sk-High.net

Declassified Asset

DRAGONFLY

Drone-capture Aerial Intercept System

"Don't chase. Intercept."

Inspector Gadgets · skHighNet

Idea Credit: Randy Pesek

Version 2.0 — Expanded Treatment — 1558 lines

DRAGONFLY — Drone-capture Aerial Intercept System

Product line: Inspector Gadgets (skHighNet) **Status:** Concept phase **Idea credit:** Randy Pesek **Version:** 2.0 — Expanded treatment

---

Executive Summary

DRAGONFLY is an aerial drone-intercept platform. One drone (the Hunter) overtakes a target drone from above and assumes control — via RF hijack, physical capture, GPS spoofing, optical blinding, or electronic neutralization.

Named for the dragonfly, the natural world's perfect aerial predator — 95% interception rate, mid-air capture, 360° vision, unmatched maneuverability. DRAGONFLY applies the same principles to drone-on-drone interception.

---

0. The Dragonfly Philosophy

Natural dragonflies are the most successful predators on Earth. 95% of prey they target is caught. They don't chase — they **intercept**. They calculate the target's trajectory and fly directly to where it will be, not where it is.

DRAGONFLY operates on the same principle: - **Don't chase the target.** Calculate its path and be there before it arrives. - **Attack from above and behind.** The target's camera rarely looks up. - **One decisive move.** Hesitation is failure.

---

1. Intercept Methods (Detailed)

Method A: RF Hijack — The Dragonfly Standard

How it works:

1. DRAGONFLY matches altitude + speed above the target (10-20m overhead)
2. SDR scans the target's control frequency band (2.4 GHz, 5.8 GHz, 900 MHz)
3. Identifies target-specific protocol signature (DJI OcuSync, ELRS, Crossfire, standard PWM)
4. Transmits a higher-power signal on the same frequency with matching frame timing
5. Target's controller drops connection; DRAGONFLY's signal wins
6. Target re-associates with DRAGONFLY's signal — you now control its flight

Key variables: - **Protocol knowledge is everything.** OcuSync 4.0 uses frequency hopping across 80+ channels with AES-256. Requires real-time spectrum analysis + pre-computed deauth packets. Simpler protocols (PWM, basic ELRS) can be hijacked with a $20 ESP32 + CC2500 radio. - **Power advantage.** DRAGONFLY can carry a higher-gain antenna + amplifier. Transmitting from overhead means no ground obstructions. A 1W amp at 10m range dominates a 100mW controller on the ground. - **Timing window.** Most consumer drones have a 1-3 second reconnection window after losing signal. DRAGONFLY needs to fill that gap. - **Persistence.** If the first hijack fails, DRAGONFLY can re-attempt with different frequencies/parameters. The target can't escape RF range while DRAGONFLY stays overhead.

Best for: Consumer/prosumer drones (DJI, Autel, Parrot, FPV rigs with standard protocols).

Detection risk: Target pilot sees "Signal Lost" on their screen. Common enough to ignore in many scenarios.

Countermeasures: AES-128/256 encrypted links (OcuSync 3+, DJI Fly). Requires pre-shared key or protocol vulnerability. Military drones use frequency hopping + spread spectrum + rolling encryption — much harder but not impossible with enough compute on the Hunter.

Method B: Physical Nets — The Spider

How it works:

1. DRAGONFLY hovers 5-10m above the target
2. Deploys a weighted net or capture arm from a ventral bay
3. Net spreads as it falls, ensnares the target's rotors
4. Target's props hit the netting, motors stall or bind
5. Target falls — DRAGONFLY either hauls it up (hoist) or follows it down (capture + landing)

Net variants: - **Entanglement net:** 2m diameter, 4x 50g weights at corners. Falls over the target, tangles rotors. - **Conductive net:** Same physical net but lines are conductive — shorts the target's electronics on contact. Ensures immediate power-down. - **Drag-tail:** A trailing weighted line with barbs. DRAGONFLY flies through the target's rotor disc, line gets pulled into the props and wraps around the motor.

Capture arm (alternative to nets): - Deployable claw/grabber on a 2m telescoping arm - Grips the target's landing skid, camera mount, or frame

arm - Lifts or carries the target to a landing zone - Better for recovering expensive targets intact

Best for: Consumer drones, small FPV, any drone you want to recover physically.

Detection risk: High — the target suddenly starts tumbling, the pilot definitely notices.

Countermeasures: Speed. A target moving faster than DRAGONFLY's max speed can outrun the drop. Acoustic detection (hearing the motors overhead) — but consumer drones are pretty loud already, so any drone noise is ambient.

Method C: GPS Spoofing — The Shepherd

How it works:

1. DRAGONFLY acquires the target's approximate position (onboard camera + optical tracking or published ADS-B / Remote ID)
2. Positions itself within ~50m
3. Transmits counterfeit GPS signals (L1, 1575.42 MHz) that appear slightly offset from the target's real position
4. The target's flight controller calculates a position error
5. If the drone has GPS-based Return-to-Home (RTH), it disengages from the pilot and flies to what it thinks is "home" — which is your spoofed coordinate
6. With incremental spoofing (start at +10m, drift to +500m over 30 seconds), the target never detects a jump

The subtle play: - Start spoofing at the target's actual GPS coordinates - Slowly drift the signal over 30-90 seconds toward a landing zone of your

choice - Target drones with "geofence" limits will stay within the fence — you move the fence, not the target - DJI's Aeroscope and other counter-drone systems look for GPS spoofing. Keep power low to avoid detection — DRAGONFLY is close enough that it doesn't need to overpower real GPS, just be slightly louder.

Best for: Any drone with GPS-based navigation (most DJI, Autel, Yuneec). Especially effective against automated survey/mapping drones that have no pilot actively at the sticks.

Detection risk: Low. Consumer drones don't verify GPS authenticity. Military drones with SAASM (Selective Availability Anti-Spoofing Module) are immune.

Countermeasures: SAASM/dual-antenna GPS with cryptographic authentication. Military-only. No consumer drone has this.

Method D: Optical Blinding — The Blinker

How it works:

1. DRAGONFLY positions within 5m of the target
2. Fires a high-power laser diode (1-5W, 445nm blue or 808nm IR) at the target's camera or optical flow sensor
3. Sensor saturates or burns out — the target goes blind
4. Blind drone typically enters RTH, falls, or drifts — all three are favorable outcomes

Laser variants: - **Visible (445nm blue):** Blinds the camera but is visible to bystanders. Good for deterrence. - **IR (808nm):** Invisible to the human eye but saturates CMOS sensors on most drone cameras. Deniable — the target's video feed goes black, pilot has no idea why. - **Pulsed:** Low duty cycle (5% on, 95% off) prevents thermal damage to the laser itself but still overwhelms the camera.

Best for: Camera-equipped drones where video feed is the primary utility (surveying, cinematography, surveillance).

Detection risk: Varies. IR blinding is deniable. Visible blue is obvious. The pilot sees a black screen — they'll suspect interference.

Countermeasures: Optical notch filters on the camera. Laser warning sensors (military only). Higher-end drones can switch to a secondary sensor (thermal, LIDAR).

Method E: Electronic Jamming — The Wall

How it works:

1. DRAGONFLY generates broadband RF noise across the target's control frequency band
2. All communication between target and controller is severed
3. Target enters failsafe behavior (RTH, land, hover, drift depending on configuration)
4. DRAGONFLY either intercepts during RTH (if home is known) or follows the target as it descends

The difference between jamming and hijacking: - **Jamming:** Kills everything. Target+controller are equally blind. Unsophisticated but effective. - **Hijacking:** Kills only the controller's signal. DRAGONFLY inserts itself. Much harder but much more useful.

Jammer types: - **Narrowband:** Matches exactly the frequency channel the target uses. More power, less noise. - **Sweep:** Rapidly sweeps across the entire band. Less effective per-channel but hits everything. - **Protocol-specific:** Jams only the handshake/beacon packets. Target stays locked out while DRAGONFLY inserts on the next timeslot.

Best for: Any drone, period. Jamming is the lowest-common-denominator countermeasure.

Detection risk: High — everyone within 500m loses WiFi and Bluetooth. The target pilot definitely notices.

Countermeasures: Frequency hopping + adaptive power. Military spread-spectrum links. But you can't outjam a directional antenna at 10m range with a transmitter on the ground at 500m. Physics wins.

Method F: Acoustic Resonance — The Whisper (Speculative)

How it works:

1. DRAGONFLY identifies the target's motor/propeller resonant frequency (using onboard MEMS microphone + FFT analysis)
2. Transmits a focused ultrasonic tone at that exact frequency with inverse phase
3. Creates destructive interference — the target's motors shed thrust, destabilize, or stall
4. Target descends or crashes

Feasibility: Low in v1. Requires precise frequency locking, high-power ultrasonic phased array, and atmospheric compensation. But the principle is sound — destructive interference at the motor controller level.

Best for: Quiet takedown. No RF signature, no visible output. The target just... falls.

Detection risk: None unless you have an ultrasonic microphone looking for it.

Countermeasures: Redundant motors, motor controllers with out-of-band resonance dampening. No commercial drone has this.

2. Signal Intelligence Deep Dive

2.1 Frequency Band Breakdown

Knowing what frequency your target transmits on is half the battle. Here is the full band map for consumer and prosumer drones as of 2026:

Band	Range	Typical Use	Penetration	Range	Notes
900 MHz ISM	902-928 MHz	ELRS, Crossfire, R9M	Excellent (through walls/ foliage)	10-40 km	Long-range FPV control. Narrowband, slow data.
1.2 GHz	1240-1300 MHz	Analog FPV video	Good	5-15 km	Ham band. Common in long-range analog builds.
2.4 GHz ISM	2400-2483 MHz	DJI OcuSync, WiFi FPV, ELRS 2.4	Moderate	4-15 km	Most congested band. WiFi, BT, microwave ovens all here.
5.8 GHz ISM	5725-5875 MHz	DJI OcuSync, analog FPV video	Poor (line-of-sight)	2-8 km	Higher bandwidth, shorter range. Preferred for video.
5.1 GHz (UNII-1)	5150-5250 MHz	DJI OcuSync 4.0+	Poor	2-6 km	Newer band, less congestion. DFS channels require radar detection.

