




# THE BIG PROBLEM WITH SMALL DRONES

And How to Address It



Governments around the globe face a growing need for flexible, tailorable, and affordable Counter-sUAS solutions

## KEY TAKE AWAYS

- Exponential growth in small Unmanned Aerial Systems (sUAS) is creating new risks for governments.
- State and non-state actors are increasingly employing military- and consumer-grade sUAS to attack personnel, facilities and critical infrastructure.
- Governments must employ a multi-layered approach to counter sUAS and keep pace with emerging threats.
- Counter-sUAS solutions must be cost effective, leveraging existing technologies through common electronic architectures and standard interfaces to ensure rapid integration of hardware and software upgrades.
- Solutions must be modular, interoperable and multi-domain; easily transportable; and capable of detecting swarms and operating in contested environments.

## AN EMERGING THREAT

On 17 January, a swarm of small Unmanned Aerial Systems (sUAS) and ballistic missiles attacked critical infrastructure in the United Arab Emirates killing three civilians and causing extensive damage to property.

This complex attack- responsibility for which was claimed by the Houthi Movement in Yemen- saw multiple sUAS successfully destroy three oil refueling vehicles at an Abu Dhabi National Oil Company facility and damage an area of Abu Dhabi's International Airport.

As one of the most high-profile sUAS incidents since the 2019 attack on the world's largest oil processing facility at Abqaiq, Saudi Arabia, this particular incursion highlighted an emerging and rapidly evolving threat facing armed forces who must protect personnel and assets from malign sUAS, both at home and abroad.

As described in the U.S. Department of Defense (DoD) Counter-sUAS (C-sUAS) Strategy, published January 7, 2021, an "exponential" growth in sUAS around the world has created "new risks" for armed forces, no matter where they may be operating.

As the strategy warned: "Technology trends are dramatically transforming legitimate applications of sUAS while simultaneously making them increasingly capable weapons in the hands of state actors, non-state actors and criminals."

Highlighting improving levels in performance, reliability and survivability of sUAS, the strategy described how low-cost systems could perform military-type missions and conduct novel offensive and defensive operations not traditionally associated with the platform type.

"Both state and non-state actors are increasingly employing purpose-built

"Technology trends are dramatically transforming legitimate applications of sUAS while making them increasingly capable weapons in the hands of state actors, non-state actors and criminals ... [used] to attack a range of targets, including leadership, military facilities and forces, and critical infrastructure."

- U.S. Dept. of Defense Counter-sUAS Strategy, Jan. 2021



# AN EMERGING THREAT

military and consumer-grade sUAS to attack a range of targets including leadership, military facilities and forces, and critical infrastructure.

“When these systems are weaponized, sUAS can present a precision strike capability; direct attacks using small munitions; provide laser designation for indirect fires or remote engagement by manned platforms; or deploy chemical, biological, and radiological agents,” the strategy warned.

Violent extremist organizations including ISIS, for example, weaponized cheap, easy-to-modify and simple-to-fly commercial off-the-shelf sUAS that could be purchased online.

ISIS have produced several propaganda films showing sUAS dropping small explosives on targets in various middle-eastern theatres of operation where the U.S. DoD and its allies grow increasingly worried about the future capability of sUAS to distribute chemical weapons.

On April 22, 2021, General Kenneth F McKenzie, Commander, U.S. CENTCOM reiterated the problem, describing to the Senate Armed Services Committee how C-UAS had become one of his “top priorities.”

“Until we are able to develop and field a networked capability to detect and defeat UAS, the advantage will remain with the attacker,” he warned.

