

# Countering the Drone Threat:

Risk Identification, Governance, and  
Mitigation of Intrusive Drones




April 2023

## Table of contents

- I. The growing need for C-UAS
- II. Determining operator intent
- III. C-UAS systems vs. C-UAS solutions
- IV. Deloitte's approach to C-UAS risk
- V. Conclusion

# The growing need for C-UAS

Hostile drones are seemingly everywhere these days<sup>i</sup>, executing crippling attacks on critical infrastructure in, disrupting airports, conducting assassination attempts on world leaders, and are rewriting decades of battlefield doctrine<sup>ii</sup>. Domestically, there are 1.7 million registered<sup>iii</sup> and myriad unregistered drones operating daily. Drones have disrupted professional sporting events, attacked electrical substations, collided with aircraft, even scouted out jewelry stores to analyze police response times. For an entity whose assets come under threat from unauthorized aerial intrusion, these dangerous conditions cannot be ignored.

		
<p>Drones have disrupted airport operations at multiple commercial airports, including London's Gatwick Airport and Dublin Airport, resulting in numerous diverted or cancelled flights, thousands of inconvenienced passengers, and millions of dollars in losses<sup>iv</sup></p>	<p>Premier League soccer matches, as well as other major sporting events, have been frequently interrupted by drone incursions, leading to broadcast disruptions and fan dissatisfaction, as well as sparking concerns over player and spectator safety<sup>v</sup></p>	<p>Drones have demonstrated the ability to conduct nefarious cyberattacks, acting as airborne WiFi sniffers, ingesting data from lightly-secured facilities and unsuspecting data users, logging keystrokes and password data, all while going undetected<sup>vi</sup></p>

**Deloitte offers Counter-Drone Solutions**

***Threat and Intel Analysis, Training and Education, Hardware Test and Evaluation, System Deployment and Installation, Equipment Maintenance and Sustainment, Regulatory Consulting, Forensics Analysis, Consequence Management***

***Strengthened by our access to a global network of subject matter specialists, Deloitte brings to bear the talent of its broad and talented workforce to help our clients address their complex challenges***

For organizations who wish to protect their personnel, facility, or critical assets from errant or criminal drone operators, a Counter-Uncrewed Aerial System (C-UAS) is becoming a necessity. However, far from simply a plug-and-play device, effective C-UAS operations require a new form of vigilance; one that combines regulatory compliance, intelligence, threat, and data analytics with specialized training, operations, maintenance, and of course equipment. Failure to perform analysis on these elements sharply increases risk to people and infrastructure, risks that can be mitigated through doctrinal Risk and Program Management. More than just C-UAS systems, owners of critical assets increasingly require **complete** C-UAS solutions.

## Determining operator intent

A pressing decision point for UAS security is determining the intent of an unknown drone operator. While many drone violations within the US are categorized as simple rule violations, incursions are not consistently the result of ignorance or accident but may be due to criminal or terrorist intent. Determining if a drone incident is a result of a rule violator—whether intentional or accidental—or a nefarious actor is one of the leading challenges within the C-UAS security industry. Nuances between the various scenarios are key to determining effective response.

