C-UAS STATE OF PLAY REPORT 2022

NEXT GENERATION C-sUAS CONCEPTS – THE QUEST FOR CONTINUITY

IDGA
Institute for Defense and Government Advancement

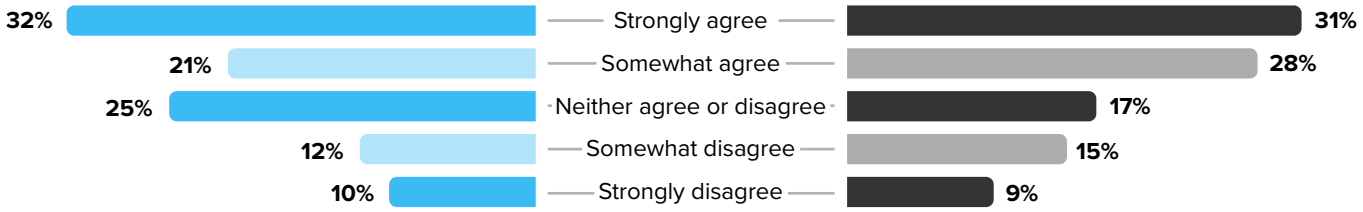
D-FEND SOLUTIONS

www.idga.org/events-counteruas-usa

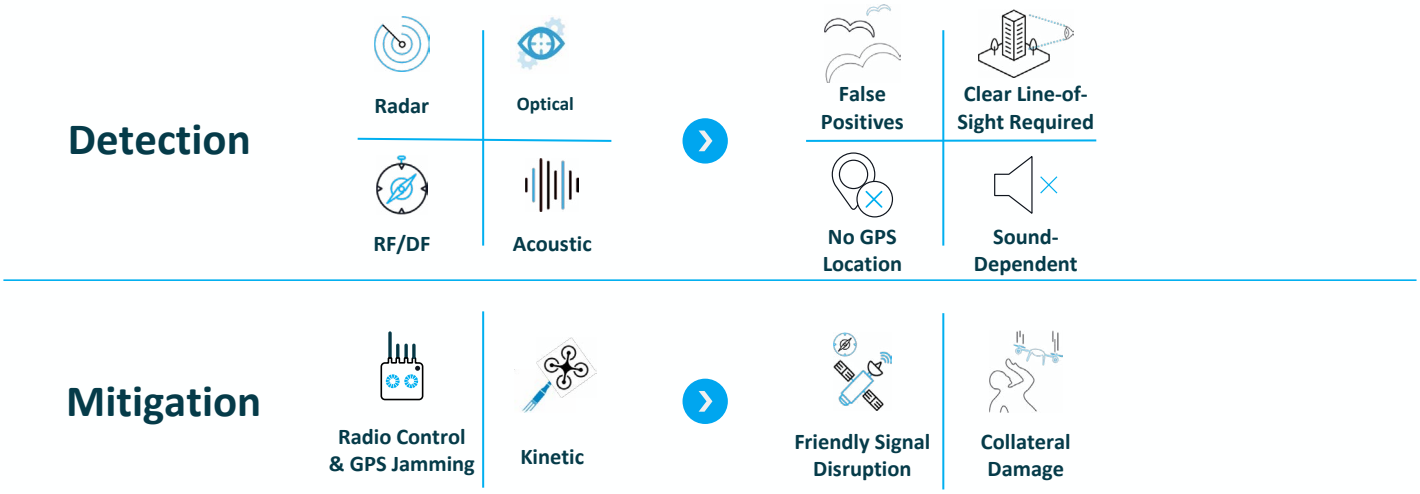
IDGA/DEFENCE IQ COUNTER-DRONE DISCOVERY SURVEY
HIGHLIGHTS FROM RESULTS AND FINDINGS

The potential of jamming-based C-UAS systems to disrupt internal or nearby communications systems is problematic enough to avoid adoption of such a system

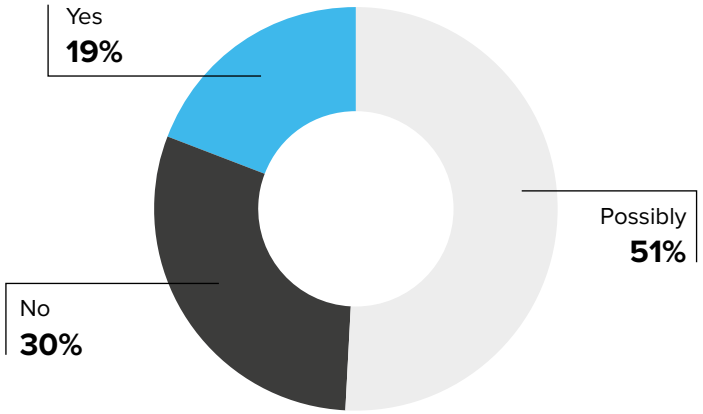
The potential of collateral damage caused by physical/kinetic C-sUAS solutions – from the projectile used to shoot down or capture the drone, the falling drone itself, or debris – is problematic enough to avoid adoption of such a system



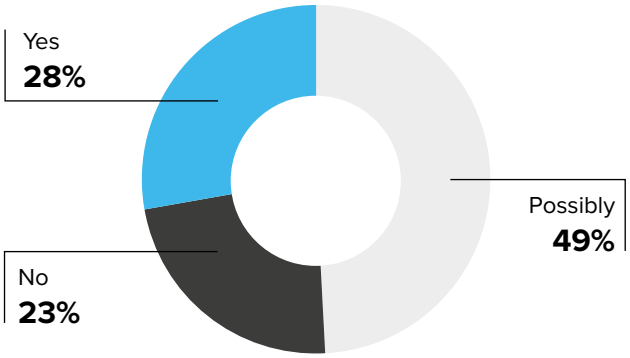
TRADITIONAL TECHNOLOGIES STRUGGLE IN SENSITIVE SCENARIOS



Do you believe that the risk of damage caused by such counter-drone system mitigation actions or methods could be worse than the damage from the rogue drone itself?