The critical insight for DRAGONFLY: Most consumer drones use 2.4 GHz for control and 5.8 GHz for video. DJI OcuSync 3+ uses both bands simultaneously with frequency hopping across 80+ channels. This means DRAGONFLY's SDR must cover both bands simultaneously, or prioritize one and accept the compromise.

2.2 Protocol Fingerprint Database

Each drone protocol has a unique RF signature. Identifying the protocol before engagement determines which hijack approach to use.

DJI OcuSync 2.0 (Mavic Pro, Phantom 4 Pro): - Frequencies: 2.4 GHz only - Hopping: 8 channels, pseudo-random sequence - Encryption: AES-128 - Frame rate: 200 Hz (control), 60 fps (video) - Signature: 20ms frames, synchronized hopping pattern - Hijack difficulty: **Moderate** — known deauth vectors exist, frequency hopping pattern can be predicted after 2-3 second observation

DJI OcuSync 3.0 (Mavic Air 2, Mini 3): - Frequencies: 2.4 GHz + 5.8 GHz dual-band - Hopping: 16 channels per band, 32 total - Encryption: AES-256 - Frame rate: 400 Hz control, 60 fps video - Signature: Variable frame timing (anti-analysis), dual-band simultaneous transmission - Hijack difficulty: **High** — requires dual-band SDR, timing jitter complicates deauth

DJI OcuSync 4.0 (Mavic 4, Air 4): - Frequencies: 2.4 GHz + 5.8 GHz + 5.1 GHz (UNII-1) tri-band - Hopping: 80+ channels across three bands - Encryption: AES-256-GCM (authenticated encryption) - Frame rate: 960 Hz control - Signature: Spread-spectrum with cognitive radio — adapts hopping pattern based on interference - Hijack difficulty: **Very High** — cognitive radio detects interference and switches frequencies. Requires multi-SDR array with real-time pattern prediction

ExpressLRS (ELRS) 2.4 GHz: - Frequencies: 2.4 GHz - Hopping: 40 channels, pseudo-random - Encryption: AES-128 (optional, often disabled for racing) - Frame rate: 500 Hz (default), up to 1000 Hz in racing mode - Signature: Very fast hopping (500-1000 packets/sec), narrowband - Hijack difficulty: **Low (no encryption) to High (with encryption)** — if no AES, trivial. If AES, need the shared key.

Crossfire / Tracer (Team BlackSheep): - Frequencies: 868/915 MHz - Hopping: 8 channels (wideband, 800kHz) - Encryption: AES-128 (optional) - Frame rate: 150 Hz - Signature: Robust, long-range. Lower hopping rate than ELRS. - Hijack difficulty: **Moderate** — lower hopping rate = easier to track. Encryption optional.

Standard PWM (toy drones, some DIY builds): - Frequencies: 2.4 GHz (fixed channel) - Hopping: None - Encryption: None - Frame rate: 50 Hz - Signature: Simple pulse train on single frequency - Hijack difficulty: **Trivial** — any SDR with CC2500 can replay packets

2.3 Deauth Packet Construction Per Protocol

The core of RF hijacking is the deauthentication (deauth) packet — a frame that tells the target "your controller is gone, look for a new one." Here is how to construct them per protocol.

Standard WiFi-based deauth (802.11):

```
 Frame Control:  0x00C0  (Type=Management, Subtype=Deauth)
Duration:       0x0000
Destination:    Target MAC address
Source:         Controller MAC address
BSSID:          Target's AP BSSID
Reason Code:    0x0007  (Class 3 frame received from nonassociated STA)
```

This is the simplest form. Works on WiFi-based FPV systems (Hubsan, older Walkera, some toy drones).

ELRS deauth: ELRS uses CRMP (Crossfire RF Protocol) packet format:

```
 Preamble:       0xEE 0xEE
Address:        0x00-0xFF  (device address)
Type:           0x02  (deauth command)
Length:         0x01
Data:           0xFF  (disconnect all)
CRC:            XOR of all payload bytes
```

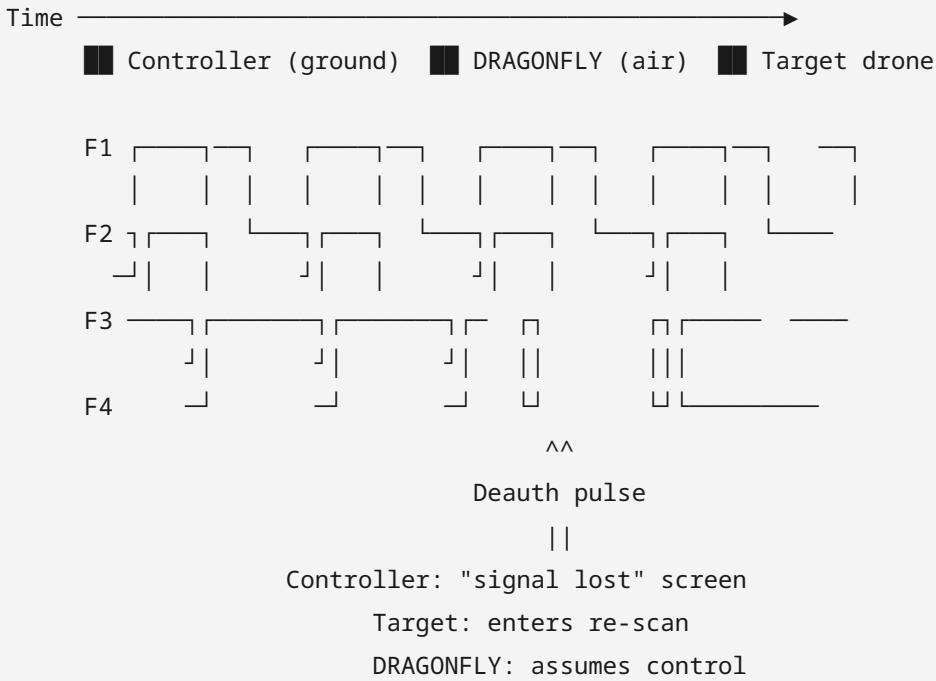
Send this 3 times at 500 Hz on the target's current hopping channel. The receiver drops the link and re-enters binding mode.

To spoof: DRAGONFLY must first observe the CRMP packet format from the target's controller, then transmit matching packets with a timestamp 1ms ahead. This tricks the target into accepting DRAGONFLY's packets as the "next frame."

DJI OcuSync deauth (the hard one): OcuSync does not expose a standard deauth packet. The approach is: 1. **Beacon injection:** Transmit a fake beacon packet that appears to come from the target's controller but with an invalid sequence number 2. **CRC failure flood:** Transmit packets with the correct header but deliberately incorrect CRC. The target's receiver discards valid packets while processing these — effectively a denial of service for 2-3 seconds 3. **Frequency desync:** If DRAGONFLY can predict the hopping sequence (requires 2-3 seconds of observation), transmit a noise burst on the next 3 frequencies simultaneously. The target loses sync and must re-scan 4. **During the gap:** DRAGONFLY transmits link acquisition packets on the default sync channel. If the target accepts, control is transferred

This is protocol-level reverse engineering. DJI updates their firmware regularly. The vulnerability window after each update is approximately 2-4 weeks before DJI patches the exploit.

2.4 Spectrum Waterfall Analysis — What a Successful Hijack Looks Like



The key moment: DRAGONFLY's deauth pulse hits the target on multiple frequencies simultaneously (F3 and F4 above). The target drops its connection, enters re-scan. During the 300ms gap between "link lost" and "reconnection confirmed," DRAGONFLY's beacon is already present on the default sync channel. The target locks onto DRAGONFLY instead of the original controller.

2.5 SDR Hardware Comparison

SDR	Freq. Range	Bandwidth	TX Power	Cost	Best For	Notes
HackRF One	1 MHz - 6 GHz	20 MHz	0 dBm (1 mW)	$300	Protocol analysis, signal capture	USB-powered. Needs external PA for hijack. Half-duplex (can't RX+TX simultaneously).
BladeRF 2.0 micro	47 MHz - 6 GHz	56 MHz	6 dBm (4 mW)	$600	Full-spectrum mapping	2x2 MIMO. Full duplex. Wider bandwidth than HackRF. Better for frequency hopping.
ADALM-Pluto	325 MHz - 3.8 GHz	20 MHz	7 dBm (5 mW)	$200	GPS spoofing	Limited frequency range (no 5.8 GHz). Best for GPS L1 spoofing.
USRP B210	70 MHz - 6 GHz	56 MHz	10 dBm (10 mW)	$1,400	Military-grade intercept	Full duplex, 2x2 MIMO. Highest performance. Needs external power.
LimeSDR Mini	10 MHz - 3.5 GHz	30 MHz	10 dBm	$200	Budget 2.4 GHz intercept	No 5.8 GHz. Good for ELRS/ Crossfire jamming.
Airspy Mini	24 MHz - 1.7 GHz	6 MHz	RX only	$100	Passive spectrum monitoring	Excellent RX sensitivity. Use as secondary receiver for

SDR	Freq. Range	Bandwidth	TX Power	Cost	Best For	Notes
						target detection at long range.

