Cyber Security Vulnerabilities of Artificial Intelligence-Enabled Counter Drone Systems: Risk and Resilience Strategies in South Asian Environment

Colonel Harmeet Singh[@]

Professor (Dr) Anurag Jaiswal[#]

Abstract

This article examines the integration of Artificial Intelligence (AI) in counter-unmanned aerial vehicle systems and its impact on modern military operations. AI-enabled counter drone technologies have significantly enhanced the speed, precision, and effectiveness of detecting and neutralising aerial threats, leading to their increasing deployment for the protection of national borders, critical infrastructure, and airspace. However, the article highlights that the growing dependence on AI also introduces significant cybersecurity vulnerabilities. These include risks such as data poisoning, evasion attacks, and adversarial manipulation of machine-learning models, which can undermine the reliability of AI-driven systems. It also identifies vulnerabilities in communication networks supporting these systems. The article argues that while AI strengthens defence capabilities, it simultaneously expands the

[@]**Colonel Harmeet Singh** was commissioned into 6 Maratha Light Infantry and has served with distinction in high-altitude, counter-insurgency, and conventional operations. He participated in Operation Parakram and commanded a Rashtriya Rifles battalion in North Kashmir. An alumnus of the Defence Services Staff College and the College of Defence Management, he also served as the Head of a United Nations Military Observers team. Currently pursuing a PhD on Artificial Intelligence and Drone Warfare, he focuses on integrating emerging technologies into defence strategies and has authored several research articles.

[#]**Professor (Dr) Anurag Jaiswal** is a distinguished professor with extensive expertise in the Department of Defence Studies at Meerut College. He completed his PhD in 2007. He is actively engaged in research work and has authored many books, along with more than 16 research papers credited to his name.

Journal of the United Service Institution of India, Vol. CLVI, No. 643, January-March 2026.

cyber threat surface. To address these risks, it emphasises the need for a multilayered cybersecurity architecture incorporating encrypted communications, tamper-resistant hardware, robust verification mechanisms, and human oversight, alongside greater indigenisation of critical technologies and a comprehensive national policy framework.

Introduction

The rise and widespread use of Unmanned Aerial Vehicles (UAVs) in recent times have changed the combat zone. Furthermore, the development of Counter-UAV (C-UAV) system has become a necessity for protecting borders and critical infrastructure of any nation state. It has led to a shift in the way military missions are being strategised and executed.

Keeping in view the peculiarities of the South Asian geopolitical environment, where this threat has become a reality, all states are, thus, rapidly investing in capacity building related to aerial defence capabilities. India has also taken quick strides to remain ahead in this race.

The next step towards threat mitigation and security is the reliance on Artificial Intelligence (AI)-based counter drone systems. These systems provide numerous advantages to include autonomous decision-making in a complicated milieu, ensuring both speed and precision while neutralising threats. Thus, it becomes a key differentiator between success and failure. However, these developments have also presented serious challenges of cyber threats. As the integration level for efficient decision making has increased in these systems, it has also expanded the range of cyberattacks and vulnerabilities.

These threats range from targeting decision making core, hardware, and software to the algorithms itself. To prevent such threats, there is an urgent need to develop a cyber security strategy which is not only multifaceted but also responsive and resilient to cater for future warfare needs.[1]

This article discusses cyber security vulnerabilities in counter drone systems which are complex, combining the dangers of cyber and physical sphere. It then proposes an all-inclusive framework

which is appropriate for India, recommending measures for enhancing robustness in progressively more contested cyber–air domain.

Evolving Landscape: A Scan

Recently conducted Operation Sindoor by India has highlighted the importance of C-UAV systems for ensuring security along the borders. Even earlier, there had been frequent incidents of misuse of aerial platforms by adversaries and non-state actors. Both the historical and recent environmental realities have brought to fore the need for prioritising defensive capabilities against such threats. In consonance with the Indian government's initiatives of 'Make in India' and *Atmanirbharta* (Self-reliance), the investment towards developing these capabilities, especially indigenous development, has got a shot in the arm. Today, indigenisation has become a permanent national security compulsion. It will reduce reliance on foreign original equipment manufacturers along with giving tactical superiority and ensuring technological autonomy.

