

Listening through the buzz of drones

Using a DVRA framework to assess airspace vulnerabilities for physical security

Drone incursions: What's your exposure?

In a [recent white paper](#), we at ZBeta discuss the proliferation of unmanned aerial vehicles (UAVs), better known as drones, and their potential as a new threat vector in many physical security instances ranging from smuggling and aviation interference to espionage and acts of terrorism. In our conclusions, we emphasize that drone security awareness entails looking and thinking beyond our industry's traditional, terrestrial measures for prevention, investigation, and response.



But do you even have a drone problem? Is your facility exposed to risk now, or will it be in the future? How do you know the extent of the actual threat drones pose to you or your clients' business?

At ZBeta, we use a framework called the Drone Vulnerability Risk Assessment (DVRA) to evaluate the vulnerabilities and risks associated with drones—both malicious and unintentional—on a per-facility basis for our clients. A well-executed DVRA will determine the reasonable and proportional risk to a business through threat analysis, critical asset identification, areas of vulnerability, and risk mitigation.

Our goal with this framework is to identify risks related to drone incursions and inform, as needed, the appropriate requirements of a counter-unmanned aircraft system (C-UAS) or “counter-drone” solution. DVRA outcomes also inform other important strategic areas, including infrastructure hardening, possible mitigation solutions, and drone awareness and response training for security and non-security staff.

What's covered in the DVRA

Our DVRA is much more than a questionnaire—it's a powerful medium for starting important conversations about how you might be exposed to drone threats. We've divided it into detailed sections of evaluation, each containing a long list of questions designed to unearth the scope of vulnerability to drone incidents at a site. As laws change, technologies evolve, and new drone-related threat vectors are discovered, we continue to adapt our DVRA to match the latest circumstances.

To summarize the sections of our DVRA, let's look at the key topical areas they fit into.

Facility context

As with any security vulnerability assessment, our DVRA starts with an in-depth analysis of your facility design, spanning many assessment factors including:

- + Location and layout, including sensitive areas
- + Environmental and geographical factors
- + Operational functions of current equipment and personnel

Our DVRA methodology examines these initial findings from the perspective of emerging drone threats, prioritizing potential vulnerabilities to help inform the development of measured response protocols.

Threat types

Next, we use our DVRA to predict the specific types of drone threats that might be actualized. This includes assessment of:

- + Drone sources and intents
- + Potential attack vectors
- + Cybersecurity vulnerabilities

The wide range of drone types is always changing, so knowing which ones are most likely to appear near your facility helps determine the best level of response. Meanwhile, a full assessment of risk must include payload analysis, data exfiltration risks, and the potential compromise of data and communications over your network resulting from a drone incursion.

Legal considerations

Lastly, it's vital to shore up any legal exposure as you set about making a counter-drone plan. To help in this effort, our DVRA asks questions that assess:

- + Regulatory compliance
- + Countermeasure limitations
- + Liability exposure

The last thing you want to do is build out a counter-drone system and then find out you're in violation of U.S. or other jurisdictional law. Privacy regulations, airspace regulations, and potential liability from countermeasure overreach are among the considerations that must all factor into any drone detection and response program you develop.



Next steps after evaluation

Once you complete the DVRA and have examined your vulnerabilities based on the DVRA assessment areas—those mentioned here and many others—you're ready to decide your path forward using the information you've collected. If that will include developing a counter-drone program for your facility and using of specialized technologies to support it, your consultant can help with the next important steps:

- + **Gathering requirements.** Choose the best strategy for your plan by identifying key functional and technical requirements for a drone detection and response solution. These start with outlining options for detection range and coverage for the new system, as well as requirements for tracking and response capabilities, and technical concerns like scalability and integration with other systems.
- + **Solution and program planning.** Determine the hardware and software solution you'll choose for your solution so you can qualify and select the right vendors who will provide the solution for your needs. At the same time, plan for the operational and business changes that your new program will entail, including system awareness, personnel training, and response planning based on drone detection and system alerts.
- + **Simulation testing.** It's easy to get ahold of several drones of various types and use them to simulate basic scenarios. An experienced consultant will work with you to validate threat scenarios and identified vulnerabilities, simulate your current drone detection effectiveness, and use post-simulation analysis to help refine your program's performance.



If you're undecided whether your facility is vulnerable to drones, conducting a DVRA with the help of an experienced partner is a straightforward and low-risk way to get a clear picture of your needs. A completed DVRA provides a comprehensive evaluation of the risks posed by drones to the facility or property, addressing legal, operational, and security concerns.

This assessment ensures that any drone detection and response solution you develop now or later on will be tailored to the specific needs and vulnerabilities of your site, giving you assurance it will enhance your overall security posture against drone-related threats. A completed DVRA also benefits future holistic planning for physical security as the importance of airspace security becomes an increasingly important part of your comprehensive security plan.



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