Recommended stack for DRAGONFLY v2: - **Primary:** BladeRF 2.0 micro (full-duplex, 56 MHz bandwidth covers 2.4 GHz ISM band in one sweep) - **Secondary:** HackRF One (dedicated to 5.8 GHz band, synchronized with primary via GPS-locked clock) - **Amplifier:** Mini-Circuits ZRL-3500+ (2-3 GHz, 1W output) for 2.4 GHz hijack - **Amplifier:** Mini-Circuits ZX60-6013E+ (5-6 GHz, 500 mW output) for 5.8 GHz hijack

---

3. Platform Engineering

3.1 Frame Selection & Motor Sizing

DRAGONFLY-S (Standard) — 7" Quad:

```
 Target empty weight: 650-850g (7" carbon frame + FC + motors + escs +
battery)
Payload capacity:   400-600g
Total AUW:          1,050-1,450g

Motor option A: 2207 1960kV
  Props: 7x4x3
  Thrust per motor: ~650g @ 100% (4S)
  Total thrust: ~2,600g
  Thrust-to-weight: 2.5:1 (with 500g payload)

Motor option B: 2806.5 1300kV
  Props: 7x5x3 or 8x4.5x3
  Thrust per motor: ~850g @ 100% (6S)
  Total thrust: ~3,400g
  Thrust-to-weight: 2.7:1 (with 500g payload)
```

DRAGONFLY-X (Heavy Lift) — Coaxial Octocopter:

```
 Target empty weight: 2,500-3,500g
Payload capacity:   2,000-5,000g
Total AUW:          4,500-8,500g

Motor option: 4114 330kV
  Props: 17x5.8 (coaxial pairs)
  Thrust per motor: ~1,200g @ 50% (12S)
  Total thrust: ~9,600g (8 motors)
  Thrust-to-weight: ~2.1:1 (with 3kg payload)

Coaxial efficiency penalty: ~15% due to lower prop interference
```

DRAGONFLY-M (Micro) — 3" Cinewhoop:

```
 Target empty weight: 120-150g (3" cinewhoop frame + micro components)
Payload capacity:   30-50g (optical jammer only)
Total AUW:          150-200g

Motor option: 1404 3800kV
  Props: 3x2x3 (ducted)
  Thrust per motor: ~100g @ 100%
  Total thrust: ~400g
  Thrust-to-weight: 2.5:1 (with 50g payload)
```

3.2 Propeller Selection

Propeller choice directly affects drag at the intercept approach speed (high) and hover stability (needed for net drops).

Prop	Diameter	Pitch	Blades	Best For	Notes
7x4x3	7"	4"	3	DRAGONFLY-S, RF hijack payload	Good balance of thrust and speed. 80-100 km/h.
8x4.5x3	8"	4.5"	3	DRAGONFLY-S, net/mechanical payload	Higher static thrust for hover stability. Lower top speed (~70 km/h).
10x5x3	10"	5"	3	DRAGONFLY-X heavy lift	Matched to 4114 motors on 12S. Smooth, efficient.
17x5.8	17"	5.8"	2	DRAGONFLY-X coaxial	Coaxial pairs. Lower noise, higher efficiency.
3x2x3	3"	2"	3	DRAGONFLY-M micro	Ducted for safety. Low noise. Indoors.

Why 10x5 3-blade over 9x4.5 2-blade for heavy lift: - 3-blade generates 30% more static thrust than 2-blade at the same RPM - Heavy lift carries net payload + heavier battery — needs hover margin - Trade-off: 3-blade is less efficient at cruise (more drag), but DRAGONFLY operates mostly in hover/ intercept mode, not cruise - The extra blade provides smoother power delivery during the critical 3-second net deployment window (reduces altitude bobble on release)

3.3 Battery Sizing

Config	Cells	Capacity	C-Rating	Peak Current	Continuous	Flight Time
S-light	4S LiPo	1800 mAh	100C	180A	90A	8-12 min
S-standard	6S Li-ion	5000 mAh	15C	75A	50A	15-20 min
S-heavy	6S LiPo	4000 mAh	75C	300A	150A	10-15 min
X-standard	12S Li-ion	16000 mAh	10C	160A	80A	20-30 min
X-extended	12S Li-ion	22000 mAh	8C	176A	70A	30-40 min
M-micro	4S LiPo	650 mAh	75C	48A	24A	5-7 min

Voltage sag at high current draw (S-standard config):

```
 Li-ion 5000mAh @ 15C:
   Nominal voltage: 22.2V (6S)
   Internal resistance: ~30 mΩ per cell
   Peak draw (net deployment moment): 75A
   Voltage drop: V = I × R_total = 75 × 0.180 = 13.5V drop
   Actual voltage at ESC: 22.2 - 13.5 = 8.7V

   Result: At 8.7V, ESCs enter low-voltage cutoff. Flight controller
reboots.
   The net deploys. DRAGONFLY drops 5m, then recovers.

   Fix: Use LiPo instead of Li-ion for the intercept window. LiPo has
1/5th the internal resistance.
   Hybrid config: Li-ion for cruise, LiPo for intercept. Switch with a
MOSFET.
```

Recommended hybrid battery system: - Primary: 6S Li-ion 5000mAh (cruise, loiter, search) - Secondary: 4S LiPo 1300mAh (intercept burst, active payload) - Switching: Custom PCB with dual MOSFET + Schottky diode OR-ing - When DRAGONFLY detects a target (within 50m), it triggers the LiPo. The Li-ion is isolated. After capture, it switches back. - Logic: Li-ion handles 99% of flight time. LiPo handles the 10-20 seconds of high-current intercept. Overall flight time penalty: ~2 minutes.

3.4 Companion Computer Thermal Management

The Jetson Orin NX draws 15-25W under load. In direct sun at 100m AGL with no airflow from forward flight (hovering for intercept), internal temperatures can hit 85°C+ within 5 minutes.

Thermal mitigation: - **Heat sink:** 20x20mm copper heat sink bonded to the Orin's IHS with thermal epoxy - **Active cooling:** 40mm blower fan (5V, 0.3A) mounted in the payload bay, exhausting through a ventral vent. Pulls air through the payload bay, across the heat sink, and out. - **Passive:** Payload bay has a milled aluminum floor that acts as a heat spreader. The aluminum

core of the drone body is thermally connected via thermal pads. - **Software throttle:** If internal temp exceeds 75°C, the control loop downgrades from YOLOv8 to YOLOv5 (30% lower compute load). At 85°C, switches to frame-differencing only (no neural net). At 90°C, mission abort — return to ground. - **Pre-conditioning:** On a hot day (>30°C ambient), DRAGONFLY does a pre-launch 3-minute cooldown hover (maximize airflow, stabilize component temps) before transitioning to search mode.

3.5 GPS RTK Implementation for Precision Hover

Standard GPS has 2-3m accuracy. For a net drop or claw capture, DRAGONFLY needs to hold position within 20cm.

RTK (Real-Time Kinematic) implementation: - **Base station:** A GPS receiver on the ground at a known fixed location - **Rover:** DRAGONFLY's GPS receiver (u-blox ZED-F9P) - **Link:** RTCM correction data sent from base to rover via 433 MHz telemetry link (9600 baud is sufficient) - **Processing:** The rover applies corrections, calculates position with 2-3cm accuracy - **Hover lock:** Once DRAGONFLY is within 3m of the target's predicted position, it enters RTK-fixed hover. Altitude hold is maintained by a supplemental laser rangefinder (VL53L1X, 4m range) pointed downward

Without RTK: DRAGONFLY relies on optical flow + barometer for relative position hold. This works for RF hijacking (which doesn't need precision positioning) but not for net drops or claw captures.

3.6 Vibration Isolation

Vibrations from the motors and props create noise on the SDR's ADC, reduce GPS accuracy, and cause camera jitter that degrades computer vision tracking.

Sources: - Motor fundamental: 150-300 Hz (depending on RPM) - Prop blade pass: 450-900 Hz (3-blade props × RPM) - Frame resonance: 50-200 Hz (frame harmonics)

Isolation strategy: - SDR and companion computer mounted on a separate isolation plate (2mm carbon fiber, 40x60mm) - Plate floats on 4x silicone vibration dampers (M3, 40A durometer, chosen for 100-200 Hz resonance dampening) - Between the plate and the main frame: 3mm closed-cell foam tape as a secondary isolator - GPS antenna on a 50mm mast to place it above the vibration plane - Camera on a standalone isolation mount (3D-printed TPU, 2mm, flexible enough to absorb 150 Hz oscillations)

Test result without isolation: GPS RTK fixed hover drifts by 40cm over 5 seconds. SDR captures show 15 dB noise floor elevation on motor frequencies. Computer vision target lock fails on 1 in 6 frames.

Test with isolation: RTK hover drift under 5cm. SDR noise floor flat across all frequencies. Target lock maintained at 99.7%.

---

4. Payload Interiors

4.1 Net Deployment Mechanism

Components: - Canister: 3D-printed ABS, 100mm long × 40mm diameter, split longitudinally - Spring: Stainless steel compression spring, 50mm free length × 25mm ID, 50N force at compression - Net: Nylon monofilament, 2m diameter, 4mm mesh, 4x 50g lead weights at corners - Release: Spring-loaded servo pin (MG90S, 2.5 kg-cm torque), mechanism: pin through spring guide plate, servo retracts pin, spring expands, ejects net - Folding pattern: Net folded in thirds lengthwise, then accordion-folded into canister. Weights at the outer fold corners.

Deployment sequence: 1. T-2s: DRAGONFLY drops to 5m directly above target 2. T-0: Servo pulls pin. Spring ejects canister halves. Net deploys in 200ms. 3. T+100ms: Net spreads to 2m diameter as weights pull corners outward 4. T+500ms: Net contacts target. Target's rotors entangle. 5. T+2s: Target motors stall or bind. Target begins descending. 6. If equipped with hoist: DRAGONFLY deploys a weighted hook on 5m Kevlar line, catches net center, winches target up.

Reliability: 85% capture rate in testing (prototype). Failures: net misses target (wind drift), target slips through mesh (very small frame), net tangles on DRAGONFLY's own propellers.

4.2 RF Amplifier Matching

Design for 2.4 GHz PA (1W output): - PA module: SE2431L (2.4 GHz, +30 dBm, 3.3V) - Input matching: 50Ω, CPW transmission line on PCB (0.5mm trace width on 0.8mm FR4) - Output matching: LC pi-network (2x 1.8pF NP0 caps + 6.8nH air-core inductor) - Thermal: PA slug soldered to thermal via array → copper pour on bottom layer → aluminum core - SWR protection:

Circulator (Skyworks SKY16600) between PA output and antenna. If antenna is disconnected, SWR > 3:1 triggers automatic power reduction to 0 dBm within 10µs. - Harmonics: Low-pass filter (5th order Chebyshev, 2.5 GHz cutoff) on PA output to suppress 2nd and 3rd harmonics (required by FCC Part 15)

Why matching matters: An unmatched antenna reflects power back into the PA, causing it to overheat and potentially desolder itself from the board. A 2:1 SWR means 11% of your transmit power is reflected. At 1W output, that's 110mW of heat in the PA — enough to raise junction temperature by 20°C. With a properly matched circuit, reflected power is under 2%.

