ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

# CYBER PSYCHOKINESIS

**Anuja kokate (10A IGCSE)**
Sanjay Ghodawat International School, Atigre
Email ID- nuja9906@gmail.com

**Abstract**

Nowadays, the most rudimentary option to spy used is drones, it carries its own features which attracts many to use it for espionage but few techies are too. This demand for more grows due to its multi-purpose application, it literally provides bird -eye to watch anything or hear too for far distance accessible almost anywhere and any time. Although, ascendency carried its own vulnerabilities too. For years, malicious use of drones among criminals and technocrats alike. The probability and frequency is highly devastating so we need specific counter measures to be taken beforehand or during one attack or even after to restrain more noxious effects on the system. This paper aims to highlight possible attacks, emerging threats, and countermeasures too. Moreover, this paper will emphasize the use of unmanned aerial vehicles in various domains (ex. Military, medical, terrorism etc.) and critically focus on association with the cyber world. On an experimental approach an adequate important citation is maintained to make readers aware of vulnerabilities of UAV in various domains and come up with enhanced techniques to detect and prevent one. As a result, various antidotes can be reviewed.

**Keywords:-** Cyber threat, Security, Drones, Malicious activities, Domains and many more.

## Introduction:-

### I. Use and vulnerabilities

The reliance of drones is increasing globally due its various hallmarks like live streaming, image capture and real time video experience, along with its capability to fly and transport goods. The prediction of size expansion to USD 11,295.1 million by 2028 while exhibiting a CAGR (Rate) of 25.39% between 2021 and 2028 [1] is very possible. This is mainly due its compatibility over commercial helicopters for price and size. These are identified as vulnerable to cyber-attacks because of their uniqueness of network and dispersed physical systems. Attacks which can result in the defective operation of the control loop, denial of service, demolition and exfiltration, and information. Drones aren't limited to civilian domains only but even used by law enforcement agencies and border surveillance proposes for intelligence. In this modern atomic world, drone technology is mainly used for military purposes and defensive areas. Its usage is rapidly growing

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal

for defense purposes. These microdevices are flying in the air 200 feet above the ground. This range of height varies from device to device and purpose to purpose. This range can be in Meters, kilometers and Feet. Flight time of these intelligent devices also varies from device to device.

| **PARAMETERS** | **2GHz** | **5Ghz** |
|---|---|---|
| **Frequency band** | Low speed | High Speed |
| **Cost** | Cheaper | Expenditure |
| **Range** | Extended range | Undersized range |
| **Noise effects** | Very much noisy | Slighter Noise |
| **Interference** | Prone to interference | Less prone to interference |
| **Physical barriers** | Overcomes physical barriers | Incapability to over physical barriers |
| **Performances** | Disturb Wi-Fi speed | Don't disturb Wi-Fi speed |

[2][3]

**A.** Effective rules and regulations

Many countries have tried to optimum to have strict rules for UVA usage for civilian purposes. For instance, in the USA a verified certification is essential for citizens of the country.

- One must be able to read, speak, write, and understand English (exceptions may be made if the person is unable to meet one of these requirements for a medical reason, such as hearing impairment).
- One must be in a physical and mental condition to safely operate a small UAS.
- 16 years age is minimum requirement
- One must pass an Aeronautical Knowledge Test—also known as the Part 107 test—at an FAA-approved knowledge testing center.
- One must undergo Transportation Safety Administration (TSA) security screening. [4]

Whereas, foreigners or special travel considerations have different sets of rules.

- Whether you plan to fly for fun or for work, you must register your drone with the FAA using the **FAADroneZone portal**.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

- If you plan to fly your drone for recreation in the U.S., you must take The Recreational UAS Safety Test (TRUST) required by the FAA.
- If you desire to fly for work, you must obtain a certification from the FAA and follow the rules for commercial flying.
- When traveling domestically in the U.S. with your drone, the U.S. Transportation Security Administration (TSA) allows the carrying of drones in carry- on luggage only. You may not pack your drone in checked luggage. [4]

Such rules are strictly expected to be followed by drone owners for safe drone flights. Heavy fines and punishments can be faced by the owners of the drone if such rules are violated.

**B.** Structural features of modern drones

A typical unmanned aerial vehicle is made of light composite materials to reduce mass and increase maneuverability. This composite material strength makes itself useful for military purposes at extremely high altitudes.