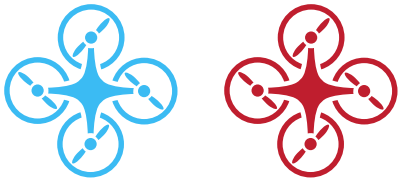
Are you concerned that a count-drone system could harm or disable internal or nearby authorized "friendly" drones during a rogue drone incident?



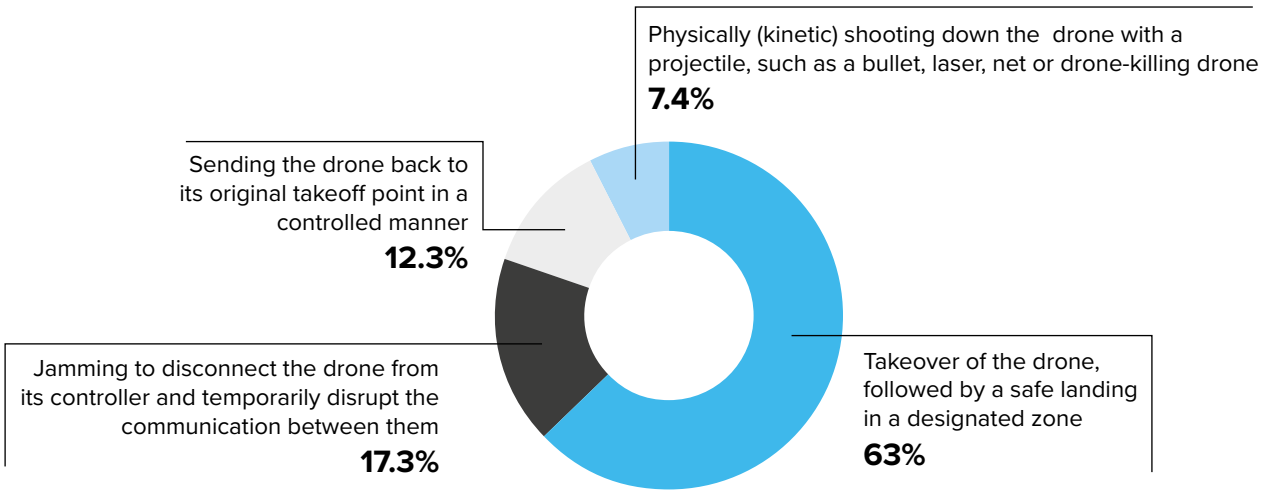
DRONE IDENTIFICATION FRIENDLY OR HOSTILE?

Authorized drones play critical roles across society

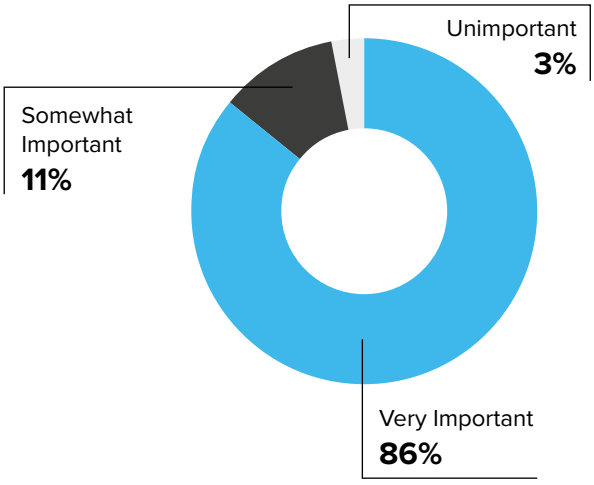
Must distinguish between Friendly and Authorized versus Rogue and Hostile, and enable continuity for authorized drones



What is the best possible outcome of a threatening rogue drone incident?



While mitigating a rogue drone incident, how important is it to preserve continuity at your site, including full function of communications, transportation, commerce and everyday life?