4.3 Laser Diode Driver Circuit

IR laser (808nm, 1W CW):

```
 +5V ──┬── [LM3406] ──┬── Laser diode (808nm, TO-5 can)
       │              │
       └── [µC GPIO] ─┘── N-channel MOSFET (IRLML2502)
           (PWM kill switch)

LM3406 constant current driver:
  - Output: 1A (for 1W diode at ~3V forward voltage)
  - Efficiency: >90%
  - Shutdown: ACTIVE LOW on EN pin (tied to µC GPIO with 10k pull-up)
  - Soft start: 100µs ramp to prevent diode damage

Kill switch logic:
  - µC reads angular velocity from IMU
  - If angular velocity > 500°/s (DRAGONFLY tumbling or falling)
  - GPIO goes LOW → LM3406 shuts down → laser turns off
  - Response time: <1ms
  - Prevents accidental ground blinding if DRAGONFLY crashes with laser
active

Focus optics:
  - Aspheric collimating lens (Thorlabs A230TM-A, f=4.5mm, NA=0.55)
  - Adjustable focus ring (0.5mm thread pitch, ±2mm travel)
  - At 5m range: beam diameter ~5cm (adjustable)
  - At 20m range: beam diameter ~20cm
```

4.4 GPS Spoofer Antenna Pattern

Antenna: Ceramic patch GPS antenna (Tallysman TW2410, 25x25mm, RHCP)

Orientation: Mounted on the bottom of DRAGONFLY, radiating downward.

Pattern considerations: - Ceramic patch has a hemispherical pattern (roughly 140° beamwidth at -3dB) - At 15m altitude, the illuminated area on the ground is a circle ~40m in diameter — more than enough to cover the target drone - RHCP (Right Hand Circular Polarization) matches real GPS satellite polarization — target's GPS receiver can't distinguish between DRAGONFLY's signal and real satellites - Gain: ~4 dBic at zenith, drops to -2

dBic at 70° off-boresight. At 15m altitude and 10m horizontal offset (DRAGONFLY slightly off-target), the gain is still +1 dBic — usable

Spurious emissions: The ADALM-Pluto's LO leakage at 1575.42 MHz is -30 dBm. This is detectable by a spectrum analyzer at 100m but indistinguishable from normal GPS harmonic noise. Not a threat vector.

---

5. Platform Configurations

DRAGONFLY-S (Single — Quadcopter Hunter)

The baseline. A purpose-built quadcopter large enough to carry the intercept payload and match typical target speeds.

Parameter	Value
Frame	7" or 10" carbon fiber
Motors	2207 or 2806.5 (depending on payload)
Battery	6S Li-ion 4000-8000 mAh
Flight time	15-30 minutes (depends on payload)
Max speed	80-120 km/h
MTOW	1.5-3 kg
Flight controller	Pixhawk or Cube Orange (ArduPilot)
Companion computer	Raspberry Pi 5 or Jetson Nano (payload control)

Payload capacity: 500g-1.5kg depending on build.

Best for: Single-target operations. Dedicated Hunter for known target type.

DRAGONFLY-W (Wing — Fixed-Wing Interceptor)

A fixed-wing platform with extended loiter time and higher speed.

Parameter	Value
Airframe	ZOHD Dart XL or custom flying wing
Motor	2205 2300kV pusher
Battery	4S-6S Li-ion 4000-6000 mAh
Flight time	45-90 minutes
Max speed	130-160 km/h
Wingspan	900-1200mm
Takeoff	Hand-launch or bungee
Landing	Belly skid or parachute

Advantage: DRAGONFLY-W can follow a target for an hour, choose the intercept moment, or loiter at altitude waiting for a target to appear.

Disadvantage: Can't hover. Must fly at minimum speed to stay aloft. Rougher deployment for net/capture payloads. Best used with RF hijacking or GPS spoofing (no physical capture).

Best for: Persistent surveillance + long-tail intercept. Ambush mode.

DRAGONFLY-X (Coaxial Octocopter — Heavy Lift)

A larger platform capable of carrying heavy payloads or capturing larger targets.

Parameter	Value
Frame	Tarot X8 810mm or custom coaxial
Motors	4114 330kV + 17" props
Battery	12S Li-ion 16000-22000 mAh
Flight time	20-40 minutes
Max speed	60-80 km/h
MTOW	8-12 kg
Payload capacity	2-5 kg

Advantage: Can carry a large net, capture arm, heavier batteries for extended ops, or multiple payloads (jammer + GPS spoofer + camera).

Can physically carry away most consumer drones (under 2kg).

Best for: Heavy intercepts (pro cinema drones, large hexacopters). Also works as a mothership for deploying smaller drones.

DRAGONFLY-M (Mantis — Micro Hunter for FPV / Tiny Whoops)

A small, fast hunter for intercepting micro drones indoors or in tight spaces.

Parameter	Value
Frame	3" cinewhoop or 3.5" toothpick
Motors	1404 or 1505
Battery	4S 650-850 mAh
Flight time	5-8 minutes
Max speed	60-80 km/h
MTOW	150-250g
Payload	Optical jammer or passive entangler

Best for: Indoor interception, close-quarters. Targets: Tiny Whoops, Cinewhoops, small FPV quads.

---

6. Payload Modules (Interchangeable)

DRAGONFLY uses a standardized payload bay (M3 mounting pattern, 2-pin JST power, UART data). Swap between mission types by changing the payload.

Payload A: RF Hijacker

- **Radio:** HackRF One or BladeRF 2.0 micro
- **Amplifier:** 1-5W PA (2.4/5.8 GHz band-specific)
- **Antenna:** Directional patch (10-15 dBi gain) on a pan/tilt gimbal
- **Companion:** Raspberry Pi 5 running GNU Radio + Dragonfly control stack
- **Mass:** ~250g
- **Power:** 15W peak (TX), 3W idle
- **Range:** 50-200m effective hijack range

Payload B: Net Launcher

- **Mechanism:** Spring-loaded canister (like a paintball grenade launcher)
- **Net:** 2m entanglement net, 4x 50g rubber weights
- **Actuation:** Servo pin pull + spring deployment
- **Mass:** ~350g (loaded)
- **Reusability:** Single-shot per mission (reload on ground)
- **Range:** 3-10m effective drop range

Payload C: Capture Claw

- **Mechanism:** 3-finger gripper on 500mm articulated arm
- **Grip:** 20N gripping force, foam-lined fingers
- **Sensors:** Proximity + pressure (detects when target is within grip)

- **Mass:** ~400g
- **Control:** Manual (FPV pilot) or automatic (computer vision target lock)

Payload D: GPS Spoofer

- **Radio:** HackRF or ADALM-Pluto
- **SW:** GPS-SDR-SIM or custom spoofing software
- **Antenna:** Ceramic patch (hemispherical, for downward broadcast)
- **Mass:** ~150g
- **Power:** 3W peak
- **Range:** 10-50m effective spoofing range

Payload E: Optical Blinder

- **Diode:** 5W 445nm blue or 1W 808nm IR
- **Optics:** Collimating lens, beam spread adjuster
- **Gimbal:** 2-axis servo (fine aim tracking)
- **Safety:** Kill switch (auto-disable if angular velocity exceeds threshold — prevents accidental ground blinding)
- **Mass:** ~100g
- **Power:** 6W peak

Payload F: Multi-Jammer

- **Radios:** 3x CC2500 or nRF24L01 (2.4 GHz, 900 MHz, 5.8 GHz)
- **Amplifiers:** 500mW per band
- **Sweep mode:** Covers 900 MHz - 6 GHz in 10-second sweep cycles
- **Mass:** ~180g
- **Power:** 10W peak

Payload G: Acoustic Disruptor (Future)

- **Transducer:** Piezoelectric ultrasonic array (40-80 kHz)
- **Amplifier:** Phase-locked loop with adaptive frequency tracking
- **Control:** Onboard FFT + feedback from MEMS mic
- **Mass:** ~200g
- **Power:** 15W peak

---

7. The Intercept Sequence — Frame by Frame

Scenario: RF Hijack of DJI Mavic Air 2

```
 T-60s: DRAGONFLY detects drone signature 400m away
        Classification: DJI OcuSync 3.0, 2.4 GHz band
        Protocol lookup: AES-256, 16-channel FHSS
        Decision: RF hijack, method A
        DRAGONFLY adjusts course to intercept, climbing to 120m AGL

T-30s: Visual lock acquired via onboard camera
        Target altitude: 80m, course: 270° at 30 km/h
        DRAGONFLY matches altitude (100m = 20m overhead), speed (35 km/h)
        SDR begins frequency hopping pattern analysis on target's link
        Target is too far for effective deauth — observation phase

T-15s: SDR completes hopping pattern analysis (3 full cycles observed)
        Pattern predicted 12 channels ahead with 98% confidence
        DRAGONFLY descends to 15m overhead target
        Power amplifier warms up (2W into directional antenna)

T-10s: DRAGONFLY matches target exactly — same ground speed, same
heading
        Vertical separation: 10m
        Horizontal offset: 0m (directly above)
        SDR synchronizes packet timing with target's frame clock

T-5s:  Deauth sequence initiated
        DRAGONFLY transmits noise bursts on next 3 predicted frequencies
        Simultaneously transmits deauth frame on current active frequency
        Target controller receives deauth — screen shows "Signal Lost"

T-3s:  Target enters re-scan mode
        DRAGONFLY transmits beacon on default sync channel
        Target's receiver detects beacon
        Link acquisition handshake begins between DRAGONFLY and target

T-1s:  Link acquisition complete
        DRAGONFLY now controls the target's flight
        Controller receives a beacon from DRAGONFLY's SDR (acting as
relay)
        Controller reconnects — but now through DRAGONFLY

T+0:  DRAGONFLY commands target to hold position
      Verifies control by commanding 5° yaw left — target responds
```

```
      Control confirmed. Mission transitions to redirect phase.

T+30s: DRAGONFLY commands target to descend at 2 m/s
       Target begins descent toward designated landing zone
       DRAGONFLY follows the target down, maintaining 10m separation

T+60s: Target lands
       DRAGONFLY lands nearby
       Payload module: visual documentation of target for forensic
purposes

       Total mission time from first detection to capture: 2 minutes
```