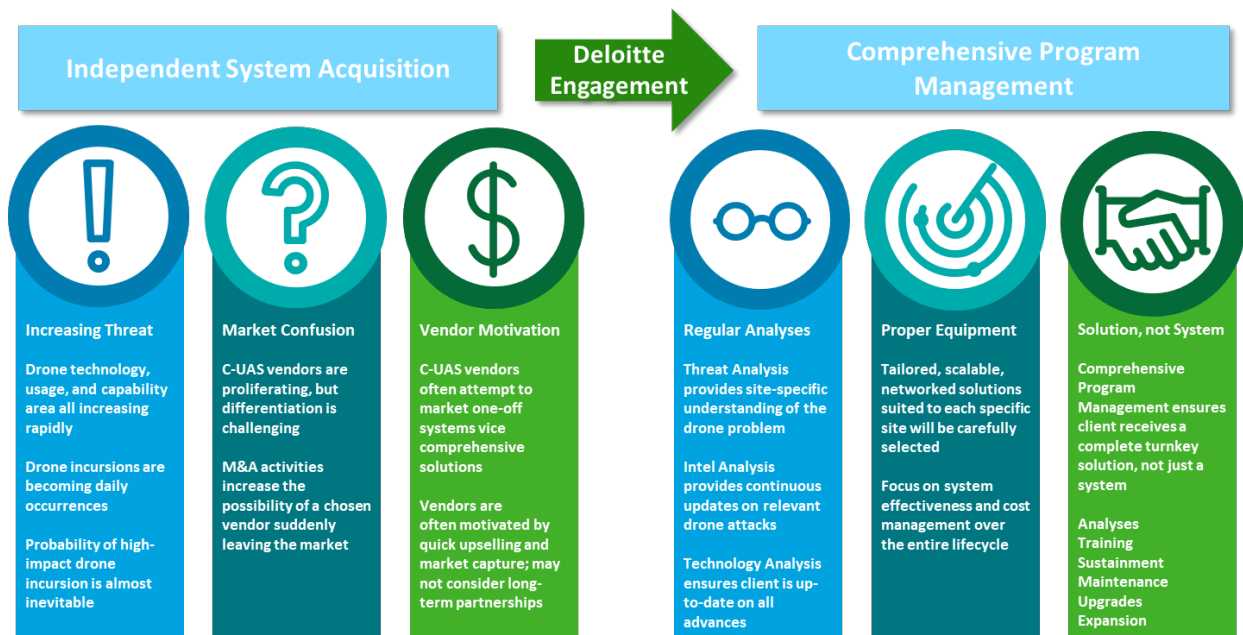
<b>Rule Violator</b>	Often, a hobbyist or small commercial operator such as real estate photographer who likely frequent a single site for recreational flying or photography. Rule violators have unintentionally interfered with first responders, including during natural disasters and medical evacuations, resulting in loss of property and life. <sup>vii</sup>
<b>Criminal</b>	Electronic/visual surveillance operators may likely launch far from the site of interest as the range of their UAS will allow, often using a small vehicle to avoid detection. Criminal operators have frequented prison yards due to their ability to covertly deliver contraband and have enabled trafficking across the Southern Border. <sup>viii</sup>
<b>Terrorist</b>	Operators likely pop up from random, concealed sites. The larger the drone, the farther away they are likely to launch. Attacks are better predicted by monitoring criminal/terrorist networks. Terrorist operators have employed drones for everything from infrastructure attacks to assassination attempts of world leaders. <sup>ix</sup>

**Figure 1:** *The Spectrum of Unlawful UAS Activities*

## C-UAS systems vs. C-UAS solutions

The increase in potential UAS threats seems only to be matched by the exponential expansion of vendors promising to meet these challenging conditions.<sup>x</sup> As many offerings are functionally similar—small phased-array radars paired with two or more additional sensors feeding data through a proprietary Command & Control interface—differentiators between the products are often difficult to perceive.<sup>xi</sup> C-UAS customers may end up with systems poorly matched to their specific conditions, that are unaccompanied by training and analysis, maintenance and sustainment, and ultimately fail to meet their goals and expectations.

Having in-depth experience providing Program Management Support enables Deloitte to assist clients in need of Group I & II (see Appendix I) C-UAS solutions – delivering regular threat, intel, and technology analyses, conducting broad market research to determine the proper equipment for exacting customers; enabling a client to effectively perform C-UAS risk management, not just purchase a system. Working with Deloitte helps a client manage risk; removing the pitfalls that come with navigating a saturated market on one’s own.



