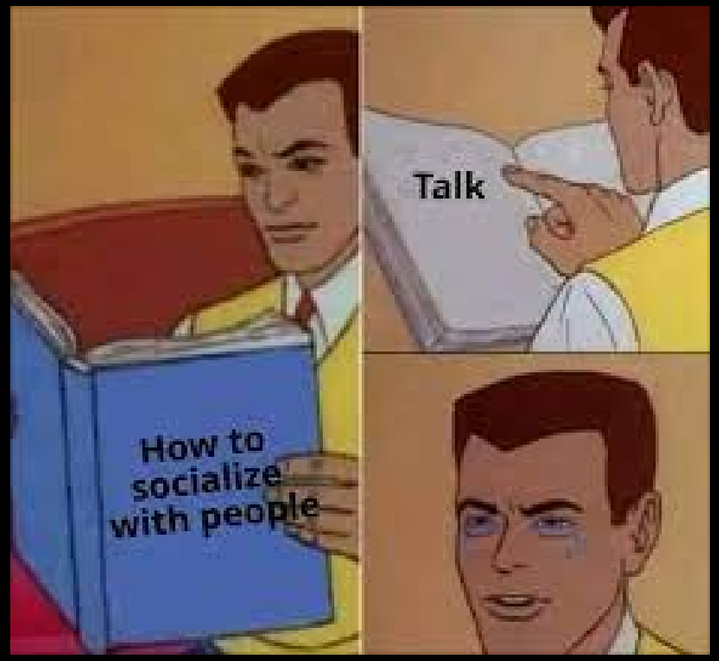
LEXIE THACH

Drone security basics

Presented by DC215 and The Tooolbox

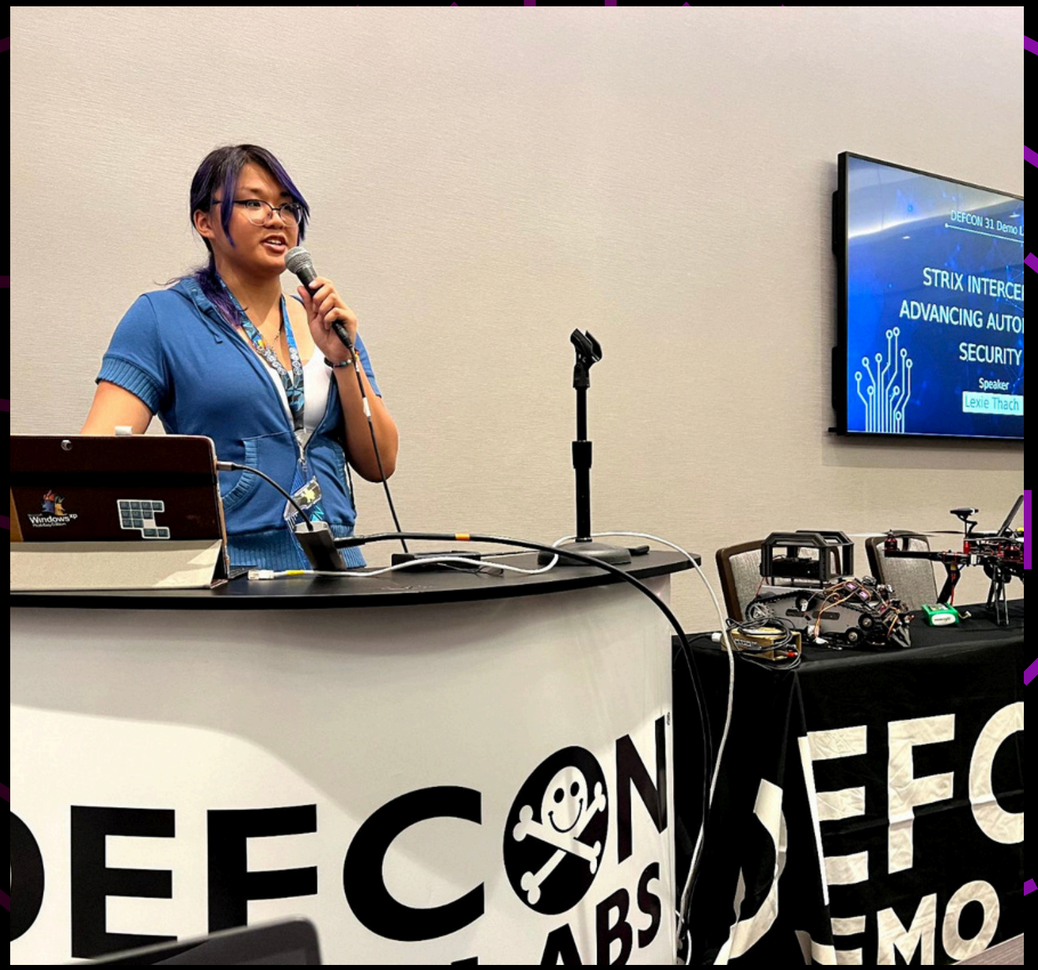
Objectives

- UAS technology foundations
- Drone security foundations
  - Legal Stuff
  - History
  - Direct Threats
  - Autonomy vs Automation
  - Attack vectors
  - Privacy and Trespass
  - Detection
  - Mitigation
- Drone Security
- Conclusion



Introduction

- My name is Lexie Thach
- I've worked around cyber, tech and development for the past 10 years
- I've done jobs from IT analyst to purple teaming and many more odd jobs in between
- Presented at local conferences and DEFCON
- My specialty is autonomous systems like drones, robotics, ICS/SCADA, and currently getting into AI/ML



Back to Agenda Page

LEGAL CONSIDERATIONS

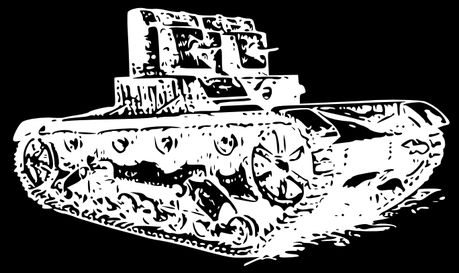
- FAA Regulations: The FAA regulates drone use, including interception and jamming. Unauthorized use could result in penalties.
- FCC Regulations: The FCC regulates radio frequencies, including those used by drones. Unauthorized interception or jamming is generally prohibited.
- Federal Criminal Laws: Various laws may apply to drone interception and jamming technologies. Interfering with licensed or authorized radio communications is generally illegal.

