leveraging each other's expertise and resources to improve their combined cyber security posture. This can help to decrease the risk of cyber attacks and improve the overall security of operations.

## ASYMMETRIC WARFARE: THE NEW NORMAL

Asymmetric warfare has become a signature in modern conflict indicating non-state actors employing non-conventional tactics

[7] Sarah Brown, Joep Gommers, and Oscar Serrano. "From Cyber Security Information Sharing to Threat Management," Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, 2015.

to counter conventional military forces.[8] Air forces are required to develop capabilities to counter such emerging threats effectively, including, but not restricted to, conventional ways of war-fighting.

### Special Operations Forces

The presence of special operations forces is crucial to counter the non-conventional tactics employed by non-state actors. These forces are by design trained to conduct precision strikes, gather intelligence and conduct non-conventional operations behind enemy lines. Special operations forces can be employed to target high-value individuals, disrupt supply chain routes and conduct raids against enemy fortifications.[9] Such capabilities can enable enhanced capacity to counter non-state actors and reduce the risk of collateral damage. These forces can provide a flexible and adaptable potential that can be utilised in different scenarios, from counter-terrorism to non-conventional operations, including active wars.

### Precision Strike Assets

In the modern era, precision strike assets have proved their test against enemy forces by targeting vulnerable areas and vital points without, or with less, collateral damage. Precision strike assets like Unmanned Combat Aerial Vehicles (UCAVs), drones and loitering munitions allow reduced damage and civilian casualties while achieving their objectives. These assets can be used to conduct strikes against high-value targets, such as enemy command centres or logistics hubs, and can be used to provide close air support to the ground troops. Precision strike assets have

[8] Omer Aamir, "Warfare's Future in the Coming Decade: Technologies and Strategies," Available at SSRN 3854390 (2021).

[9] Louis Andries Bester, *The Appropriate and Optimal Role and Function of Special Forces in Peace Missions* (Diss. Stellenbosch: Stellenbosch University, 2022).

revolutionised the way air forces conduct operations which is evident in the post-Gulf War era, enabling them to achieve greater accuracy and effectiveness, while reducing the risk of harm to civilians.[10]

### Intelligence, Surveillance, and Reconnaissance (ISR) Capabilities

Enhancing ISR capabilities is critical for air forces to detect and track non-state actors effectively. Advanced sensors, Unmanned Aerial Vehicles (UAVs) and satellite imaging ensure improved situational awareness, enabling them to gather intelligence on enemy movements and operations. ISR capabilities are used to monitor enemy supply chains, track the movement of high-value individuals and identify potential targets for precision strikes.[11] ISR capabilities are gaining importance in modern conflict as they enable processes to gather intelligence and conduct operations in near real-time. They would reduce the risk of surprise attacks and provide a persistent presence over the battlefield, enabling monitoring of enemy activity and thereby a quick response to a dynamic threats.

## IMPLEMENTATION ROADMAP

### Conduct of Cyber Security Risk Assessment

The first step in enhancing cyber security for air forces is to conduct comprehensive risk assessment. This involves identifying potential vulnerabilities in the air force's cyber security systems,

[10] Anthony H. Cordesman, "The Air War Lessons of Afghanistan: Change and Continuity," Centre for Strategic and International Studies, 27, 2002, pp. 253-81.

[11] N. Blakcori, et al., "The Evolving UAS Threat: Lessons from the Russian-Ukrainian War Since 2022 on Future Air Defence Challenges and Requirements," NATO, Integrated Air and Missile Defence Centre of Excellence, 2024.

including networks, software, and hardware. The goal of the risk assessment is to determine the likelihood and potential impact of cyber attacks by the following:[12]

- Identify critical assets and systems that require protection.
- Assess the current state of cyber security controls and protocols.
- Evaluate the effectiveness of incident response plans and procedures.
- Develop a plan to address identified vulnerabilities and risks.

The risk assessment should be conducted by a team of experienced cyber security professionals, using established frameworks and methodologies. The results of the risk assessment will lead to the development of a comprehensive strategy, prioritising mitigation efforts and resource allocation.

### Develop an Asymmetric Warfare Strategy

A comprehensive strategy is necessary for countering non-state actors, including terrorist organisations and insurgent groups. This involves creating a tailored approach that leverages special operations forces, precision strike assets and other capabilities to disrupt and defeat asymmetric threats. The following is recommended for inclusion:

- Define the role of air power in counter-asymmetric warfare.
- Identify key targets and objectives such as command and control nodes, logistics hubs and propaganda centres, etc.

[12] Halima Ibrahim Kure, et al., "Asset Criticality and Risk Prediction for an Effective Cybersecurity Risk Management of Cyber-Physical System," *Neural Computing and Applications*, 34.1, 2022, pp. 493-514.

