SKYTRACKER™

Countering the UAS Threat to Public Safety and Valuable Assets

AFCEA and USNI WEST Conference and Exposition

February 17-19, 2016

Alan Kraft
Senior Executive,
CACI International Inc

Kenneth Israel
CACI Corporate Communications

SkyTrackerUAS.com

CACI
EVER VIGILANT

Table of Contents

Executive Summary

Commercial drones, or unmanned aircraft systems (UAS), are small, commercially available aircraft that use radio frequency (RF) signals to communicate with their operators. The misuse of UAS represents an escalating threat to public safety and national airspace. This paper discusses how CACI's SkyTracker™ system can be used to counter these threats.

SkyTracker deploys an array of sensors that exploit the commercial drone's own RF signals to detect, identify, locate, and track misused UAS, as well as identify and locate their operators. This software-defined solution also applies non-kinetic, RF-based countermeasures to mitigate the drone threat without disrupting legitimate electronics or communications systems in the area, or interfering with law enforcement or responsible UAS.

SkyTracker is applicable to the defense of such high-value assets as buildings and stadiums, airports, military bases, and areas under temporary flight bans such as locations experiencing forest fires. The system provides continuous, automated monitoring, and is unaffected by time of day, weather, or non-UAS flying objects.

Cyber Platform Protection and Exploitation

The protection and exploitation of platforms, such as unmanned aerial vehicles, ships, vehicles, and foreign weapons systems is an emerging field in the cyber arena. All of these platforms emit electromagnetic signals to communicate in the radio frequency (RF) spectrum. These signals may be exploited for an information or operational advantage; for example, U.S. forces disrupting adversarial wireless broadband communications. CACI's capabilities in this domain include the protection and exploitation of vehicles, ships, space systems, and weapons systems, and further include the delivery of cyber payloads on computer networks and computer networks and platforms.

Unfortunately, today's adversaries are not limited to nation states with physical and political delimitations. They may be terrorist organizations spanning borders or they may be individual actors. Furthermore, available commercial technologies provide these adversaries with significant information and communications capabilities. CACI designs and develops technologies to counter the threat posed by such technologies. The company engineers software-defined, RF-based solutions that are capable of delivering passive detection and autonomous, non-kinetic electronic attack against commercially available WiFi and communications platforms.

CACI's RF-based detection and offensive platform exploitation is being applied to addressing the potential threat posed by another recent technology, once restricted to military use and now available for retail purchase: the commercial drone.

The Threat to Valuable Assets and National Airspace

Commercial drones, or unmanned aircraft systems (UAS), are small, commercially available aircraft. They are sold in a variety of sizes and models, and use RF signals to communicate between the operator and the aircraft. The Consumer Electronics Association estimates the global commercial drone market may exceed $1 billion by 2020.[1] The upsurge of this new technology offers many advantages to hobbyists, but misuse of UAS poses diverse safety challenges. Furthermore, the push from commercial retailers such as Amazon to utilize drones for package deliveries compounds the potential threat to the most complex, heavily trafficked airspace in the world.

According to the Federal Aviation Administration (FAA), airline pilots report nearly two drone sightings a day, including a total of 238 sightings in 2014 and more than 650 by August 2015.[2] Other reports of UAS misuse include:

- Multiple reports of drones used to deliver cell phones, narcotics, or other small packages inside the perimeter of U.S. prisons;[3]
- Drones spotted flying above 13 French nuclear power plants;[4]
- An emerging threat of weaponized drones, including drones with traces of radiation landing close to the Japanese parliament;[5]
- Reports of drones illegally flying over stadiums, in one instance crashing into the bleachers at the U.S. Open Tennis Championship;[6] and
- Drones interfering with firefighters and first responders.[7]

Currently available technologies lack the precision and reliability to effectively address the threat of UAS misuse. For example, areas in which drones commonly intrude often contain sensitive equipment, and counter-UAS technologies such as broadband jamming significantly disrupt area electronics and communications systems, making them an unviable solution for airports or military bases. Radar, which is designed to detect large platforms, is unable to detect smaller objects such as UAS. Geo-fencing technology involves outfitting commercial drones with built-in safety parameters, yet these safeguards may be circumvented by operators modifying their aircraft.

Moreover, none of these technologies has the capability to locate the drone operator, significantly limiting law enforcements' ability to find and engage operators in incidents of inadvertent or unlawful misuse. CACI's SkyTracker solution effectively addresses the scope and scale of all these challenges.