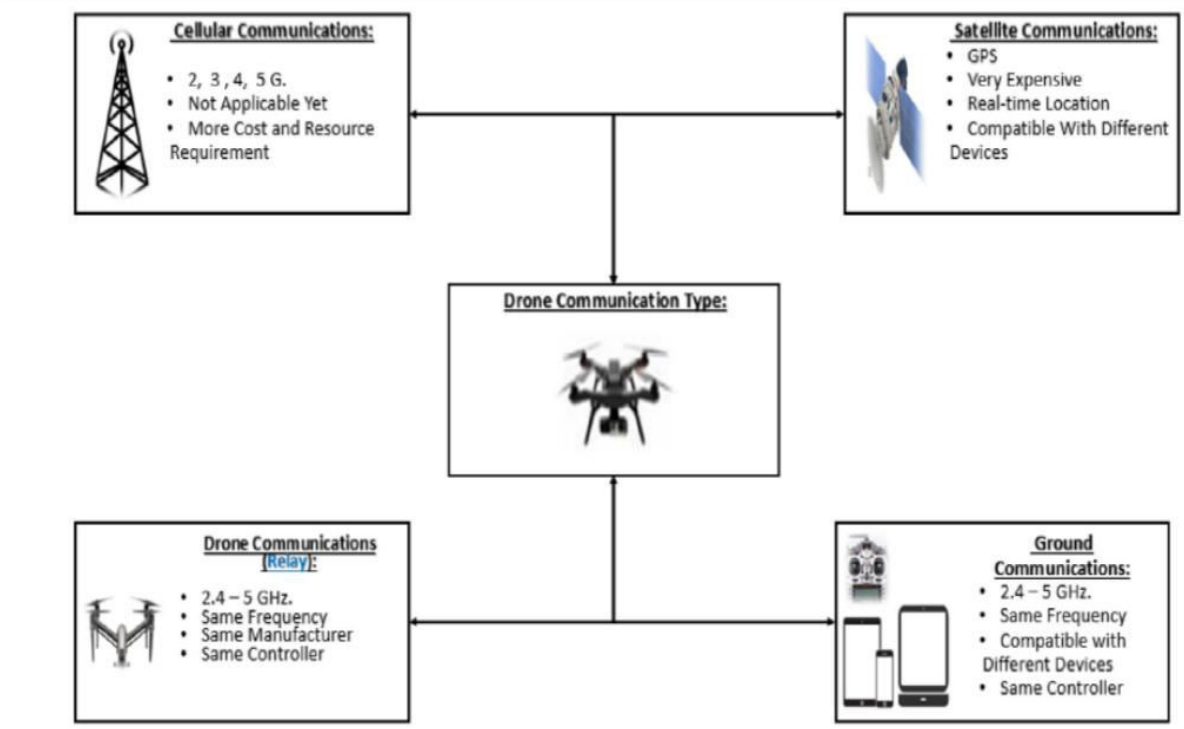
- UAV drones are equipped with different state of the art technology such as infrared cameras, GPS and lasers (consumer, commercial and military UAV). Drones are controlled by remote on ground called ground control systems (GSC) and also called as ground cockpit.
- An unmanned aerial vehicle system mainly has two parts, its own system and the control system.
- Sensors and navigational system are present in noisy parts of these air vehicles
- The rest of the body is full of drone technology systems since there is no space required to accommodate humans.
- highly complex composites are used to design to absorb vibration, which decreases the sound produced. These materials are very light weight.
- Few high tech drones follow various sensors making them really useful. For instance, Vision Sensor, Ultrasonic, Infrared, Lidar, Time of Flight (ToF), Monocular Vision [5]

**C.** Drone Communication Categorisation

- **Drone-to-drone**: Drone to Drone communication is not yet legalized.In wireless environment machine learning can be used as mode of communication. This is also known as peer-to-peer communication. Such communication is more prone to jamming and DoS attacks.
- **Drone-to-ground location**: This type of communication is mainly standardized specific protocols with 2 GHz and 5 GHz frequencies. It can also be operated via Bluetooth and Wi-Fi. Due security and authentication issues these kinds of communication modes can't be used in public areas. Such communication is more prone to eavesdropping and man-in-the-middle attacks as shown in Fig. 1.
- **Drone-to-network**: Such communication allows network selection for control and transfer of information. Several Wi-Fi networks can be used at different frequencies in such communication.
- **Drone-to-satellite**: GPS devices are involved to provide real-time communication in such types of drone communication. Drone communicates with the satellites for

