

# Planning a holistic counter-drone program

First steps you can take to strategize drone deterrence, detection, and response

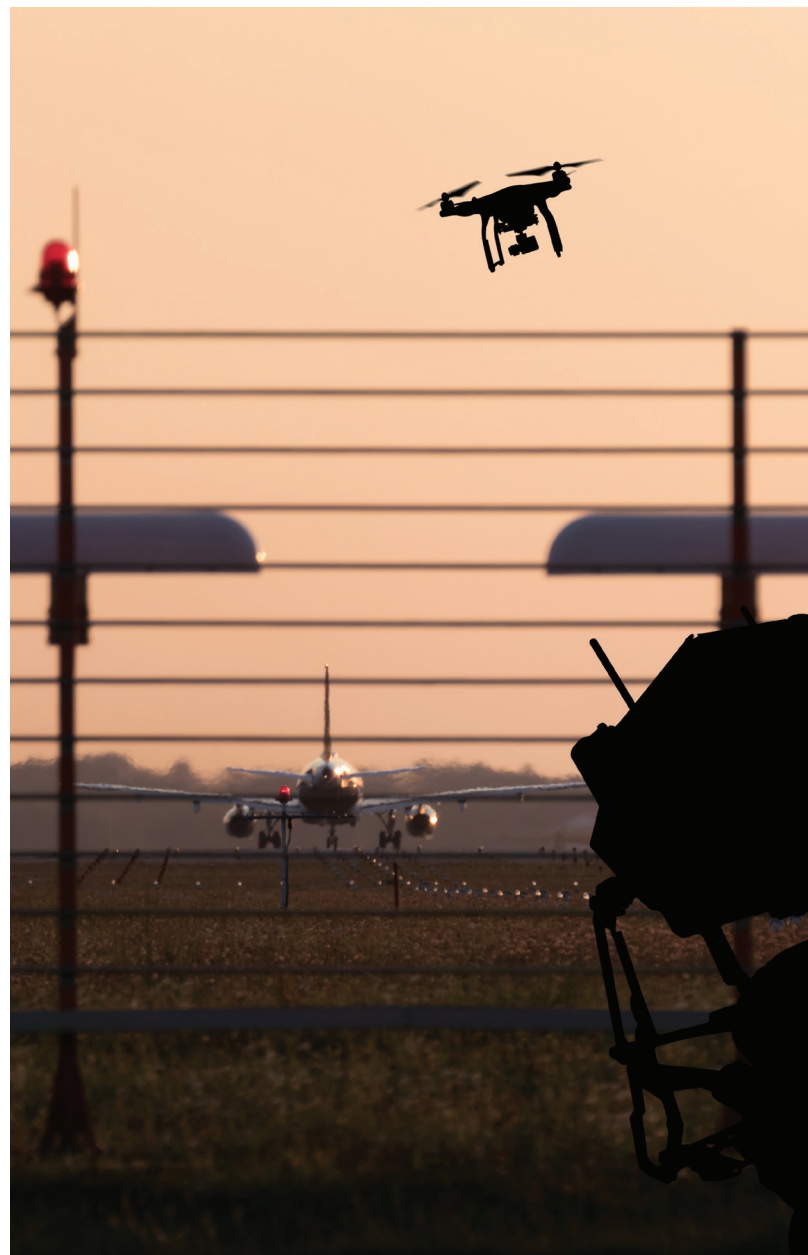
## When drones attack

As discussed in our [recent white paper](#), the proliferation of unmanned aerial vehicles (UAVs)—better known as drones—presents unique challenges for physical security. From nuisance incidents to deliberate malicious actions, the potential for drones to threaten public privacy, safety, and security is prompting many U.S. companies to consider revising their physical security programs accordingly.

But where to start? In recent articles, we described how following a structured assessment process like the ZBeta Drone Vulnerability Risk Assessment (DVRA) can yield a clear sense of priorities based on your exposure to drone-related threats, and provided guidance for developing a multi-sensor counter-drone solution.

