IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

UAV Technology And National Security Challenges

Prof. Prashant Agarwal,

Department of Defence and Strategic Studies, University of Allahabad, Prayagraj, Uttar Pradesh

Brigadier Sunil Mishra

Research Scholar, Department of Defence and Strategic Studies, University of Allahabad, Prayagraj, Uttar Pradesh

"We are entering an era in which Unmanned Aerial Vehicles of all kinds will take on greater importance in space, land, air and sea.[1]"

- *President George W Bush*

Introduction

Unmanned Aerial Vehicle (UAV), Remotely piloted vehicles (RPV), Remotely piloted Aircraft (RPA), Unmanned Aerial Systems (UAS) and the most used terminology, "Drone"[2] (Matthew Urwin, 2022) is proving itself to be a revolutionary technology due to its affordability, versatility, and ability to adapt to the user requirement. It has increased from daily entertainment to logistics, policing, law enforcement, communication coverage, remote sensing and surveillance, weather forecasting, and remote seeding of forests to agriculture. Drone technology is emerging as a game changer that offers practical, efficient, and reliable solutions. Integrating AI and ML with the onboard Sensors, optical devices, thermal imagers, and deep penetration radars with the UAVs in future warfare will be pivotal as the present fighting tactics and equipment are oriented for ground operations with limited air and underwater orientation. The emerging shape and the possibilities the UAV hold make it a "weapon system of the future"[3] (Gettinger Dan, 2021) and a potent tool for Network Centric Warfare.

Development of UAVs as Strategic Tool.UAVs, from mock-up targets for Air Defence Guns in WW I to deception models in WW II, entered the domain of Unarmed Combat Aerial Vehicles(UCAV) with the USA, UK, USSR, Israel, China, Turkey and Iran as significant players. Defence Advance Research Project Agency (DARPA)[4]of the US weaponised UAVs with stealth technology, real-time onboard data management and satellite integration. China miniaturised and commercialised the UAVs at an affordable price, and the "proliferation of UAVs is vast and diverse, and the drone capability has also been exploited by Non-State Actors, UN-designated terror groups and armed rebel groups"[5] (Bergen et al., 2020) coupled with a lack of tools needed to prevent misuse will a significant security challenge in the future.

The use of unmanned aerial platforms started in 1849 during the siege of Venice, sowing the idea of using an unmanned aerial platform to attack from unexpected directions. The UK developed the first remotely controlled pilotless aircraft (Hewitt-Sperry (1917), leading to Queen Wasp (1938), Germany's V1 Bomb, and the US developed Project Fox (1940). Post-war, UAVs were developed and used by the US during engagements in Vietnam and North Korea.

Armed use of UAVs

The USA, Israel, the USSR, China, and France invested in UAV technology to develop it as a strategic tool. The US used UAVs in 2001 to target Al-Qaeda and the Taliban, Israel used them during the Gaza conflict (2004), and Pakistan used NWNP in 2016.The "capture of the US Predator UAV during a failed mission in Iran"[6](Peterson Scott,2011) in 2011 and the uncrewed underwater vehicle by China in 2016 brought the counter UAV technology into the limelight. China invested heavily in developing commercial drones, holding "80% of the (USD 20.8 billion) world market share"[7], and the commercial drone market will likely" grow to USD 501.4 billion by 2028"[8].

The weaponised use of Drones during the Global War on Terror led to the loss of civilian life and property at Federally Administered Tribal Areas (FATA) on 12 Sep 08", at Makin (Pakistan) on 23 Jun 09, and in North Waziristan on 17 Mar 11,raised severe human rights concern. The US and Israel launched multiple UAV missions to target Iran, and Iran, in turn, captured an American RQ-170 UAV on 05 Dec 11toproduce its drones from the captured technology. The killing of Maj. Gen. Qassim Suleimani, the architect of Iranian intelligence on 03 Jan 20,becamea "significant and landmark security event in the US-Iran relationship"[9].Terror groups such as ISIS used commercial DJI Phantoms drones to drop explosives in Iraq and Syriain 2016 and 2017. Other prominent uses include: -

- A pre-programmed, autonomous drone swarm on Russian Airbase in Syria on 09 Jan 18.
- "Assassination attempt on Venezuelan President Maduro"[10]on 04 Aug 18.