As regards next generation C-UAV system, the primacy is on integrating multiple sensors through AI algorithms. These models fuse together inputs received from radars, Radio Frequency (RF) analysers, electro-optical and infrared cameras, and acoustic sensors. These integrated inputs are then used by the model to develop a comprehensive intelligence picture, accurately classify the threat, predict trajectory of the aerial system, and present a neutralisation response which is layered in nature by using jamming, spoofing, and kinetic measures.

Though these smart systems are efficient, but they are double edged. With each added sensor and layer of fusion, these are also potential targets for attack. Since these systems function on interdependencies of sensors, any failure of one component may lead to complete failure of the system of system.

Multifaceted Threats: Cyber Vulnerabilities

It is well known that AI-based systems have vulnerabilities which exist across the spectrum, from hardware to datasets used for training AI models:

- **Deceiving Digital Mind**. The machine learning models, which are the heart of C-UAV systems, are primarily used for recognising patterns. Any attacks on these models make it

susceptible to digital deception. Since these systems lack reasoning capability like humans, they continue to remain vulnerable to manipulation.

- **Data Poisoning**. This is undertaken through prolonged efforts deliberately trying to disrupt or undermine the system by creating a secret backdoor. Datasets dealing with visual recognition and signal identification are targeted by inserting corruption into the foundation itself.[2] During the training phase of a model, a hidden trigger may be inserted systematically or even manipulation of data samples may be carried out. This mislabelling of data can lead to misclassification of specific drones as birds. This hidden trigger is activated when required to make the system fail, especially during the critical phase. Normally, the system would work flawlessly during testing, thereby, preventing the user to know about the flaw. However, when the adversary intends to exploit the vulnerability, the trigger is activated. Even once the vulnerability is known, it will require cleaning entire dataset and resource-intensive retraining of the systems which is costly.

- **Evasion Attacks**. This is a real-time trick by fooling the state-of-art system. Unlike data poisoning, this attack occurs after deployment of the system. An adversary creates subtle, small changes from normal and negligible changes causing miscalculation.[3] For instance, a hostile drone may carry special design or patterns or use a projection system to change the appearance, thereby, fooling the AI-based system to recognise it as a bird, though it remains visible as a drone to human eye.

Exploitation and Command-and-Control Interference: Cyber Physical System and Command Chain

The effectiveness of AI-based C-UAV system is dependent on timely and accurate detection along with decision making which is based on secure exchange of data and command. The exploitation of the vulnerabilities in communication links between sensors, processors, and effectors (jammers or Interceptors) will lead to command-and-control interference. An adversary may use spoofing or jamming to insert false data or block commands, thereby, leading

to denial-of-service attack. It is also feasible that false alarms are introduced in the system which will exhaust operators to reset the systems. This may lead to crippling of system during an actual attack and waste resources. It is feasible that the system may be able to identify the threat, but since it would not be receiving any command for neutralisation, it would fail to accomplish the aim.

Supply Chain Compromise: A Pertinent Threat

In the global world, nation states are interdependent, especially when it comes to supply chain. The dependency for technology, advance components, chips, sensors, and processes lends it to a realistic vulnerability. This vulnerability of exploitation of hardware by an adversary poses grave risk. A non-state actor or a state may compel a manufacturer to embed hidden backdoor into the firmware. This malicious component may remain dormant for years before being activated at an opportune time. As elucidated earlier, this backdoor can be used to corrupt calculation by algorithms or used to exfiltrate data or even disable a system at critical juncture. These threats will require costly audit of hardware, since normally these may be nearly impossible to detect through software scans.[4]

Artificial Intelligence: Use as an Offensive Means

The last of the vulnerabilities is related to the use of AI as an offensive tool wherein 'Generative AI' is used for crafting convincing phishing emails to target key persons related in manufacturing, defence contracting business, or research institutions. AI may even be used to write unique malware, which can easily circumvent detection systems. Another option is to use AI for automatic scanning thousands of codes to detect new vulnerabilities, which are then used for exploitation.[5] This usage lends itself to scaling operations at a large scale and effectively targeting intended person. Overall, AI can be used for cyber campaigns with a greater ease.