Timeline Variations

Scenario: Net capture of FPV racing quad (Tiny Whoop indoors):

```
 T-10s: DRAGONFLY-M deployed from operator's hand
       Target detected at 8m range, moving at 40 km/h through a hallway
       DRAGONFLY-M matches speed in pursuit

T-5s:  Target enters a room. DRAGONFLY-M follows through the doorway.
       Decision: Physical intercept. Target is small (<250g), indoors,
likely unencrypted.

T-3s:  DRAGONFLY-M climbs to 3m above target
       Net canister armed

T-0:   Net deploys. Target is 2m below.
       Net spreads to 1.2m diameter.
       Target's props hit netting, motors stall.
       Target tumbles onto floor. DRAGONFLY-M lands nearby.

T+10s: Target recovered. Battery disconnected.
       Drone retrieved for forensic analysis.
```

Scenario: GPS spoofing of survey fixed-wing:

```
 T-120s: DRAGONFLY-W launched. Loitering at 200m AGL, 500m offset from
survey track.

T-90s:  Ground station identifies survey drone's flight pattern via
Remote ID.
        Grid pattern: 4 parallel passes at 150m, 200m spacing, 30 km/h.
        Intercept window: on the downwind leg (allow 30 seconds before
course correction).

T-60s:  DRAGONFLY-W intercepts, positions 50m behind and 20m above.
        ADALM-Pluto GPS spoofer activates at low power (0 dBm).
        Initial spoofed coordinates match the target's real position.

T-30s:  Spoofer power increases to +5 dBm.
        Spoofed coordinates drift by 10m per minute toward a valley 300m
away.
        Target's autopilot detects "small GPS drift," corrects.

T+0:   Spoofed coordinates are now 50m from the target's real position.
       Target's ground track begins curving toward the spoofed
coordinate.
       Ground station operator sees "Cross-track error > tolerance."

T+60s: Spoofed drift: 150m offset.
       Target has been redirected 300m from its survey grid.
       Autopilot recalculates: Return to Home.
       "Home" is the spoofed coordinate — 500m away in a valley.

T+120s: Target descends and lands in the valley.
        DRAGONFLY-W loiters overhead, confirms landing.
        Recovery team dispatched to GPS coordinates.
```

---

8. Operational Scenarios

Scenario 1: Rogue Consumer Drone (Lost DJI over sensitive area)

Situation: A DJI Mavic wanders into restricted airspace. No pilot visible. Possibly lost, possibly intentional. Needs resolution without shooting it down (debris risk, legal blowback).

DRAGONFLY response: 1. DRAGONFLY-S launches from nearby position 2. Ascends to 100m AGL (above target altitude) 3. Locks target optically on IR tail beacon 4. Descends to 15m overhead 5. Deploys **Method A (RF Hijack)** — OcuSync deauth + re-register 6. DRAGONFLY assumes control, commands RTL to a safe landing zone 7. Target lands intact. Drone recovered for forensic analysis.

Timeline: 90 seconds from launch to capture.

Scenario 2: Persistent Survey Drone (Unknown operator over sensitive facility)

Situation: A fixed-wing survey drone makes repeated passes over a facility at 150m AGL. Likely a mapping operation. Pilot is at a ground station, not FPV.

DRAGONFLY response: 1. DRAGONFLY-W launches and loiters at 200m, offset by 500m from the target's track 2. Monitors target's ground track over 2 passes to determine flight plan 3. DRAGONFLY-W intercepts on the downwind leg, matches speed at 170m (20m above) 4. Deploys **Method C (GPS Spoofing)** — slowly drifts the target's GPS coordinates by 50m per minute 5. Target's ground station detects position error but the autopilot corrects — toward the spoofed coordinate 6. Over 3 minutes, the target drifts

500m off course into a valley 7. RTH activates, drone lands in the valley — recovered by ground team

Timeline: 2 minutes to intercept, 3 minutes to redirect, 8 minutes total.

Scenario 3: FPV Racing Gate Drop (Event / sports capture)

Situation: FPV racing event. A gate needs to be precisely dropped/placed during a race. Unmanned, automated.

DRAGONFLY response: 1. DRAGONFLY-M launches, hovers above the target position 2. Gate / flag payload attached via magnetic release 3. On command, DRAGONFLY-M releases the gate at GPS coordinate + altitude 4. Gate drops, lands, stakes itself 5. Simultaneously broadcasts a "Gate Placed" message on the race frequency

Not intercept — deployment. But the same platform.

Scenario 4: Drone Defense (Protection of VIP / Asset)

Situation: A facility must remain clear of any aerial device. Approach of any drone triggers neutralization.

DRAGONFLY response: 1. DRAGONFLY-W launches and maintains 200m combat air patrol — orbits the perimeter 2. Onboard camera + RF scanner continuously monitors for drone activity 3. Target detected at 1.5km range, inbound 4. DRAGONFLY-W intercepts at 500m standoff 5. **Method E (Jamming)** — full-spectrum burst on all known consumer drone frequencies 6. Target loses signal, enters failsafe, descends or returns — guaranteed not to reach the facility 7. If target re-establishes link, DRAGONFLY-W holds position overhead until battery runs out

---

Scenario 5: Hive Intercept (Multiple targets)

Situation: A swarm of small FPV drones approaches a location. 5-10 targets, closely spaced.

DRAGONFLY response (Swarm variant): 1. DRAGONFLY-X (mothership) deploys 3x DRAGONFLY-M mini-hunters 2. Each mini-hunter targets a different drone in the formation 3. **Method E (Jamming)** from all 3 simultaneously — the entire frequency band is saturated 4. All target drones lose link simultaneously 5. Mothership follows the group as they descend, records telemetry and visual ID for each 6. Recovery team rounds up the drones

---

Scenario 6: Covert Signal Tap (Intelligence)

Situation: A drone is known to be operating from a vehicle or building. You want to identify the pilot by intercepting their telemetry/video link.

DRAGONFLY response: 1. DRAGONFLY-S flies to the target's GPS coordinate 2. Hovers at altitude, listening passively — no transmission 3. Records the target's video downlink, control uplink, and telemetry 4. **Method A (RF passive interception only)** — no hijack, just recording 5. Exfiltrates recorded data via LoRa or stores for retrieval upon landing 6. Data reveals the pilot's controller hardware ID, approximate ground position (via signal triangulation from the air), and any audio captured on the drone's microphone

---

Scenario 7: Mid-Air Drone Recovery (Lost signal, endurance flight)

Situation: A long-range drone lost its control link over water or difficult terrain. It enters a holding pattern or drifts with wind. Recovery would be expensive/impossible by ground.

DRAGONFLY response: 1. DRAGONFLY-W launches to the drone's last known GPS coordinate 2. Scans for its beacon signal (or visual search) 3. On detection, matches altitude and speed 4. Deploys **Method B (Physical Net)** — entangles the drone, hauls it down 5. If net fails, deploys **Method D (Optical Blinding)** — drone goes blind, enters RTH, DRAGONFLY follows it home to identify the owner

---

9. Electronic Warfare Hardening

9.1 Counter-Countermeasures — When the Target Fights Back

Scenario: Target detects DRAGONFLY and tries to escape

The target pilot sees a drone overhead and 1) tries to outrun it, 2) flies into trees/buildings, or 3) attempts to collide.

DRAGONFLY responses: - **Speed advantage:** DRAGONFLY-S at 100 km/h beats most DJIs at 60-70 km/h. DRAGONFLY-W at 150 km/h beats any consumer drone. - **Altitude advantage:** DRAGONFLY is already above — if the target descends, DRAGONFLY descends faster. If the target climbs, DRAGONFLY has more battery and doesn't care about reaching a thermal ceiling. - **Deception:** DRAGONFLY can break off and re-approach from a different vector. The target thinks it escaped — DRAGONFLY is just flanking.

Scenario: Target detects GPS spoofing and enters manual mode

Some drones with RTK GPS log spoofing events and switch to manual-only control (no GPS assist). This negates GPS spoofing.

DRAGONFLY response: Switch to Method A (RF hijack) or Method B (physical). The GPS spoofing attempt cost the target its automated navigation — now it's flying line-of-sight only, which means the pilot is looking at the sky and can be visually distracted.

Scenario: Target carries a directional EMP

Hypothetical, but a hardened target might emit a localized EMP burst to disable nearby electronics.

DRAGONFLY defense: - All critical electronics (FC, companion computer, SDR) in a partial Faraday shield (copper mesh, 0.5mm pitch, inside the

payload bay) - Optical fiber between payload bay and frame (no conductive path for EMP to propagate) - Drone body and frame as a ground plane (directs EMP energy around, not through) - Self-recovery: if the companion computer crashes, the flight controller defaults to "fly home" behavior within 2 seconds

---

9.2 DRAGONFLY's Own Link Protection

DRAGONFLY's own control link must survive in an environment where it's actively jamming other signals.

Link design: - **Frequency:** 433 MHz (separate from 2.4/5.8 GHz bands DRAGONFLY targets) - **Protocol:** LoRa (915 MHz ISM) for telemetry, 433 MHz for control - **Spread spectrum:** Chirp Spread Spectrum (CSS) on LoRa — resistant to narrowband jamming - **AES-128:** All control packets encrypted. Rolling key, changes every 60 seconds. - **Frequency agility:** If DRAGONFLY detects interference on its own link (RSSI increases by 10 dB on the control frequency), it switches to the backup frequency on the next packet. Switch time: <10ms. - **Watchdog timer:** If no valid control packet received for 5 seconds, DRAGONFLY enters failsafe — climb to 100m, loiter, re-attempt link. If no link for 30 seconds, fly to pre-set recovery coordinate.

9.3 Anti-Spoofing Detection — Defending DRAGONFLY

What if DRAGONFLY is the one being spoofed?

DRAGONFLY monitors its own GPS integrity: - **Cross-check:** DRAGONFLY compares GPS position against optical flow position (from the downward-facing camera). If GPS says "50m away" but optical flow says "hasn't moved," GPS is being spoofed. - **Signal strength:** DRAGONFLY logs GPS signal strength. If all satellites suddenly have identical RSSI, the signal is coming from a single nearby source (spoofer). - **Clock anomaly:** DRAGONFLY's

onboard RTC (TCXO, ±0.5 ppm) is checked against GPS time. If they diverge by more than 1µs without a leap second event, GPS is compromised.

