Proactive Anti-Drone Defense with the BRO C-UAS Platform

Published on 14/01/2026

Shift from "reacting" to "anticipating". This is the idea with which the Israeli company **Omnisys** is rethinking counter-drone defense: no longer just intercepting a target when it appears on the radar, but **anticipating probable routes, coverage weaknesses, and deployment options** before the threat reaches a useful distance. The key piece of this transformation is the evolution of the **Battle Resource Optimization (BRO)** suite, which is enriched with a next-generation **C-UAS mission planning platform** (Counter-Unmanned Aerial Systems).

From reactive response to "pre-strike" planning

In current scenarios, the drone threat has become more varied and difficult to contain: small commercial quadcopters, **FPV (first-person view)** systems, up to loitering munitions. Omnisys argues that the turning point is not just having more sensors or more jammers, but **better using those already available**, placing them in the right positions and with the right

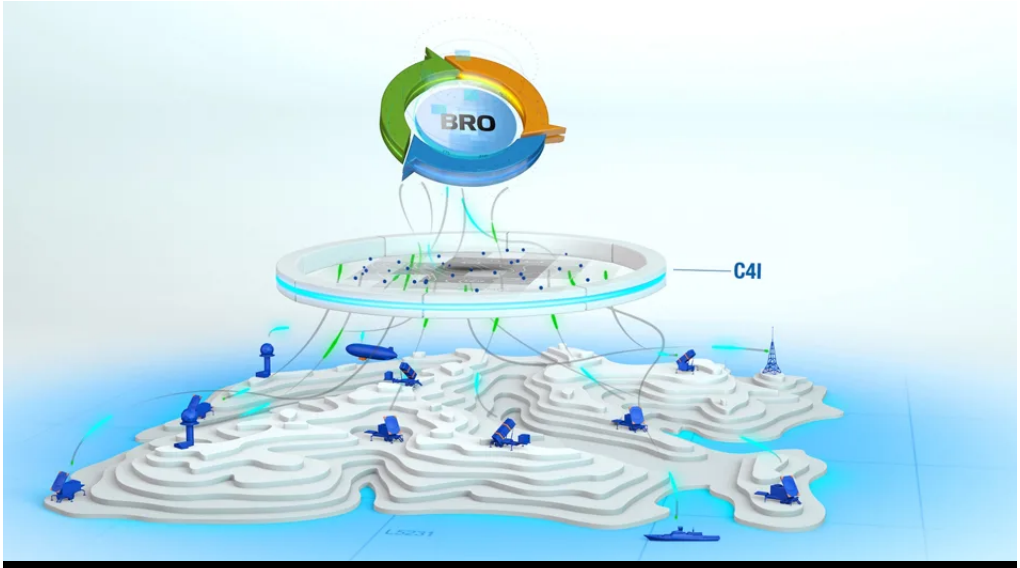
priorities.

The new BRO C-UAS platform is designed precisely for this: **modeling and optimizing** the use of existing resources, helping decision-makers understand *where* and *how* to position sensors, electronic jamming, and interception systems to maximize overall effectiveness.

Advanced models to track the most plausible routes

One of the typical problems of anti-drone defense is that the sky is not “empty”: **terrain, buildings, infrastructures, and obstacles** alter lines of sight and coverage, creating natural corridors for an attacker. The platform described by Omnisys uses **modeling and optimization** tools to estimate **plausible attack routes**, identify points where the threat is more likely to “pass” and, consequently, propose a deployment that increases the probability of detection and interception.

It is not a system that “commands” during engagement, but a planning support: the goal is to **raise the quality of decisions upstream**, when there is still room to correct vulnerabilities and fill gaps.



Proactive Anti-Drone Defense with the BRO C-UAS Platform

The “digital twin” of the operational field: seeing the gaps before the enemy exploits them

The conceptual core of the platform is a **digital twin** of the operational area: a digital representation of the environment that allows simulating coverage and “shadows” generated by

terrain and infrastructures. In practical terms, this approach aims to highlight **where the defense does not see** or sees poorly, and why.

For commanders, the value is immediate: if it emerges that a critical area (a base, a logistics depot, a communication node, an energy infrastructure) is only partially protected due to the terrain morphology or urbanization, priorities and positions can be **redefined** before the adversary turns that gap into an attack corridor.

AI-driven optimization: alternatives, trade-offs, courses of action

Omnisys emphasizes an **AI-driven optimization** engine that works as an “analysis multiplier”: it evaluates **different deployment options**, compares alternative operational concepts, and generates **recommended courses of action** to improve coverage and success probability against hostile drones.

In a context where variables are many (types of threat, logistical constraints, range limits, interactions between sensors and effectors, protection priorities), AI here is not presented as an “autopilot”, but as a system capable of:

- **quickly evaluating alternative scenarios**;
- highlighting **trade-offs** (for example: protecting one site 100% may reduce coverage on a second target);
- estimating how results change with varying operational constraints.

Another important aspect highlighted: the platform is designed to **not replace** real-time command and control systems, but to work “alongside”, with the ambition of improving preparation, positioning, and decision readiness.

Proactive Anti-Drone Defense with the BRO C-UAS Platform

No “vendor lock-in”: simulate different mixes of sensors and effectors

A critical point often in the adoption of C-UAS solutions is dependence on a single supplier and a closed ecosystem. Omnisys claims to want to avoid **vendor lock-in**, allowing operators to simulate **heterogeneous combinations** of sensors and effectors and test them against known or more generic threats.

In practice, the idea is to offer a platform that helps answer very concrete questions, without imposing a single “technological chain”: with the arsenal I already have, what is the most efficient configuration? Where should I place what? What gaps remain, and which sites should I protect first?

Why “proactivity” matters (especially against fast and numerous threats)

The direction is clear: in drone attacks, especially if conducted with saturation tactics or flight profiles that exploit the environment, **reaction time may not be enough**. Increasing proactivity means trying to win even before engagement, reducing uncertainty and raising interception probabilities thanks to:

- better initial coverage;

- positioning consistent with the most probable routes;
- employment plans optimized for real constraints.

In summary

With the next-generation mission planning platform integrated into the **BRO C-UAS** suite, Omnisys proposes a cultural as well as technological shift: an anti-drone defense **based on simulation, digital twin, and AI optimization**, designed to transform the set of sensors, jammers, and interceptors into a more “intelligent” and adaptable system.

It does not promise to replace real-time command, but to **better prepare** the battle: identify vulnerabilities, test alternatives, and arrive at engagement with an advantage—which, against small, fast, and hard-to-detect drones, can make the difference.

News link: https://www.jpost.com/defense-and-tech/article-883193