Back to Agenda Page

SPECIFIC LAWS

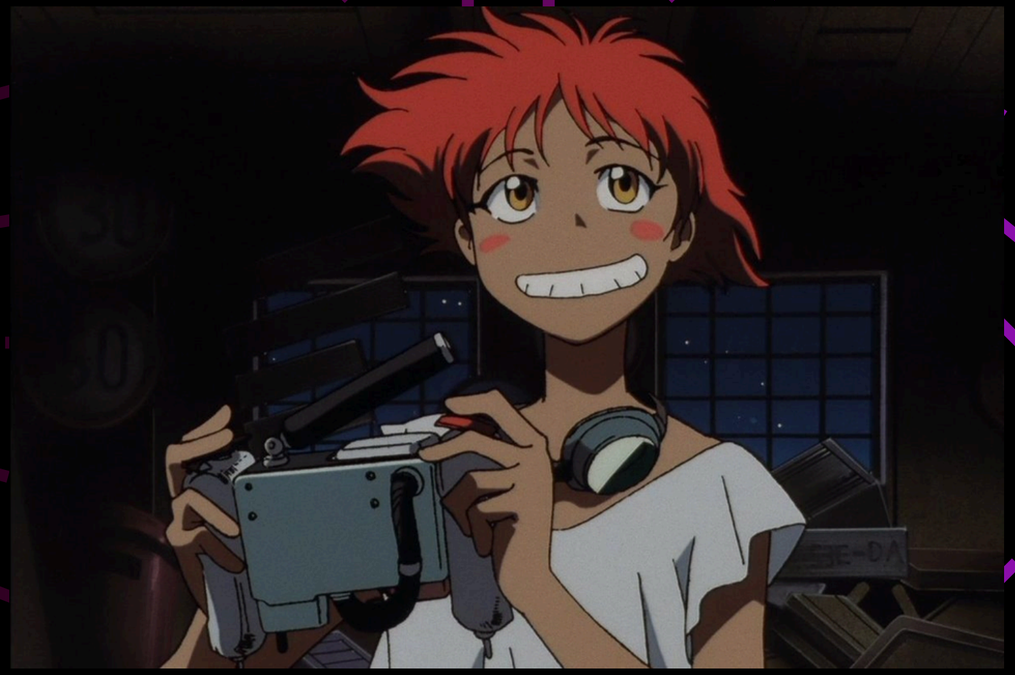
49 U.S.C. § 44801(5): Defines a counter-UAS system as a device capable of lawfully and safely disabling, disrupting, or seizing control of a drone. Does not cover detection-only systems.
Wiretap Act and Pen Trap Statute: These laws may apply to the interception of electronic communications, including those used by drones. Unauthorized interception could result in criminal penalties.
FAA Reauthorization Act: Allows certain government agencies to intercept or take control of drones that pose a security threat. These powers are not extended to private individuals or companies.
DHS Regulations: The DHS has regulations that may apply to drone interception and jamming, particularly in relation to national security and critical infrastructure protection.

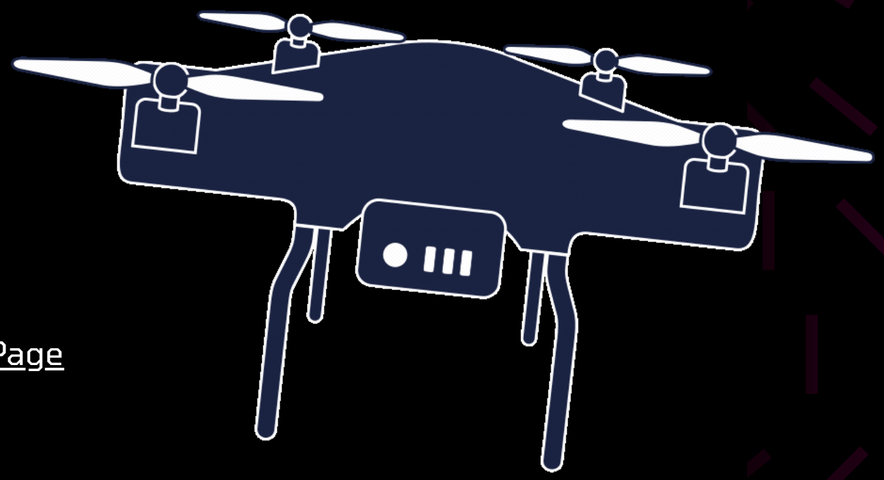
Back to Agenda Page



DRONE/UAV/UGV/RPAS/UAS/SUAS

ALSO CALLED: MULTICOPTER, QUADCOPTER, UNMANNED, REMOTE-CONTROLLED, GROUND VEHICLE





Back to Agenda Page

Unique uses

Search and rescue for hazardous fire operations

Drone light ‘firework’ shows

History

Back to Agenda Page

Late 1990s:

Initially used mostly by the military with minimal focus on cybersecurity, drones operated with low risk of cyber threats due to their limited technology and connectivity.

Early 2000s:

As civilian use of drones for photography and surveillance increased, so did the awareness of cyber vulnerabilities like GPS spoofing and signal interception, although comprehensive cybersecurity measures were still nascent.

2010s:

The widespread adoption of drones highlighted the need for robust cybersecurity, spurred by incidents like Iran's interception of a U.S. military drone, leading to advancements in secure communication and firmware protection.

2020s:

With drones now integral to various sectors and equipped with advanced technologies like AI, there is a critical focus on implementing sophisticated cybersecurity solutions including encryption and secure communication channels to protect against evolving cyber threats.

Typical Commercial Drones

Hobby

Make: DJI Phantom 4
Cost: $1000+
Range: 3-5km @ 30mins
Functionality: Video, Photos
Laws & Regulations:
30m from people and buildings 120m height limit
Night time flying with permit

Farming

Make: Yuneec H520
Cost: $5000+
Range: 1.5km @ 25mins
Functionality: Media, thermal vision, 3D Modelling, seed sowing, Laws & Regulations:
Notification and certs commercial Night time flying with approval

FPV Racing

Make: JohnnyFPV AstroX
Cost: $600+
Range: 500m @ 5-10mins
Functionality: Media, FPV vision Laws & Regulations:
Authorised ISM bands only

Core Concepts – Drone Security

Protection of friendly drones against attackers

Protection of the systems that support, manage (UTM) and counter drones (CUAS)

Protection against rogue drones

Christchurch Mosque Terrorist

Whilst the drone was not used directly in the attack, Forensic analysts seized a drone from his property which contained footage of the Mosque that had been attacked, and its vicinity.

This ISR aided in the planning of the attack and exfiltration of the area in the weeks leading up to the attack.

The footage was used as evidence in the criminal investigation.

ISR with a drone gives a much more detailed and updated look that Google Maps or satellite imagery.

https://www.stuff.co.nz/national/christchurch-shooting/122232602/christchurch-mosque-terrorist-used-drone-over-mosque-before-march-15-attack

DIRECT THREATS

Back to Agenda Page

C4 explosive with ball-bearings canister attached to a Mavic

Wireless detection device attached to an FPV drone

Malicious drone usage by Cartels

Raids continue to discover drones that are weaponised to attack other rival cartels or provide ISR before a raid.