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

latitudinal and longitudinal measurements. This communication is more secure and safe as compared to other categories and is used in the military. [6]

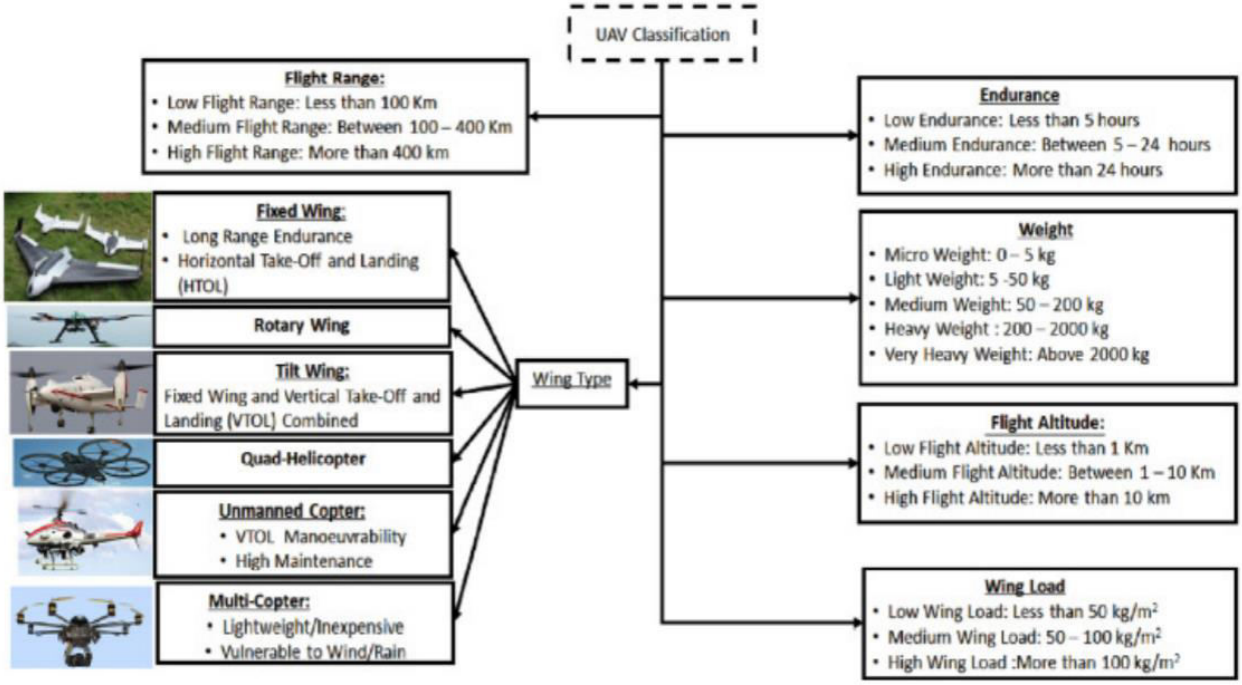



**D.** Types of Unmanned Aerial Vehicles

1) **Single-Rotor drones** Helicopters are very popular in manned aviation, but currently only fill a small niche in the drone world.
2) **Multi-Rotor drones** UAVs that use more than two rotors with fixed-pitch spinning blades that generate lift. ... By varying the speeds of particular rotors, it is also possible to make the drone turn or move in a various direction. One of the biggest ascendancy of this kind of aircraft is their manoeuvrability compared to fixed-wing aircraft. This enables them to fly in areas other drones can't reach, hover in a stationary position and provide vertical take-off and landing (VTOL) ability.
3) **Fixed-Wing drones** These usually carry heavier payloads for longer distances and flight times than VTOL (Vertical Take-off and Landing) UAVs, while using less power. This makes them functional for long distance missions, such as mapping, surveillance and defense, where long endurance can be an important factor.
4) **Micro Drones** are efficiently monitor the progress and track volumes and stockpiles, and can create real-time project overviews for better planning, safety and collaboration. Job tracking even reduces labor and materials waste for construction companies. These are even used in detecting gas leakages in methane pipelines specially.

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

5) **Racing Drones** Recently they added the Pro Class racing drone, which is currently the largest competitive drone racing format in the world. Racing drones are designed for speed and agility, as opposed to a photography/video drone which is focused more on hovering. [7][8][9][10][11][12]




## II. Drone security and Secrecy Apprehensions

Drone technology is always proven advantageous for surveillance needs. Security and privacy breaches are also addressed properly. Recording and capturing individuals without their consent can be proven illegal as privacy is hammered.