Building Multi-Layered Resilience Strategy

Keeping in view the numerous risks and vulnerabilities, no single solutions exist to ensure the security of AI-dependent counter drone system. It would require a holistic approach to formulate a coherent and robust strategy, which addresses strategic, operational, and technical aspects.[6] To overcome the vulnerabilities,

numerous measures can be adopted. To arrive at a holistic way forward, one can carry out the strengths, weaknesses, opportunities, and threats analysis. The biggest strength of AI-driven systems is their capability to detect and identify threats with speed and accuracy. However, as elucidated earlier, AI dependence also brings forth vulnerabilities due to integration of multiple layers, which becomes its weakness once exploited by an adversary. As regards threats is concerned, South Asian states need to understand that if the AI-based system misidentifies a target, it may adversely impact security of the region, especially with the increased risk of miscalculation and consequent escalation due to the existing mistrust. Nevertheless, it also provides an excellent opportunity to collaborate and formulate a strategy which caters for all aspects.

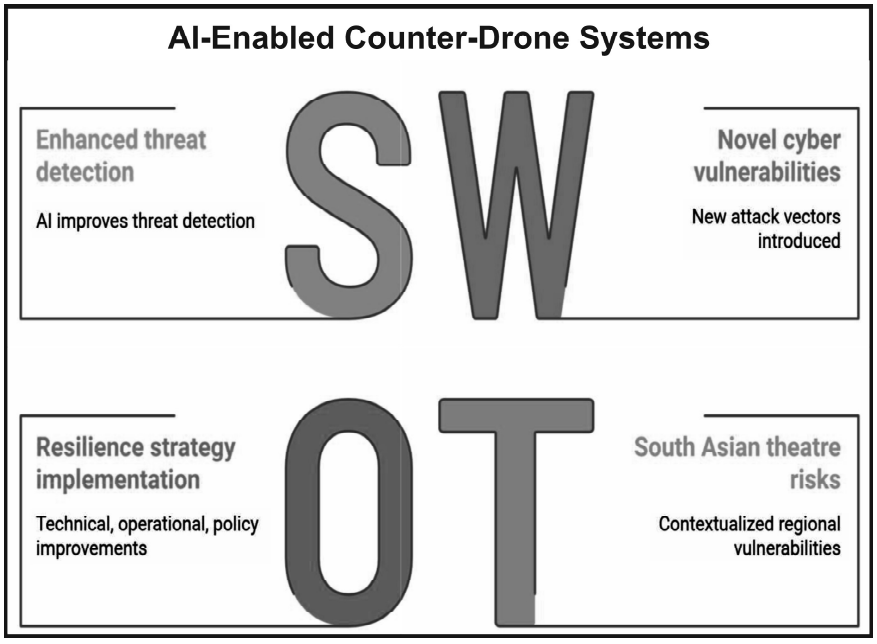

Figure 1: SWOT Analysis of AI-Enabled Counter Drone Systems

***Source*: Curated by Author**

These can be at technical, organisation, and national level. The resilience can be built through technical countermeasures as under:

- **Robustness against Adversarial Attacks**. The best defence against adversarial attack is to develop a robust AI system. This can be conducted by planning at the initial stage of development itself. The models being developed should be trained to identify such malicious attempts by providing datasets with adversarial examples. This will enable the system to develop a capability to detect and resist suspicious inputs. This inherent anomaly detection capability will enable the AI system to flag deceptive inputs and tackle them by masking before it causes harm.[7]