- Houthi rebels attacked Aramco's Abqaiq oil-processing plant and Khurais oil field on 14 Sep 19, a military parade on 10 Jan 19 in Yemen and a second attack on an oil facility and the airport of Abu Dhabi on 17 Jan 22
- Pakistan used explosive-laden drones to target an Indian Air Force (IAF) base at Jammu on 27 Jun 21.

Drones have also been used to disrupt public life, which has raised serious concerns among security agencies worldwide. A few examples are as under: -

- On 18 Sep 13, an explosive-laden quad copter crashed in front of German Chancellor Angela Merkel during a rally in Dresden.
- On 15 Oct 14, during the Euro 2016 Qualifier match at Belgrade, a DJI Phantom drone carrying an Albanian flag flew over the pitch.
- On 26 Jan 15, a DJI Phantom2 drone flew over the White House fence and crashed on the lawn.
- On 22 Apr 15, a DJI Phantom 2 carrying a radioactive payload crash-landed on the Japanese Prime Minister's residence.
- On 19 Dec 18, 93 drone sightings at Gatwick Airport in the UK led to the suspension of air operations for two days and the cancellation of over One thousand flights, affecting around 140,000 passengers.

Military use of Drones: The use of Drones in conflicts like the Vietnam War and Iraq was limited to surveillance; however, in recent conflicts, the use of UAVs tilted the results in favour of the weaker side, highlighting the strategic significance of UAVs. The **Armenia-Azerbaijan** conflict from 27 Sep to 10 Nov 2020 was the 'first conflict to witness extensive and effective use of UAVs'[11].Armenia conventionally had "marginal superiority over Azerbaijan, and Azeris, to overcome the same, invested extensively in drones from Israel and Turkey"[12]It adopted the "war strategy of surveillance by drones to identify positions of troop, tanks, artillery, and air defence systems locations months in advance"[13]forces. The Drone strikes, with voice overlays and captions, were released to news channels and social media, which generated public outrage in Armenia and lowered the morale of the armed forces and the national leadership. The **Russia-Ukraine War** saw 'active participation in the Drone Warfare by both sides'[14]. The Ukrainian Ground Forces (UGF) unit "Aerorozvidka is leading the drone war with active assistance from the West'[15], to 'successfully avert the fall of Kyiv by dropping explosives with mines on the advancing Russian columns'[16] and attack Moscow.

Drones with better manoeuvrability, lower operational cost, better sensors, precision-guided weapons, and difficulty in interception proved to be 'affordable airpower' and a challenge to the conventional Air Force using expensive human-crewed aircraft. These conflicts also highlighted the difficulty in defending static assets and mass mobilisation. The UAVs, though, offer advantages, but they are also prone to vulnerabilities and concerns, including privacy concerns, clarity in Policies, safety issues, cyber-attacks regarding GPS spoofing, and data exploitation.

National Security Challenges

Policy Issues: Utility UAVs have increased to all walks of life, and their operation remains largely unregulated. Rajeswari and Rahul Krishna (May2018) articulate it as 'globally, rules and regulations around the use of drones are still in its infancy[17]'or, as Amit Bansal (Aug 2021) puts it for a country like India 'legal framework to own and operate a drone just do not exist,[18]and the regulatory body required to address these concerns are yet to be nominated in most countries. Due to sizeable global demand and limited supplier countries, manufacturers remain dominant in influencing favourable policies. The import and export of UAVs and their components lack accounting, and even the countries with UAV laws lack enforcement tools, a mechanism to monitor, reliable Counter UAV systems and a protocol to fix responsibilities for violations. Under such circumstances, a sound national policy to prevent rogue use and ensure genuine user rights will remain challenging for policymakers.