It is highly recommended to maintain secrecy, reliability, obtainability, verification and non-denial possessions above message passing in network range. This can be achieved through AAA procedures and progressions:

1. Authorization can be achieved by providing access to the control unit of the drone/UAV.
2. Verification can be obtained by using multi-level authentication using specific knowledge

Security threats to drones are not necessarily to be physical but cyber attacks are highly welcomed too. It's highly important to minimize civilian drone use only for military and

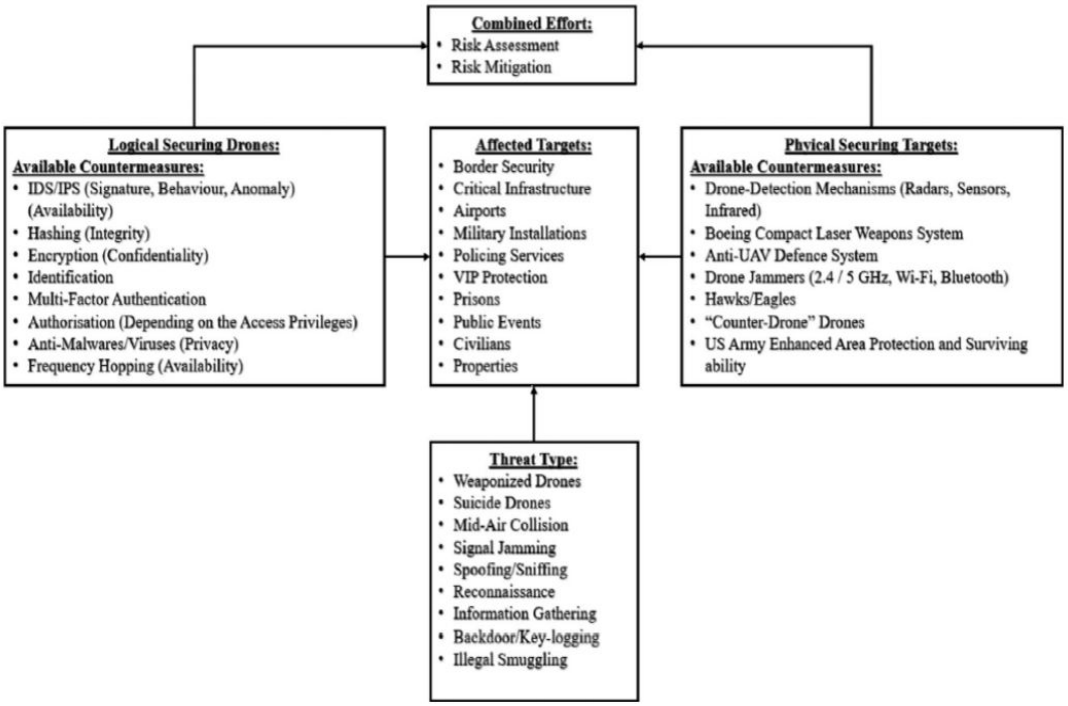
ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

surveillance purposes drone certification should be permitted. Drone owners use bluetooth or Wi- Fi to control drones in restricted areas, these kinds of breaches give techies a chance to hold control over drones and other electronic devices connected to the network. [13]

**A.** Safety apprehensions

A drone is very tiny, lightweight, and has high mobility characteristics. It can be used to monitor criminal activities which are done at a high level of privacy. Such acts can create damage to civilians. Several terrorist groups can associate armed objects with a drone to perform their illegal activities. Security doesn't constantly deliver protection. There are chances of damage done by the civilians in civilian areas which can result in financial loss [14]. The following list follows some safety concerns in brief.

1. Minimum safety features in architecture can lead to control drone usage. This can result in damage and loss [15].
2. Minimum mechanical and operative ethics include smashing avoidance techniques which can lead to drone's incapability to identify airliners [16].
3. Absence of Administrative knowledge: especially it mainly occurs when people have less knowledge of safety features [17].




**B.** Confidentiality apprehensions

Privacy is also the main factor to be considered by or for people. Drones must be kept out of those areas which are private. One must know the level of privacy of people before capturing or entering a private legacy. Three types of privacy threats are discussed below.

• Flying drones over someone's property is considered a major issue because of the risks associated with this act. Because such data can be used by scammers for negative purposes.