- **Multi-layered Verification**. To build resilience against the cyber vulnerabilities, cross verification and redundancy would be required. The basic philosophy must be based on 'Zero Trust' and no reliance on single sensor or single data stream be adhered to. For instance, if radar signature and RF profile confirm conclusively that an aerial object is a drone, though visual sensor is reporting it as a bird, then the AI system must be able to override the deceiving input. With this capability, the attackers will require multiple spoofers to mislead which will be very difficult and challenging.[8]

- **Secure Communication**. Lastly, end-to-end encryption is a necessity in current times to secure communication between sensors and AI-based system. There is a need to have hardened components with robust standards capable of resisting jamming. Use of Frequency Happing Spread Spectrum (FHSS) along with directional antennas is the way forward. Very importantly, the security of physical access points needs to be ensured apart from having a secure process of booting these systems by developing tamper-proof hardware.[9]

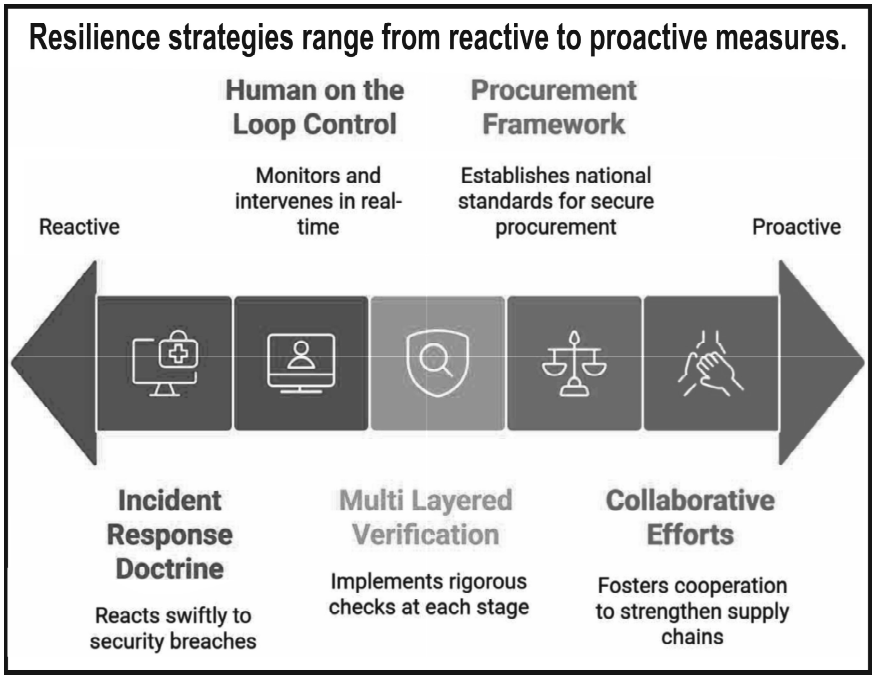

Figure 2: Framework for Cyber Resilience in AI-Enabled Counter Drone Systems

***Source*: Curated by Author**

People and Process: Organisational Measures

The people and process responsible to manage and manage AI-based Counter-Unmanned Aerial Systems (C-UAS) are as critical as the technology itself. Certain measures, which can be adopted to counter cyber risks and vulnerabilities at organisational level, are as under:

- **Human-on-the-Loop Control**. It is imperative that AI systems are treated as potent assistant rather than to give it freedom as autonomous decision maker of life and death. Hence, the need for human-on-the-loop is a necessity, especially to safeguard against errors which can be due to malicious intent or even a natural error of the system. The human operator who is trained over the period retains the final authority for lethal engagement.

- **Wargaming: Red Team Concept**. At organisational level, skilled ethical hackers should be employed to act like an adversary to try and find weaknesses in the system.