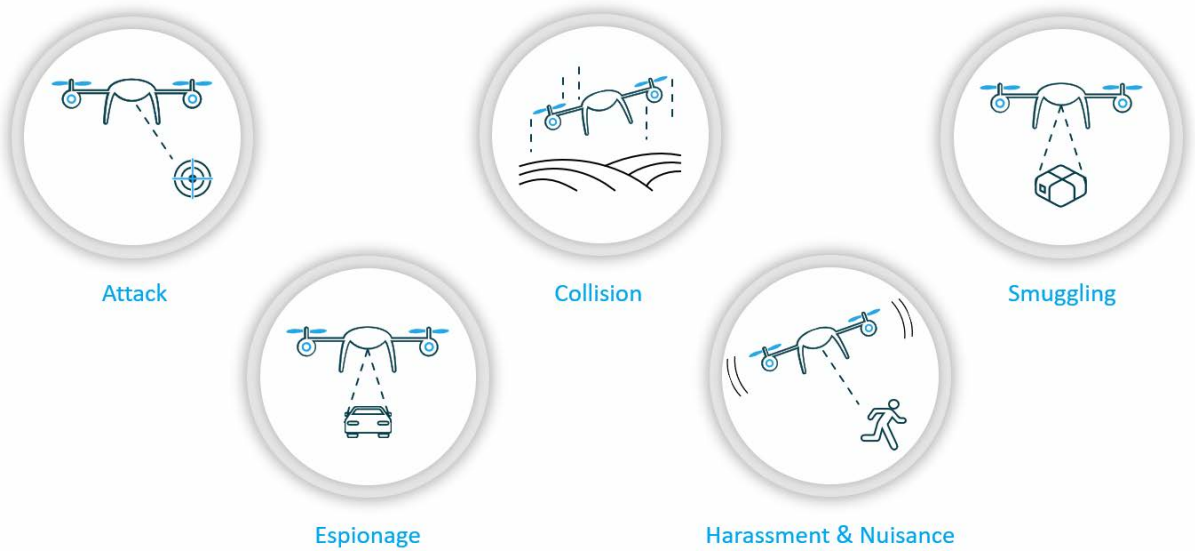
SELECTED 2022 DRONE INCIDENTS

Incident Date	Title	Location	Sector	Type
February 26, 2022	Drone Delays Gatwick Flights Again	Gatwick, England, UK	Airports	Collision or Near Collision
February 27, 2022	Drone at Porto Airport Causes Diversion & Delays	Porto, Portugal	Airports	Collision or Near Collision
March 15, 2022	Near Collision over London	London, England, UK	Airports	Collision or Near Collision
March 21, 2022	The number of drones violating Charlotte's airspace is on the rise	Charlotte, North Carolina, USA	Airports	Collision or Near Collision
March 27, 2022	Drone Halts Operations at Dublin Airport	Dublin, Ireland	Airports	Collision or Near Collision
March 28, 2022	Near Collision at Leeds Bradford Airport	Leeds, UK	Airports	Collision or Near Collision
May 4, 2022	Drone Caused Flight Delay at Glasgow Airport	Inchinnan, Scotland, UK	Airports	Collision or Near Collision
May 14, 2022	Delay and Rerouting at Berlin-Brandenburg Airport Due to Drone	Schönefeld, Germany	Airports	Collision or Near Collision
May 20, 2022	Near-miss Between Plane & Drone in Nuremberg	Nuremberg, Germany	Airports	Collision or Near Collision
May 31, 2022	Drone Causes Two Flights to Reroute to Avoid Collision	St. Simons, Georgia, USA	Airports	Collision or Near Collision
June 10, 2022	Flights at EMA Airport Diverted Due to Drone Sightings	Derby, UK	Airports	Collision or Near Collision
April 14, 2022	DIY Lithuanian Drone Shot down at Belarusian Border	Belarus	Borders	Smuggling
April 29, 2022	Drone Used by Gun Smugglers to cross Canada-U.S. Border	Port Lambton, Ontario, Canada	Borders	Smuggling
May 14, 2022	Jordan Downed a Drug Smuggling Drone From Syria	Jordan	Borders	Smuggling
May 28, 2022	Narcotics Payload Seized in J&K	Jammu and Kashmir, India	Borders	Smuggling
May 29, 2022	Pakistani Drone with Explosive Payload Shot Down in India	Jammu and Kashmir, India	Borders	Attack
February 25, 2022	Invasion of Privacy at Burnaby High Rise	Burnaby, Canada	Community and Neighborhood	Privacy
February 25, 2022	Concern Over Drones Flying Near Windows in Leicestershire	Mountsorrel, England, UK	Community and Neighborhood	Privacy
June 27, 2022	Suspicious Drone Drops Candy Near Children Fishing	St. Cloud, Minnesota, United States	Community and Neighborhood	Harrassment and Nuisance
April 19, 2022	Drone Injured Boy in Park	UK	Community and Neighborhood	Collision or Near Collision
July 3, 2022	Drone and Helicopter Collide in North Carolina	Boonville, North Carolina, USA	Community and Neighborhood	Collision or Near Collision
January 14, 2022	Drone Over Forsmark & Oskarshamm Nuclear Plants	Forsmark, Sweden	Critical Facilities and Infrastructure	Espionage
January 17, 2022	Houthis Launch Drone Attack on UAE	Abu Dhabi, UAE	Critical Facilities and Infrastructure	Attack
March 25, 2022	Jeddah Drone Attack Days Before Formula 1 Race	Jeddah, Saudi Arabia	Critical Facilities and Infrastructure	Attack
January 30, 2022	Drone Crashed Into i360 Observation Tower	East Sussex, England, UK	Landmarks and Govt Buildings	Collision or Near Collision
March 1, 2022	Drone Spotted at Taj Mahal	Agra, India	Landmarks and Govt Buildings	Harrassment and Nuisance
January 29, 2022	Drones Over Truckers Rally in Canada	Ottawa, Canada	Landmarks and Govt Buildings	Harrassment and Nuisance
April 17, 2022	Tourist's Drone Crashed into the Leaning Tower of Pisa	Pisa, Italy	Landmarks and Govt Buildings	Collision or Near Collision
April 23, 2022	Tourist's Drone Hit the Palazzo Venezia	Rome, Italy	Landmarks and Govt Buildings	Collision or Near Collision
May 23, 2022	Drone Crashed Doge's Palace	Venice, Italy	Landmarks and Govt Buildings	Collision or Near Collision
March 16, 2022	Criminals Using Drones to Target Homes in Ireland	Laoise County, Ireland	Law Enforcement Agencies and First Responders	Privacy
April 8, 2022	DIY Drone and Narcotics Seized in Montenegro	Shkodra Lake, Montenegro	Law Enforcement Agencies and First Responders	Smuggling
April 4, 2022	Invasion of Privacy in Prince George	Prince George, Canada	Law Enforcement Agencies and First Responders	Privacy
April 21, 2022	UAV Starts Wildfire During Crash in Colorado	Longmont, Colorado, USA	Law Enforcement Agencies and First Responders	Collision or Near Collision
May 19, 2022	Drones Halt Firefighting Response at Two Fires in England	Preston, England, UK	Law Enforcement Agencies and First Responders	Harrassment and Nuisance
May 23, 2022	Arrests Over Illegal Drone Use at Cannes Film Festival	Cannes, France	Law Enforcement Agencies and First Responders	Harrassment and Nuisance
June 3, 2022	Drone Drop of Fireworks Leads to an Arrest	American Canyon, California, USA	Law Enforcement Agencies and First Responders	Attack
June 25, 2022	Illegal Drone Flight Over Glastonbury Festival	Glastonbury, UK	Law Enforcement Agencies and First Responders	Harrassment and Nuisance

SELECTED 2022 DRONE INCIDENTS (CONTINUED)