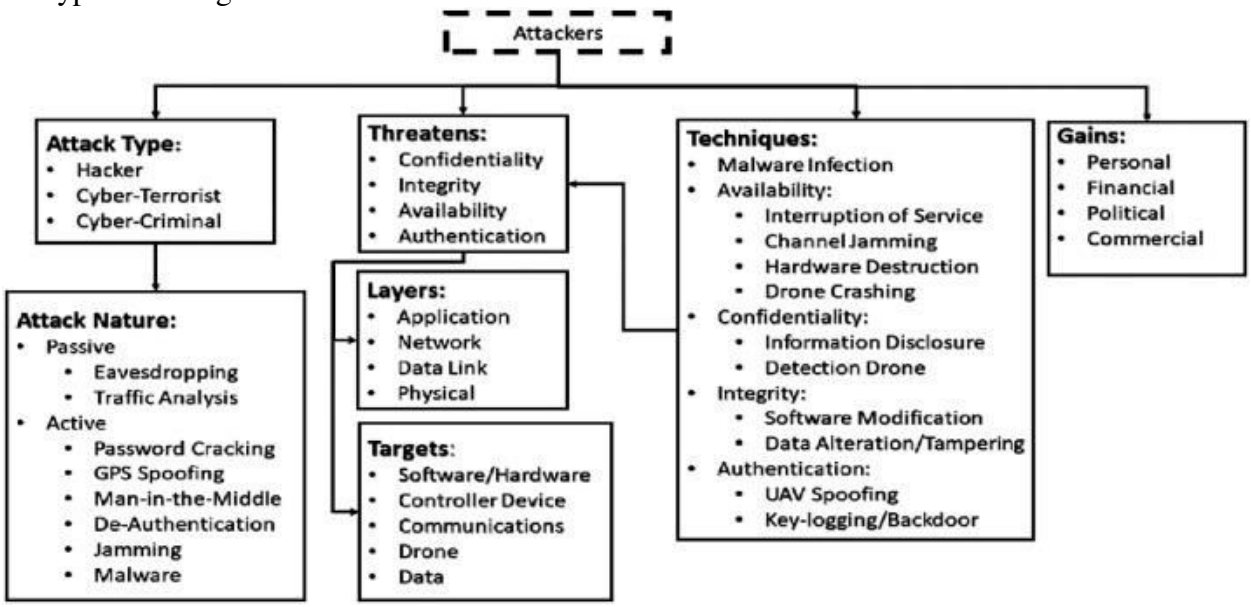
• Monitoring somebody's location must be avoided without their permission [18].

ISSN 2350-109X
www.indianscholar.co.in
Indian Scholar
An International Multidisciplinary Research e-Journal
MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

• Monitoring someone's acts and doings is also another unethical act which is also a matter of concern [19].

## III. Security threats to drones

Drone vulnerabilities differ according to its size, use and controlling mechanism. The typical designs of drones using the communication network are Wi-Fi networks with ground stations. These networks are vulnerable to security breaches. Moreover, due to improper chip encryption most pro drones are vulnerable to get hijacked. The bottleneck so far emerged was that with no encryption drones may be hijacked by individuals. The concept of IoD is highly fancied yearly millions are attracted to buy advanced drones connected to the internet but these drones are not designed with security mechanisms in mind. Few of the major issues are security and privacy leakages in IoD domains, data confidentiality, data protection, data flexibility, data accessibility, and data encryption and decryption strategies.




## IV. Relative counter measures

**A. Updating drone's firmware regularly**-There is always a security threat emerging when new drones are established, so regular updating can keep your drone ahead of the hackers.

**B. Use a strong password** for your base station application. Using a mix of characters, numbers and special signs to create a very strong passcode which might deter hackers; most can give up and go after easier prey. This should help avoid a malefactor hacking the drone signal.

**C. If you're using a smartphone or laptop as your controller**- Secure it and don't let malware infect the system. Use anti-virus software, and prevent downloading dodgy programs or apps.

**D. Subscribe to a Virtual Private Network (VPN)** from stopping hackers from accessing your communications connected to the network. VPN can act as a secure gateway to the internet and encrypts your connection, so a hacker can't get in.

ISSN 2350-109X
www.indianscholar.co.in

Indian Scholar

An International Multidisciplinary Research e-Journal

MISA MEMBERS OF INTERNATIONAL SCHOOLS' ASSOCIATION

E. **Set a limit**- Firmly number the devices to be connected to the base station, so that less vulnerabilities have occurred.