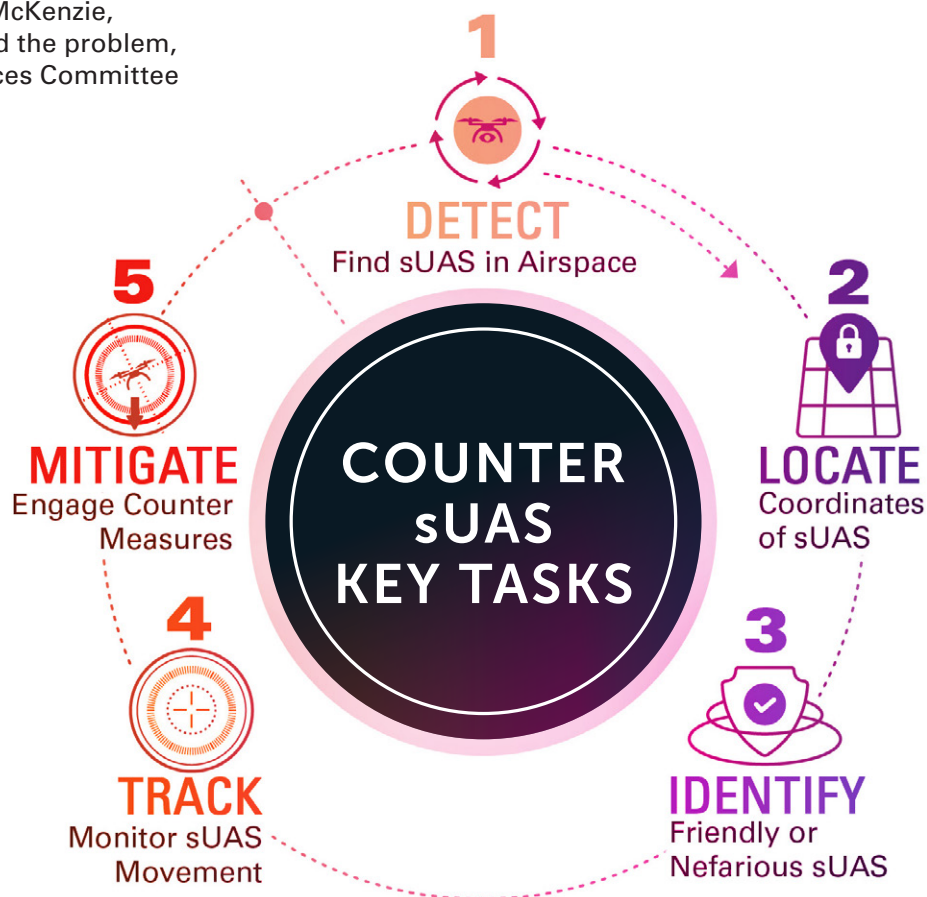
In response, governments around the world continue to invest millions of dollars into commercially-built C-sUAS solutions to address the more immediate risks posed by sUAS threats.

To date, efforts have been focused on protecting deployed units and critical infrastructure with C-sUAS solutions designed to “Find, Fix, Track, Target, Engage & Assess” UAS Groups 1, 2 and 3.

In service C-sUAS solutions are available in a variety of form factors ranging from handheld and man-wearable/portable systems up to more capable vehicle-mounted or fixed site platforms. Solutions can provide a variety of capabilities for end users, featuring any type of mix of radar payloads; radio frequency and acoustic sensors; electro-optical, infra-red cameras and neural network target classifiers (NNTC); as well as soft and hard kill countermeasures.

However, they can be expensive and standalone in nature, unable to be integrated into wider, multi-domain surveillance networks.

As the DoD’s strategy warned, today’s C-sUAS solutions must be equipped to address a series of critical challenges facing armed forces in the future as they seek to keep pace with the constantly evolving threat of sUAS.



# CHALLENGES IN THE PROCUREMENT AND DEPLOYMENT OF MATURE, EFFECTIVE C-SUAS SOLUTIONS

---

In order to successfully field a robust, mission-relevant and cost effective C-sUAS capability, governments must employ a multi-layered approach to address emerging threats both today and in the future.

Concepts must be supported by increased levels in research, development, test and evaluation as well as rapid innovation with significant focus on common electronic architecture and standard interfaces to ensure plug-and-play capability and information sharing.

As governments seek to invest in the most mature, effective and future-proofed C-sUAS technologies available, they face a series of significant challenges.

These include:

## 1. DISPROPORTIONATE COSTS

Today, governments spend millions of dollars on expensive C-sUAS solutions to protect personnel and assets from a threat that can cost just a few hundred dollars. Instead, they must demand more cost-effective means to defend against sUAS without exhaustive procurement fees and ongoing maintenance, repair, overhaul and operating costs.