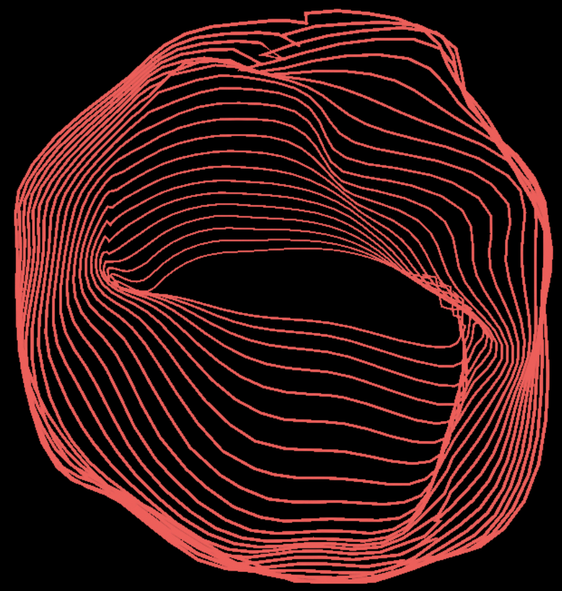
The innovation has included out-of-band, electronic triggers for both payload-dropping mechanisms and remote IEDs.

Whilst usually not used against civilians (other than those caught in the crossfire) the cartels are well-funded and often use larger drones (DJI Inspire, Matrice series) which can carry heavier payloads.

This weaponised use of drones is often foreshadowed by the much higher rate of use for narcotics smuggling over the US- Mexico border, and conducting ISR against human trafficking or border agents.

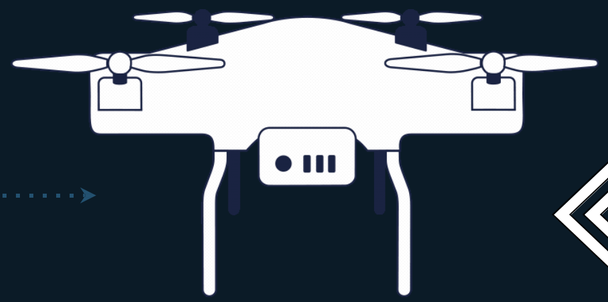
Autonomy vs Automation

- Autonomous drones can make decisions and adapt to changes in their environment on their own, using advanced sensors and AI.
- Automated drones follow pre-set instructions and routes, with limited ability to adapt unless manually adjusted by a human operator.



How does an autonomous drone work?

GPS



Drone

Approximate Location (5-10km)
Hardware Information (serial #s) Mobile/Controller GPS Location Drone GPS Location
Flight data (optional) NFZ zones
Profile Information / Username

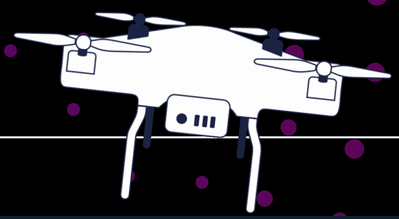
Fleet Management Server

4G/LTE control & video link

Telcom Tower

Drones vs Computers

Hacker with a laptop	Hacker with a hovering computing system
An attacker using a Virtual-Private-Network (VPN) for anonymity	A malicious operator disconnected to the threat via distance, controller and mobility
Malware with custom payloads to bypass Anti- Virus protections	Drone employs custom communication frequencies to bypass Counter-UAS protections
Internet Providers and foreign government log and record web activity and information	Drone manufacturers record flight data, logs and information to overseas servers



ATTACK VECTORS

Back to Agenda Page

Modding

A large portion of ‘hacking drones’ is reverse engineering them to modify, roll-back or patch the software, flash the firmware in order to bypass restrictions. This usually provides root access to the system, and can also be useful to forensic or security staff investigating a downed drone.

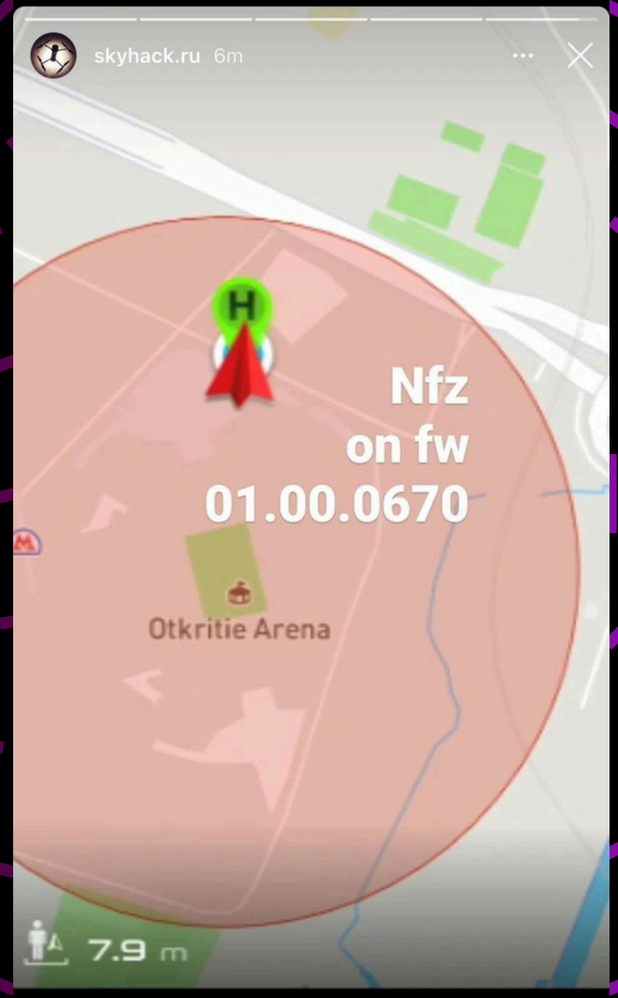
Common manufacturer-embedded restrictions and bypasses include:

- Height limits (e.g. removing 400ft altitude limit)
- No-Fly-Zones (e.g. flying in geofenced sensitive areas)
- ADB Root shell (access to the underlying drone filesystem)
- FCC-Boost (CE mode to FCC mode) Power output

- Moscow-based, Russian drone modding company SkyHack.RU release new DJI NFZ bypasses https://www.skyhack.ru/hacking/

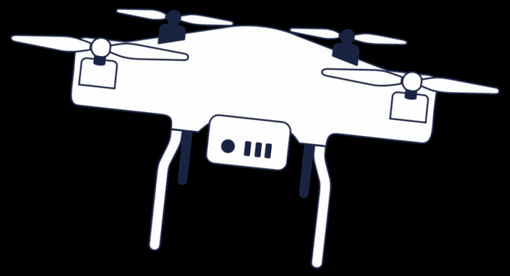
- No Limit Drones group has a Bug Bounty Program to fund the discovery of new modding bypasses https://nolimitdronez.com/bounty