SkyTracker

CACI's proprietary SkyTracker system detects, identifies, tracks, and mitigates UAS threats. The system protects geographically compact areas surrounding such high-value assets as buildings, stadiums, and prisons, and is scalable to provide wide-area defense of airports, military bases, critical infrastructure, as well as areas under temporary flight bans such as locations experiencing forest fires.

SkyTracker works by establishing an electronic perimeter around sensitive locations that cannot be circumvented by individuals modifying their aircraft. SkyTracker:

- Identifies and locates UAS and their operators, speeding law enforcement's and authorities' response time in intercepting unlawful operators;
- Rapidly detects UAS and can deliver countermeasures within seconds;
- Is not affected by drone size or shape;
- Does not disrupt legitimate electronics, area communications systems, or responsible UAS operators due to its non-kinetic mitigation;
- Can achieve mitigation from long distances; and
- Is unaffected by weather, time of day, or non-UAS flying objects such as birds or large aircraft platforms.

Passive Detection

The SkyTracker system is composed of multiple sensors that can be networked to existing command and control centers. SkyTracker deploys this sensor array to create an electronic perimeter boundary around sensitive locations.

The RF-based system provides long-range, high-fidelity detection and identification with low, near-zero, false alarm rates. The sensors detect and exploit the RF communication link between the drone and its operator. SkyTracker's passive RF detection ensures that the system does not interfere with other RF-spectrum-dependent functions, such as WiFi hotspots and personal cellphone use, or with authorized drones operating in the area.

The modular system provides scalable defense options:

1. **Point defense** sensors protect geographically compact areas such as buildings, embassies, and stadiums. This option also supports mobile defense for such purposes as executive protection. Point defense is effective against threats suddenly appearing at a close-proximity (termed "close-in/pop-up" threats).
2. **Area defense** sensors are scalable to provide wide-area defense for sites such as airports, and is especially effective against open-air threats. Area defense sensors may also be networked to existing command centers.