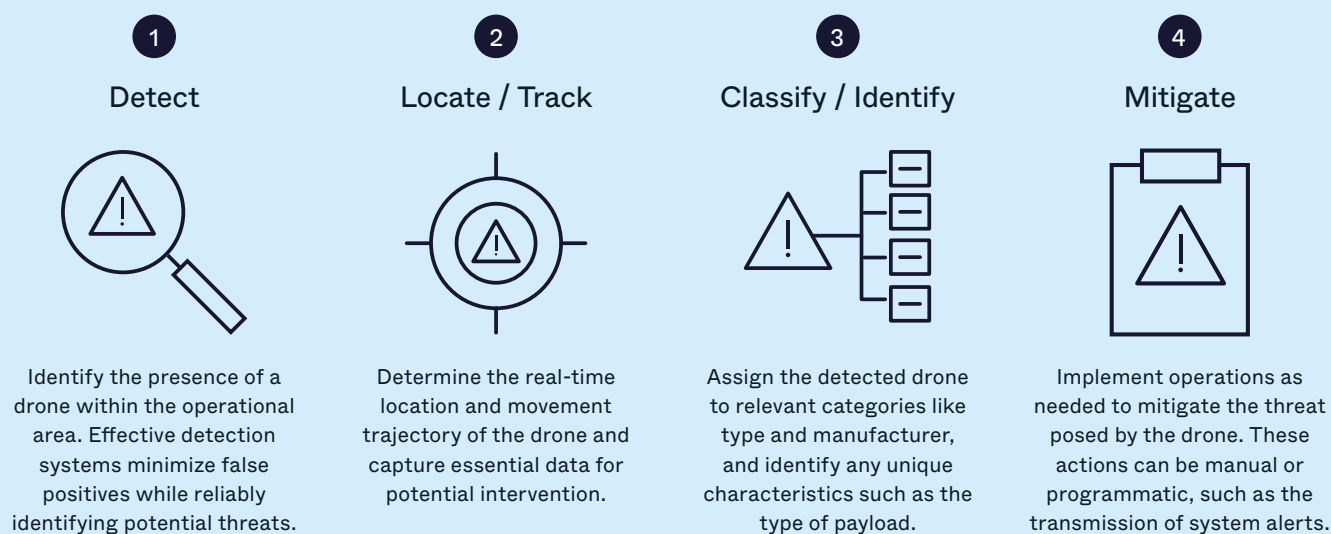
Apart from gauging and specifying the software and hardware components of your solution, however, there are various program-level aspects to consider. This article provides some next steps you can take to begin assembling a counter-drone program, including:

- + Studying the program essentials
- + Structural and architectural strategies for deterring drones
- + Planning operational changes, including awareness, reporting, staffing, and training



## Understanding counter-drone program essentials

Broadly speaking, we at ZBeta counsel our clients to think of drone response as four sequential activities. Our industry currently refers to this sequence as the counter-unmanned aircraft system (C-UAS) processing chain. This approach helps drive counter-drone program development by outlining the key capabilities and requirements for your systems and processes, as summarized in the following graphic.



The C-UAS processing chain: Detect drones, track their locations, identify them, and mitigate any risks they pose.

The US commercial drone market, valued at **\$4.79 billion** in 2023, is projected to exceed **\$8.8 billion** by 2030

Source: [Grand View Research](#)

Of these four activities, mitigation is the trickiest to address technologically—in part because such solutions are in a nascent state, constantly evolving to match the evolution of drones themselves, and also because U.S. laws disallow all mitigation techniques, at least in non-military scenarios. In lieu of applied technology, we advise organizations to think of this final activity (for now) as creating robust operational procedures that clarify how personnel should respond when a drone threat is assessed. That said, risk mitigation can also take the form of proactive measures you deploy to ward off the threat of drones in the first place. Let's look at some of these options next.