- Drone-Hacks provides tooling that can save and share parameters https://drone-hacks.com/

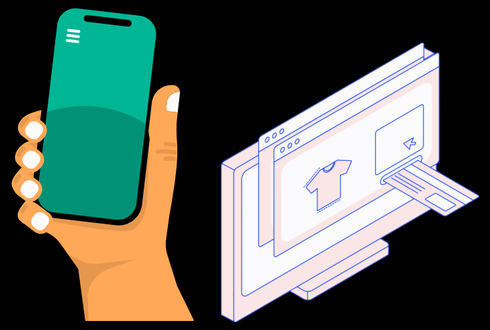


Back to Agenda Page

Security Classes (DJI Bug Bounty Program)



Drones and Hardware



Mobile Applications, Websites, Servers and Infrastructure

Severity	Server	Software & APP	Products & Firmware
Critical	Up to $5,000	Up to $30,000	Up to $30,000
High	Up to $1,000	Up to $5,000	Up to $5,000
Moderate	Up to $500	Up to $1,000	Up to $1,000
Low	Up to $200	Up to $500	Up to $500

The DJI Bug Bounty program outlines what is important risks to them. This includes not just their drones, but the underlying infrastructure and applications that connect it all together. Likelihood, impact and consequnce all play a part in the risk and payouts.

DJI Bug Bounty Policy

Back to Agenda Page

Attack Chain (Wi-Fi based drone)

1. Assess the air for drone MAC addresses

2. Connect/hack into to the drone's wireless network

3. Telnet/FTP/SSH into the drone's Operating System. Check your IP address

4. Use IPTables to block out the operator's IP address and whitelist your own

5. Hijack the video stream to your device

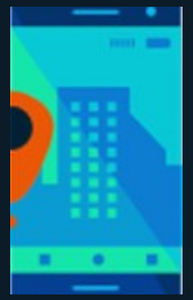
6. Port the controls to your system using Robot Operating

7. Fly drone away from the operator, steal data

Back to Agenda Page

Common Security Risks

Device/Application



- Hardcoded SSH/FTP/WiFi/Telnet passwords
- Vendor control, visibility and remote patching

Controller

- Provide more focused power/bandwidth (deauthenticate)
- Open WEP, Default/Weak WPA2 passwords
- Spoof controller commands and

Drone

- Prevent/lockout pilot on-board linux tools
- Privesc to extract data and video
- Hijack the video stream to the controller

Vendor Server

- Access user purchases, pictures, video, audio
- Access user flight records and telemetry data
- Access flight controls (automated drones)

Back to Agenda Page

hijack drone control

PRIVACY AND TRESPASS

Back to Agenda Page

Privacy

One of the most common privacy complaints are of hobby
drones ‘spying’ on people’s homes, backyards and children.
Often, these cases fall into the category of CCTV or public recordings; law enforcement seeking to use drones for crime control and first responder purposes have faced public backlash.
Another key privacy concern is the data collected by vendors and/or nation states. Drones can capture sensitive vision, survey, 3D modelling, thermal or wireless data which is stored and transmitted. Both a competitive and personal privacy risk, many are worried about the impact of nation states (where the vendors reside) utilising the information.
Examples include very detailed and clear imagery of:

- Critical infrastructure and telecommunications
- Airports, Ports, Power Plants and Military Bases

Person stalked 8 miles in car by rogue drone
https://bangordailynews.com/2020/01/25/news/portland/a-maine-woman-was-stalked-by-drone-but-police-said-they-were-unable-to-help/

Golden Valley PD drones caught in privacy outrage from community after surveilling nudists
https://edition.cnn.com/2020/07/19/us/drones-nudity-minnesota-trnd/index.html

Back to Agenda Page

Trespass

In many countries, the airspace above private property is not theirs to own or control. In most cases drones can fly (safely) over private property – the operator however cannot be situated on the property.

Slaughterhouses have had a long history of dealing with Animal Activists who fly drones to capture footage of animal cruelty – in most cases, the activists are acting legally.
Drones have also been connected with robberies of equipment and goods within stockyards. However, when the drones are spotted by crew, they are unable to react due to the operators piloting from a public area of land.
Reacting to a drone which is believed to have been trespassing is likely going to result in legal action against the land-owner, due to the drone being classified as an aircraft.

Man arrested and charged for shooting intruding drone:
https://www.news-leader.com/story/news/local/ozarks/2018/04/20/can-legally-shoot-down-drone-hovering-over-my-house-backyard-property/530286002/

Back to Agenda Page

COUNTER DRONES

counter-drone / anti-drone

Also known as:
CUAS, C-UAS, C-sUAS, C-UAV

Back to Agenda Page

“Drone Defense is Still Illegal”

One of the most succinct and in-depth frameworks for understanding Counter-Drones, and their legal implications.
It is useful for identifying the various types of detection and mitigation technologies today.

Regulation and legislation has driven more innovation in CUAS than cost, technology or technique.

Modality		No Control Possible	Positive Control Possible
Electro-magnetic Spectrum	Signal Disruption	Jam[20]	Spoof[21]
	EMP or Directed Energy	Fry[22]	-
	Protocol Manipulation or Malicious Payload	Brick[23]	Hack[24]
Cyber (preflight)		Brick	Hack
Kinetic		Shoot	Grab[25]

https://papers.ssrn.com/sol3/papers.cfm?abstra ct_id=3304914
“Drone defence is still illegal” – 2017
Jacob Tewes @flyinglawyer