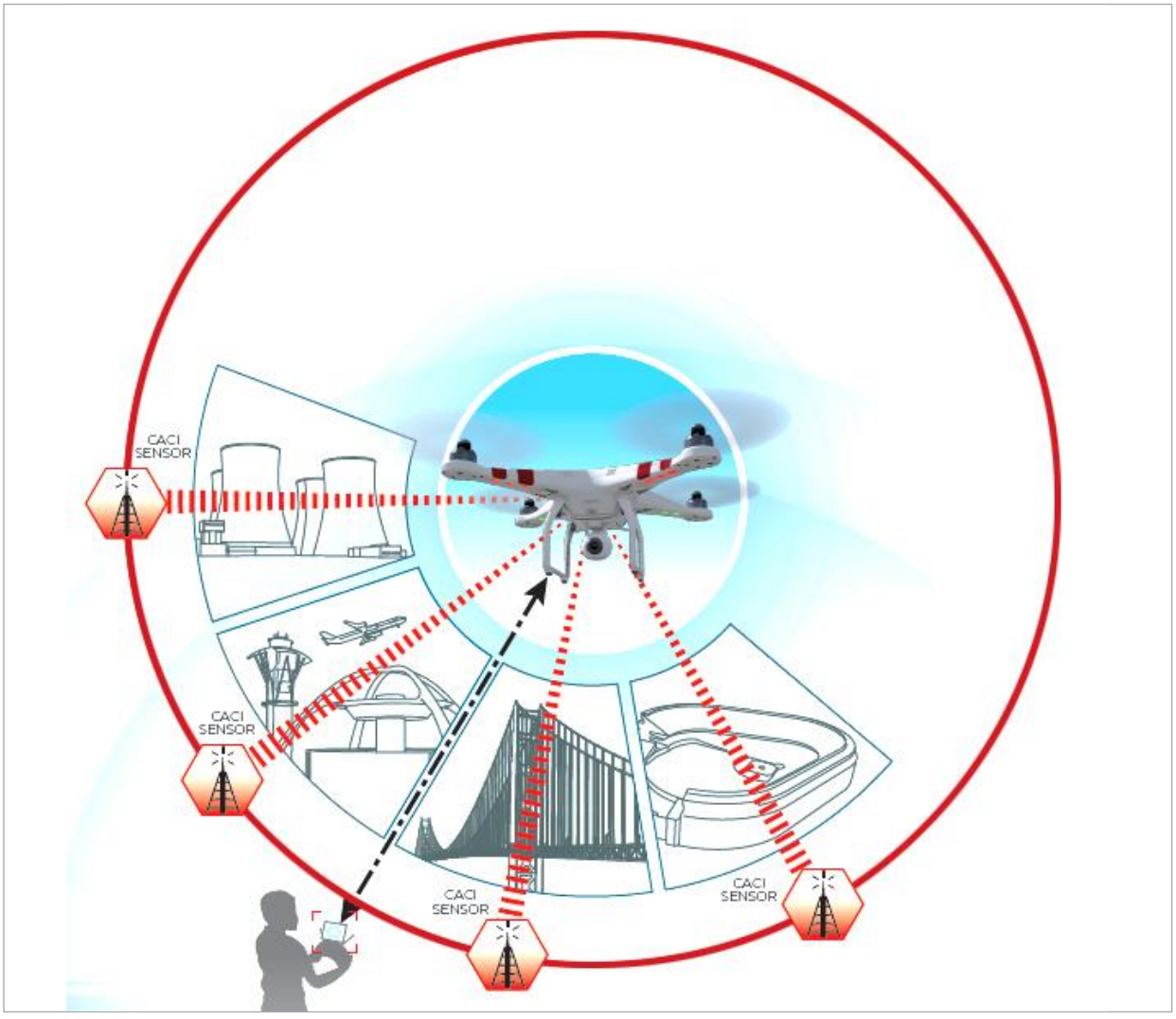

Figure 1. SkyTracker deploys an array of sensors to create an electronic perimeter boundary in order to protect high-value assets and national airspace.

SkyTracker is designed to support automated functionality, using an intuitive graphical user interface (GUI) for system operation. Because SkyTracker relies on software-defined technology, simple web-based software updates are provided to ensure that the sensors are properly configured to the latest drone technologies and communication protocols. The sensors are in constant communication with networked command and control centers, reporting detected signals, forensic data collected from selected signals regarding the identity and location of UAS and their handheld controllers, as well as the health and status of the sensor system – all displayed to users via the GUI.