Conduct of regular exercises to attempts and break into the system by this red team will ensure that any vulnerability in the system is identified and plugged before being exploited.[10]

- **Doctrine for Incident Report**. For an effective response system, clear protocols laying down mission continuation while being under cyberattack should be prepared. These protocols must address method to isolate any compromised subsystems and alternate safe system to fall back to during such an eventuality. Thus, clear doctrines and policies for response to any incidents will increase safeguard against cyberattacks.

Security Plan and Nationwide Frameworks: Alleviate Supply Chain Vulnerabilities

Bearing in mind the South Asian environmental realities, it is practical for India to have a national security plan or policy, which takes a long-term view of incorporating international partnership efforts in supplementing resilience through progressive policy. Following aspects need special attention:

- **Procurement Framework: National Standard**. To mitigate supply chain vulnerabilities, it is a necessity to establish national standards which lay down security performance for AI system. These standards should define robustness levels in defence-related system, and these should be mandatorily incorporated in procurement contacts.[11] Moreover, to encourage manufactures, they should be incentivised for incorporating security parameters.

- **Supply Chain Sovereignty and Audits**. The way ahead for ensuring self-sufficiency in technology is to have a concerted drive for indigenisation. This only shall become a strategic solution to reduce dependence on imported components, especially microchips, critical parts, and AI software. Moreover, laying down vetting standards is a necessity.[12] It will involve rigorous checks with multi-layered certification along with mandatory records of ownership and protocols to verify integrity of the components.

- **Collaborative Efforts: Foster Cooperation**. Collaboration and cooperation should be planned both at regional and national level. Dividends will be accrued when

a structured public–private partnership is encouraged between industry and academia, resulting in the development of a cutting-edge technology through research. At regional level, India can collaborate by sharing threat intelligence and the best practices so that any cyberattack is utilised as an opportunity to strengthen defensive system of neighbours and Computer Emergency Response Team can play a crucial role in this regard.

Conclusion

The advancement of technology has enabled improvement in defensive capabilities against aerial threats. However, development of C-UAS and their deployment brings to fore certain concerns. To address these, it leads to a continuous cycle of taking measures or counter measures by innovating and adaptation. South Asian nation states stand at crossroads of both development and vulnerabilities related to AI bases systems. These vulnerabilities, related to supply chain dependence and AI models, are real and would require a holistic resilience strategy. This strategy would require technical inventiveness, operational alertness, and visionary outlook, leading to development of strong, dependable, and intelligent system. Future of India will, thus, be dependent on how dynamic, righteous, and virtuous AI-based counter drone systems are developed, which can defend the nation and its common people.

Endnotes

[1] "Anti-Drone Systems Offer New Ways to Counter Rising Threats", *AP News*, 2023, accessed 15 Jan 2026, https://apnews.com/article/anti-drone-systems-counter-rising-threat

[2] Bowei Xi, "Adversarial Machine Learning for Cybersecurity and Computer Vision: Current Developments and Challenges", *arXiv* preprint, 2021, accessed 16 Jan 2026, https://arxiv.org/abs/2107.02894

[3] "Hackers Could Manipulate What AI Sees", *TechRadar Pro*, 2023, accessed 16 Jan 2026, https://www.techradar.com/pro/security/hackers-could-manipulate-what-ai-sees

[4] "Chinese Threat in Indian Drones", *India Today Insight*, 06 Feb 2025, accessed 16 Jan 2026, https://www.indiatoday.in/india-today-insight/story/chinese-threat-in-indian-drones

[5] "AI Battle Lines", *Axios*, 2024, accessed 17 Jan 2026, https://www.axios.com/2024/05/30/ai-battle-lines

[6] R Verma, "Fortifying the Skies: Securing India's Military Drones", *LinkedIn Defense Commentary*, 2024, accessed 17 Jan 2026

[7] Xi, "Adversarial Machine Learning"

[8] Ibid.

[9] Verma, "Fortifying the Skies"

[10] Ibid.

[11] Ibid.

[12] Ibid.