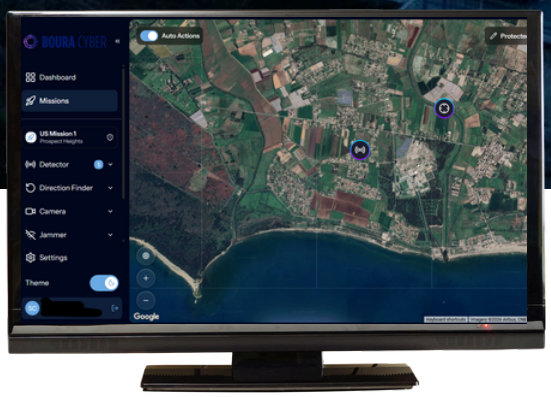
BOURA CYBER BOURA CYBER

Nexus360
The Command & Control (C2) Platform for Counter-Drone Defense

Nexus360° gives operators instant situational clarity against airborne threats. Its intuitive interface highlights only critical data, powered by an open-orchestration engine that unites diverse sensors and mitigation systems into one seamless defense network.



Overview

Modern counter-drone protection is rarely a "single box" problem. Most security organizations already operate a mix of sensors (RF detection, radars, EO/IR cameras, acoustic, ADS-B, etc.) and, where permitted, response systems. The operational challenge is integration, correlation, decision workflow, and auditable reporting: especially for critical infrastructure sites and internal security organizations.

Our platform is a vendor-agnostic Counter-UAS Command & Control (C2) and Data Platform that unifies third-party detection and response systems into a single operational picture. It is designed to start small (one site, one or two systems) and grow over time: adding sensors, improving fusion, enabling training, and optionally scaling to multi-site or national-level oversight.

BOURA CYBER

Nexus360 - Platform Overview

The platform includes a practical, map-centric operator console featuring missions, sensor views, alerts, and operator workflows, with an emphasis on auditability, replay, and evidence-grade reporting.

A. UNIFIED OPERATIONS CONSOLE

A map-centric user interface provides one operational picture across all connected systems

- Mission / Site workspace to manage each protected facility as a "mission" with its own sensors, rules, and operators
- Real-time notifications (detections, health, and operational events)
- Sensor views and tools (e.g., Detector, Direction Finder, Camera) presented consistently regardless of vendor
- Operator status modes (e.g., Operational, Scheduled) to support shift changes and planned readiness

The UI concept is optimized for security operations: quick identification of alerts, geographic context on the map, and immediate access to the incident workflow.

B. INCIDENT MANAGEMENT AND DECISION WORKFLOW

Instead of raw alerts, the platform structures work as incidents:

- Create and manage incidents (open, assess, assign, act, close)
- Document operator actions and outcomes
- Attach evidence (screenshots, camera snapshots, external documents)
- Maintain a complete audit trail of who did what and when

The incident workflow can operate Manual and/or Automatic modes, depending on the customer's operational policy and regulatory constraints.

MANUAL MODE

Threats are surfaced to the operator via on-screen notifications and pop-up messages. The operator can acknowledge, classify, and initiate actions directly from the pop-up (e.g., locate, task a sensor, or trigger an approved response), with full audit logging.

AUTOMATIC MODE

For authorized deployments, it can execute pre-approved countermeasure playbooks immediately upon detection. Automatic actions are governed by policy rules (zones, confidence thresholds, time windows) and are recorded end-to-end for traceability and after-action review.

This turns counter-drone operations into a measurable, reviewable process: especially important in regulated and high-consequence environments.

Manual camera cueing from the C2 system to obtain visual confirmation of an unauthorized drone.

C. OPEN INTEGRATION LAYER

The core differentiator is a generic integration framework that prevents vendor lock-in.

STANDARDIZED DATA MODEL

Alerts, tracks, target attributes, system health, and actions

3RD PARTY CONNECTORS

"Adapters" connect third-party sensors and systems to the unified model

INCREMENTAL GROWTH SUPPORT

Start with one detection system + one camera system, then add more over time without replacing the C2

This makes the platform an enabling layer for multi-vendor environments, both at single sites and across larger organizations.

D. EVIDENCE, REPORTING, AND EXPORT

Critical infrastructure and government customers need more than a live screen: they need evidence.

