



Counter-UAV Site Design Guide

From threat profile to lawful deployment

1. Threat Profile

Define the drone classes

Consumer multi-rotors, FPV drones, fixed-wing reconnaissance, and autonomous pre-programmed flights each stress different sensors.

Map approach corridors

Line of sight, terrain, buildings, and typical wind decide realistic detection and jamming ranges.

Set the consequence target

Early warning only, deterrence, evidence capture, or physical defeat drive very different architectures.

2. Layered Architecture

Detect

Ku-band radar for anything that flies; passive RF for link classification and pilot bearing; handheld detectors for staff on the ground.

Identify

EO/IR cameras cued by tracks provide visual confirmation and evidence before any response.

Track

A C2 platform fuses sensors into one picture with zones, whitelists, and recording.

Defeat

Apply the narrowest effective effector: directional or omnidirectional jamming, GNSS deception, or net capture.

3. Site Survey Checklist

Mounting and power

Tower, rooftop, or mast positions with clear sky view; AC 110-240 V or vehicle/battery power; network backhaul to the control room.

RF environment

Baseline spectrum scan to protect Wi-Fi, telemetry, aviation, and emergency services before band planning.

Operations

Operator roles, confirmation workflow, escalation to police or aviation authority, and evidence handling.

4. Compliance Preparation

Authorization

Jamming and GNSS deception usually need spectrum-regulator and sector-authority approval; start licensing early.

Export control

End-user certificates and end-use statements are standard; procurement timelines should include license lead time.

Documentation

Keep event logs, authorization scopes, and training records; insurers and regulators increasingly require them.

Contact

torch@uavblocker.com // www.uavblocker.com // Zhongshan, China