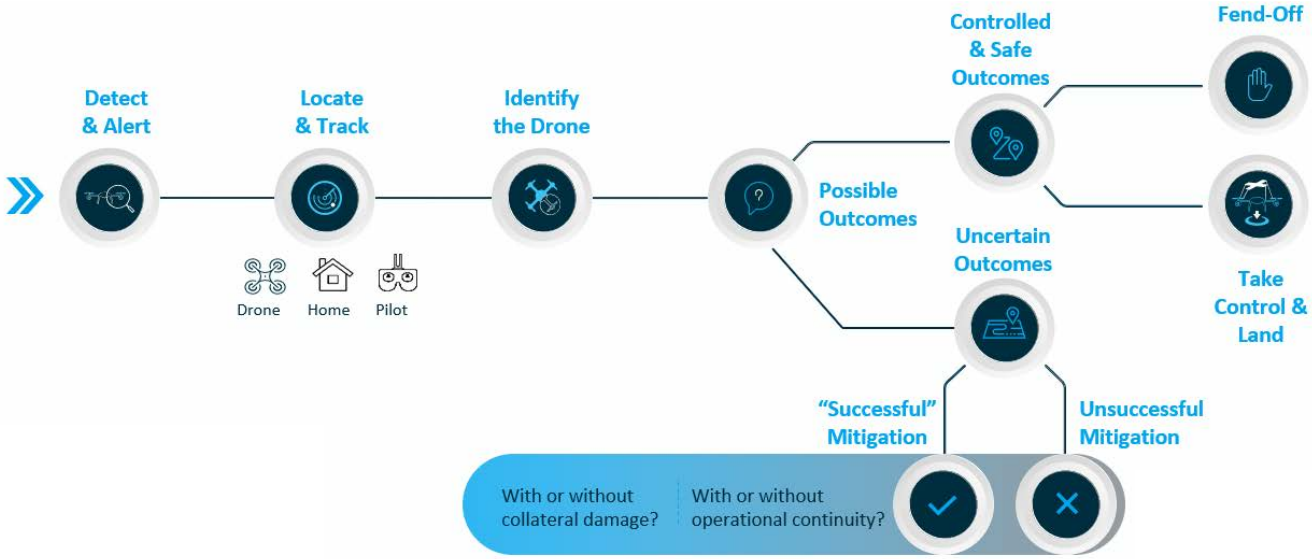
Incident Date	Title	Location	Sector	Type
January 6, 2022	Third Failed Drone Attack Against US Troops in Iraq	Baghdad, Iraq	Military and Special Forces	Attack
January 30, 2022	Cartel Drones Dropped Bombs on Mexican Soldiers	Tepalcatepec, Mexico	Military and Special Forces	Attack
March 10, 2022	DJI Inspire Drone Modified to Drop Molotov Bottles on Russian Forces	Kyiv, Ukraine	Military and Special Forces	Attack
April 13, 2022	PDF Used Modified DJI Phantom 3 to Attack Military Positions	Shwebo, Myanmar	Military and Special Forces	Attack
May 17, 2022	Hezbollah Drone in Israel Airspace Downed by IDF	Israel	Military and Special Forces	Attack
June 13, 2022	Modified Mavic 3 Drones used to Bomb Ukrainian Front Line	Marinka, Ukraine	Military and Special Forces	Attack
July 4, 2022	Ukraine Uses Weaponized Autel Drone	Ukraine	Military and Special Forces	Attack
June 21, 2022	Ukrainian Kamikaze Drone Crashed into Russian Oil Refinery	Rostov, Russia	Military and Special Forces	Attack
February 20, 2022	Houthi Drone Targeted School in Yemen	Marib, Yemen	National Security and Homeland Security	Attack
June 8, 2022	Weaponzied Drone Attack in Iraq	Irbil, Iraq	National Security and Homeland Security	Attack
January 30, 2022	Drones Disturb Wildlife at St Mary's Island	St. Mary's Island, England, UK	Nature Preservation	Harrassment and Nuisance
March 10, 2022	Drone Used to Drop Contraband into Georgia Prison Seized	Georgia, U.S.	Prisons	Smuggling
April 7, 2022	Drone Contraband Delivery at South Carolina Prison	Columbia, South Carolina, USA	Prisons	Smuggling
April 15, 2022	DJI Mavic Pro with Contraband Found Crashed at Norgerhaven Prison	Veenhuizen, Netherlands	Prisons	Smuggling
May 8, 2022	Contraband Drone Dropped into Gameleira Prison	Belo Horizonte, Brazil	Prisons	Smuggling
May 10, 2022	Attempted Drone Drug Delivery at HMP Liverpool	Liverpool, England, UK	Prisons	Smuggling
March 24, 2022	Collins Bay Drone Drug Smuggler Arrested	Kingston, Canada	Prisons	Smuggling
June 8, 2022	Attempts Made to Drone Drop Contraband into FDC Miami	Miami, Florida, USA	Prisons	Smuggling
January 15, 2022	Cincinnati Football Game Illegally Videotaped by Drone	Cincinnati, Ohio, USA	Stadiums and Arenas	Harrassment and Nuisance
January 22, 2022	Drone Suspends Play at Premier League Match	Brentford, England, UK	Stadiums and Arenas	Harrassment and Nuisance
February 1, 2022	Team Name Leaked from Drone Flying Above Stadium	Washington, D.C., USA	Stadiums and Arenas	Harrassment and Nuisance
March 31, 2022	Drone Disrupts Training at Morocco Stadium	Casablanca, Morocco	Stadiums and Arenas	Harrassment and Nuisance
May 6, 2022	Three Times in one Game, Drone Interrupts Soccer Match	Drogheda, Ireland	Stadiums and Arenas	Harrassment and Nuisance
May 25, 2022	Drone Over Ed Sheeran Concert in Cork	Cork, Ireland	Stadiums and Arenas	Harrassment and Nuisance
June 27, 2022	Drone at Hellfest Festival	Clisson, France	Stadiums and Arenas	Harrassment and Nuisance
January 30, 2022	Drones Over the Swedish Royal Palace	Drottningholm, Sweden	VIP Protection	Privacy
March 29, 2022	Drone Activity Suspected at Will Smith's Home	Los Angeles, California, USA	VIP Protection	Privacy
April 16, 2022	Drone Over President Macron's Speech	Marseille, France	VIP Protection	Harrassment and Nuisance

