%27

Attacking & Defending against Drones

By Rod Soto
@rodsoto

$whoami

Researcher at Hackmiami. Worked at Prolexic, Akamai, Caspida. Won BlackHat CTF in 2012. Co-founded Hackmiami, Pacific Hackers meetup, and conferences.

%27

Drones or UAV or UAS

An **unmanned aerial vehicle** (**UAV**) (or **uncrewed aerial vehicle**,[2] commonly known as a **drone**) is an aircraft without a human pilot onboard and a type of unmanned vehicle. UAVs are a component of an unmanned aircraft system (UAS); which includes a UAV, a ground-based controller, and a system of communications between the two. The flight of UAVs may operate with various degrees of autonomy: either under remote control by a human operator or autonomously by onboard computers.[3] *Wikipedia

%27

Brief History

- **1800s** Earliest recorded use of an UAV for warfighting serving as a balloon carrier (the precursor to the aircraft carrier)[22] in the first offensive use of air power in naval aviation.[23][24][25] *
- **1900s** WWII, Vietnam war (Recon, Attack)*Note: USA lost over 5K airmen during Vietnam (Miniaturized components, RC Controllers 50-60s-70s)
- **1990s** US-Israel collaboration → Gulf War I
- The late 1990s - 2000s Weaponization use, enhanced C2 (WOT post 911)
- **The 2010s** - Increased Autonomy, Aircraft Carrier, Stealth, increased commercial availability
- **2020** - Testing and deployment in the commercial sector. (Delivery, transportation, surveillance, media, home use, etc.)

Some UAS Milestones

1917 First drone Ruston Proctor Aerial Target

1950+ Advances in RC technology and flying systems

November 5th 2002 First American lethal drone attack

2006 FAA issues first commercial drone permits

2010 France Company Parrot releases first commercial WiFi controlled drone

February 2012 First Hackmiami Drone prototype flight by @d1sc0rd1an

2013 First Aircraft carrier take-off- USA

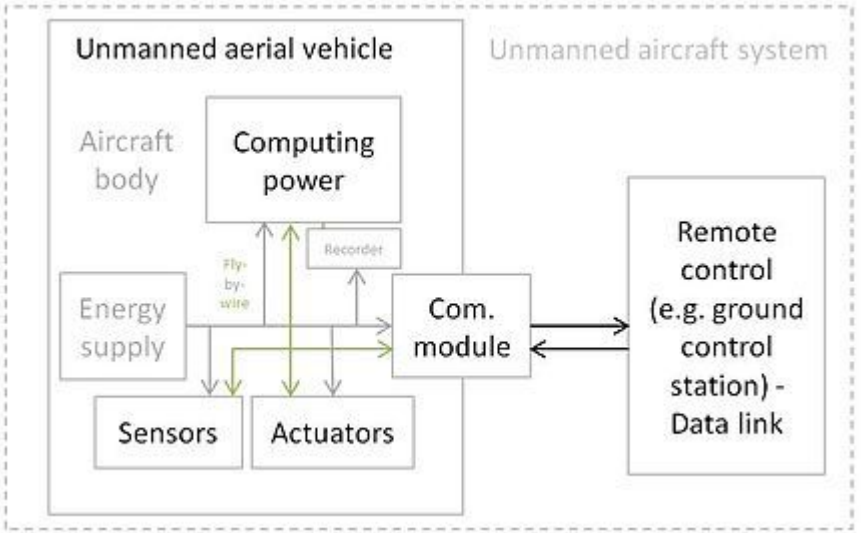
2016 First Amazon Prime delivery via Drone