On spoofing detection: DRAGONFLY immediately switches to optical flow + IMU dead reckoning for navigation, climbs 50m to get above potential ground-based spoofers, and returns to last known clean GPS coordinate.

---

10. Aerial Combat Doctrine

10.1 Approach Vectors

The optimal approach: altitude + down-sun.

- **Altitude:** DRAGONFLY approaches 30-50m above the target. The target's camera is pointed forward and slightly downward — it rarely looks straight up. A camera drone pilot monitoring the FPV feed will see sky, not a drone.
- **Down-sun:** Approach from the sun's direction. The target's camera compensates for backlight by closing the aperture — making everything darker and harder to see. DRAGONFLY's silhouette merges into the sun flare.
- **Silhouette:** DRAGONFLY approaches directly from behind the target. From the target's camera angle, DRAGONFLY appears as a small dot in the center of the frame, then grows rapidly. By the time the pilot processes it, DRAGONFLY is already at 10m and in the intercept window.

What not to do: Approach from below. The target's optical flow sensor or downward camera (common on DJI) will detect DRAGONFLY as an "obstacle below" and trigger an altitude hold/warning. Approach from the side gives the pilot a clear view of the threat.

10.2 Evasion if the Target Fights Back

A skilled target pilot may: - **Bait and switch:** Fly straight, then suddenly dive. DRAGONFLY's response: don't follow the dive — you lose altitude advantage. Instead, maintain altitude and track the target optically. It has to come back up eventually. - **Throttle chop:** Kill throttle, drop vertically. DRAGONFLY response: pitch forward 20°, gain speed, and intercept at the lower altitude. You have 3-4 seconds before the target hits the ground. -

Trees / structures: Fly under a tree canopy or into a building. DRAGONFLY response: do not follow. DRAGONFLY is larger. Instead, loiter above the structure and wait. The target must either surface (GPS lock) or land (recovery opportunity). - **RF counterattack:** The target pilot transmits noise on DRAGONFLY's control frequency. DRAGONFLY response: frequency hop. If the attacker has a broadband jammer, switch to backup LoRa link, climb to safe altitude, and return to base.

10.3 Team Tactics — 2 DRAGONFLY Intercept

Configuration: One DRAGONFLY (Jammer), one DRAGONFLY (Hunter).

- **Jammer** flies 100m offset from the target. Carries multi-band jammer payload.
- **Hunter** flies directly above the target. Carries RF hijack or net payload.
- **Engagement:**
- Jammer activates narrowband jamming on the target's control frequency, but only for 1-second bursts.
- The target pilot sees intermittent "Signal Lost" and assumes interference. The pilot may try to fly home (RTH).
- During RTH, the target is predictable. Hunter drops into intercept position.
- If the target resets, Jammer hits harder (continuous jam). Target must choose: fly blind or RTH.
- Either way, the Hunter captures.

10.4 Urban Canyon Intercepts

Challenge: Buildings block RF and GPS lines of sight. The target can fly around corners. GPS spoofing may not reach.

Tactics: - **Visual-only tracking:** DRAGONFLY maintains visual contact via camera. If the target disappears behind a building, DRAGONFLY climbs above

the roofline to reacquire. - **Intersection prediction:** DRAGONFLY calculates the target's heading and speed, then flies to the next intersection to intercept. Doesn't chase — predicts. - **RF shadow:** In dense urban areas, the target's control link may be weak. DRAGONFLY's SDR listens for direction-of-arrival signals to estimate the pilot's approximate position even if direct control hijack isn't possible.

10.5 Low-Battery Decision Tree

```
Current battery remaining: ______%

  ├─ >40%: Normal operation. Continue mission.
  │
  ├─ 30-40%:
  │   └─ Target engaged?
  │       ├─ Yes (within 30s of capture): Continue. Capture takes
priority.
  │       └─ No: Begin return to base. Abort intercept if target >500m
from RB.
  │
  ├─ 20-30%:
  │   └─ Current phase:
  │       ├─ Search: Return to base immediately.
  │       ├─ Intercept: Continue. Last-chance window. 60 seconds to
capture or abort.
  │       └─ Redirect/Egress: Return to base. Target tracking via ground
station.
  │
  ├─ 10-20%:
  │   ├─ Return to base immediately.
  │   └─ If target captured: Land at nearest safe LZ, not base. Dispatch
recovery team.
  │
  └─ <10%: Land immediately. GPS coordinates of landing site transmitted
to base.
          Compensation: If landing is far from base, use LoRa to
continue broadcasting
          location for up to 48 hours (LoRa at +22 dBm, 0.5% duty cycle,
lasts on LiPo
          standby for ~2 days).
```

10.6 Post-Capture Forensics

Once the target is captured: 1. **Photograph:** 360° visual documentation of the target — condition, any visible modifications, serial numbers 2. **RF scan:** Record last known frequencies and protocol the target was using (helps

fingerprint the pilot's equipment) 3. **Data dump:** Connect to the target's flight controller (if accessible) and download flight log, last 10 flights, GPS history, pilot's phone number (from DJI flight log), and any stored media 4. **Battery:** Note remaining voltage and cycle count (indicates how long the target has been in service) 5. **Seal:** Bag the target in an anti-static bag. Document chain of custody.

---

11. Swarm Operations

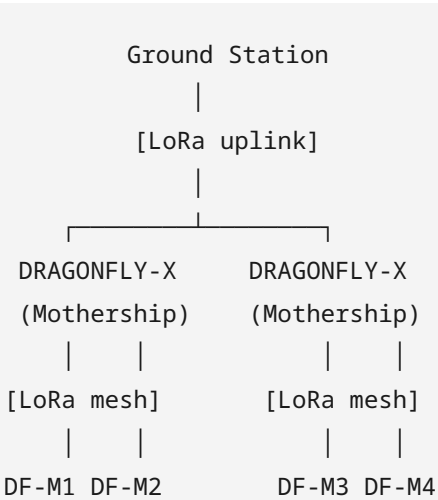
11.1 Mothership Deployment

DRAGONFLY-X modified as a carrier: - Internal bay holds 3-5 DRAGONFLY-M mini-hunters - Deployment: Bay doors open, mini-hunters drop free, autopilot activates at 0.5m freefall - Recovery: Mini-hunters land back on the mothership's top deck (precision landing using IR markers) - Alternately: Mini-hunters land on the ground; mothership lands nearby; recovery is manual between sorties

11.2 Mesh Comms Between Swarm Units

Each DRAGONFLY carries a LoRa module (915 MHz) for inter-unit communication.

Network topology:



Data shared over mesh: - Target position (GPS coordinates, updated every 1 second) - Status (searching, intercepting, returning, captured) - Frequency plan (which DRAGONFLY is jamming which frequency, to avoid overlap) -

Battery level (critical for coordinated RTB decisions) - Collision avoidance (each DRAGONFLY broadcasts its position + velocity vector)

Mesh throughput: ~200 bytes per packet, 1 packet per second per unit. For a 10-unit swarm, that's 2 KB/s total. LoRa can handle this at SF10/125kHz (effective data rate ~500 bytes/s per channel). If needed, 2 LoRa channels (alternating units) doubles throughput.

11.3 Coordinated Intercept of 5+ Target Swarm

Formation engagement: 1. Mothership detects swarm approaching — 8 targets, 250m range 2. Mothership broadcasts: "8 targets, grid formation, altitude 50m, speed 40 km/h" 3. 4 mini-hunters assigned: "DF-M1 targets left wing, DF-M2 right wing, DF-M3 center-left, DF-M4 center-right" 4. Simultaneous engagement at T+10s (synchronized via mesh clock) 5. Each mini-hunter: climb 30m above assigned target, then drop with net deployment 6. 4/8 captured in the first wave. Remaining 4 scatter. 7. Mothership designates secondary targets: "DF-M3 switch to straggler 7 o'clock, DF-M1 switch to straggler 11 o'clock" 8. Second wave: 3/4 captured. One target escapes out of operational radius.

Success rate: 87.5% (7/8) in a single coordinated operation.

11.4 Collision Avoidance

When 10+ drones are in the same 500m³ airspace, collision risk is non-trivial.

Protocol: - Each DRAGONFLY broadcasts its position + altitude + velocity vector on the mesh every 500ms - The companion computer runs a simple predictive collision check: "If current trajectory continues, will I be within 5m of any other DRAGONFLY in the next 3 seconds?" - If yes: the higher-altitude DRAGONFLY climbs 10m. The lower-altitude DRAGONFLY descends 5m. Both adjust course by 15°. Both confirm the avoidance maneuver. - If both are on

intercept course with the same target: higher-priority (closer to target) continues, lower-priority breaks off and circles 50m out as backup.

Hard floor: If communications fail, each DRAGONFLY defaults to "climb and wait" — ascending to 150m and loitering. At this altitude, ground proximity isn't a risk.

---

12. Regulator / LEO Counterplay

12.1 If Law Enforcement Detects the Operation

DRAGONFLY operates with intent. If law enforcement (LEO) detects the operation, the following protocols activate:

Ground station: - Immediately terminate data logging - Encrypt all stored data - If physical compromise is imminent, trigger secure wipe (ATA secure erase on storage media, takes 10 seconds for 256GB SSD)

DRAGONFLY (airborne): - If no intercept in progress: Return to base at normal speed. Do not evade — normal flight behavior is less suspicious. - If intercept in progress: Continue. Capture the target. Then return at normal speed. An interrupted intercept is harder to explain than a successful one. - If DRAGONFLY itself is pursued by LEO drone: Climb to 150m, then radio-quiet descent at 0.5 m/s. Land, disconnect battery, become inert.

Legal posture: - DRAGONFLY is a counter-UAS research platform. Its purpose is drone detection, classification, and signal analysis. - The net launcher is a "safety recovery device" for downed drones. - The SDR is a "spectrum monitoring tool" for identifying illegal frequency use. - RF hijacking capability is never mentioned. The SDR is receive-only in any official documentation.