Air Defence Challenges: Modern air defence systems have put a very high degree of caution on fighter aircraft, making them cost-prohibitive. The AD systems proved ineffective against low-cost drones and anti-radiation missiles, and the "air defence systems of the Assad regime failed repeatedly"[19], "Israel destroyed the Russian Pantsir in Idlib"[20]in Syria, and "Russian SHORAD's used by Libyan National Army (LNA) met a similar fate against Turkey drones"[21]. The "precision attack on the Saudi Arab's Abqaiq & Khurais oil faculty"[22]by a swarm of 18 drones and seven cruise missiles exposed the efficacy of US-supplied Patriot AD Systems. The drones will be a significant challenge for the countries dependent on Russian and USAD systems.

Aviation Security: The exorbitant costs of aircraft, highly flammable aviation fuel, and low survival rates in aviation accidents make aviation security a challenge. In the case of the armed forces aviation assets, the sensitivity increases manifold due to the cost and strategic depth they provide. Aviation assets are most vulnerable when they are static, as even a minor blast near the fuselage or aviation oil storage tanks will lead to a sympathetic detonation to other aircraft parked in the open. The use of UAVs to disrupt the air operation at Gatwick airport and the ease with which it dropped the explosive at the Jammu air base is a testament to this fact. Similarly, the UAVs can engage the rotary wing assets operating at low altitudes using direct impact or by firing low-cost projectiles.

Sub-Conventional Challenges: Non-state actors are carrying out UAV operations to inflict economic and military damage to the opponents while keeping the deniability and the damages below the threshold of war. Improvised explosive device (IED) blasts have been the most successful tool used by terrorist groups to inflict casualties, and UAVs have become another potent tool in the hands of terrorists. The US-Russia, Russia-NATO, 'South China Sea (SCS) littoral countries'[23]and the US-Iran engagements will see the increased use of UAVs by non-state actors to execute surveillance, sabotage, intercept strategic moves, assassinate the leadership, disrupt communication, and deny internet-based services.

Commercial Vs Security Concerns: The UAV tech is a significant boom to commerce and industry, as it enables the exploration of unchartered areas, helps to cut costs, and enhances equipment efficiency. Governments are encouraging the use of UAVs to aid industry commerce and contribute to the overall economy of the Country, resulting in uncontrolled use of air space by UAVs. The increase in unregulated air traffic is a potential danger to life and property below the airspace due to accidents and deliberate misuse. Imposing restrictions to address security concerns will be a grave injustice to genuine users. Similarly, unregulated use of airspace, unhindered proliferation of technology, and lack of user policy on UAVs provide a potent tool in the hands of inimical elements. UAV-using countries face the challenge of balancing the two factors.

War Fighting Challenges: The innovative use of UAVs during the Armenia - Azerbaijan and Russia - Ukraine war will redefine the concepts of war fighting concepts in future. The simplicity with which it can engage a broad spectrum of targets ranging from well-entrenched infantry to manoeuvring armoured columns, from well-camouflaged artillery to widely dispersed air defence radars and air assets to emerge as Poor Man's Air Force. From an eye-in-the-sky role to a communication disruptor, from a jammer to a low-cost bomber, the technology has immense potential to disrupt conventional war fighting. This development will force conventional armies to relook at the military hardware they want to keep, as UAVs give enormous possibilities to the weaker side to stand and fight innovatively.

Lessons for the Future

Every decade, new technology challenges strategists and security planners, and Drone technology is the new challenge for the present generation. The disruptive potential of misuse of technology needs to be handled holistically as the use of rouge in a geographical location will be minuscule compared to the number of genuine users. Governments, especially in developing countries, need to adopt this technology, encourage its use and facilitate its growth through favourable policies. Counties with hostile borders and internal security threats need to countermeasure the rogue use of UAVs by a combination of regulated import and export of UAVs and their components and registration for use. Military leaders and policy planners must adopt the UAV technology in the overall military strategy.

Policy Measures: The legal framework being framed and promulgated for using UAVs and preventing their misuse must meet future challenges, encourage, empower and ensure the rights of genuine users at the same time be exemplary prohibitive to the rouge users. The policy measures must guarantee that the manufacturer and the end user adhere to the internationally accepted safety protocol. The policy measures should ensure easy and ample availability of the components, economic assembly and custom-made UAVs for exploitation. This entails identifying components, supporting infrastructure, defining the regulatory framework, exemptions, and facilitation measures by the government.