2018 First air to air kill USA

2020 Drone deliveries - COVID-19 Kits in Ghana

General Components of UAVs

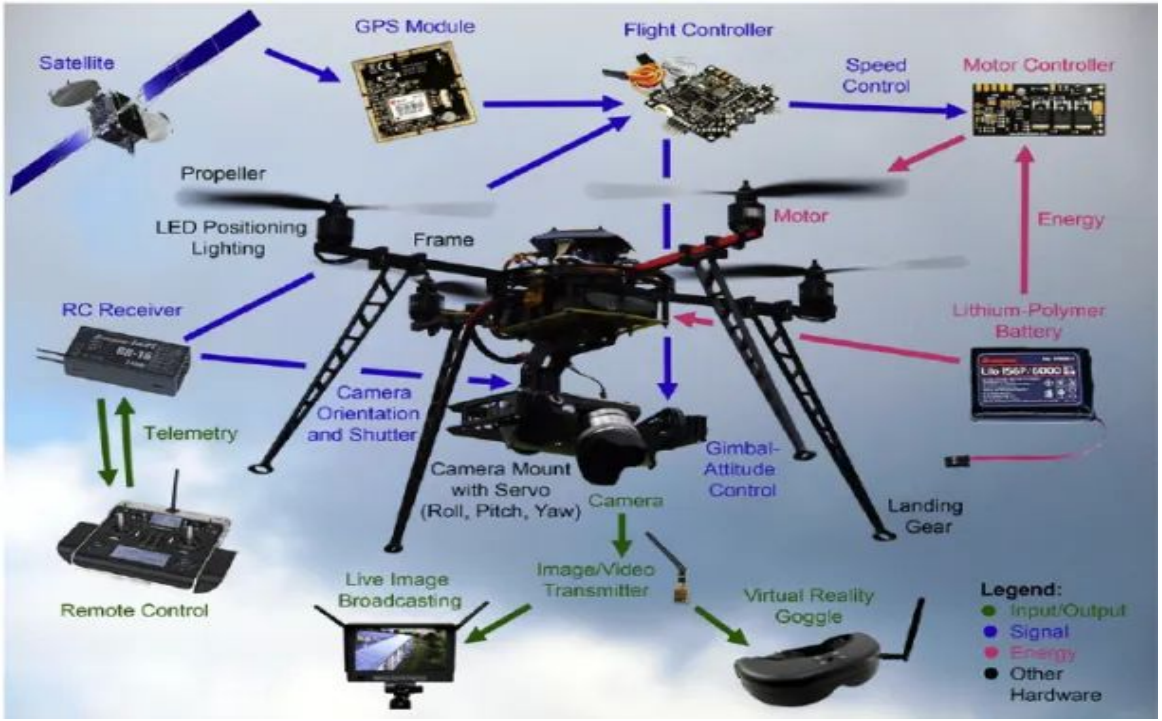
- **Body**
- **Power supply & Platform**
- **Computing unit**
- **Sensors**
- **Actuators**
- **Software**



Source: https://en.wikipedia.org/wiki/Unmanned_aerial_vehicle

%27

UAV - Drone Components Example



Source: https://www.mechlectures.com/introduction-unmanned-aerial-vehicle-uavs/

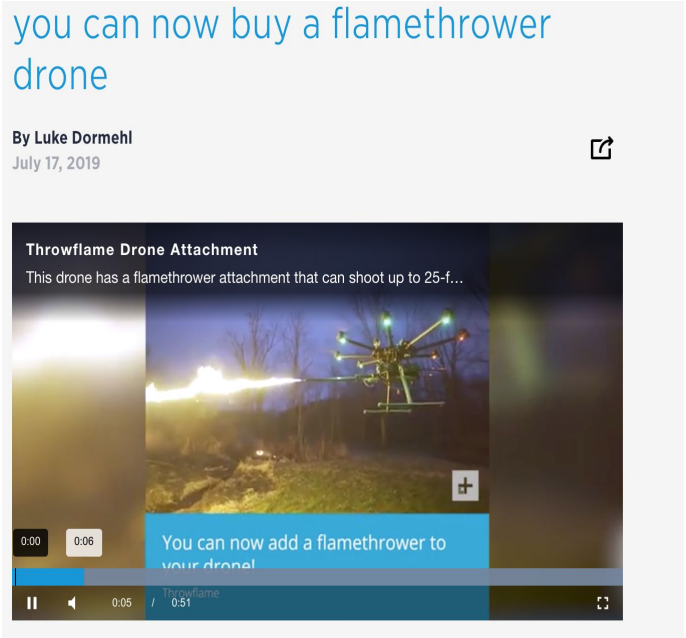
Use Examples

Mostly divided in Military & Civilian

- **Military:** Recon, logistics, combat, surveillance
- **Civilian:**
  - **Industrial:** Utilities, Surveying, Construction
  - **Commercial:** Delivery, inspections, photography
  - **Home:** Security, Entertainment, Photography