DIFFERENT DRONE THREATS



DRONE RISK DRIVERS

ROGUE DRONE INCIDENT LIFECYCLE



EVALUATING AND COMPARING COUNTER-DRONE (C-UAS) DETECTION TECHNOLOGIES

DETECTION TECHNOLOGY

Radar Detection

KEY CHALLENGE

False positives & signal refraction

Radars are a popular legacy detection technology that offer long-range coverage. Older legacy systems, which were used mostly in military and aviation, can detect larger aircraft but often cannot track drones, due to the small size of sUASs. More modern anti-drone radar systems use advanced technologies, such as electronically scanned array (ESA) and micro-Doppler, but they cannot always differentiate between small drones and other flying objects such as birds, generating false positives. Radars are also impacted by weather, with limited detection in rainy and foggy environments, as clear line-of-sight is necessary for optimized proper operation.

In addition, radars are sensitive to refractions and reflections, which can lead to multiple signals from different directions originating from the same object being received by the radar. This is a quite common effect in urban environments, where tall buildings can create such refractions and reflections.

DETECTION TECHNOLOGY

Electro-optical

KEY CHALLENGE

Requires line-of-sight

While electro-optical sensors are used for identification of drones, they are usually triggered by other defection and tracking systems, such as radars. When combined with radars, they are used as a validation technology to reduce the number of false detections. These sensors employ sophisticated electro-optical infrared thermal imaging (EO/IR) cameras to identify drones based on their visual and temperature-related identifiers, verifying that any object detected is indeed a drone. The biggest disadvantage of EO/IR solutions for detection is that they require a clear and direct line-of-sight, which is not always available in dense, crowded, or urban environments. Darkness, fog and rain can also hinder the effectiveness of EO/IR detection solutions. In addition, relying on EO sensors for verification may require human intervention in real time to determine whether the image is of a drone or not, demanding continuous staffing resources.

DETECTION TECHNOLOGY

RF directional finders

KEY CHALLENGE

Achieving exact precision and accuracy

RF directional finders utilize sensors to detect and track UAVs. They monitor common frequency bands that they can match to a library of drone control signal profiles to classify these types of signals and can estimate the radial direction these signals come from. Using measurements from multiple sensors helps to narrow down the possible location of the drone, which is helpful in tracking and during the transition from detection to mitigation. But directional finders are limited only to detection and to some limited tracking, without identification. They may not be able to identify specific airframes or provide the most accurate real-time location of the drone. In addition, in urban and complex terrains, directional finders may point to the wrong direction due to RF reflections from objects like buildings or mountains. Directional finders may not always provide the most precise location, as their spatial resolution is limited. Multiple directional finders are needed to determine the approximate position of the drone. As such, a complex deployment of multiple sensors with varying accuracy levels may be necessary, depending on the deployment scheme and the drone flight area.

DETECTION TECHNOLOGY

Acoustic

KEY CHALLENGE

Noisy environments and quiet drones

As the name implies, acoustic detection systems rely upon the sound signature of the drone and its engines. Acoustic sensors can match the sounds that drones produce to a library of drone noises. They are mobile and easy to deploy. The limitation of this technology is fairly evident: many of today's sensitive environments – such as airports, crime scenes, outdoor stadiums and arenas, tend to be loud, while some newer drones are becoming quieter. Acoustic solutions are ineffective in noisy environments, and cannot be reliably used for directional finding, location, or identification.

EVALUATING AND COMPARING COUNTER-DRONE (C-UAS) DETECTION TECHNOLOGIES (CONTINUED)

DETECTION TECHNOLOGY

Cyber takeover

KEY CHALLENGE

Overcoming advanced drone protocols

Advanced, anti-drone, radio frequency (RF)-based cyber solutions passively and continuously scan and detect unique communication signals used by commercial drones, without producing false positives. Once detected, the solution can understand drone information and protocols, for a classification process, and tag specific drones as authorized or unauthorized. The system can extract the telemetry information, determine the type of drone, and accurately determine the drone position. This includes the take-off position and often also the pilot position in real-time, which can help security officials deal with the drone pilots. Cyber solutions do not require a quiet environment or a direct line-of-sight.

RF cyber solutions may be impacted by signal/noise ratios, although often the range of flight that the drone will havein the same RF noise level will also be reduced. The detection distance can also be affected by the drone's operating frequency band.

integrated to offer an intuitive, end-to-end, counterdrone solution. Cyber technology used for detection, tracking and identification provides no false detections. It delivers accurate location, is not affected by weather and may operate without clear line-of-sight. In addition, there is no need for human intervention to identify threats.

RF cyber-takeover focuses on specific RF-based manufactured or Do-It-Yourself commercial drones and overcoming their specific protocols.

In summary, next-generation RF cyber-detection provides accurate detection, without line-of-sight required, and can be fully integrated, if permitted and needed, with cyber-takeover mitigation for an end-to-end solution. The technology eliminates false positive detections, provides accurate location information, and is effective in noisy environments. RF cyber-detection can determine not only the drone position but also its take-off position, and, in some cases, can also

EVALUATING AND COMPARING COUNTER-DRONE (C-UAS) MITIGATION TECHNOLOGIES

MITIGATION TECHNOLOGY

RF Jammers

KEY CHALLENGE

Communication/GNSS interference

RF jammers channel large bursts of RF energy which mask the signal from the controller and prevent the drone from receiving instructions. Some jammers concentrate their radiation in the direction of the drone.

This technology is comparatively cheap, simple to operate and may achieve some desired effect – temporarily incapacitating all drones in the immediate area. These are appealing benefits, but they are accompanied by some significant disadvantages.