The government must also establish a dedicated regulatory authority delinked from the present setup controlling the airspace to formulate and promulgate policies. The tasking of the proposed regulator body should include the following:-

- Ensure user guidelines and declare prohibitionary zones.
- Check the utilisation of critical components and ensure the worthiness of the airframe.
- Coordinate the functioning of multiple agencies involved in drone operations.
- Nominate testing agencies and training schools for drone operations.

Indigenisation of Technology: The weapon-exporting countries will hype the UAV threat to force developing countries to buy off-the-shelf solutions to meet immediate challenges at an exorbitant cost. It will be in the interest of the developing countries to invest and seek indigenous and cost-effective countries UAV solutions. Dependence on improvised solutions will keep the importing countries in a constant loop of recurring expenditure with minimal scope of getting out of it as the technology will evolve to overcome the countermeasures.

It is also advisable that if the technological threshold is not available within the country, transfer of technology and joint production be preferred over outright purchase to indigenise the technology and lower the cost of production.

Regulated Production: Commercial UAVs can be assembled from components available on online commercial platforms, such as YouTube videos, and can be customised for specific use. China is the largest manufacturer of UAV components at cheap rates, and it dominates the market. Government protection gives Chinese companies a decisive edge in establishing a monopoly. The sale of UAVs and their distribution needs to be guarded by electronically numbering the UAVs. Secondly, the components must also be bar-coded to identify the point of origin and sale. Lastly, drones capable of flying beyond the line of sight with guided mechanisms need to be registered on the regulator's website before flying permission is granted. To make the system user-friendly and avoid cumbersome processes, the complete process is suggested to be paperless and accessible online.

Airspace Management: The workable solution for regulating air space for seamless monitoring and detection of drones is to declare sensitive areas such as military installations, airports and VIP residential areas as no-fly zones. Areas needed temporarily for security reasons to be marked as restricted or orange zone, and balance areas were to be declared green zones for UAVs. The process of nomination of red and orange zones to be automated and geo-fencing of the area be carried out to indicate the UAV user of no flying area. The process will allow law enforcement agencies to treat any UAV in the red and orange zone as hostile. The other measure that can be mandated for UAVs with longer endurance, sophisticated onboard sensors, and payload capacity is GPS-enabled homing beacons for real-time monitoring. The Government of India's initiative to launch the

Digital Sky Platform lays down the drone rules and counter rogue drone policy, which is the correct way of progressing the technology as it encourages self-compliance instead of intrusive.

Counter Drone Measures: The government of India has formulated rules to counter the rogue use of drones to empower security agencies, discourage misuse, and provide technical guidance and education to the agencies. At the functional level, there are many gaps to cover, including the need to understand the technology, formulate methods to secure the sensitive areas and acquire counter-drone equipment for detection, monitoring and engagement. The technical threshold in counter-drone with most developing countries is shallow, and the available options are expensive and cannot be procured in large numbers. To overcome this, there is a need to encourage academia, industry, and technology partners to invest in research and development and produce in-house capability for mass use and broader coverage.

Law enforcement border guarding and guarding sensitive installations require different systems and equipment to detect, monitor and engage hostile UAVs.UAV Radars are the most reliable equipment for identifying UAVs, however, there is a need to reduce the bird clutter activity by employing artificial intelligence and machine learning tools. The best way to confirm radar detection is to employ an electro-optical device, radio frequency analyser, or infrared device. Training and orientation of handlers of the anti-drone equipment will be critical for success. To cover the larger area, automation and integration issues and gaps in the existing system, GIS tools must be used to identify probable launch points and drone approaches. Similarly, layered deployment of anti-drone resources and physical denial methods are also suggested.

UAV radar, GPS jammer, RF analyser, electro-optical, and IR devices used by Indians and other developing countries require integration to make the drone operator effective. The integration will give a fail-proof picture to the operator for positive engagement in the limited time available, as manual confirmation from all the sub-systems will not be practically possible in critical situations. The present configuration of UAV equipment needs to be miniaturised to make it suitable for handling, mobile warfare and rapid deployment. The anti-drone equipment cost is too high for developing countries to afford at a mass level. The answer to the above technicalities is indigenisation, investment in R&D, involving all stakeholders in a common approach to the issue, and seeking low-cost, innovative solutions to counter the emerging threat. The drone-based architecture for detecting, monitoring, and neutralisation should also be considered to make counter-drone operations effective.

