Counter Drone Warfare

Major HS Mankoo@

Abstract

The proliferation of consumer-grade drones has ushered in a new era of technological innovation and convenience, yet it has also given rise to formidable security challenges. Unmanned aerial vehicles are increasingly being exploited for nefarious purposes, ranging from espionage and smuggling to acts of terrorism. As a response to this emergent threat, the field of counter drone warfare has rapidly evolved. This article provides a comprehensive overview of the current state of counter drone warfare, examining the multifaceted nature of the drone threat and the intricate strategies employed to mitigate it.

The article delves into the technical aspects of countering drones, analysing the diverse methods used for detection, identification, and neutralisation. From radar and radio-frequency technologies to kinetic and non-kinetic counter measures, the discussion encompasses the full spectrum of tools and approaches utilised by military and security forces worldwide.

Furthermore, the article explores the types of counter drone systems being used in the Ukraine-Russia conflict, the lessons learnt in the Indian context and the future of counter drone systems.

Introduction

The Ukraine-Russia conflict has been seen as the first full-fledged drone war with both sides using drones extensively. Drones have been used for tasks like recce, surveillance, and direction of own artillery fire, even in the form of loitering

@**Maj HS Mankoo** is an alumnus of Officers Training Academy and was commissioned into Army Aviation in April 2015. The officer has also served with 3rd Battalion, The Madras Regiment during the attachment period. He has served in various operational areas and currently posted as Instructor Cl 'B' at Indian Military Academy.

Journal of the United Service Institution of India, Vol. CLIII, No. 634, October-December 2023.

munitions. Looking at the success of drones in this war, it is likely that in future conflicts drones are going to play a larger role than ever. Hence, it is very important that a nation possesses the capability to defend itself from such weapon systems.

Counter Drone Tech

Counter drone technology refers to the methods and systems that are used to detect, track, and mitigate unauthorised Unmanned Aerial Vehicles (UAVs) or drones. These technologies are designed to identify and neutralise drones that may pose a security threat, such as those carrying explosives, conducting surveillance, or interfering with airspace. This technology typically involves a combination of sensors, radars, cameras, and other equipment that can detect and track drones, as well as jamming or interception devices that can disable or take control of the drones. Some examples of counter drone technology include radio frequency jammers, Global Positioning System (GPS) spoofers, net guns, and even trained eagles.

As the use of drones becomes more widespread, the need for effective counter drone technology is becoming increasingly important, particularly in areas such as airports, military installations, critical infrastructure, and public events. However, there are also concerns about the potential misuse of counter-drone technology and the need to balance security with privacy and civil liberties.

In a conventional war scenario, counter drone technology plays a crucial role in defending against enemy drones, which can be used for recce, surveillance or attack purposes. Some examples of counter drone technology in a conventional war scenario are:[1]

Detection and Tracking Systems.[2]

- Radar — Detects the presence of small unmanned aircraft by their radar signature, which is generated when the aircraft encounters Radio Frequency (RF) pulses emitted by the detection element. These systems often employ algorithms to distinguish between drones and other small, low-flying objects, such as birds.

- RF — Identifies the presence of drones by scanning for the frequencies on which most drones are known to operate. Algorithms pick out and geo-locate RF-emitting devices in the area that are likely to be drones.
- Electro-Optical — Detects drones based on their visual signature.
- Infrared — Detects drones based on their heat signature.
- Acoustic — Detects drones by recognising the unique sounds produced by their motors. Acoustic systems rely on a library of sounds produced by known drones, which are then matched to sounds detected in the operating environment.
- Combined Sensors — Many systems integrate a variety of different sensor types in order to provide a more robust detection capability. For example, a system might include an acoustic sensor that cues an optical camera when it detects a potential drone in the vicinity. The use of multiple detection elements may also be intended to increase the probability of a successful detection, given that no individual detection method is entirely failproof.

Interdiction.[3]

- RF Jamming — Disrupts the radio frequency link between the drone and its operator by generating large volumes of RF output. Once the RF link, which can include Wireless Fidelity links, is severed, a drone will either descend to the ground or initiate a 'return to home' manoeuvre.
- GNSS Jamming — Disrupts the drone's satellite link, such as GPS or Global Navigation Satellite System, which is used for navigation. Drones that lose their satellite link will hover in place, land, or return home.
- Spoofing — Allows one to take control of the targeted drone by hijacking the drone's communications link (also known as protocol manipulation).

- Laser — Destroys vital segments of the drone's airframe using directed energy, causing it to crash to the ground.
- Nets — Designed to entangle the targeted drone and/or its rotors.
- Projectile — Employs regular or custom-designed ammunition to destroy incoming unmanned aircraft.
- Combined Interdiction Elements — A number of counter-unmanned aircraft system systems also employ a combination of interdiction elements-most commonly and Global Navigation Satellite System (GNSS) jamming systems that work in tandem.