Back to Agenda Page

DETECTION

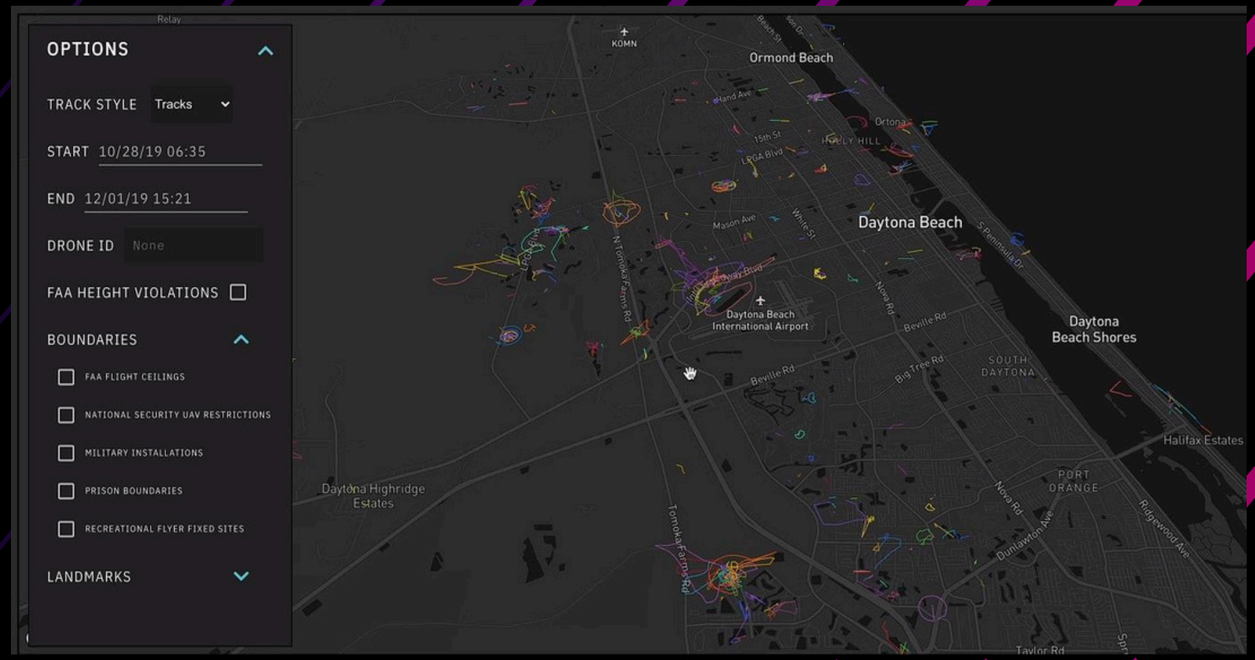
Back to Agenda Page

Types of Detection Technology

Detection is where no mitigation actions are taken against a drone. It solely relies on identifying the target drone, and if possible, the operator's location (controller).

Detection is useful for:

1. determining the drone traffic, trends or numbers before
   investing in mitigation technology
2. Alerting security teams to operator locations instead of making them aware by mitigating the drone
3. Enactment of SOP when a drone is identified, due to legal
   restrictions in mitigating the system
4. Aiding joint-air (UAM/UTM) scenarios where multiple drones, or aircraft and drones, may be present in the same airspace.



The URSA Inc platform visualising multiple UAS flights telemetry data

Back to Agenda Page

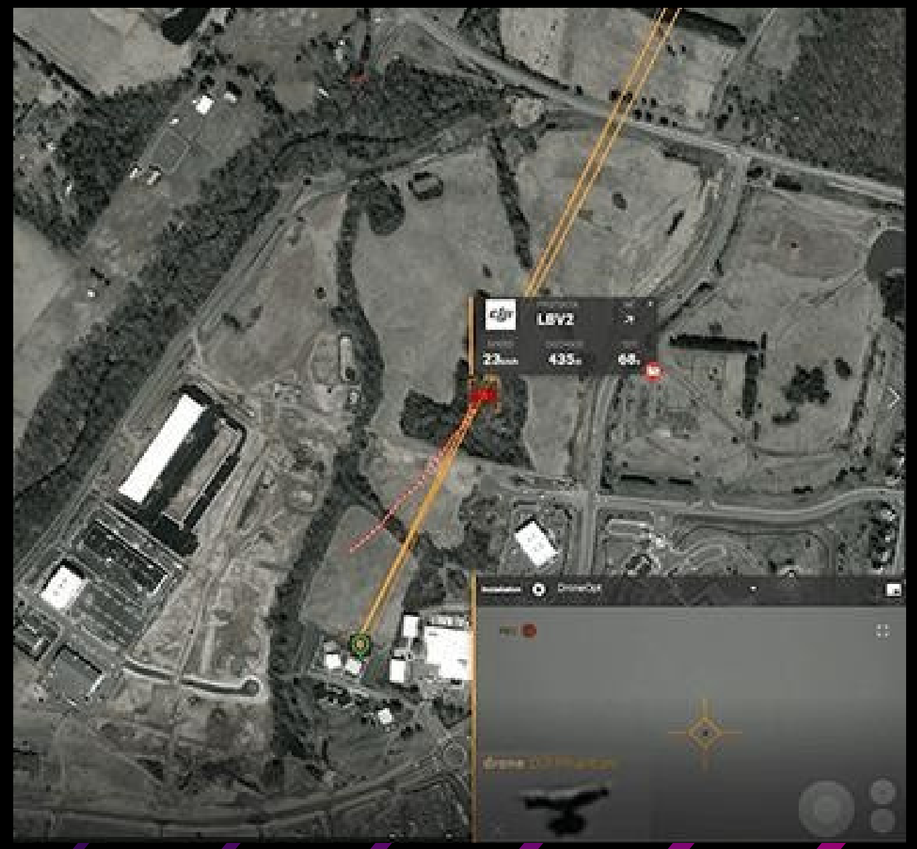
Types of Detection – Radio Frequency

- Pros:
  - Location of drone and operator can be determined
  - Passive technology, even PoC with a HackRF
  - Detection of multiple drones
  - Characterisation and details of drone/operator may be obtained
  - No interference for other communications on the network or in the operational area
- Cons:
  - A lot of frequency spectrum to cover
  - Only drones operating in the frequency being listened to will be detected
  - Not useful if communication protocol is manipulated or modified
  - May pick up false positives and noise in high-density areas
  - May not detect fully autonomous drones without any transmission

Back to Agenda Page

Types of Detection - Optical

- Pros:
  - Can be enhanced with AI and computer aided technology
  - Visuals can be taken and recorded digitally as evidence
- Cons:
  - Performance affected by weather conditions
  - Visual range is narrow, and detection is small
  - Possibility of false positives (birds, balloons, plastic bags)



Back to Agenda Page

Types of Detection - Radar

- Pros:
  - Long range with large azimuth coverage
  - Detection of multiple drones (swarms) and tracking capabilities
  - Geolocation of drone can be determined (3D, including elevation data)
  - Multiple frequency bands for emission for different penetrative capability
  - Weather independent
- Cons:
  - Possible false positives due to interference from environment or clutter
  - Transmissions may interfere with environment
  - Small vertical angle (10 to 30 degrees), leading to possible blind spots
  - Usually requires approval from authorities due to emission
  - Has azimuth and range resolution limitations

FLIR radar detector

Open database of drone cross-section radar signatures:
https://ieeexplore.ieee.org/document/9032332

Back to Agenda Page

Types of Detection - Acoustic

- Pros:
  - Can detect autonomous drones regardless of frequency used
  - Azimuth location of drone can be determined
- Cons:
  - Requires a huge database of drone audio signatures
  - High tech drone may be more silent, rendering this detection system useless at longer ranges
  - Modified drones may produce different sounds
  - May detect false positives (lawn mowers, planes, helicopters)
  - May not be able to accurately track multiple drones consecutively (swarms)

Robin Radar Acoustic System

Back to Agenda Page

Mitigation

Back to Agenda Page

Types of Mitigation Technology

Mitigation seeks to disrupt, destroy or capture the target drone
system. This may be conducted against the system, it's transmission or even disruption to the operator's controller. Mitigation has varying techniques each nuanced by their own legal implications and
dilemmas.

