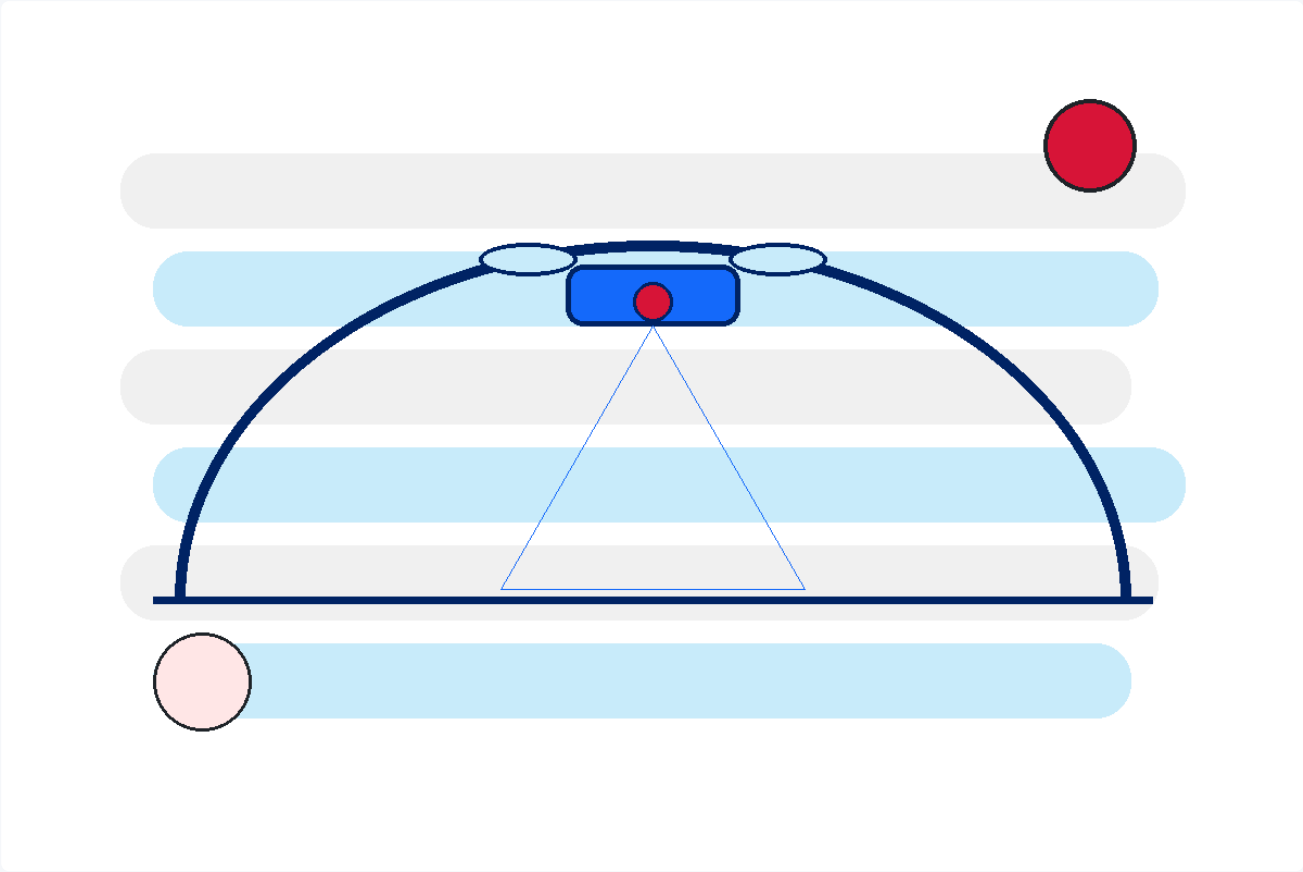
Counter-UAS (C-UAS): 'The Stuff That Shoots Down Drones' & Airspace Security

Multi-Sensor DTI (Radar, Passive RF, EO/IR, Acoustic, RID) & Neutralization Effectors (Cyber Takeover, Jamming, Net Drones, Kinetic, HPM, Lasers)

08. Counter-UAS (C-UAS): "The Stuff That Shoots Down Drones" & Protects Critical Transport Infrastructure

Prepared for the Architect of Tech — Transport for NSW (TfNSW)



Counter-UAS Kill-Chain & Effector Taxonomy

1. Why Transport for NSW Needs C-UAS & 3D Airspace Security

Critical transport networks are high-value, exposed linear assets operating inside a contested **Low-Altitude Airspace envelope ($0–400 ext{ ft AGL}$)**. For **TfNSW**, key threat scenarios include:

- **Iconic Bridges (Sydney Harbour Bridge, Anzac Bridge):** Rogue FPV drones crashing into multi-lane deck traffic; protest drones suspending banners (paralleling the 2018 Gatwick Airport 36-hour paralysis that stranded 140,000 passengers); or payload-carrying UAS targeting structural cables.
- **Electrified Rail & GoA4 Metro (Sydney Trains & Sydney Metro):** Drones colliding with **$1500 ext{ V DC}$ Overhead Wiring (OHW)** causing catastrophic arc faults, pantograph entanglement, or bushfires; unauthorized drones hovering over open-cut GoA4 driverless metro viaducts triggering automated emergency braking; or espionage of signalling substations.