## Deterring drones through architectural modifications

Imagine a critical facility—perhaps a datacenter that is one-of-a-kind—being under constant surveillance from the skies. What options do you have for modifying your facility's exterior design that will keep drone-based attacks and surveillance at bay? Specifically, what features can you add to the existing architecture that can prevent drones from coming too close? Here are some building design strategies you can build into your counter-drone program that help shore up your risk against drone incursions before they happen:

- + **Nets.** Retractable netting systems, strategically deployed during periods of heightened risk or alerts from your counter-drone technology, can shield key sensitive areas from unauthorized drone access. The flexibility of on-demand protection makes this a compelling drone defense option in some scenarios.
- + **Canopies.** Mesh canopies, either rigid or semi-rigid, offer a more permanent solution than netting. Crafted from durable materials like metal or reinforced polymers, canopies are designed to prevent drones from descending into protected zones.
- + **Barriers (permanent).** In addition to overhead solutions, vertical barriers such as tall fences with overhangs add another layer of defense. These barriers force drones to navigate more complex flight paths, making them easier to detect and intercept.
- + **Barriers (modular).** For facilities with changing security needs, modular barriers offer a flexible solution. These portable barriers can be quickly assembled, relocated, or removed, providing adaptable protection as required.
- + **Fences.** Layered fencing systems build on the barrier concept. Barbed wire, electric fencing, and anti-climb designs combine to create a formidable perimeter that significantly delays and complicates a drone's attempts to breach it and land inside the secure area.
- + **Facades.** Counter-drone facades present another innovative approach, targeting the drones' need for stable surfaces to land or hover. By retrofitting buildings with textured or angled facades, facilities can disrupt the smooth surfaces upon which drones rely.
- + **Domes.** For extreme areas, such as combat areas and sensitive national borders, protective dome structures provide comprehensive coverage. Typically made from polycarbonate (either transparent or opaque), domes serve as the ultimate impenetrable barrier against drones.



Whatever physical deterrent methods you choose, it's important to integrate them with your drone detection systems. If a drone makes it past your structural deterrents, you're more likely than ever to need the capabilities that a smart deterrent system provides—using sensors and camera for detection and real-time monitoring, and triggering alarms and alerts at appropriate times as needed. And while this combination of physical and electronic defense demands significant investment in both components and carries the risk of false alarms if not properly calibrated, when thoughtfully designed and executed it will offer heightened situational awareness at critical times.

## Preparing for operational readiness

Our next article in this series will focus on the functional and technical requirements you'll gather when planning your counter-drone solution. However, the best solution only works if you also plan your physical security operations to accommodate and support it.

As you proceed with designing your counter-drone program, be sure to consider the following operational areas:

- + **Technical training.** When selecting the technology that will run your counter-drone system, find out from your solution vendor who among your personnel they'll need to train, starting with the employees who will monitor the system.

The training level of these employees typically falls within the range of a mid-level security professional or a technically proficient individual, with skills that include basic technical knowledge, attention to details, decision making abilities, and adaptability to future additional training. When investigating potential drone threats, they'll also need access to the data systems such as those provided by a third-party vendor. The user will rely on this data for up-to-date reference information about drone threats, along with historical data about drones previously detected in your environment.

- + **Process documentation.** Develop a operations "run book" that guides system users and other stakeholders on exactly what to do at each step during a drone incursion response. An appendix to this document can include a detailed communications plan with links to your system database or other websites for purposes of investigation, along with contact links for notification and escalation. Steps include...

1. **Detection:** How will users receive notification of a potential incursion?
2. **Threat classification:** How will users investigate to learn more about the threat?
3. **Notification:** Who must be notified, and what events will trigger each notification?
4. **Escalation:** Under what circumstances must the issue be escalated, and to whom?
5. **Recovery:** What response must be taken in the case of each potential outcome?

- + **Routine reporting.** Build drone monitoring reports into your regular cadence of security briefings. Drone-related information in these reports can include the number of detections—including false positives or incursions determined not to be a threat—and what happened as a result of each detection, both on the physical security side and in terms of your business.
- + **Operations plan maintenance.** Over time, regularly revisit your operations plan to make sure it's up to date. Has any contact information changed? Does the system have new capabilities that require revising the run books or retraining any employees? Are there opportunities to improve the process documentation to better align with new kinds of threats?



Once you've discussed and planned for these operational basics, you're prepared to move forward with requirements gathering for your counter-drone solution. Meanwhile, read our white paper [Physical security in the drone dimension: Assessing and addressing new threats from the air](#) to learn more about how the recent surge of drone activity affects physical security strategies at companies like yours.

### Our Office:

700 Larkspur Landing Circle, Suite 150  
Larkspur, CA 94939

### E-mail and Web:

info@zbeta.com  
www.zbeta.com

### Phone:

(855) 559 2382