**Figure 2:** *Benefits of a Deloitte Program Management Engagement*

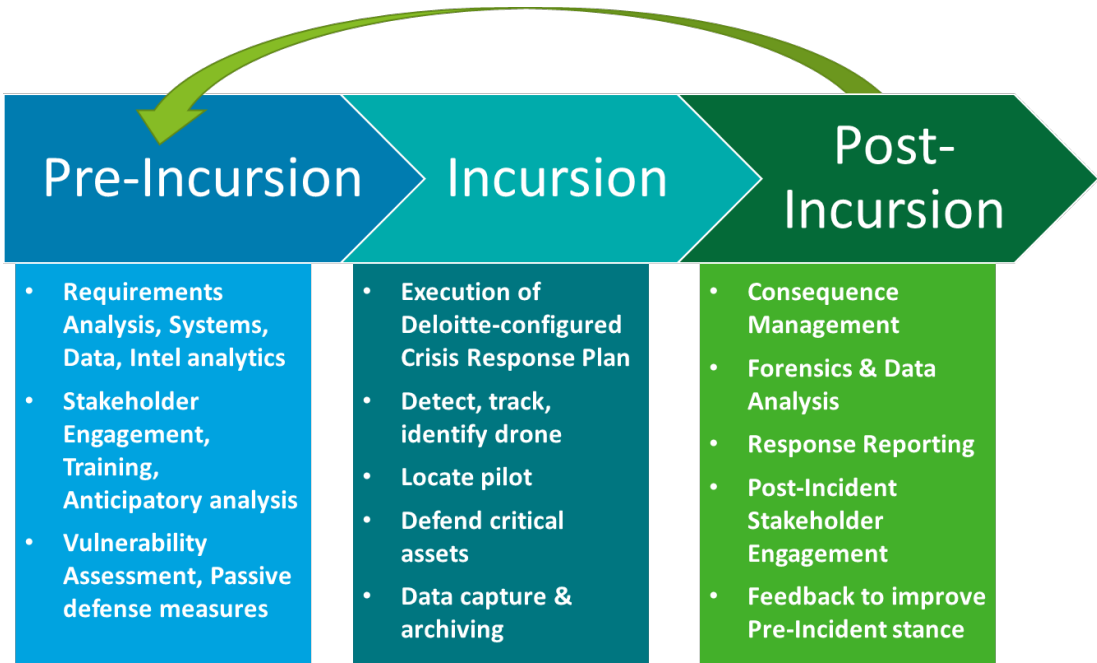
# Deloitte’s Approach C-UAS Risk

Deloitte’s approach to helping agencies manage C-UAS risk takes a broad view of the UAS incursion chain, from well before the vehicle ever becomes airborne to post-incident assessment and feedback. The Deloitte team leverages many aspects of knowledge management across this spectrum, integrating lessons learned post-incident into pre-incident planning.

**Pre-Incursion:** Well before a client suffers the effects of a drone incursion, Deloitte performs an analysis of a client’s C-UAS circumstances through implementing or updating the client’s requirements management process, using a dedicated capability and portfolio risk assessment process. A threat assessment quantifies the nature of the UAS issue facing the client, and a technology and funding assessment determines the proper system—or even if a system is required—that fits the client’s requirements and limitations; all enabled by Deloitte’s proprietary horizon scanning tools.

Deloitte brings subject matter specialists steeped in regulatory knowledge across the federal space and beyond. RegExplorer™—Deloitte’s artificial intelligence platform that was purpose-built to help clients along their regulatory transformation journey—searches, analyzes, and compares regulatory text and regulation updates so clients are abreast of the ever-changing policy environment. Table-top exercises, crisis response plans, and an associated training syllabus all help clients set conditions for an effective response to a drone incursion incident.

**Incursion:** Should a drone incursion occur, the client will be positioned to execute a Deloitte-configured crisis response plan, utilizing the tailored and integrated C-UAS framework to detect, track, and identify the drone as well as locate the drone operator. In addition to protecting critical assets through a series of defensive measures, Deloitte’s risk management framework (see Appendix 2) implementation determines that incident data is captured and archived. As a result of stakeholder engagement and associated pre-incident coordination, the organization’s response ecosystem is trained and ready to effectively respond and appropriately communicate across the multitude of key personnel, leaders, and response-related internal and external organizations.



**Figure 3:** Deloitte’s Methodology for UAS Incursion Chain Assessment

**Post-Incursion:** Following a confirmed or suspected drone incursion, Deloitte conducts consequence management operations that includes forensics and data analysis. Post-incident stakeholder analysis can enable incorporation of lessons learned that need to be readdressed in future pre-incident planning to enhance response planning. Deloitte's experience and knowledge in equipment test and evaluation provides a full understanding of a system's capabilities and/or shortfalls, streamlining constructive feedback to the system manufacturer. Finally, Deloitte helps clients address the broad threat, risk, and vulnerability assessment process, implementing lessons learned into pre-incident planning and fostering a process wherein gaps are understood, mitigated, and closed.