Mitigation is useful for:

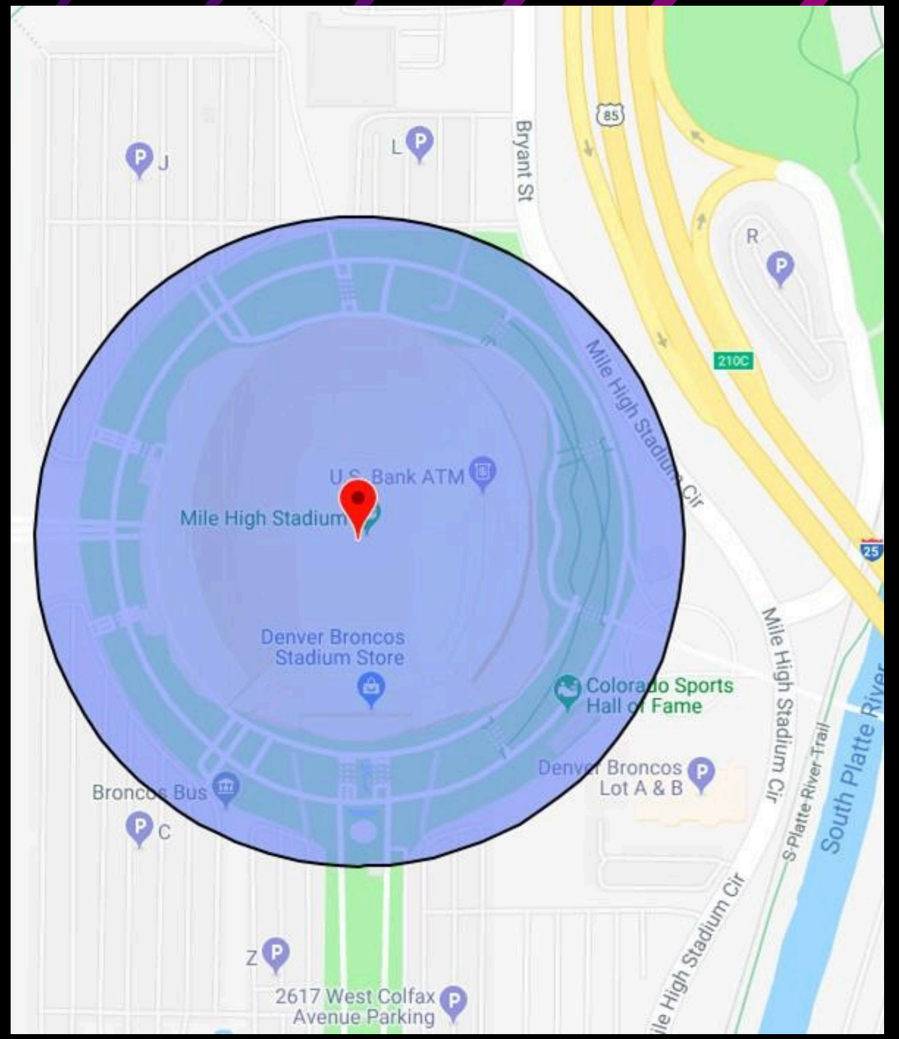
1. Preventing a drone from taking off at all in a sensitive area
2. Preventing a drone from entering a specific geographical area
3. Destroying a drone that might be carrying hazardous payloads
4. Force-landing a drone that may be of use to forensic analysts
5. Forced direction change for potential collisions
6. Forced spoofing back to the operator location for apprehension

Back to Agenda Page

SCI AeroGuard capturing a drone with a tethered net

GeoFences / GeoFencing

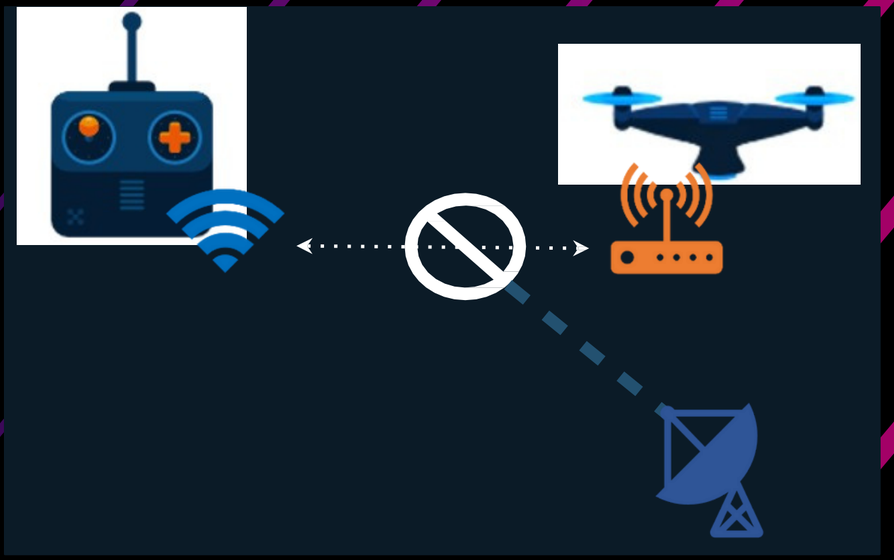
- Database of GPS Coordinates
- Sits on the controller/app and drone
- Prevents the drone from being flown in that geolocational area via GPS



Back to Agenda Page

RF & GPS Jamming

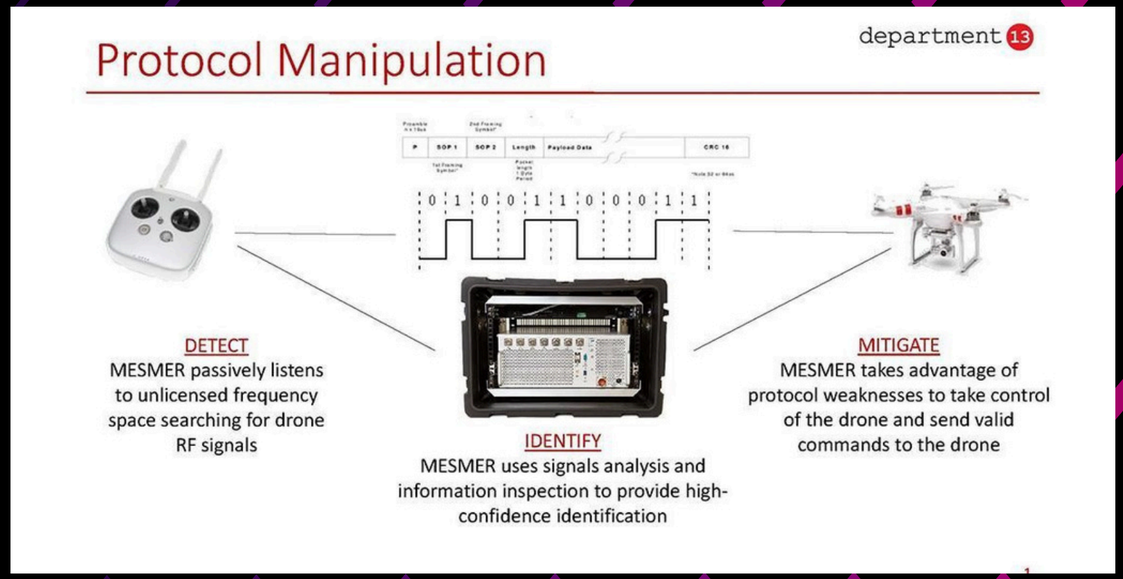
- Jams the connection between the controller and the drone, or the drone and GPS
- Most of the time is directional
- May include just RF or GPS/GLONASS jamming