F. **Ensuring drones have a "Return to Home" (RTH) mode**. Once home point is set, it will enable the drone to return if it loses signal, if signal is jammed, or if the battery is depleted. This will make it easier to recover a drone from a hijack situation. However, because RTH depends on GPS to work, it's not immune to GPS spoofing.[20]

Above are preventive measures but if a surveillance drone is already bombarded by an attack detection can also follow methods.

- Radar is one of the useful methods used for detection, but completely not reliable; for instance, it can mistake birds for drones. Acoustic sensors can also be better way to detect unwanted drones, since they can be programmed to recognize the sound signatures of a particular type of drone.
- By using electromagnetic spectrum RF scanners can spot rones in open skies by recognizing drone transmissions. But GPS drones and non radio drones for navigation are completely impossible to find by this way.
- Finally, thermal imaging is also an effective method.Using thermal footprints electronics objects can be detected. However, there's a high rate of false positives too.[20]

**V. Future**

The (FAA) Federal Aviation Administration believes drones are expected to have a better market for commercial purposes than hobbtical ones. Drones could soon be reliable for deliveries, support surveying and mapping services, monitor crops, and be used for building up safety inspections too.

Given the possibilities, there will certainly be more drones around in air and will create a bigger drone security threat.

It may not yet be clear how drones can be proven functional to improve their security, but businesses will have to do so before commercial drone use becomes widespread. So, it's important that drone security issues are properly addressed by drone manufacturers or even owners too, and that you lock down your internet and home network to be safe from the menace of drone hacking.[20]

**References [20]**

1. https://www.globenewswire.com/news-release/2021/06/14/2246684/0/en/Commercial-Drone-Market-Size-to-Reach-USD-11-295-1-Million-by-2028-Stoked-by-Growing-Demand-for-Drones-across-Several-Applications-Says-Fortune-Business-Insights.html
2. E. Biddlecombe, “UN predicts 'internet of things',” July 6, 2009.
3. D. Butler, “2020 computing: Everything, everywhere,” Nature, vol. 440, no. 7083, pp. 402-409, 2006.
4. https://uavcoach.com/drone-laws-in-united-states-of-america/
5. dronezon.com/learn-about-drones-quadcopters/what-is-drone-technology-or-how-does-drone-technology-work/
6. https://thesai.org/Downloads/Volume12No5/Paper_84-Drone_Security_Issues_and_Challenges.pdf
7. https://aerocorner.com/blog/types-of-drones/

8. https://www.unmannedsystemstechnology.com/category/supplier-directory/platforms/multirotor-drones/
9. https://coptrz.com/fixed-wing-vs-multirotor-drones-for-surveying/
10. https://www.auav.com.au/articles/drone-types/#:~:text=Single%2DRotor%20Helicopter&text=Helicopters%20are%20very%20popular%20in,motor%20for%20even%20longer%20endurance.
11. https://www.unmannedsystemstechnology.com/category/supplier-directory/platforms/fixed-wing-uav/
12. https://www.microdrones.com/en/content/10-ways-microdrones-systems-are-being-used-for-business/#:~:text=Drones%20can%20efficiently%20monitor%20progress,materials%20waste%20for%20construction%20companies.
13. https://thesai.org/Downloads/Volume12No5/Paper_84-Drone_Security_Issues_and_Challenges.pdf
14. R.L. Finn and D. Wright, "Unmanned aircraft systems: surveillance, ethics and privacy in civil applications", Comput. Law Secur., vol. 28, no. 2, pp. 184–194, 2012.
15. H. Du and M.A. Heldeweg, "Responsible design of drones and drone services: Legal perspective synthetic report", 2017.
16. K. Wackwitz and H. Boedecker, "Safety risk assessment for UAV operation, Drone Industry Insights", Safe Airspace Integration Project, Part One, Hamburg, Germany, 2015.
17. E.B. Carr, "Unmanned aerial vehicles: examining the safety, security, privacy and regulatory issues of integration into us airspace", Natl. Centre Policy Anal. (NCPA), 2014.
18. R.L. Finn, D. Wright and M. Friedewald, "Seven types of privacy", European data protection: coming of age, Springer, 2013.
19. R. Clarke, "The regulation of civilian drones' impacts on behavioural privacy", Comput. Law Secur. Rev., vol. 30, no. 3, pp. 286–305, 2014.
20. https://www.kaspersky.co.in/resource-center/threats/can-drones-be-hacked