- Design tactics, techniques and procedures for conducting precision strikes and special operations.
- Establish partnerships with other military arms, government agencies and international partners to enhance coordination and cooperation.

The asymmetric warfare strategy should be flexible and adjustable, reflecting the dynamic nature of the employed tactics. ISR capabilities to support targeting, and battle damage assessment concurrently need to be prioritised.

**Invest in Research and Development (R&D)**

We need to allocate resources for R&D of new technologies that enhance cyber security and asymmetric warfare capabilities. The same will go a long way in ensuring accurate, integral and robust response systems.

- Invest in Al-based threat detection systems, advanced ISR capabilities and precision strike assets.
- Develop new materials and technologies such as stealth coatings and advanced propulsion systems.
- Explore innovative concepts such as swarming drones and autonomous systems.
- Collaborate with academia and industry partners to leverage cutting-edge R&D.

Research and development efforts should be focussed on addressing specific capability gaps and priorities, such as improving cyber security controls, enhancing precision strike capabilities, and developing more effective counter-asymmetric warfare tactics. Air forces must also prioritise testing and evaluation to ensure that new technologies are effective and operationally relevant.

## INNOVATIVE SOLUTIONS

The changing face of modern warfare is majorly driven by technological advancements and rapidly evolving strategies in all domains of warfare. Thus, the solutions that are necessary to mitigate the complex dynamic challenges posed by these factors need to be equally potent and credible to stand the test of future landscapes of security. Towards this, we are necessitated to act considering a farther perspective of time which would cater to the development, testing and employment of solutions so devised. The following aspects may be brainstormed further:

### Artificial Intelligence and Machine Learning

Artificial Intelligence (Al) and Machine Learning (ML) algorithms can be leveraged to enhance cyber security and asymmetric warfare capabilities. AI and ML can be applied for:[13, 14]

- **Threat Detection**: AI-based systems can analyse an enormous volume of data to identify probable threats such as malware, phishing attacks and other types of cyber threats.
- **Incident Response**: ML algorithms can assist automation during incident response processes, reducing analysis and decision time to respond to, and contain, security breaches.
- **Situational Awareness**: Al-driven systems can provide quick and enhanced situational awareness, enabling better understanding of the operational environment and thereby making more informed decisions.

[13] Prince Nayem Uddin, et al., "AI-Powered Data-Driven Cyber Security Techniques: Boosting Threat Identification and Reaction," *Nanotechnology Perceptions*, 20, 2024, pp. 332-353.

[14] Jim Daily, and Jeff Peterson. "Predictive Maintenance: How Big Data Analysis Can Improve Maintenance," in *Supply Chain Integration Challenges in Commercial Aerospace: A Comprehensive Perspective on the Aviation Value Chain* (Cham: Springer International Publishing, 2016), pp. 267-278.

- **Predictive Maintenance**: Al and ML can be used to predict when aircraft or other assets are likely to require maintenance, hence, reducing downtime and improving efficiency.

## Cloud Computing and Cyber Security

Cloud computing offers a wide range of benefits, including greater scalability, cheaper costs and better security. These factors can be further amplified as:[15]

- **Enhance Scalability**: Quickly scale up or down to meet changing operational demands, foregoing the need for significant investments in new or additional infrastructure.
- **Reduce Costs**: Reduce costs associated with hardware, software and maintenance which also minimise the risk of systems becoming outdated sooner than expected. This aspect is vital in enabling capacity development, ensuring economy of effort in view of the rapidly evolving technological expansion.
- **Improve Cyber Security**: Leverage cloud-based security solutions like encryption, access controls and threat detection to enhance the security of assets. Robust security framework development contributes towards information security adding to survivability in the actual operational environment, which directly assists intelligence gathering.

## CONCLUSION

In the contemporary threat environment, war-fighting capabilities are no longer are a luxury, but a strategic imperative for the safety of the nation. The increasing complications of cyber threats and the adaptability of non-state actors to overcome and evolve is a

[15] Mazhar Ali, Samee U. Khan, and Athanasios V. Vasilakos. "Security in Cloud Computing: Opportunities and Challenges," *Information Sciences*, 305, 2015, pp. 357-383.

new signature in modern conflicts. This necessitates a proactive and innovative approach to stay abreast, if not ahead, of such emerging and evolving challenges. By capitalising on cutting-edge technologies, we can considerably enhance our cyber security postures and improve our ability to counter asymmetric threats.

The idea articulated above provides a structured framework for achieving control over situations in asymmetric warfare, ensuring that development remains adaptable, resilient and effective, undeterred by an increasingly complex and dynamic security situation. Ultimately, the key to success lies in embracing innovation and being willing to take calculated risks to stay ahead of emerging threats. It is necessary to maintain a competitive edge to protect national interests and ensure the continued effectiveness of operations which is possible with visionary foresight on the strategic landscape.