Drone Risk

- **Civilian misuse** (There are other things flying as well…)
  - Drone hits plane at Heathrow airport
- **Invasion of privacy**
  - Man fires shotgun at neighbours drone
- **Surveillance & Espionage**
  - DOI banned on Chinese made drones
  - DJI donates drones to police department
- **Smuggling**
  - Narco Drones
- **Weaponization**
  - Terrorists using drones



Source https://www.businessinsider.com/flamethrower-drone-attachment-fire-1500-buy-from-throwflame-2019-7:

%27

Recent Notorious Drone Incidents

2019 Abqaiq–Khurais attack

Event

On 14 September 2019, drones were used to attack the state-owned Saudi Aramco oil processing facilities at Abqaiq and Khurais in eastern Saudi Arabia. Wikipedia

Start date: September 14, 2019

Casualties: 0 killed; Unknown injured

Target: Saudi Aramco facilities

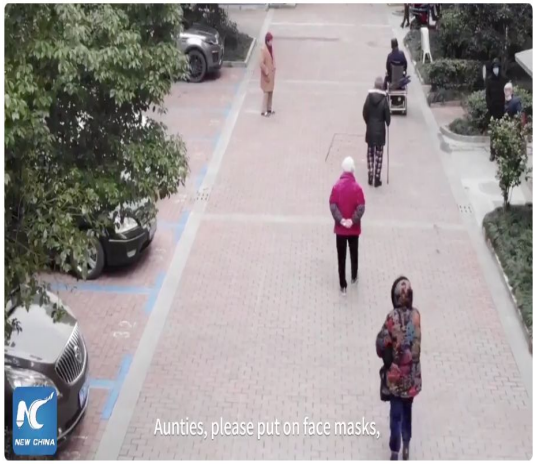
PIENSAPRENSA 210,6 mil seguidores
@PiensaPrensa

Momento en que manifestantes hacen caer un DRON con un "ataque" de luz láser, en Plaza Italia (21:00)
(video @PiensaPrensa)

♡ 11.5K 8:25 PM - Nov 12, 2019

China Xinhua News
@XHNews

Camera drones are employed in Hangzhou, China to urge elderly residents to stay indoors, amid the novel #coronavirus outbreak. #pneumonia



♡ 172 7:02 AM - Feb 4, 2020

%27

Weaponized non military commercial small drones or sUAVs. Increasing adoption, market availability ready and easy to fly, drives risk of weaponization and malicious use.

A drone carrying two gas grenade is deployed during a clash between insurgents and security forces in Kabul, Afghanistan (AP Photo/Massoud Hossaini)

Analysis supports claim drones were used in assassination attempt of President Maduro

Haye Kesteloo - Aug. 9th 2018 9:38 am ET

1 Comment | Facebook | Twitter | Pinterest | LinkedIn | Reddit

Source: https://thesoufancenter.org/intelbrief-terrorists-use-of-drones-and-other-emerging-technologies/

%27

sUAVs

- Less than 55 lbs.
- Cheap to acquire
- Ready and easy to fly (No need for special training)
- Commercially available (No regulations, restrictions, etc.)
- Can carry few pounds of payloads
- Can evade most of the current countermeasures
- Size easy to conceal and deploy
- Can be used in multiple numbers with no infrastructure
- Can be used for surveillance and cyber attacks (WIFI, Cellphones)

Category	Weight	Operating Altitude	Range	Payload
Nano	<0.2 kg	<90	90 m	<0.2 kg
Micro	0.25-2 kg	<90 m	5 km	0.2-0.5 kg
Mini	2-20 kg	<900 m	25 km	0.5-10 kg
Small	<150 kg	<1500 m	50-100 km	5-50 kg
Tactical	>150 kg	<3000 m	>200 km	25-200 kg