- **Ferries & Ports (Circular Quay, Port Botany, Newcastle):** Low-flying drones blinding ferry masters during docking at Circular Quay or interfering with automated container cranes.
- **Smart Motorways & Future Vertiports (Western Sydney Aerotropolis):** Distraction/impact with $110 ext{ km/h}$ vehicles, $5.9 ext{ GHz}$ C-ITS RF interference, or mid-air collision (MAC) risks with emergency helicopters and future eVTOLs.

---

2. Phase 1: Full Taxonomy of Detection, Tracking & Identification (DTI)

Because "dark" autonomous drones fly on pre-programmed GPS/INS or visual SLAM without emitting any radio signals, no single sensor suffices. Best-practice C-UAS fuses **5 complementary sensor modalities**:

Sensor Modality	Physics & Mechanism	Key Advantages	Urban Transport Limitations
1. 3D/4D AESA & Micro-Doppler Radar	Active Electronically Scanned Array or Metamaterial ESA (e.g., *Echodyne EchoGuard*, *Blighter A400*, *RADA RPS-42*) in X/Ku/S-band. Detects **Micro-Doppler modulation** from spinning carbon/plastic rotor blades even when airframe RCS is $<0.01 ext{ m}^2$.	**Detects "dark" RF-silent autonomous drones.** Provides exact 3D range, azimuth, elevation, and velocity vector day/night in all weather.	Multipath clutter from steel trusses (Sydney Harbour Bridge), high-rises, and moving trains; requires AI micro-Doppler filtering to reject seagulls/cockatoos.
2. Passive RF Spectrum Sensing (RF-DF)	Software-Defined Radios (SDRs) scanning $400 ext{ MHz}–6 ext{ GHz}$ using Time Difference of Arrival (TDOA), Angle of Arrival (AoA), and deep-learning packet fingerprinting (*DroneShield RFAI*, *DedroneDNA*).	**100% passive (zero ACMA legal friction!).** Detects and geolocates **both the airborne drone AND the pilot's ground controller** often as soon as the controller is switched on before takeoff!	**Blind to RF-silent "dark" drones** or drones controlled via fiber-optic tether / unmonitored 5G cellular links.
3. EO/IR Optical & Thermal AI Vision	High-speed Pan-Tilt-Zoom (PTZ) 4K daylight CMOS + cooled/uncooled MWIR/LWIR thermal cameras driven by CNN/YOLO computer vision (*DroneOptID*).	Slew-to-cue **visual verification of payload** (distinguishing a harmless wedding camera drone from a drone carrying a drop-hook or incendiary) and records court-admissible forensic video.	Narrow field of view (must be cued by Radar or RF); degraded by thick sea fog or heavy rain.
4. Acoustic Phased Microphone Arrays	Weatherproof microphone arrays (*Squarehead*, *DroneShield Acoustic*) using acoustic beamforming to match rotor harmonic signatures.	Passive Non-Line-of-Sight (NLOS) gap-filler **under bridge decks** or inside **tunnel portals** where radar/optics are blocked.	Short range ($300–500 ext{ m}$); masked by loud freight trains, motorway traffic, and ferry diesels.
5. Remote ID (RID) & ADS-B Receivers	Captures broadcast Wi-Fi NaN / Bluetooth 4/5 packets (**ASTM F3411**) plus $1090 ext{ MHz}$ ADS-B.	Instantly decodes drone serial number, operator registration, and take-off GPS for cooperative drones.	Ignored or spoofed by malicious actors and DIY FPV builds.

---

3. Phase 2: Full Taxonomy of Mitigation & Interdiction ("The Stuff That Shoots Down Drones")

Category A: Surgical Cyber Protocol Takeover (CRPC — The Urban Gold Standard)

- **Representative Systems: D-Fend Solutions** `EnforceAir2` (`https://www.d-fendsolutions.com/`) & **Department 13** `MESMER` (Australia).
- **How It Works:** Passively sniffs the target drone's communication protocol, reverse-engineers the telemetry/control handshake in real time, severs the rogue pilot's control link, and injects legitimate root-level flight commands.
- **Why It Is Ideal Over Rail & Motorways:** Instead of jamming GPS or blasting a drone out of the sky so it crashes onto live $1500 ext{ V DC}$ railway wires or a 6-lane motorway, Cyber Takeover commands the rogue drone to **fly along a safe pre-defined route and land gently on a designated recovery pad**, while extracting the pilot's home-point coordinates for police arrest.
- **Limitation:** Only works against known commercial/custom RF protocols; cannot hijack a completely radio-silent autonomous drone.