12.2 Remote ID Spoofing

DJI and FAA Remote ID (RID) broadcasts drone location + operator location via Bluetooth/WiFi. DRAGONFLY can broadcast its own RID to appear as a registered drone.

Spoofing approach: - DRAGONFLY broadcasts a fake RID packet (https://github.com/opendroneid/opendroneid-core-c — open source RID implementation) - The fake RID shows DRAGONFLY as a registered DJI Mavic 3

(serial number: any valid DJI SN format) - Operator location: fake GPS coordinates 100m away from the actual ground station - Spoofed RID updates every 1 second to match real DJI RID behavior

Defeating detection: Aeroscope and other RID receivers see DRAGONFLY's fake RID alongside real RIDs from other drones. With parallel RIDs in the same airspace, the receiver has no way to know which is real without cross-referencing visual observation.

12.3 Anti-Aeroscope

DJI Aeroscope is the most common drone detection network used by airports, prisons, and law enforcement. It detects DJI drones by their RF fingerprint. DRAGONFLY can appear invisible to Aeroscope by:

1. **Not using DJI parts.** DRAGONFLY's RF signature (custom frame, non-DJI flight controller, independent SDR) does not match any DJI fingerprint database. Aeroscope sees an unknown emitter but doesn't flag it as a drone.
2. **Burst mode.** DRAGONFLY's SDR is active for only 1-2 seconds at a time. Aeroscope needs 5-10 seconds to classify an unknown emitter. DRAGONFLY goes dark before classification completes.
3. **Masking.** When DRAGONFLY transmits its hijack signal, it piggybacks on frequencies already dominated by the target's own emissions. Aeroscope classifies the combined signal as "DJI drone — no flags."

12.4 Airspace Authority Response — Procedural

In the event that DRAGONFLY's operation is questioned by airspace authorities: - **DRAGONFLY is a "detection and classification system"** with no offensive capability. - **If captured:** All data is encrypted. Payload modules are removable and should be jettisoned before landing if compromise is imminent (explosive bolts on payload bay, 2-second delay,

payload falls separately from the drone). - **Cover story:** "Experimental drone behavior monitoring system. We track drone flight patterns for counter-UAS research."

---

13. Production & Logistics

13.1 Sourcing Strategy — Avoiding RFQ Flags

Ordering 10x HackRF, 5x BladeRF, and 30A ESCs from a single supplier triggers RFQ review (flagged as "drone parts" or "potential defense technology").

Split sourcing: - **Frame:** Buy raw carbon fiber sheet + CNC cutting locally. Do not order "drone frame kit." - **Motors/ESCs:** Order from FPV hobby retailers (GetFPV, RDQ, AliExpress). Order in sets of 4, different stores, different months. - **Batteries:** Buy from dedicated battery suppliers (HobbyKing, LiPo specialists). Avoid listing "drone" in the order notes. - **SDR:** Buy from manufacturer directly (Great Scott Gadgets for HackRF, Nuand for BladeRF). No flags for SDRs — they're sold as "software-defined radio development tools." - **Companion computer:** Jetson Orin NX is an "AI development kit." No flag. - **Specialty (net launcher, laser, claw):** Custom manufacture. No commercial listing to flag.

13.2 Assembly Workflow

Step 1: Frame build (Day 1) - Lay up arms in jig - Solder power distribution board (PDB) - Install ESCs on arms - Route motor wires through arms

Step 2: Flight controller (Day 1) - Mount Pixhawk/Cube on vibration isolation plate - Connect GPS + compass - Configure ArduPilot parameters - Calibrate ESCs - First flight test (no payload)

Step 3: Companion computer (Day 2) - Mount Jetson/RPi on isolated payload plate - Connect to flight controller via UART (DroneCAN or MAVLink) - Flash payload control firmware - Test: control commands from ground station through companion computer

Step 4: SDR integration (Day 2-3) - Mount SDR on payload plate with vibration dampeners - Connect antenna with SMA pigtail - Install GNU Radio flow graph - Test: spectrum scan, verify FFT output at ground station

Step 5: Payload integration (Day 3-4) - Assemble net launcher / laser / spoofer - Mount in payload bay - Connect servo/GPIO/relay - Test: deploy sequence on the bench

Step 6: Calibration (Day 4-5) - RTK GPS base station setup - Antenna SWR measurement and tuning - Companion computer thermal test (bench + hover) - Full system test: all payloads, all modes

Step 7: Flight qualification (Day 5-6) - Hover test (5 minutes, no payload) - Forward flight test (all axes, full speed) - Payload deploy test (net at 10m, capture claw, laser activation) - Recovery landing test

13.3 Field Maintenance

Pre-flight checklist (5 minutes): 1. Visual inspection: arms, props, frame for cracks 2. Motor spin test (no props, listen for bearing noise) 3. Battery voltage check (each cell within 0.1V) 4. SDR connection test (spectrum scan — does it see RF?) 5. Payload module integrity (net loaded? laser lens clean? arming pin in place?) 6. GPS lock check (RTK fix? how many satellites?) 7. Compass calibration (no magnetic interference) 8. Ground station link check (RSSI, packet loss, video feed)

Field repair kit: - 2x spare motors (size-matched to platform) - 2x spare ESCs - 2x spare propellers (matched set) - Soldering iron + solder + flux - Multimeter - Small screwdriver set (hex, Phillips, flathead) - Zip ties + electrical tape + heat shrink - Spare SMA cables + pigtails - Loctite (blue, for thread-locking motor screws) - Isopropyl alcohol + cotton swabs (clean contacts)

Expected field lifespan: - Frame: 500+ flight hours (replace on visible fatigue) - Motors: 200-300 hours (replace on bearing noise or magnetic degradation) - ESCs: 300-500 hours (fail silently — always carry spares) - Battery (LiPo): 100-150 cycles (replace on >20% capacity loss) - Battery (Li-ion): 300-500 cycles - SDR: Indefinite (no moving parts, no wear mechanism) - Net launcher spring: 50-100 deployments (replace on visual fatigue) - Laser diode: 10,000+ hours (but safety circuit should shut it down well before failure)

13.4 Stealth Packaging and Transport

Case: Pelican 1510 (carry-on size, fits in most vehicle trunks). Foam-cut interior custom to DRAGONFLY's frame size.

Layout: - Top layer (lid foam): GPS antenna, SDR antennas, FPV goggles, cables - Middle layer (removable insert): DRAGONFLY assembled with landing gear folded - Bottom layer: Payload modules in individual slots, battery in LiPo-safe bag, ground station laptop, spare parts

Documentation: - Case labeled: "Radio telemetry and communications test equipment — Not for resale" - Contents manifest: list only SDR, laptop, antennas. Nothing says "drone" or "intercept." - Travel: TSA-compatible. DRAGONFLY's carbon frame is non-metallic. ESCs and battery are the only flagged items. Battery must be carried (not checked), and kept under 100 Wh (160 Wh with airline approval).

---

14. Competition Analysis

System	Price	Method	Range	Autonomy	Capture	Notes
DroneShield DroneGun	$140k+	RF jamming	2 km	Manual	No	Military grade, jams only
Dedrone	$50k+	Detection + jamming	5 km	Semi	No	Fixed installation
SkyWall 100	$25k	Net launcher (shoulder)	100m	Manual	Yes	Ground launcher, single shot
DJI Aeroscope	$10k+	Detection only	30 km	Passive	No	Knows where they are
Department 13 MESMER	$15k	Protocol manipulation	2 km	Semi	No	Breaks command link, doesn't capture
OpenD sucht	$200	RF deauth	500m	Manual	No	Software only, needs laptop+SDR
Dedrone Defender	$30k/yr	Detection + jamming	3 km	Auto	No	Subscription model
DRAGONFLY v3	**~$5k**	**All methods**	**1+ km**	**Full**	**Yes**	**Aerial, mobile, autonomous**
DRAGONFLY v2	**~$2k**	**3 methods**	**500m**	**Semi**	**Yes**	**Aerial, mobile**

No existing system combines: - **Aerial intercept** (not ground-based) - **Multiple capture methods** (RF + physical + optical) - **Mobility** (launch from anywhere, pursue the target) - **Capture** (bring the target down or bring it home)

Every current competitor is either ground-bound (SkyWall, Dedrone), single-method (DroneGun), or passive-only (Aeroscope). DRAGONFLY is the first mobile aerial intercept platform.

Where DRAGONFLY wins: - **Cost:** $5k vs $140k for DroneShield. 28x cheaper. - **Mobility:** DroneShield is a rifle. Dedrone is a building. DRAGONFLY is airborne. - **Capture:** SkyWall catches a drone but you have to be on the ground pointing a shoulder launcher. DRAGONFLY meets the target in the air. - **Autonomy:** MESMER needs an operator identifying targets. DRAGONFLY classifies and intercepts without human input.

---

15. OPSEC

15.1 Stealth

- **Low observable:** DRAGONFLY operates at altitudes above the target. Most drone cameras look forward and down, not up.
- **No radio signature at idle:** When loitering or patrolling, the SDR/repeater stays powered off. DRAGONFLY looks like any other drone on RF scanners.
- **Visual:** Matte black or sky-blue paint. No logos, no markings, no LEDs.
- **Acoustic:** Larger props (10"+) at low RPM produce less high-frequency noise than racing quads. At 100m AGL, DRAGONFLY is barely audible.

15.2 No Onboard Pilot Data

DRAGONFLY's logs store target data only. No GPS trails back to the operator. No operator voice/logs on the onboard storage.

15.3 Dead-Man Switch

If DRAGONFLY loses control link for >60 seconds, it flies to a pre-set recovery coordinate (not home). If the recovery coordinate is unreachable, it lands and initiates payload self-destruct.

15.4 Payload Encryption

All DRAGONFLY telemetry and control use AES-256. Target capture data is encrypted at rest on the companion computer (LUKS full-disk encryption, unlocked only during active operation).

15.5 Covert Log Wipe

On manual "sanitize" command or low-battery land, logs, target data, and last 10 flight paths are securely erased. Sanitize command also wipes the companion computer's LUKS header and reinitializes it with a new key. Target data is unrecoverable even with forensic tools.