Source: https://arxiv.org/pdf/1903.05155.pdf

Mitrev UAS Threat Spectrum - Characteristics

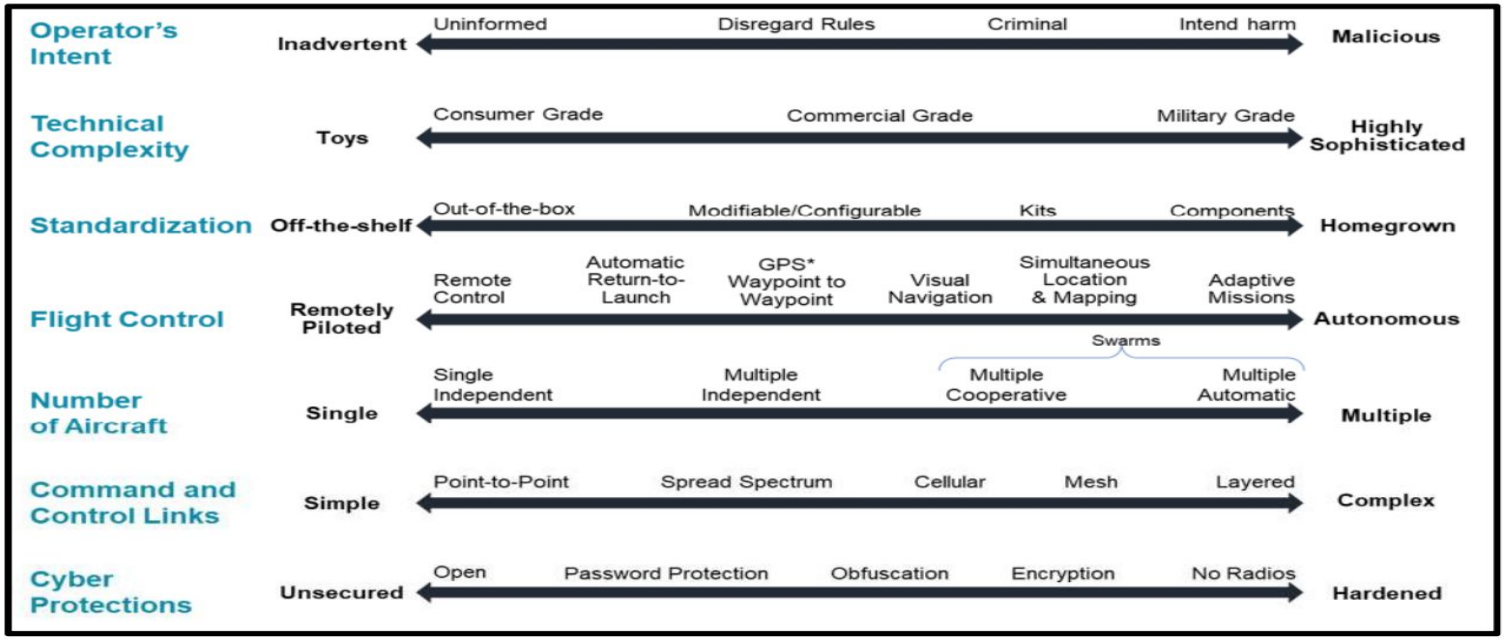
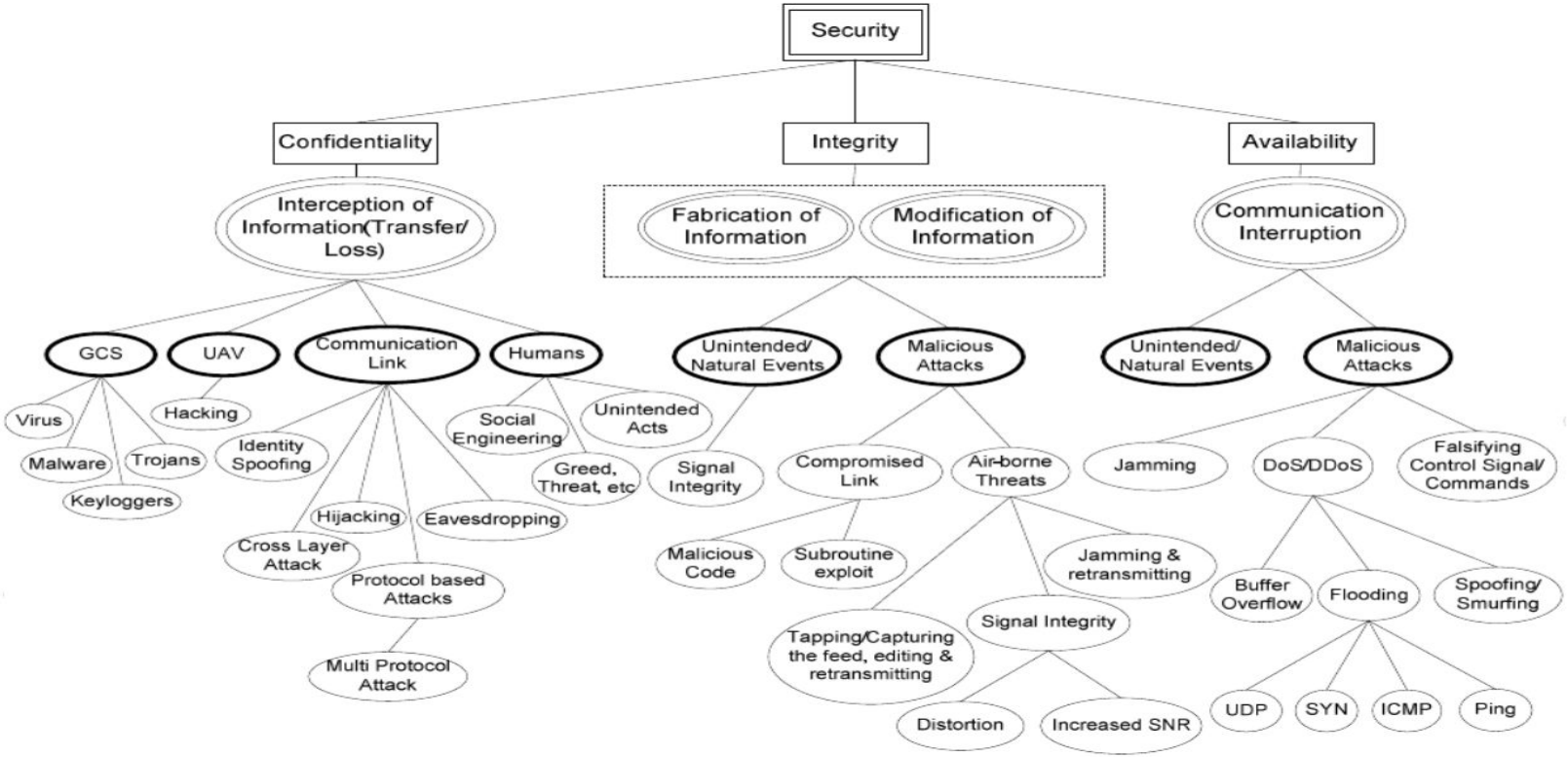