## 2. KEEPING PACE WITH NOVEL AND RAPIDLY EVOLVING THREATS

What could provide an effective defense against sUAS today may well quickly become redundant as the threat environment continues to evolve at pace. Governments therefore require flexible and modular C-sUAS solutions, supported by sovereign C2 systems which allow for the rapid integration of hardware and software upgrades without reliance on systems integrators.

## 3. RANGE AND ACCURACY CONSTRAINTS

As demonstrated during the Abu Dhabi attack, swarms of sUAS can be launched from stand-off ranges hundreds of miles away from their designated targets. Armed forces require maximum fields of view for sensors tasked with the “detection, identification and tracking” of threats to provide operators with maximum amounts of time to assess and respond to any emerging situations.

## 4. AIR DOMAIN AWARENESS & REGULATION RESTRICTIONS

In an increasingly cluttered airspace, the ability of C-sUAS solutions to successfully detect and classify threats has never been more important. C-sUAS sensors must be able to deconflict threats from wildlife, government, commercial and hobbyist aviation. C-sUAS solutions must also be integrated into wider ground, air, maritime and space surveillance networks to ensure accurate and real-time monitoring of threats.

## 5. MOBILITY

Whether tasked to protect a forward operating base or extensive border, C-sUAS should be as mobile as possible, allowing them to be redeployed whenever and wherever necessary. Additional requirements call for a mobile capability which would allow C-sUAS to detect and engage threats while operating “on-the-move” on the ground, in the air and at sea.

## 6. COUNTERING SWARMS AND ‘DARK MODE’ DRONES

Finally, C-sUAS solutions must counter multiple threats operating in a swarm as illustrated during the recent attack in Abu Dhabi. C-sUAS must also be capable of detecting, identifying and tracking sUAS not controlled by RF signals or Global Navigation Satellite Systems (GNSS).

# CRITICAL CAPABILITIES FOR FUTURE C-SUAS

---

According to the U.S. Army's Joint C-sUAS Office (executive agent for C-sUAS operations across the wider DoD), solutions must be agile enough to respond to emerging threats in both the contemporary and future operating environments.

This can be enabled through rapid innovation and synchronization of materiel and non-materiel solutions, interoperability, integration and information sharing, which allow governments to leverage current and develop future capabilities; improve processes to support rapid procurement and deployment of solutions; and maintain and update doctrine, regulations, and authorities as threats evolve.

To successfully deploy the most effective protection against sUAS, governments must consider:

## LEVERAGING EXISTING AND PROVEN PRODUCT RANGES

Today, the threat of sUAS is as prevalent as ever. As a result, urgent operational needs must leverage existing, proven technologies and products to provide an immediate solution. Solutions must benefit from system maturation and risk reduction efforts to provide users with the most efficient means of responding to an emerging threat at the earliest opportunity. User confidence must also be increased through the reduction of false alarm signals, system complexity and training requirements.

## MULTI-FACETED, MODULAR AND INTEROPERABLE SOLUTIONS

The modern C-sUAS solution should also comprise a layered, system of systems approach, benefiting from modular open systems architecture allowing end users to tailor capability in response to specific threats and environments as and when they arise. This can be enabled through conformity of data and common standards which allow the "plug and play" of additional capabilities. Also critical is centralized guidance for future command and control and joint interoperability standards. Such an approach provides increased flexibility for C-sUAS to deploy in

more complex operating areas such as dense urban environments where tall buildings can obstruct RF signals and fields of view of radar and EO/IR payloads, for example. Detection and identification of sUAS in such an environment could be enabled by upward-looking cameras running NNTCs.

## RAPID DEPLOYMENT AND SIZE, WEIGHT AND POWER CONSTRAINTS

Modern C-sUAS should be designed with minimal size, weight and power requirements in mind to enable rapid deployment anywhere in the world, at any time. Solutions must also be rugged, reliable, easy to maintain, quick to set-up and collapse and easy for new end users to operate with minimal cognitive and training burdens.