## Conclusion

Impacts from drone incursions can result in monetary and reputational losses, data, and security compromises; even destruction of property and loss of life. Managing C-UAS risk takes much more than simply buying equipment. Guarding against potential UAS threats requires an analysis of terrain, doctrine, training, equipment, and applicable policies to identify existing shortfalls to develop an effective response to this rapidly evolving threat. Deloitte's experience in Program Management assists clients in analyzing potential threats, exploring available systems, crafting impactful training, and conducted broad data analysis to collectively develop an effective solution. Deloitte performs risk management by combining materiel and non-materiel solutions using a risk-informed, tiered approach to agencies provide protection and defense of personnel, assets, and facilities.

Deloitte provides clients with operational resilience, capability, and portfolio risk assessment – assessing root cause, scope, and severity of capability gaps within a requirements portfolio; conducting risk assessment and model capability gaps, priorities, and operational scenarios; and understanding capability gaps by refining strategy, requirements, or funding decisions. Bringing the full force of Program Management experience, Deloitte provides clients with turnkey operations of not just C-UAS systems, but **broad** C-UAS solutions.

## For more information, please contact

### Jared Salazar

Managing Director  
Deloitte US Global Counter-Drone Solutions  
Deloitte Consulting LLP  
[jaredsalazar@deloitte.com](mailto:jaredsalazar@deloitte.com)

### Jacob Jones

C-UAS Deputy Program Lead  
Deloitte US Global Counter-Drone Solutions  
Deloitte & Touché LLP  
[Jacojones@deloitte.com](mailto:Jacojones@deloitte.com)

### Terry Body

Managing Director  
Deloitte Operational Transformation Risk  
Deloitte & Touché LLP  
[Tbody@deloitte.com](mailto:Tbody@deloitte.com)

### Contributors:

#### Joshua Jacobson

Deloitte Financial Advisory Services LLP  
Government and Public Services  
Deloitte & Touché LLP

### John Walton

C-UAS Program Leader  
Deloitte US Global Counter-Drone Solutions  
Deloitte & Touché LLP  
[johwalton@deloitte.com](mailto:johwalton@deloitte.com)