Figure 1 - UAS Threat Characteristics Spectrum

Source: https://www.mitre.org/sites/default/files/publications/pr-18-3852-small-uas-characterizing-threat.pdf

UAS/UAV - Threat Surface

%27



Source:
https://www.researchgate.net/publication/235676360_Cyber_security_threat_analysis_and_modeling_of_an_unmanned_aerial_vehicle_system

Examples of UAV Attack Vectors

Sensors: Video, Audio, Navigation→ Blind drone with Lasers
Physical Layer: Kinetic → Shoot the drone
Link Layer: Telemetry→ Disrupt LOS, DDoS
Network Layer: RF, Wi-Fi, Satellite, Mobile -> Compromise Wi-Fi/RF takes over the drone.
Traffic Control: GNSS, GPS, ADS-B -> Jam/Spoof GPS, Create object aircraft.

Drone Defense

Geofencing: embedded geofencing software in it's UAVs that prevents them from flying over thousands of sites worldwide.

Source: https://drone-dossier.com/tag/geofencing/

Drone Defense, cont.

Detection Systems: UAVs observed to be smaller and difficult to detect by traditional radar systems. New radar systems focus on small UAVs.

Source: https://www.army-technology.com/features/feature-when-drones-go-rogue-plextek-small-enemy-uavs/

Drone Defense, cont.