RF noise may interfere with nearby communications systems and/or GNSS, rendering this mitigation technology problematic in many sensitive environments, including the potential of shutting down friendly, authorized drones.

As the jamming effect depends on the strength of the RF noise the jammer creates, its effect relies on the relative strengths of signals the drone receives from the remote controller and the jammer, and this depends both on the power of transmission and on the distance to the drone. The jammer only works if its signal prevails. This condition has several implications:

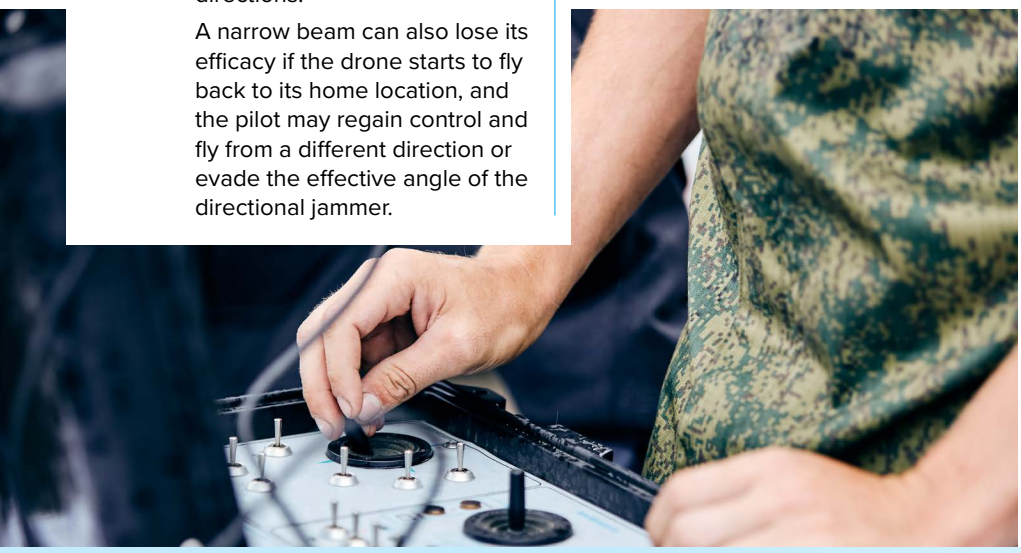
- The jammer will work only when the drone is far enough from its remote controller but close enough to the jammer
- In case the drone returns home, its pilot can regain control once the drone gets close enough to the remote controller
- In case the jammer stops transmitting, the pilot may immediately regain control; this method depends on continuous transmission

Jammers do not gain control over a drone; they only disconnect it from its remote controller. Once disconnected, it usually tries to return to its take-off ("home") position, but it may also hover in place or try to land, and some drones can be programmed to do other emergency default actions. Each of these options may pose a threat (e.g., a drone returning home may fly through sensitive airspace like the take-off corridor of an airport); when the drone flies without control, not even its pilot can prevent damage. Unless the drone is within line of sight, the jammer's operator may not even know whether the drone was disconnected. Jammers may not always permanently eliminate the specific threat, but rather only temporarily block it, since in many cases, the drone will return to its pilot.

DIRECTIONAL JAMMERS

These jammers mitigate drones flying in from a specific direction. This technology offers a longer range than other types of jamming and causes less disruption and signal interference in the immediate environment. It does require continuous transmission to remain in effect. It cannot, by itself, efficiently overcome swarms, which by their nature usually approach from multiple directions.

A narrow beam can also lose its efficacy if the drone starts to fly back to its home location, and the pilot may regain control and fly from a different direction or evade the effective angle of the directional jammer.



OMNI-DIRECTIONAL JAMMERS

Omni-directional jammers can mitigate drones from all directions and thus better handle swarms. But it offers a shorter range than directional jammers, meaning the protected area is smaller.

Omni-directional transmission also increases the collateral effect over authorized and non-threatening drones, and over other communication systems in the vicinity.

HAND-HELD JAMMERS

These jammers are mobile and simple to use. The operator just pulls out the device and aims it. Disadvantages: Because this method is manual, a security team member must always have the handheld jammer on his/her person and remain vigilant.

If the operator cannot immediately activate the handheld jammer, or is not paying attention, the chance to mitigate the rogue drone could be quickly lost. Also, handheld jammers operate at a low power level so as not to endanger the health of the operator, but also making the range of the device limited.

This type of jammer is effective in scenarios where a certain sensitive point should be protected, and the threatening drones are in proximity and within eyesight. It is practically useless in cases where a perimeter or a border must be defended as the drone can simply fly high enough to be beyond the range of the handheld jammer.

EVALUATING AND COMPARING COUNTER-DRONE (C-UAS) MITIGATION TECHNOLOGIES (CONTINUED)

MITIGATION TECHNOLOGY

Kinetic solutions

KEY CHALLENGE

Collateral damage risk

Kinetic solutions cause the drone to stop operating by some sort of physical intervention, e.g., a projectile, and they vary in size and portability, ease of operation, cost, and capabilities against specific drone types.

Less favorably, some, though not all, kinetic technologies may require line-of-sight, which is not always available in urban or sensitive environments due to tall buildings, vehicles, signage, etc.

Kinetic solutions aim to cause the drone, in most cases, to fall from the sky, which can create severe collateral damage or human injury. The projectiles themselves may also hit other objects and pose risk, especially in sensitive environments such as airports or critical infrastructure. block it, since in many cases, the drone will return to its pilot.

DRONE-KILLING DRONES

Drone-killing drones can capture unauthorized targets with nets and tow them to a controlled landing. Alternatively, this category can also include drones that attempt to ram into rogue drones and disable them. Finally, some of these defensive drones can shoot nets or other projectiles at unauthorized drones. Accurate hits can be challenging for these methods when trying to mitigate a drone that flies in a nonpredictable manner.