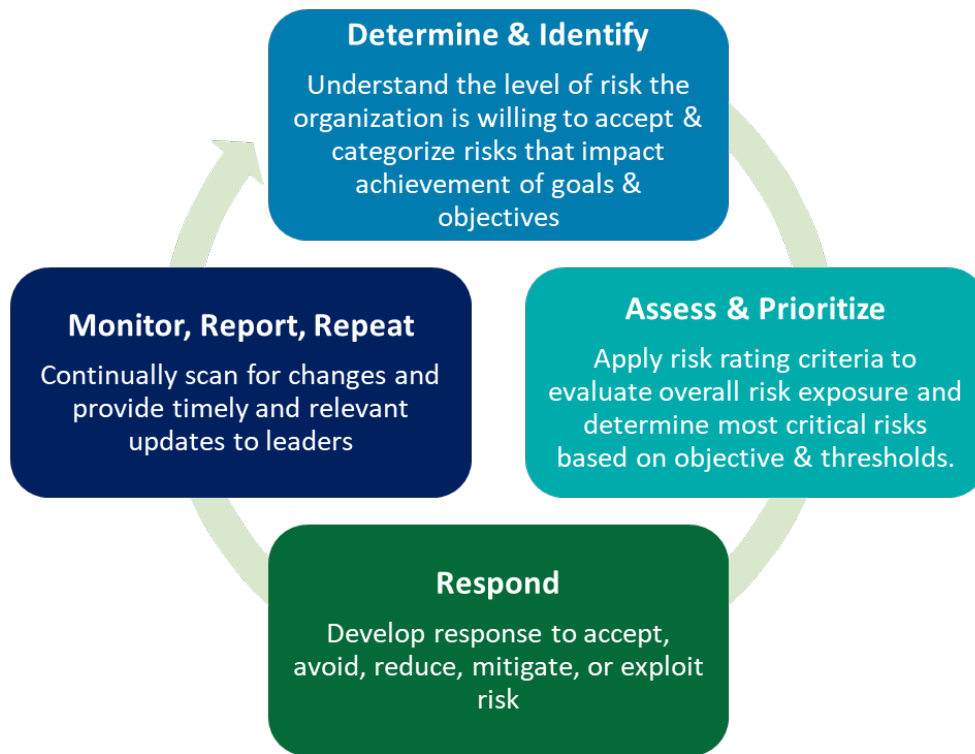
# Appendices

Appendix 1: DoD C-UAS Group Classifications<sup>xii</sup>

UA Category	Maximum Gross Takeoff Weight (lbs.)	Normal Operating Altitude (feet)	Speed (KIAS)
Group 1	0-20	< 1200 AGL	100 knots
Group 2	21-55	< 3500 AGL	< 250 knots
Group 3	< 1320	< 18,000 MSL	< 250 knots
Group 4	> 1320		Any Airspeed
Group 5	> 1320	> 18,000 MSL	Any Airspeed

**Legend: AGL – above ground level; MSL – mean sea level; KIAS – knots indicated airspeed**

Appendix 2: Deloitte’s Risk Management Framework



This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, 'Deloitte' means Deloitte & Touche LLP, which provides audit, assurance, and risk and financial advisory services. These entities are separate subsidiaries of Deloitte LLP. Please see [www.deloitte.com/us/about](http://www.deloitte.com/us/about) for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved.

---

<sup>i</sup> FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan | The White House. Retrieved 8 April 2023 from <https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/>

<sup>ii</sup> The Role of Drones in Future Terrorist Attacks. Retrieved 7 April 2023 from <https://www.ausa.org/publications/role-drones-future-terrorist-attacks>

<sup>iii</sup> Unmanned Aircraft Systems (UAS) | Federal Aviation Administration ([faa.gov/uas](http://faa.gov/uas))

<sup>iv</sup> Ireland vows to tackle drones after Dublin Airport shut six times. Retrieved 13 April 2023 from <https://www.reuters.com/world/uk/ireland-vows-tackle-drones-after-dublin-airport-shut-six-times-2023-03-03/>

<sup>v</sup> AlBaroudi, Wajih. Jan 2022. "Drone interrupts Premier League game between Wolverhampton and Brentford, causes 15-minute delay." Retrieved 9 Feb 2023 from <https://www.cbssports.com/soccer/news/drone-interrupts-premier-league-game-between-wolverhampton-and-brentford-causes-15-minute-delay/>

<sup>vi</sup> Bishop, Rollin. Aug 2015, "A \$2,500 Drone Sniffs Out Hacking Targets From the Sky." Retrieved 9 Feb 2023 from <https://www.popularmechanics.com/flight/drones/a16873/drone-hack-sky/>

<sup>vii</sup> Childs, Jan Wesner. Nov 2019. "Unauthorized Drones Interrupt Efforts to Fight California Wildfire." Retrieved 27 Jan 2023 from <https://weather.com/news/news/2019-11-02-drones-grounded-firefighting-aircraft-maria-fire>

<sup>viii</sup> Wright, Tim. June 2020. "How Many Drones Are Smuggling Drugs Across the U.S. Southern Border?" Retrieved 27 Jan 2023 from <https://www.smithsonianmag.com/air-space-magazine/narcodrones-180974934/>

<sup>ix</sup> Crino, Scott & Conrad Dreby. May 2020. "Drone attacks against critical infrastructure: A real and present threat." Retrieved 27 Jan 2023 from <https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/drone-attacks-against-critical-infrastructure-a-real-and-present-threat/>

<sup>x</sup> "Top 10 Leading Manufacturers of Counter UAS in the World." April 2022. Retrieved 27 Jan 2023 from <https://www.emergenresearch.com/blog/top-10-leading-manufacturers-of-counter-uas-in-the-world>

<sup>xi</sup> Helfrich, Emma. May 2020. C-UAS philosophy and needs dictate system advancements. Retrieved 27 Jan 2023 from <https://militaryembedded.com/unmanned/counter-uas/c-uas-philosophy-and-needs-dictate-system-advancements>

<sup>xii</sup> Reference: U.S. Department of Defense Counter-Small Unmanned Aircraft Systems Strategy, pg 33. Retrieved 30 March 2023 from <https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/0/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.pdf?source=GovDelivery>