Other Detection Systems:

- **Acoustic:** distinct noise made by the motors that drive the propellers of UAVs (Can't stop fixed-wing, free fall rotors, and sound can be spoofed and replayed).
- **Radio Frequency:** UAV communicates back to C2 this RF data link can be detected. (Can be evaded via radio silence).
- **Electro-Optical:** Optical and Thermal sensors. (Issues with actual birds).

%27

Drone Defense, cont.

Electronic Defense:

- **Jam C2 link:** Every UAV has some C2 call home, usually via RF even the most autonomous systems. Target C2 RF link and jam it. Commercial drone frequencies are known and can be tampered with to affect drone operation.

https://ctstechnologys.com/3-in-1-drone-jammer-gun-2016-2-4g-5-8g-and-gps.html

Drone Defense, cont.

Electronic Defense:

- **GNSS Global Navigation Satellite System Jamming:** Most UAVs capable of autonomous flying use GNSS. Signals from GNSS can be jammed or spoofed leading to take over of UAV. Collateral damage to other UAVs, Navigation systems, and even airport landing guidance systems possible. Non-GNSS embedded navigation can bypass this countermeasure.
- **ADS-B:** Generate fake aircraft via SDR, overwhelm radar, and trigger collision avoidance systems. Will Nett's **Hackmiami 2017** presentation https://www.youtube.com/watch?v=VD455LEVsIQ

%27

Drone Defense, cont.

Kinetic:

%27

Beware - Counter, Countermeasures

- Inertial navigation systems
- Fix winged optimized airframe
- Embedded autonomous navigation
- Multi-layered sensor flying systems
- Botnet mesh-like resilience C2 (Hackmiami DARPA Challenge 2012)
- Reduced signal countermeasures (No RF, Propulsion, Noise, Heat)

%27

Toolz

Video (5.8GHz)

SDR
~$300 HackRF One

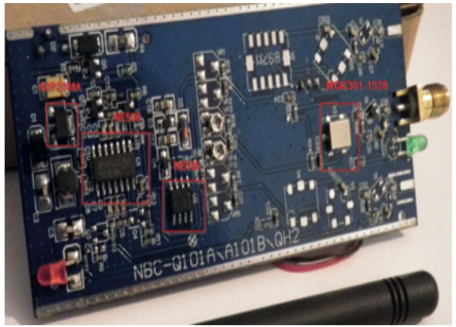
FPV Video Transmitter
$30-$60 high power version

5.8 GHz Jammer
~$300

GPS (1575.42 Mhz)

SDR
~$25 NooElec NESDR v4 (up to 1700MHz)
~$300 HackRF One (up to 6000MHz)

GPS "signal generator"
~$25



Please see more at Hackmiami Henry Secove's presentation on Drone Security.