The drone-killing drone needs to "dog-fight" or chase the rogue drone, and it is extremely challenging to do so through an autonomous system or through drones that are controlled by a pilot from the ground. This method can also result in collateral damage from a plummeting drone and projectile.

INTELLIGENT SHOOTER

Intelligent shooters possess a system mounted on a rifle that enables accurate shots against nearby drones. A special scope performs a calculation before the shot. The probability of a hit, compared to other kinetic methods, is therefore increased. This technology is more economical and may play a role in a multi-layer counter-drone system, particularly in rural, or open-field environments. This technology is accurate up to a few hundred meters (generally, less than 250 meters) and may face difficulties to hit smaller drones. The security team must act immediately – drones fly fast, and there are only a few seconds to respond.

MITIGATION TECHNOLOGY

Lasers

KEY CHALLENGE

Accuracy affected by weather conditions

These high-energy devices warrant their own sub-category. By emitting an intense beam of light, laser-based systems can destroy the drone structure, or its electronics. Lasers destroy drones and can confront many types of drones. On the downside, they require line-of-sight, burn the drone to pieces (destroying intelligence) and can also result in plummeting drone fragments. Collateral damage is possible, and obstacles such as buildings or other flying objects may pose challenges.

For these reasons, lasers may, in some cases, be less suitable for sensitive environments. It is also more difficult to hit smaller drones using lasers.

MITIGATION TECHNOLOGY

Electromagnetic Pulse (EMP)/High Power Microwave (HPM)

KEY CHALLENGE

Significant collateral damage to electronics in area

This is a radiation-based technology. It utilizes a high-powered burst of electromagnetic energy in short blasts, potentially damaging everything electrical in the area. EMP works indiscriminately and can cause heavy collateral damage.

For instance, it can permanently damage nearby electronics or computers, damaging their circuits. EMP is often viewed as a last resort option.

EVALUATING AND COMPARING COUNTER-DRONE (C-UAS) MITIGATION TECHNOLOGIES (CONTINUED)

MITIGATION TECHNOLOGY

GNSS electromagnetic

KEY CHALLENGE

Navigational disruption

Global Navigation Satellite System (GNSS) spoofing broadcasts a false GNSS signal such as GPS in a specific area. A GNSS receiver that receives the spoofed signal may determine its location wrongly. By controlling the perceived location of a drone, it may be possible to cause it to fly in a desired direction and thus navigate it. Alternatively, it can prevent the drone from flying according to a pre-programmed flight plan or from returning home.

In terms of disrupting the environment and affecting continuity, this technology can be even more problematic than jamming. Every navigation device in the area may receive the spoofed GPS signal and determine a wrong global position. GPS spoofing could affect, for instance, civilian cars' navigation systems, or drivers' navigation apps, causing confusion, accidents and worse. It may also disrupt friendly drone operation. This technology obviously should not be used near friendly authorized ships, planes or helicopters.

MITIGATION TECHNOLOGY

Cyber takeover

KEY CHALLENGE

Overcoming advanced drone protocols

This RF cyber-takeover is end-to-end, meaning it seamlessly flows from the initial rogue drone detection, all the way through to takeover and then safe landing. It can also be deployed automatically, eliminating the chance of human error.

Unlike the other mitigation technologies, RF cyber-takeover preserves continuity by avoiding collateral damage or interference with other communications systems. It can also distinguish between authorized and unauthorized drones, enabling an organization's authorized drones to keep functioning during the mitigation of rogue drones.

As it depends on a short transmission, it may also contend with swarms of unauthorized drones by quickly mitigating each of them in their own frequency and transmission patterns.

Because RF cyber-takeover mitigation does not destroy the drone, like lasers or EMP, organizations can reap the benefits of the intelligence inside the drone (as allowed by applicable laws, of course).

RF cyber-takeover focuses on specific RF-based manufactured or Do-It-Yourself commercial drones and overcoming their specific protocols.

DEPLOYMENTS

C-UAS NEEDS MULTIPLE DEPLOYMENT OPTIONS FOR OPERATIONAL FLEXIBILITY

MILITARY VEHICLE

VEHICLE

GROUND-LEVEL TACTICAL

HIGH-ALTITUDE TACTICAL

LONG-RANGE DIRECTIONAL

HIGH-ALTITUDE STATIONARY

THE WHITE HOUSE DOMESTIC COUNTER-UAS NATIONAL ACTION PLAN: DEVOLUTION, TECHNOLOGY, INFRASTRUCTURE, AND INCIDENT TRACKING

A POINT OF VIEW FROM THE CEO OF D-FEND SOLUTIONS 2022 - ZOHAR HALACHMI

The White House has issued a long awaited and sorely needed Counter-UAS National Action Plan.

The Action Plan acknowledges the well-established benefits from the proliferation of drones, as privately owned drones are likely to surpass 2 million in the US alone this year, with forecasts reaching 3-4 million in the coming years.

The impetus for the Action Plan, however, is recognition of the heightened risk associated with this proliferation. These risks are multi-faceted across environments and sectors. For example, the cost of an airport operational interruption due to a drone entering its airspace is remarkably high. Similarly, while authorized drones may be used to film large sporting events, space launches, presidential inaugurations and the like, rogue drones cannot be allowed to access these sensitive areas, or others like nuclear power sites and other critical infrastructure.

The Action Plan also expresses a significantly heightened level of concern about the concurrent associated risks from malicious actors weaponizing commercial unmanned aircraft systems (UASs).
The strategic goal is to safeguard the expansion of positive UAS activity while also safeguarding airspace by closing notable gaps in current laws and policies with new ground rules. In particular. The need for local authorities to be able to engage in detection and mitigation is becoming highly urgent.

While the Action Plan is quite detailed, comprehensive, and multifaceted, there are a few core elements which are at the centerpiece of the Plan, and which warrant special attention.

Below I will highlight these positive steps, and, for each one, present a perspective on how to take it further to optimize the benefits to our national airspace.