Category B: Non-Kinetic Electronic Warfare (RF & GNSS Jamming / Spoofing)

- **Representative Systems: DroneShield** `DroneGun Tactical` , `DroneGun Mk4` & `DroneSentry-X Mk2` (Sydney, NSW — `https://www.droneshield.com/`), **Anduril** `Pulsar` , **Dedrone** `DedroneDefender` .
- **How It Works:** Transmits high-gain directional or 360° electromagnetic noise across ISM control/video bands ($433 ext{ MHz}, 915 ext{ MHz}, 2.4 ext{ GHz}, 5.8 ext{ GHz}$) and optionally satellite navigation bands (**GPS L1/L2/L5, GLONASS, Galileo, BeiDou**).
- *RF C2 Jamming Only:* Triggers the drone's failsafe—typically **hover in place, vertical auto-land, or Return-to-Home (RTH)** (which conveniently leads police straight back to the pilot!).
- *RF + GNSS Jamming:* Deprives the drone of both pilot commands and satellite positioning, forcing an immediate vertical descent or uncontrolled drift.
- *GNSS Spoofing (e.g., Regulus Cyber):* Broadcasts counterfeit satellite ephemeris data telling the drone it has entered an airport No-Fly Zone (NFZ), forcing its firmware to auto-land.
- **Transport Infrastructure Warning: Broadband GNSS jamming or spoofing near transport hubs is highly hazardous**—it can disrupt civil aviation approaches at Sydney Airport, Sydney Ferries harbour navigation, and Stratum-1 GPS timing clocks used in rail signalling and telecom towers.

Category C: Autonomous Net-Capture Interceptor Drones (Non-Destructive Kinetic)

- **Representative Systems: Fortem Technologies** `DroneHunter F700` (`https://fortemtech.com/`), **Delft Dynamics** `DroneCatcher` , **OpenWorks** `SkyWall Auto` .
- **How It Works:** When radar detects a **"dark" RF-silent autonomous drone** (immune to cyber takeover and RF jamming), an autonomous interceptor quadcopter launches, locks onto the intruder using onboard AI radar (**Fortem TrueView R20**), and fires a **Droid™ net with an attached parachute**.
- **Why It Excels for Bridges & Corridors:** Snaring the hostile drone's rotors in a net and **towing it away or lowering it gently under a parachute** ($>85\%$ capture success rate) neutralizes dark autonomous drones without shrapnel or falling wreckage over roadways.

Category D: Autonomous Kinetic "Hit-to-Kill" Ramming Interceptors

- **Representative Systems: Anduril `Anvil` / `Anvil-M`** (Major APAC Engineering Hub in Sydney, NSW — `https://www.anduril.com/`), **RTX `Coyote Block 2`**, **MARSS `Interceptor-SR`**.
- **How It Works:** Launched from a weatherized readiness box, **Anduril Anvil** accelerates to **150–200 mph ($240–320 ext{ km/h}$)** guided by an onboard computer-vision/infrared seeker, physically ramming hostile Group 1–2 drones mid-air to shatter them using kinetic energy alone (no explosive warhead in the base variant).

Category E: Directed Energy Weapons — High-Power Microwave (HPM) Swarm Defeat

- **Representative Systems: Epirus `Leonidas`** (`https://www.epirusinc.com/`), **Raytheon `Phaser`**.
- **How It Works:** Solid-state Gallium Nitride (GaN) phased-array transmitters fire intense nanosecond-pulsed microwave beams. The electromagnetic pulse couples into the internal PCB traces and wiring of drones, instantaneously frying their flight controllers and MOSFETs.
- **Swarm Advantage:** Can drop **10 to 50+ drones simultaneously** inside an electronically steered beam cone regardless of whether the drones are autonomous, fiber-guided, or RF-controlled. *Caution:* Causes drones to fall dead like bricks and can damage unshielded roadside electronics in the beam path.

Category F: Directed Energy Weapons — High-Energy Lasers (HEL) & Smart Airburst Cannons

- **Representative Systems (Australian Sovereign Leader!): Electro Optic Systems (EOS, Canberra — `https://eos-aus.com/defence/`) `Slinger` & `Titanis`**, **Rafael `Drone Dome Laser / Iron Beam`**, **Raytheon `HELWS`**.
- **EOS `Titanis` High-Energy Laser ($35 ext{ kW}–100 ext{ kW}$ class):** Focuses a thermal laser beam onto a $1–2 ext{ cm}$ spot on a drone at **$1–4 ext{ km}$ range**, melting composite wings, severing rotor arms, or igniting LiPo batteries in **2–5 seconds** at a cost of **~$1 of electricity per shot** (engaging up to 20 drones/minute). *Urban limitation:* Severe eye-safety (nominal ocular hazard distance) and airspace dazzle risks if the beam misses the target skyward.
- **EOS `Slinger` Counter-Drone RWS:** Lightweight ($355 ext{ kg}$) 4-axis gyro-stabilized Remote Weapon Station integrating an **Echodyne 4D radar**, thermal optics, and a **30×113mm Bushmaster M230LF cannon** firing radio-frequency proximity-fuzed airburst rounds out to **$1 ext{ km}+$**. Built for military, naval, and high-threat offshore port defense.