https://www.youtube.com/watch?v=-6jHh_YUNvQ

Other Interesting toolz

- SkyJack

  0https://github.com/samyk/skyjack

- DroneJack

  https://github.com/brospars/wic-ter-dronejack

- Dronesploit

  https://github.com/dhondta/dronesploit

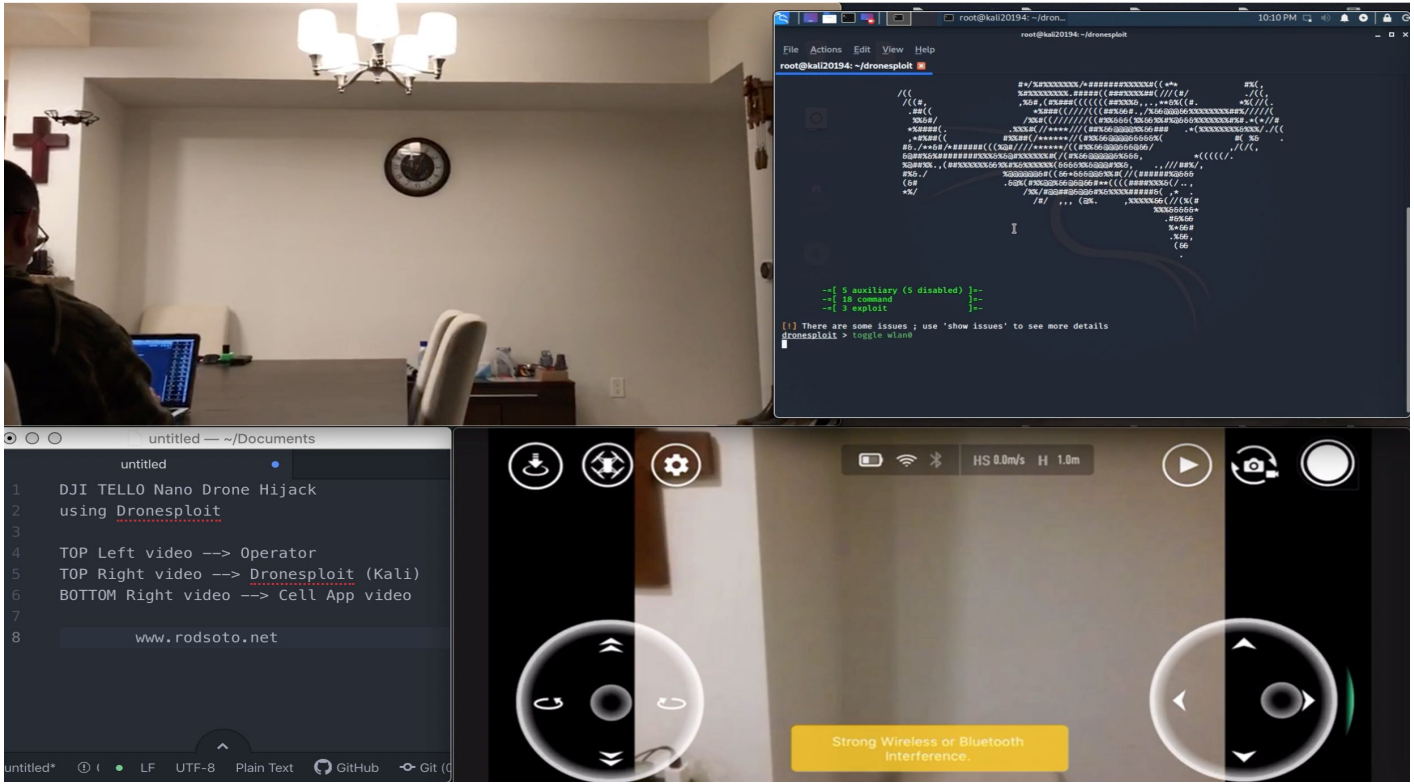
%27

Demo 1 → DroneSploit

- Compromise Wi-Fi C2 and force drone to land
- https://github.com/dhondta/dronesploit
- Target: DJI Tello - Indoor Nano Drone
- https://www.amazon.com/Tello-Drone-Quadcopter-Batteries-Charger/dp/B07HLL7KFJ/ref=sr_1_4?dchild=1&keywords=dji+tello&qid=1589830727&sr=8-4

Model	Wi-Fi	Flight Range	Speed (Km/H)	Flight Time	Weight (grams)	Altitude	Video Resolution	Year
DJI Tello	x	~ 100 m	~ 29	13 min	80	~ 100 m	720p	2018