Conclusion

It is established that UAVs will dominate the battlefield for at least a decade as war-fighting tools. The developing countries should maintain different versions of UAVs to provide multiple options for the tactical,

operational and strategic commanders. Similarly, using manned aircraft classically for the offensive roles due to effective air defence measures will be cost-prohibitive and demoralising, and there is a need to explore the possibility of strike capability by unmanned aircraft. As a war fighting concept, a new approach and policy orientation are required at all levels to use UAVs for offensive and defensive roles. Hardening of AD and air assets, innovative methods for deception, camouflage and concealment need to be revised to survive the drone threats. UAV threat awareness during the training of troops and developing survival tactics against drone attacks is also required to minimise damage. The anti-drone measures are time-consuming and resource-intensive and should target the drone handler instead of the drone, which should be the correct approach.

References

1. *President George W Bush*
2. Drone?https://builtin.com/drones
3. Gettinger, Dan, May 25, 2021, Weapons of the future: Trends in drone proliferation,https://www.defensenews.com.
4. https://www.darpa.mil/about-us/darpa-history-and-timeline
5. Bergen Peter, Melissa & Sterman David, July 30th, 2020, World of Drones, https://www.newamerica.org.
6. Centre for a New American Society, http://drones.cnas.org.
7. Auto- Journalism, April 4, 2022, Top 10 Stealth Drones In The World, https://autojournalism.com/top-10-stealth-drones-in-the-world/
8. Armstrong Williams, JANUARY 21, 2022, Weaponized drones are here - it is time for the US to act, https://thehill.com/opinion.
9. BBC News, December 8, 2011, Iran shows film of captured US drone, https://www.bbc.com/news/world-middle-east-16098562
10. McLaughlin, Eliott C, Sterling, Joe and Pozzebon Stefano, August 7, 2018,https://edition.cnn.com/2018/08/06/americas/venezuela-maduro-apparent-assassination-attempt/index.html
11. The Print, November 14, 2020, How drones helped Azerbaijan defeat Armenia, and the implications for future modern warfare, https://theprint.in
12. Shaikh, Shaan, Wes Rumbaugh, December 8, 2020, The Air and Missile War in Nagorno-Karabakh: Lessons for the Future of Strike and Defense, https://www.csis.org.
13. Shaikh,Shaan,Wes,Rumbaugh,December,8,2020, https://www.csis.org/analysis/air-and-missile-war-nagorno-karabakh-lessons-future-strike-and-defense
14. Bryen, Stephen, June 20, 2022, Russian counter-drone capabilities are improving https://asiatimes.com.
15. Hambling, David, May 25, 2022, https://www.forbes.com.
16. Stephen Rice, Feb 4, 2019, https://www.forbes.com.
17. Shukla, Samir, Times of India, April 29, 2022, Government policies for AI to Drones: Bridging socialist agriculture with the capitalist market using emerging technologies. https://timesofindia.indiatimes.com.
18. Surajeet Das Gupta, 'In the danger zone: Why regulating drones is a policy challenge for India', Feb 11, 2019,https://www.business.
19. Kevin Townsend, September 26, 2019, Sky-high concerns: Understanding the security threat posed by drones, https://blog.avast.com.
20. Frantzman, Seth June 06, 2020, Russian air defence systems outmatched by Turkish drones in Syria and Libya, https://www.longwarjournal.org

21. Eurasian Times Desk, May 23, 2020, From Syria To Libya, Turkish Drones Outsmarting Russian Air Defence Systems? https://eurasiantimes.com.
22. Stephen Kalin, Sylvia Westall, September 18, 2019, Costly Saudi defences prove no match for drones, cruise missiles, https://www.reuters.com.
23. Chan Minnie, February 12, 2022, the Chinese military plays a game of drones from the Himalayas to the South China Sea.