Platform Types.[4]

- Ground-based — Systems designed to be used from either stationary or mobile positions on the ground. This category includes systems installed on fixed sites, mobile systems, and systems mounted on ground vehicles.
- Hand-held — Systems that are designed to be operated by a single individual by hand. Many of these systems resemble rifles or other small arms.
- UAV-based — Systems designed to be mounted on drones, which can come into proximity with the targeted unmanned aircraft in order to employ interdiction elements at close range.

Types of Counter Drone Systems Being Used in Ukraine-Russia Conflict

Both Ukraine and Russia have reportedly used various counter-drone systems in the ongoing conflict in Ukraine. Here are some examples:

- **Leleka-100 Drone Detection System**. This system uses cameras and acoustic sensors to detect drones and provide early warning alerts to soldiers on the ground.[5]

- **Zaslon Electronic Warfare System**. This Russian-made system is capable of jamming the signals of drones and other UAVs, as well as disrupting the communications of ground-based command and control systems.[6]

- **Aero Scope Drone Tracking System**. Both Ukraine and Russia have reportedly used the DJI Aero Scope system to detect and track drones that are being flown near military installations and other sensitive areas.[7]

- **Drone Shield Counter Drone System**. This system, which is designed to detect and track drones using radio frequency and acoustic sensors, has reportedly been used by both Ukraine and Russia.[8]

- **Sky Net Anti-Drone System**. Developed by a Taiwanese company, this system uses a combination of radar, cameras, and jammers to detect and neutralise drones.[9]

- **Kupol Counter Drone System**. This Russian-made system is designed to detect and track drones using a combination of radar, cameras, and other sensors, and can be integrated with other air defence systems.[10]

It is important to note that the use of counter drone systems in the Ukraine-Russia conflict is constantly evolving, and both sides are likely to continue to invest in and deploy new technologies to gain a tactical advantage. However, it is also important to consider the potential implications of these technologies, particularly in terms of civilian safety, privacy, and human rights.

Lessons Learnt for India

There are several lessons that India can learn from the use of drones in the recent conflicts. Here are some key takeaways:

- **The Need for Effective Counter Drone Systems**. The Ukraine-Russia conflict has highlighted the importance of having effective counter drone systems to defend against potential drone threats. India may need to invest in and deploy a range of counter drone technologies, such as

radar systems, electronic warfare systems, and anti-drone guns, to protect military installations, critical infrastructure, and public safety.

- **The Potential for Asymmetric Warfare**. The use of drones in the Ukraine-Russia conflict has demonstrated the potential for asymmetric warfare, where smaller and less technologically advanced forces can use drones to inflict damage on larger and more advanced military forces. India may need to consider the potential for asymmetric threats from drones and develop strategies to counter this threat.

- **The Need for Effective Regulations**. The use of drones also raises important legal and ethical considerations, particularly in terms of privacy and human rights. India may need to develop clear guidelines and regulations for the use of drones and counter drone technologies to ensure that they are being used in a responsible and ethical manner.

- **The Potential for Technological Innovation**. The use of drones in the Ukraine-Russia conflict has led to a significant amount of technological innovation in this field. India has a strong technology industry and could potentially play a leading role in the development of new and innovative drone technologies.

- **The Importance of Intelligence Gathering**. The use of drones for surveillance and reconnaissance purposes has been a key aspect of the Ukraine-Russia conflict. India may need to enhance its intelligence-gathering capabilities to detect and track potential drone threats, particularly in areas where there are security concerns.

In summary, the Ukraine-Russia conflict has highlighted the importance of effective counter drone systems, the potential for asymmetric threats, the need for effective regulation, the potential for technological innovation, and the importance of intelligence gathering. India may need to consider these lessons in the context of its own security concerns and develop appropriate strategies and capabilities to address potential drone threats.

India's standing in Counter Drone Tech

India has been working on developing counter drone technology to address the increasing threat posed by UAVs or drones. We have made some progress in this area, but it is still behind some other countries in terms of its capabilities and infrastructure.

- One of the key initiatives in this area is the development of the National Counter Rogue Drone Guidelines by the Indian Ministry of Civil Aviation. The guidelines provide a framework for managing the threat of rogue drones and include measures such as the establishment of a counter-drone task force, the creation of no-fly zones, and the use of counter drone technology.[11]

- India has also started developing its own counter drone technology, with the Defence Research and Development Organisation (DRDO) leading the charge. In 2021, DRDO developed a counter drone system called 'D4' which can detect and jam drone signals up to 3 km away.[12]

- Indian start-ups are also working on developing counter drone technology, with companies such as Idea Forge, Detect Technologies, and Drone Shield offering various solutions for drone detection, tracking, and interception.[13]

Despite these efforts, India still faces some challenges in countering drones. The country has a huge border that is difficult to monitor, and there have been several incidents of drones being used for smuggling and espionage activities. Additionally, the market for drones is rapidly evolving, with new technologies and capabilities being introduced all the time. As a result, India will need to continue to invest in research and development to stay ahead of the threat posed by drones.