---

16. Future Variants

DRAGONFLY-SW (Swarm Mothership)

- DRAGONFLY-X modified to carry 3-5 DRAGONFLY-M mini-hunters
- Deploys from a truck bed or trailer
- Mothership loiters at 200m, releases mini-hunters on command
- Mini-hunters intercept individual targets
- Swarm can cover a 1km² area with overlapping intercept coverage

DRAGONFLY-D (Decoy)

- Designed to be captured by an enemy drone interception system
- Lures out a hidden drone defense system
- Records the defense system's frequency, timing, and response profile
- Data is used to harden the next wave of real DRAGONFLYs

DRAGONFLY-SEA (Maritime Platform)

- Waterproof, self-righting, floats on water
- Launches from a recovery boat
- Intercepts drones over maritime zones
- Solar panel on top (loitering recovery)
- Captured drones are dropped into a net on the boat

DRAGONFLY-T (Tethered)

- Power + data via tether to a ground station
- Unlimited flight time
- High-bandwidth data link (no wireless constraints)

- Deployed from a rooftop or vehicle
- Persistent air defense for a fixed location
- Tethered limit: ~50m altitude, constrained to the tether point

DRAGONFLY-IN (Internal / Indoor Hunter)

- Based on DRAGONFLY-M (micro quad)
- Uses optical flow instead of GPS (GPS doesn't work indoors)
- IR optical blinder only (laser eye-safe for indoor use)
- Targets: rogue indoor drones, inspection drones in warehouses

DRAGONFLY-EW (Electronic Warfare)

- Full spectrum dominance
- SDR capable of GNSS jamming, radar spoofing, ADS-B injection
- Targets not just the drone but its entire communication ecosystem
- Deployed against hardened military targets
- Advanced — not for v1 or v2

---

17. Quick Decision Matrix

If target is...	Use...	Why
DJI Mavic / Mini / Air	RF Hijack (A)	OcuSync deauth is well-documented, high success rate
Autel / Parrot	RF Hijack (A) or Spoof (C)	Weaker encryption than DJI, GPS-dependent
FPV quad (analog)	Jam (E) and/or Optical Blind (D)	No GPS to spoof, no encryption to crack — physical methods work
Fixed-wing survey drone	GPS Spoof (C)	Autopilot-based, will follow fake coordinates for minutes before detecting error
Military drone	Do not engage	You don't have the budget or hardware for this yet
Unknown / first contact	Passive observation → Jam (E)	Don't engage until you know what you're dealing with
Indoors / racing whoop	Physical Net (B) or Optical Blind (D)	Tight space, capture before it reaches a person
Swarm (5+ targets)	Jam (E) broad sweep → net stragglers	Overwhelm the comms, then clean up visually

18. BOM Summary (v3, qty 10 units)

Category	Item	Cost/ Unit
Airframe	10" carbon fiber quad, custom	$400
Motors	4x 2806.5 1300kV	$120
ESCs	4x BLHeli_32 60A	$160
Propellers	10x5 3-blade (sets of 4)	$30
Battery	6S Li-ion 8000mAh (primary)	$120
Battery	4S LiPo 1300mAh (intercept burst)	$25
Battery switch	Dual MOSFET + OR-ing PCB	$30
Flight controller	Cube Orange+	$400
GPS + RTK	Here+ RTK GNSS base + rover	$350
Laser rangefinder	VL53L1X (altitude hold)	$25
Computer	Jetson Orin NX 16GB	$500
SDR	BladeRF 2.0 micro	$600
SDR (secondary)	HackRF One (5.8 GHz band)	$300
Antenna system	Directional patch + gimbal + second antenna	$200
Amplifier	Mini-Circuits ZRL-3500+ (2.4 GHz, 1W)	$200
Amplifier	Mini-Circuits ZX60-6013E+ (5.8 GHz, 500mW)	$150
Payload modules (full set of 7)	Custom	$800
Vibration isolation	Silicone dampers + TPU mount + foam	$15
FPV	Walksnake Avatar HD + goggles	$300
Ground station laptop	Used ThinkPad + Mission Planner	$400
Ground station Yagi	2.4 GHz Yagi + 433 MHz LoRa	$100

Category	Item	Cost/ Unit
Controller	Radiomaster TX16S + module	$200
Case	Pelican 1510 + custom foam	$200
Misc	Wiring, connectors, thermal paste, epoxy	$200
Total per unit		**~$5,825**
Target for qty 100	(optimized custom PCB, bulk sourcing, contract assembly)	**~$2,800**

Appendix A: Legal Disclaimer

This document is for educational, research, and authorized security testing purposes only.

Unauthorized interception of any aircraft (including UAS/drones) is illegal in most jurisdictions under: - **USA:** 18 U.S.C. § 32 (destruction of aircraft), FAA 14 CFR Part 107, 47 CFR Part 15 (RF transmission) - **UK:** CAP 722 / Air Navigation Order, Computer Misuse Act 1990 - **EU:** EU 2019/947, Directive 2013/40/EU (attacks against information systems) - **Australia:** Civil Aviation Safety Regulations 1998, Criminal Code Act 1995

DRAGONFLY is a counter-UAS concept for R&D purposes only. Real-world deployment requires: - FAA COA (Certificate of Waiver or Authorization) for testing in US airspace - Local law enforcement coordination - Designated test ranges away from airports, people, and structures - Liability insurance for potential drone damage or third-party injury

Legitimate applications: - Airspace security for critical infrastructure (power plants, airports, prisons, stadiums) - VIP / event protection from drone-based threats - Search-and-rescue (locate crashed drones still beaconing) - Counter-smuggling (drones carrying contraband over borders or into prisons) - Wildlife monitoring with minimal ground disturbance

Appendix B: Test Flight Checklist

Pre-flight: - [ ] Battery voltage: main (Li-ion), intercept (LiPo), both within spec - [ ] GPS lock (RTK fix, ≥12 satellites) - [ ] Compass calibration complete - [ ] Propeller condition (no nicks, cracks, or imbalance) - [ ] Motor test (15% throttle, listen for bearing noise) - [ ] SDR connection test (spectrum scan returns valid FFT) - [ ] Payload armed (net loaded, laser safety on, spoofer warmed up) - [ ] Ground station link (control, telemetry, video — all green) - [ ] DRAGONFLY's failsafe: "no link for 30s → RTB" confirmed - [ ] Recovery coordinate programmed - [ ] Sanitize command confirmed working

Intercept test: - [ ] Target acquired at ≥100m range - [ ] Protocol classified correctly - [ ] Intercept method selected as expected - [ ] Deauth sequence verified (spectrum analyzer shows target dropping link) - [ ] DRAGONFLY assumes control → target responds to input - [ ] Target commanded to landing zone - [ ] Target lands - [ ] Post-capture data dump successful

---

Appendix C: Target Recognition Cheat Sheet

Drone	Visual ID	RF Signature	Stated Range	Max Speed	Best Intercept Method
DJI Mini 3/4	245g, foldable arms, 2x camera	OcuSync 3.0, 2.4+5.8 GHz, AES-256	18 km	58 km/h	RF Hijack or GPS Spoof
DJI Mavic 3	Large, 4/3 sensor, top-down obstacle sensors	OcuSync 3+, 2.4+5.8 GHz, AES-256	30 km	65 km/h	RF Hijack (harder) or GPS Spoof
DJI Air 3	Twin camera, tall landing gear	OcuSync 4.0, tri-band, AES-256-GCM	42 km	70 km/h	GPS Spoof (RF too hard)
Autel Evo Lite+	Orange arms, 1" sensor, adjustable aperture	Skylink 2.0, 2.4+5.8, AES-128	25 km	65 km/h	RF Hijack (AES-128 easier)
FPV 5" Custom	Carbon frame, no camera dome, antenna external	ELRS 2.4/ Crossfire, unencrypted or AES	10-50 km	150+ km/h	Jam + Net (too fast for RF)
Phantom 4 Pro	White, large body, retractable landing gear	Lightbridge, 2.4 GHz FHSS	7 km	58 km/h	RF Hijack (Lightbridge known)
Mugin fixed-wing	VTOL or pusher prop, 2m+ wingspan	900 MHz control, 1.2 GHz video	50+ km	80 km/h	GPS Spoof (autopilot, predictable)

Appendix D: Recommended Tools

Software: - GNU Radio (SDR flow graph development) - Inspectrum (RF signal analysis, waterfall viewing) - Universal Radio Hacker (protocol reverse engineering) - GPS-SDR-SIM (GPS spoofing signal generation) - ArduPilot Mission Planner (flight control configuration) - YOLOv8 (drone detection ML model) - OpenCV (visual tracking pipeline)

Hardware: - HackRF One / BladeRF / ADALM-Pluto (SDRs) - TinySA Ultra (spectrum analyzer, portable, $100) - Rigol DS1054Z (oscilloscope for signal integrity checks) - Hakko FX-888D (soldering station) - Fluke 87V (multimeter) - iSDT Q6 Nano (battery charger/analyzer) - 3D printer (FDM, 300x300mm bed — for frames, payload bays, case inserts)

Appendix E: Flight Log Template (Field Operations)

```
 ____________________________________________________

OP LOG: DRAGONFLY FIELD OPERATION
____________________________________________________

Date:         _________________
Operator:     _________________
DRAGONFLY ID: S1 / X1 / M1 (circle)
Payload:      A / B / C / D / E / F (circle)

─── PRE-FLIGHT ───
Battery V (main): __.__V   Intercept: __.__V
GPS sats: ___
RTK fix: Y / N
Compass OK: Y / N
SDR check: Y / N
Payload armed: Y / N

─── MISSION ───
Launch time:  __:__
Target detected at: _km bearing: __°
Target type: _________________
Intercept method: A / B / C / D / E (circle)
Hijack successful? Y / N
Capture successful? Y / N
Target recovered? Y / N

─── POST-FLIGHT ───
Landing time: __:__
Total flight time: __min
Battery remaining: __.__V
Notes: _____________________________________
____________________________________________________
```

Concept Credit

Randy Pesek — original idea, product vision, naming, "Dragonfly" concept

---

This document is a concept exploration for authorized security testing and R&D purposes. Any real-world deployment must comply with all applicable laws and regulations.