Extension of Detection: Devolution and Expansion of UAS Detection Authority to State, Local, Territorial, Tribal (SLTT) and Critical Infrastructure Levels

- Granting UAS Detection Authority to local levels represents a major step forward,
- Extending the authority for detection alone will not fully address the problem unless corresponding mitigation authority is also extended. Urgent consideration should be given to including some degree of mitigation allowances in this devolution and expansion program.

Extension of Mitigation: Federal Pilot Program for Expansion of C-UAS Mitigation to SLTT Level

- Piloting safe and controlled mitigation authority at SLTT levels could serve as a rapid validation step
- The proposed mitigation pilot programs should have defined goals to then allow the localized mitigation authority to become permanent and expand in scope.

Technology: List authorized detection equipment that avoids operational or communications disruption of airspace.

- Spotlighting C-UAS solutions and technology is essential to advance beyond the shortcomings of legacy detection technologies towards innovation for safety, control, and continuity.
- Consistent with this goal, the stated need to avoid or minimize adverse impact on the broader communications spectrum and on the National Airspace System (NAS) are essential and must be a core goal, with measures focused on the rogue drone itself.
- This exercise of authorizing and listing technology should be extended to cover focused and safe mitigation technologies in addition to detection technologies, for a full solution
- Distinguishing between friendly authorized drones and rogue or hostile unauthorized drones is an essential capability to preserve the rights of legitimate drone pilots and safeguard the airspace, including drones performing mission critical tasks.

Critical Infrastructure: Enable and oversee placement of C-UAS Mitigation equipment at critical infrastructure sites

- The emphasis on protecting critical infrastructure from hostile or unauthorized drones is encouraging and timely.
- Consideration could then be given to allowing site security staff similar or defined permissions with proper qualification, training, and approvals.

Incident Tracking: UAS Incident Database.

- Incident tracking databases can make a major contribution to better understanding the threat and should track all facets of the incident including sectors, use cases, nature of the incident (attack, near collision, etc.) and the actual drone make and model.

CONCLUSION
A SOLID FIRST STEP FOUNDATION FOR NATIONAL C-UAS PROTECTION

The Counter-UAS Action Plan includes many relevant and timely recommendations and mechanisms to address the rapidly rising danger of rogue drones from both actively hostile and simply careless pilots. These components are promising in their capability to bring the nation's C-UAS readiness to the next level of heightened urgency with a more systematic and comprehensive defense.

The devolution and extension of drone detection and mitigation authority to more local levels; the support for new generation technologies that specifically address the problem in ways that emphasize safety, control, and continuity; the focus on the protection of critical infrastructure; and the tracking of incidents in a comprehensive manner all represent steps that should be adopted rapidly and applied in the broadest possible manner to maximize the value in reducing risk and achieving the widest homeland protection coverage possible. In all these steps, strong consideration should be given to extending mitigation possibilities to the same degree that detection responsibilities will expand, such that the full incident lifecycle is covered for the safest possible outcomes.

The Counter-UAS Action Plan brings many urgently needed countermeasures to address the rapidly rising danger of hostile and unauthorized drones. These steps promise to bring the nations C-UAS readiness to the next level of heightened urgency and provide a more robust, systematic and comprehensive defense. Strengthening and expanding these authorities and plans will enable the new drone society and economy to flourish while safeguarding the homeland from the rapidly rising risks of rogue drones

COUNTER UAS USA

17-18 August 2022 | Washington DC

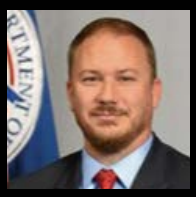
At a crucial time when the United States Department of Defense plan to at least $636 million on Counter-UAS research and development and at least $75 million on C-UAS procurement in 2022, the IDGA Counter-UAS Summit will bring together senior decision-makers from both the Federal Government and the military to discuss key challenges, requirements and procurement programs.

Lieutenant General Karsten S. Heckl
Commanding General
Marine Corps Combat Development Command

Blake Stone
Strategy and Policy – Homeland Defense Policy,
Joint C-sUAS Office

Colonel Tony Behrens
Deputy Director
Joint Integrated Air and Missile Defense Organization (JIAMDO)

Tarun Gupta
Acting Director, Directed Energy Project Office
Rapid Capabilities and Critical Technologies Office (RCCTO)



Brent Cotton
Director, C-UAS PMO
Department of Homeland Security

Scott Parker
Branch Chief, Strategic Planning Section, Soft Targets and Crowded Places Task Force
Cybersecurity and Infrastructure Security

Brigadier General Volker Samanns
Commander of Ground Units in the Air Force Forces Command
Bundeswehr

Kevin M. Jinks
Senior Counsel, Office of Legal Policy
U.S. Department of Justice

Todd Craig
Acting Assistant Director, Information, Policy, & Public Affairs (Ret.)
Federal Bureau of Prisons

Thomas Adams
Supervisory Special Agent, FBI cUAS Program Manager
FBI

Lieutenant Colonel Paul F. Santamaria
Product Manager Medium Caliber Ammunition PM MAS
JPEO Armaments and Ammunition

Ted Maciuba
Deputy Director, Robotics Requirements
US Army Futures Command

Ryan Berry
Manager, UAS Security Division
Federal Aviation Administration

Don Rassler
Director of Strategic Initiatives
Combating Terrorism Center at West Point

Dr Alexandre Papy
Defense Against Terrorism (DAT) Counter UAV Chairman
NATO

Tim De Zitter
Lifecycle Manager
Belgian Defence

Zachary Kallenborn
Unmanned Systems (Swarms)
CBRN Warfare and Terrorism Analyst

Tom Driscoll
CTO & Co-Founder
Echodyne

Bill Haraka
Vice President Defence & Security at Robin Radar Systems
Robin Radar Systems

Zohar Halachmi
Chairman & CEO
D-Fend Solutions

Timothy Bean
CEO
Fortem Technologies

DOWNLOAD THE AGENDA

D-FEND SOLUTIONS

www.idga.org/events-counteruas-usa