## OPERATIONS IN CONTESTED ENVIRONMENTS

In line with emerging demand signals from the DoD and its NATO partners, modern C-sUAS need to be capable of conducting operations in contested environments where the ability to Find, Fix, Track, Target, Engage and Assess threats can be disrupted by peer adversaries' Electronic Warfare capabilities.

## INTEGRATION INTO MULTI-DOMAIN SURVEILLANCE NETWORKS

C-sUAS solutions must be easily integrated into wider air, ground, maritime and space surveillance systems, even belonging to other government agencies. This extends ranges in terms of detection, providing end users with the greatest amount of time to respond to a threat accordingly. Supporting software must also correctly identify friend, foe, neutral and unknown objects, feeding intelligence into a Common Operating Picture which is visible to all multi-domain users across a theater of operations. Furthermore, modern C-sUAS solutions must be capable of interoperating with multi-lateral networks during multi-national operations and aggregate capacity across a wider area of responsibility.

## STREAMLINING DECISION-MAKING PROCESSES

More rapid and effective decision-making processes can be enabled by machine learning and artificial intelligence algorithms which also promise to learn the behavior of sUAS in real-time.

Operator intervention should be minimized although many armed forces will still require a human-in-the-loop. This can include Automatic Target Recognition (ATR) software which features a centralized threat library relevant to a particular theater of operation. Such capability will also assist in the identification of swarming sUAS threats and allowing C-sUAS to more quickly assess and react to a situation.

## SOFT AND HARD KILL COUNTERMEASURES

Today, a variety of hard kill (kinetic) and soft kill (non-kinetic) countermeasures are available to armed forces seeking to neutralize UAS threats. Retaining flexibility to operate the full spectrum of effectors and countermeasures is critical to modern and future C-sUAS solutions, allowing them to operate anywhere in the world in accordance with local restrictions and rules of engagement. Examples include the protection of critical infrastructure at home where appetite to launch kinetic countermeasures (missiles, munitions and air burst ammunition) will be limited due to the potential of collateral damage to property and civilians. Instead, soft kill countermeasures can be employed to safely neutralize a threat. Options include RF jammers; high power microwave emitters; and even high energy lasers although collateral damage to government communications and surveillance assets (even in Space) must be carefully avoided. C-sUAS must also be capable of triangulating the position of UAS ground control stations as part of an effort to counter enemy sUAS networks.

## COST EFFECTIVENESS

Finally, the modern C-sUAS must provide a more cost effective solution for armed forces who can typically spend more than several million dollars on a single sensor, standalone solution. Fully integrated, multi-sensor turnkey solutions maintained by a single systems integrator could provide a less expensive option for defense departments and also enable rapid upgrade in capabilities in line with emerging operational requirements.



## THREATS FROM ABOVE

### LASER DESIGNATION



### SMALL MUNITIONS



### CHEMICAL BIOLOGICAL RADIOLOGICAL







## CONCLUSION

Around the world, the threat of small drones in the wrong hands promises to remain significant for government and military decision-makers as they seek to defend forward-deployed units, airports, power grids, and other critical infrastructure. Only the deployment of mature, flexible, and cost effective C-sUAS solutions will provide the required levels in protection as this threat continues to evolve at pace.



## AMERICAS

7055 Troy Hill Dr. Suite 300  
Elkridge, MD 21075 USA

Questions? Contact Mark Blanco, Sr. Director, Unmanned Systems and Integrated Solutions, at:  
[Mark.Blanco@TeledyneFLIR.com](mailto:Mark.Blanco@TeledyneFLIR.com)

[www.TeledyneFLIR.com](http://www.TeledyneFLIR.com)

Equipment described may be subject to United States export regulations and may require US authorization prior to export, reexport, or transfer to non-US persons or parties. Diversion contrary to US law is prohibited. For assistance with confirming the Jurisdiction & Classification of Teledyne FLIR, LLC products, please contact [exportquestions@flir.com](mailto:exportquestions@flir.com).  
©2022 Teledyne FLIR LLC. All rights reserved.

UIS C-UIS\_White Paper 22-0130 - Updated 03/08/22