Back to Agenda Page

Hacking (Spoof, Brick)

- Takes control of the wireless communication, controller or drone
- Uses protocol manipulation or exploits wireless weaknesses



Back to Agenda Page

The Drone Cyberattack That Breached a Corporate Network

Attack drones landed on the roof of an investment firm, ready to carry out their secret mission: breaking into the corporate network below. This is the true story of a drone attack that led to a corporate data breach.

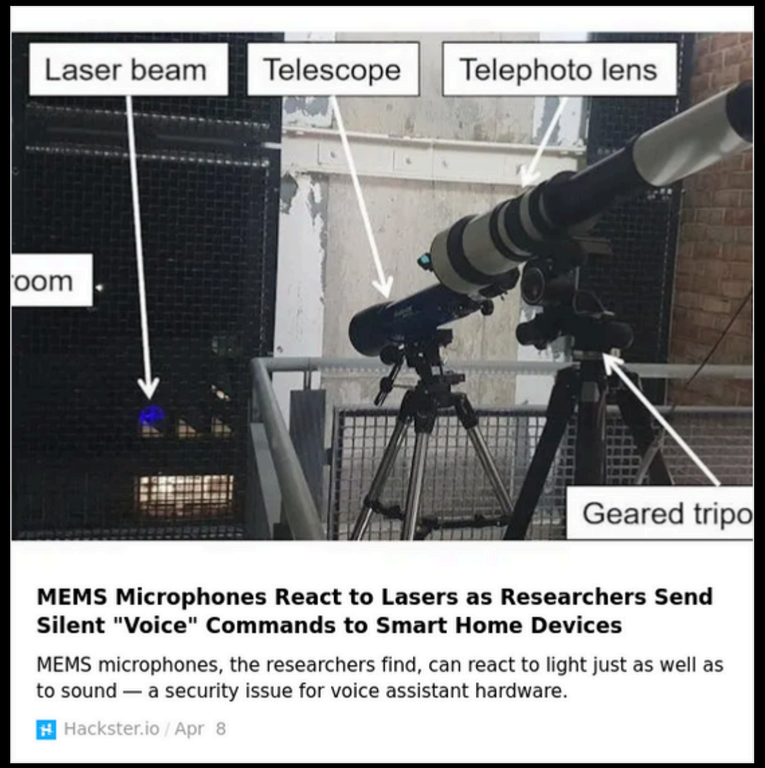
BlackBerry / Oct. 21, 2022

USE CASES

Background: Modified consumer-oriented drones were used for a hacking incident at a US East Coast financial firm. The concept of using drones for hacking has been explored over the past decade at security conferences.

The Incident: The hacking incident was discovered when unusual activity was spotted on the firm's internal Atlassian Confluence page. Investigation led to the discovery of two modified drones on the roof, equipped with devices used for network penetration testing

Back to Agenda Page



USE CASES

Background: Researchers at the University of Electro-Communications in Tokyo (UEC Tokyo) and the University of Michigan have discovered a way to send voice commands to the MEMS microphones used in the majority of smart home voice assistants using silent laser light — making them inaudible to anyone else in the room.

The Incident: By shining the laser through the window at microphones inside smart speakers, tablets, or phones, a far away attacker can remotely send inaudible and potentially invisible commands which are then acted upon by Alexa, Portal, Google Assistant, or Siri,

Back to Agenda Page

Kinetic (Physical)

- Involves firing a projectile such as ballistics or
  ammunition at the drone

- Extremely directional

- Most likely will compromise any recovery or forensic investigation efforts

  Examples:
- Firing from a gun
- Laser (direct energy)
- Chaser net drone
- Collision by another drone

Back to Agenda Page

The role of regulations

- Various Counter-UAS have spawned (to bypass regulations) as a result.
- Already-restricted controls now need to tackle the digital and physical aspect of a drone.
- The cost of a CUAS ($25k - $400 million) far surpasses the cost of a drone ($500 - $100k)

Back to Agenda Page

Drone Security

Back to Agenda Page

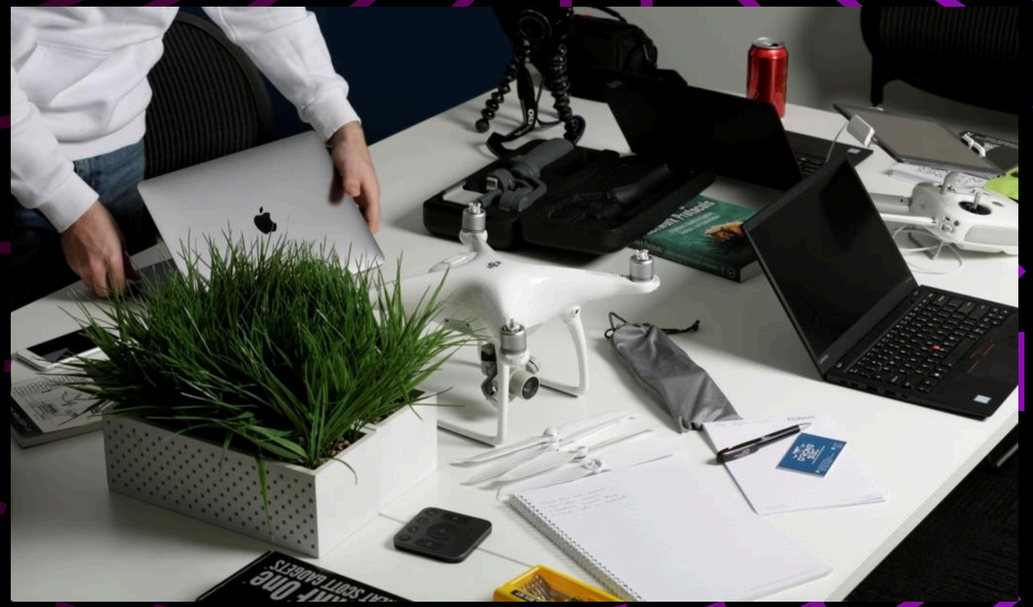
Bringing it all together

- Now you have a basic understanding of the risks posed to,
  by and with drones

- There are various things people can do to help, assess, or remediate (fix) issues in this area