Demo 1 - Video



Youtube: https://youtu.be/CcUKaeEJ0cg

%27

Demo 2 → WIFI FENCE

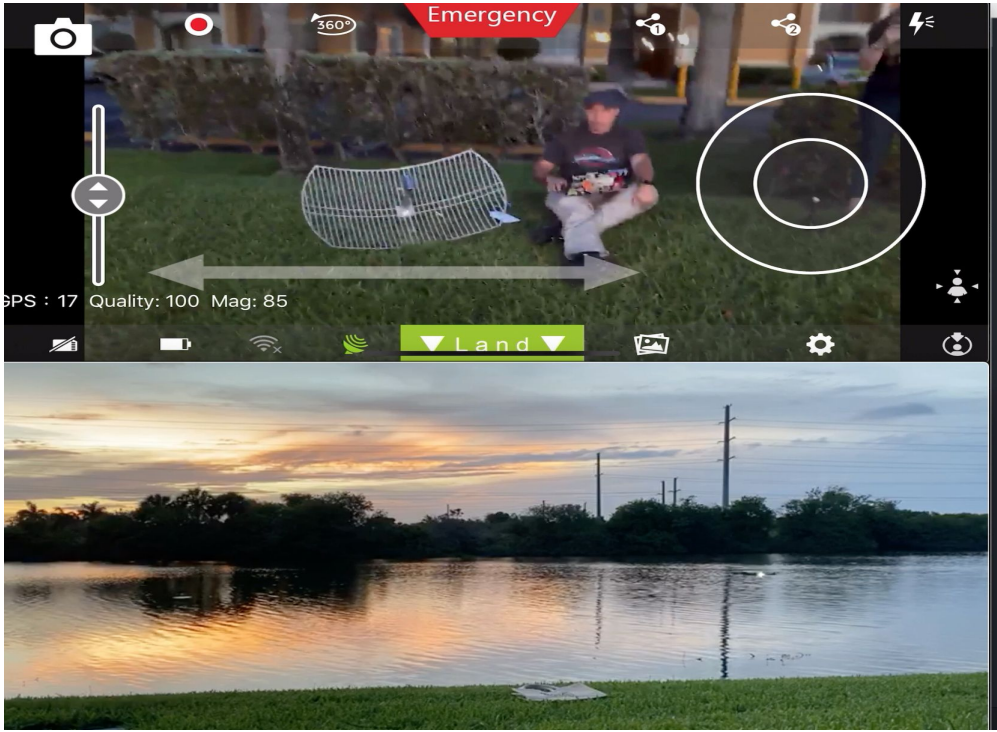
- Use outdoor WIFI antenna plus Alfa card
- Drones performs RTL once WIFI is out
- Target: Outdoor GPS C-ME Drone

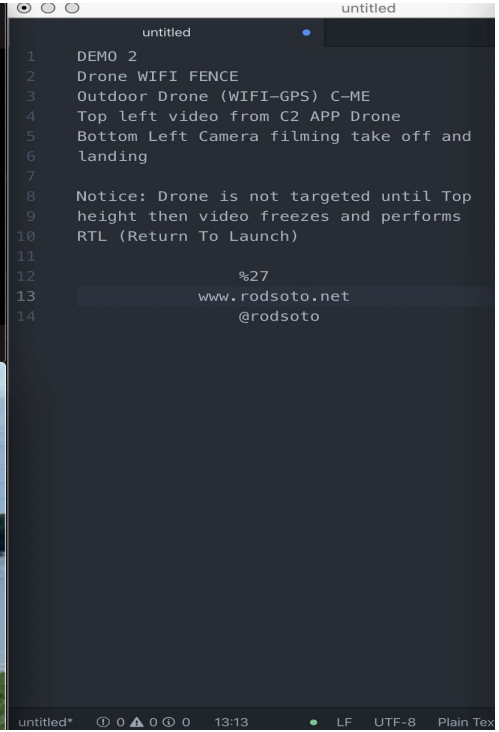
- https://www.amazon.com/C-me-Social-Media-Flying-Camera/dp/B07172JQYP/ref=sxts_sxwds-bia-wc-p13n1_0?cv_ct_cx=C-ME+selfie+drone&dchild=1&keywords=C-ME+selfie+drone&pd_rd_i=B07172JQYP&pd_rd_r=20b34b62-9633-4f1e-ab1e-19cfedabbb1e&pd_rd_w=WUD5f&pd_rd_wg=q4Vm0&pf_rd_p=d027eaac-7531-45fe-a61e-20ae30db06de&pf_rd_r=P4F2P7197A4S2F6TZWP9&psc=1&qid=1589830929&sr=1-1-70f7c15d-07d8-466a-b325-4be35d7258cc

Model	Wi-Fi/GPS	Flight Range	Speed (Km/H)	Flight Time	Weight (grams)	Altitude	Video Resolution	Year
C-ME	x	~ 100 m	~ ?	10 min	~160	~ 60 m	1080p	2017

%27

Demo 2 - Video





Youtube: https://youtu.be/qoQyOfu5lj8

Thank you

Rod Soto

@rodsoto (Twitter)

rodsoto.net