Future of Counter Drone Technology

Counter drone technology is evolving rapidly, and we can expect to see significant advancements in the future. As drones become more common and accessible, there is a growing need for effective countermeasures to prevent them from being used for malicious purposes, such as spying, terrorism, or smuggling.

Here are some potential future developments in counter-drone technology:[14]

- **Detection and Tracking**. Advancements in machine learning and computer vision technology will enable more accurate and reliable detection and tracking of drones. This could include the use of advanced radar, thermal imaging, or acoustic sensors to detect and track drones in real-time.

- **Jamming and Disabling**. Counter drone technology may include the use of radio frequency jammers or other techniques to disrupt the drone's communication with its operator, causing it to lose control or even crash. Other technologies may include the use of lasers or electromagnetic pulse to disable drones in mid-air.[15]

- **Interception and Capture**. Future counter drone systems could include the use of specialised drones designed to intercept and capture other drones. This could include the use of nets or other physical barriers to trap the rogue drone.

- **Cyber security**. As drones become more connected and autonomous, there will be an increasing need to secure them against cyber-attacks. Counter drone technology may include the use of advanced encryption and authentication protocols to prevent unauthorised access to drones.[16]

- **Artificial Intelligence (AI) and Machine Learning**. Counter drone systems are already using AI and machine learning algorithms to detect and classify drones. In the future, we can expect to see even more sophisticated AI algorithms that can accurately differentiate between authorised and unauthorised drones, and can quickly respond to new and emerging threats.[17]

- **More Advanced Sensors**. The use of advanced sensors such as radar, lidar and cameras will continue to improve the ability of counter drone systems to detect drones in all types of weather and lighting conditions.

- **Improved Jamming and Disruption Techniques**. As drones become more advanced, counter drone systems will need to become more sophisticated in their ability to disrupt and disable them. Future technologies may include jamming techniques that can target specific frequencies or even individual drones, as well as more advanced laser-based systems.[18]

- **Collaborative Systems**. Counter drone systems will increasingly need to work in collaboration with other technologies such as air traffic control systems, satellite networks, and other sensors to create a comprehensive and effective drone defence network.

We can expect to see a significant increase in the sophistication and effectiveness of counter drone technology in the coming years. As the threat of malicious drone use continues to grow, the development of effective countermeasures will become increasingly important.

Conclusion

Counter drone technology is essential for India for several reasons. First, drones can pose a significant threat to national security, particularly in sensitive areas such as border regions or military installations. Drones can be used for espionage, smuggling, or carrying out attacks, and countering these threats is crucial to maintaining the country's security.

Second, the use of drones is becoming increasingly prevalent in civilian applications, such as agriculture, transportation, and infrastructure inspections. While this has several benefits, it also creates security concerns, as drones can be used for illegal activities such as smuggling or terrorist attacks. Therefore, it is essential to have the capability to detect and neutralise unauthorised drones in sensitive areas.

Third, India has a significant defence industry and is home to several defence manufacturers. Developing indigenous counter drone technology would not only enhance the country's security but also provide opportunities for domestic companies to enter the global market.

Overall, counter drone technology is essential for India to protect its national security, prevent illegal activities, and support its defence industry.

Endnotes

[1] https://www.robinradar.com/press/blog/10-counter-drone-technologies-to-detect-and-stop-drones-today

[2] https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[3] https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[4] https://dronecenter.bard.edu/files/2019/12/CSD-CUAS-2nd-Edition-Web.pdf

[5] http://uacuas.com

[6] https://apps.dtic.mil/sti/trecms/pdf/AD1137511.pdf

[7] https://www.airport-suppliers.com/product/anti-drone-system/

[8] https://www.droneshield.com/products

[9] https://anti-drones.net

[10] https://www.defensemirror.com/news/32431/Russia_s_Avtomatika_Demos_New_Anti_drone_Electronic_Warfare_System

[11] https://capsindia.org/wp-content/uploads/2022/08/R-K-Narang.pdf

[12] https://vajiramias.com/current-affairs/what-is-d4-dronesystem/63d8f9bac302e759e0f7ebee/

[13] https://inc42.com/startups/eyes-in-the-sky-india-drone-startups-looking-for-major-pie/

[14] https://www.mdpi.com/2504-446X/6/11/317

[15] https://www.electronicsforu.com/market-verticals/aerospace-defence/counter-drone-techniques-to-detect-neutralise-hostile-drones

[16] https://dronesurveyservices.com/can-military-drones-be-hacked-2/

[17] https://sigblog.hexagon.com/integrating-ai-and-machine-learning-into-c-uas-systems/

[18] https://dronesurveyservices.com/can-military-drones-be-jammed/