- The following services make up the typical engagements one might be involved with, within Drone Security

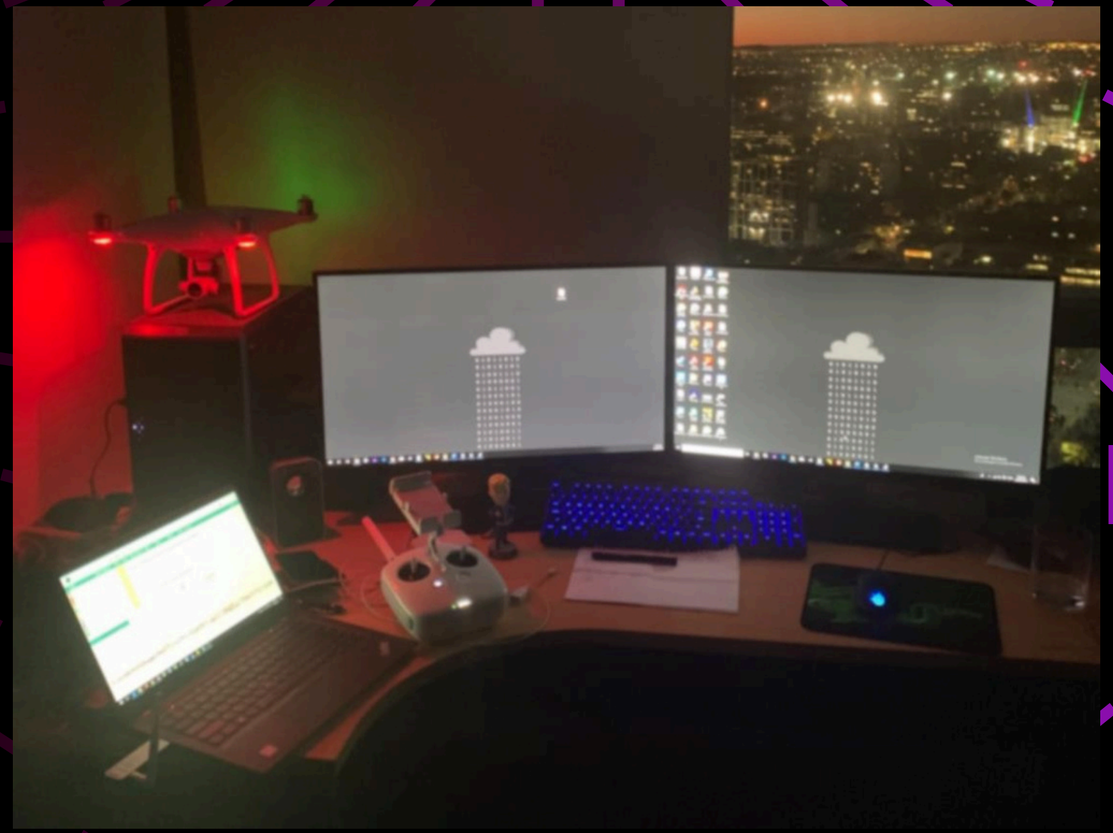
- Each services description is followed by a typical use case or engagement as examples to help understanding



Back to Agenda Page

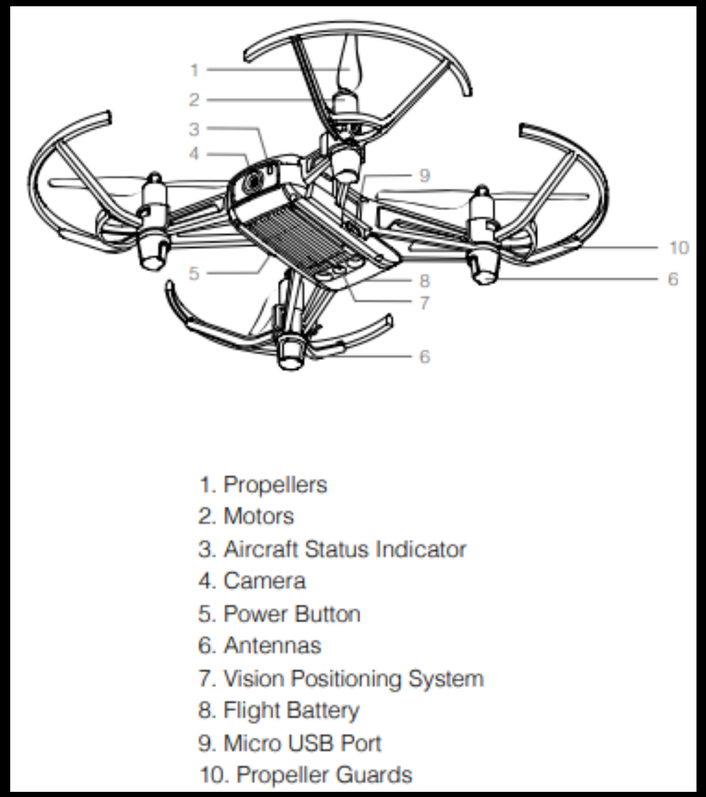
Penetration Testing

Testing drones, their fleet management software, counter-drone technology and providing hardening advice for their drones / environment.



Back to Agenda Page

DEMO



1. Propellers
2. Motors
3. Aircraft Status Indicator
4. Camera
5. Power Button
6. Antennas
7. Vision Positioning System
8. Flight Battery
9. Micro USB Port
10. Propeller Guards

- We've got 4 DJI Tellos with 2-3 working WiFi deauth devices
- These drones take python code (unsigned) over an open 2.4 Ghz wifi network

DO NOT USE ur own tools

Back to Agenda Page

Conclusion

End-to-end Drone Security includes many components:
Devices, Wireless Technologies, Counter-UAS, Laws & Regulations, Forensics, Threat Intelligence…

Drones are inherently a cyber-security problem

- **Computers**
- **Wireless Communications**
- **Remote Control & Ubiquitous**

Drones make up three quadrants

- **Electronic**
- **Kinetic**
- **Close-proximity and air-space**

Back to Agenda Page

LEXICON

Do you have any questions?

Feel free to reach out!

Back to Agenda Page

Lexie Thach

@lexiecon121

lexicon21@proton.me

B4UFLY FAA Smartphone App – Install now

Know Before You Fly
Free for
iOS & Android.

Check for specific restrictions in parks, near sensitive facilities, and places where you might disturb wildlife.

https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/b4ufly/

- Fly below 400 feet
- Keep your drone in eyesight always
- Stay clear of planes, helicopters, etc.
- Do not fly over people, wildlife, or vehicles
- Contact the airport &control tower before flying within five miles of an airport or heliport
- Check and follow all local laws and ordinances before flying

B4UFLY Example FAA use: drag the pin