- Timeline / replay of incidents and detections
- Evidence packs: consistent exports for internal investigations and after-action review
- Reports (PDF/CSV/JSON) for operational KPIs and compliance needs
- Controlled data export to support local R&D and (where authorized) cross-agency collaboration

E. OPTIONAL: CONTROLLED "ACTION" INTEGRATION

Where allowed by law and organizational policy, the platform can integrate with approved response systems through a policy and permission layer:

- Role-based permissions and approval workflow
- Clear operator controls (e.g., "Locate", "Stop") with audit logging
- Safety-oriented design: actions are governed by rules, roles, and approvals

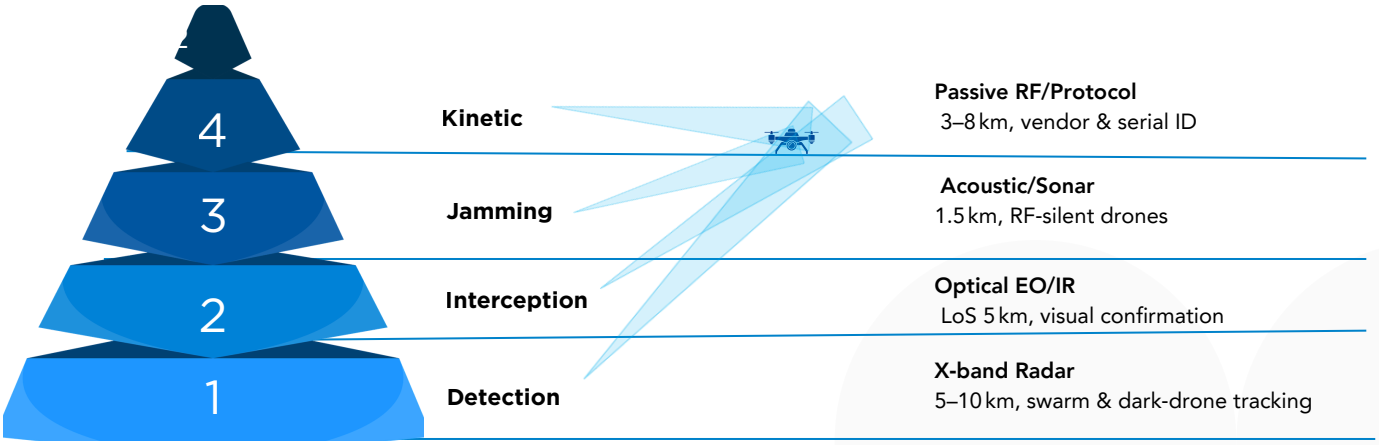
Note: The platform is designed to integrate with authorized response/effectors; actual use is subject to local laws, licenses, and customer operating procedures.

How It works

On-prem / site deployment is the default for sensitive environments:

- **Sensor/Systems Layer:** third-party detection and surveillance systems (RF, radar, EO/IR, etc.)
- **Integration Layer (Adapters):** vendor-specific connectors translate into the platform's generic data model
- **C2 Application Layer:** operations console, incident workflow and audit, reporting/replay/exports, rules/policy engine (phased)
- **Data Layer:** event and track storage, metadata and retention policies, secure export mechanisms ("research packs")
- **Enterprise Integrations (Optional):** interfaces to SOC/SIEM/PSIM, VMS, access control, and ticketing systems

This architecture supports a smooth bootstrap path: begin with minimal integration and a working console, then expand capabilities with each customer deployment.



Security and Operational Readiness

Designed for internal security and critical infrastructure environments:

- **Role-based access control (RBAC)** and strong audit logging
- **On-prem operation** with network isolation options (including air-gapped patterns)
- System health monitoring to ensure sensors and integrations are functioning
- **Data retention policies** aligned with customer requirements

BOURA CYBER

Typical Customer Use Case - Critical Infrastructure

Customer: Internal security organization protecting a power generation site.

Phase 1 - Immediate Value:

- Connect one detection system + selected cameras
- Unified alerting and incident workflow
- Evidence pack and reporting for security leadership
- Basic operational procedures supported by the platform

Phase 2 - Expansion:

- Add additional sensors (different vendors) without changing the C2
- Implement correlation rules and reduce false alarms
- Improve operator readiness with replay-based training

Phase 3 - Enterprise / Multi-site:

- Multi-site fleet view
- Central oversight, metrics, and controlled information sharing
- Standardized operating procedures across sites

Why Nexus360?

Our platform addresses the real operational bottleneck in counter-drone deployments: multi-vendor integration, operational workflow, evidence, and scalable growth. It provides immediate value as a unified C2 console for a single critical site, while laying a clear path to advanced fusion, training, and multi-site/national coordination, built incrementally according to the customer's budget.

SECURE YOUR AIR-SPACE TODAY. CONTACT US.

BouraCyber Solutions, founded by cyber intelligence experts with 30+ years of domain experience, offers comprehensive security services. We prioritize field-proven, best-of-breed innovative products, top-notch execution, and customer service.

BOURA CYBER

bouracyber.com SERVICE@BOURACYBER.COM +972 54 776 9507