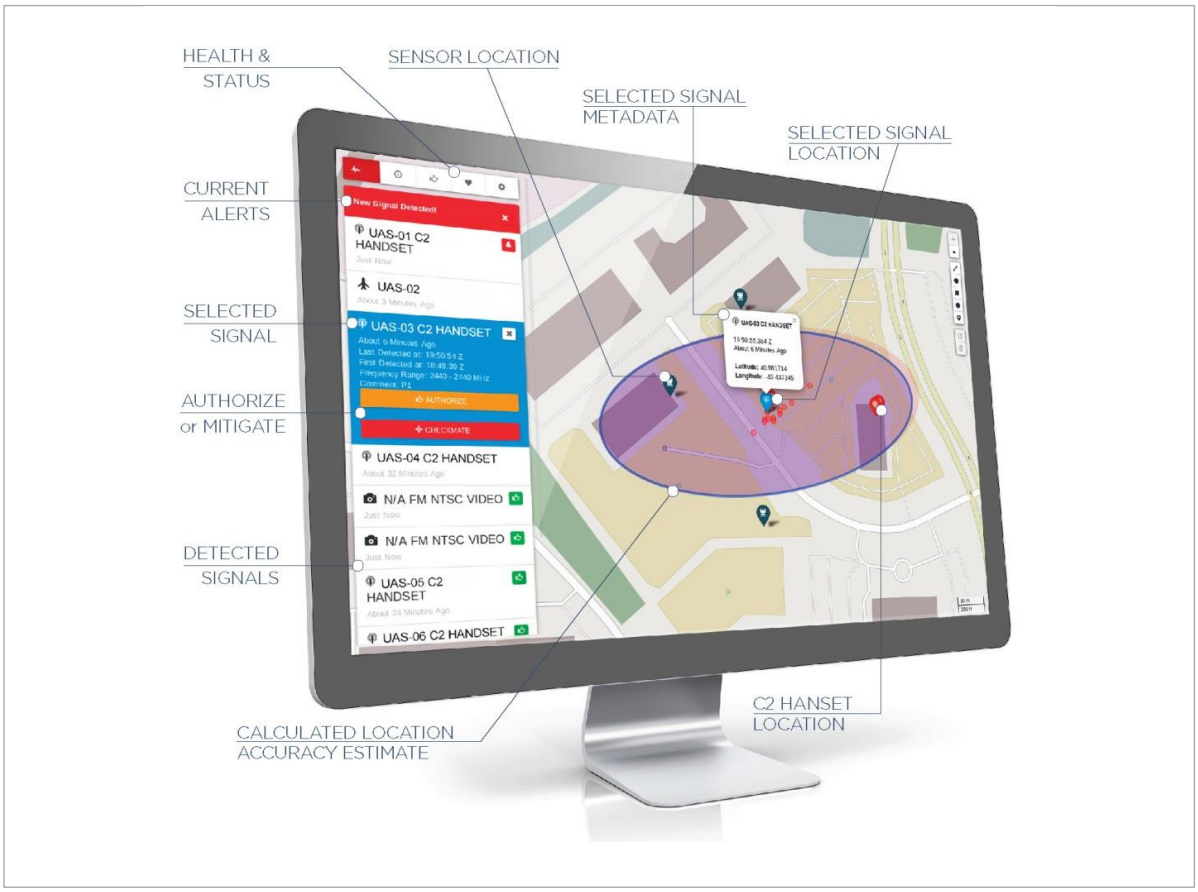

Figure 2. SkyTracker's graphical user interface (GUI).

Location and Tracking

SkyTracker utilizes UAS RF emissions to identify and locate aircraft systems flying within the electronic perimeter defined by the sensor system. Multiple sensors extract the UAS communication signals, working in coordination to provide accurate geolocation and tracking both of UAS and their operators, and a greater number of deployed sensors provides highly accurate geolocation and tracking. The efficacy of the sensor system is unaffected when increasing the scale of the electronic perimeter boundary.

Detected UAS are specifically identified by matching their unique signals characteristics to a predefined database of known drone-related signals. This database library of known signals is constantly being updated and expanded. The system is also capable of recording high-fidelity forensic data from detected

drone activity. Detected signals are verified as emanating from commercial drones by comparison to the library of known UAS signals that exists onboard the GUI, or through the forensic data collection process. Because the sensors are intercepting known drone-specific RF signals, the system is not disrupted or confused by non-UAS flying objects such as geese or bats, or larger aircraft platforms, either of which may confuse other counter-drone technologies such as radar.

The sensor system's targeted location and tracking capability can further differentiate between misused UAS and other drones operating within the electronic perimeter boundary. This capability provides responders with full situational awareness of the area, and enhances law enforcement's ability to track and engage only misused UAS.

The SkyTracker system supports multiple users and automatically alerts users to drone tracking data and drone operator and handset location. The forensic data collected by the sensors may be further used for post-event analysis or in support of legal enforcement efforts.

Mitigation

From the moment UAS threats are detected, SkyTracker rapidly locates the misused aircraft and can deliver non-kinetic mitigating countermeasures. Because these countermeasures are RF-based, mitigation can be achieved from long distances and will not interfere with legitimate electronics or communications systems in the area, or with responsibly operated aircraft. SkyTracker's targeted ability to stop specific UAS allows responders' aircraft systems to remain unaffected and mission capable.

Mitigation is platform-specific, and typically multiple techniques are used simultaneously, enhancing responders' capability to achieve desired results. In some cases, the system enables responders to seize remote control of misused UAS and fly them to a safe zone. SkyTracker's mitigation capability can be deployed automatically or manually, at the responder's discretion and in adherence to applicable laws and regulations.

SkyTracker Capabilities vs. Other Counter-UAS Technologies

Table 1 summarizes SkyTracker's capabilities against all deployed counter-UAS technologies.

Desired Action	SkyTracker Capability	Deficiencies of Other Counter-UAS Technologies
Detection	Automated passive detection of UAS and their handsets Detections not dependent on drone size, speed, altitude, or material composition Allows the sensor system to locate both the aircraft and its operator 360 degree coverage	Many require active sensors that can pose a radiation safety hazard Many are not 24/7 or all weather In many cases, do not offer automated detection and require expert operators for detection Do not offer detection of UAS operator

Desired Action	SkyTracker Capability	Deficiencies of Other Counter-UAS Technologies
	24/7 all-weather operation High probability of detection with low false alarm rates	
Location/Tracking	Sensors detect and report UAS flight patterns and the location of the operators in seconds Tracking data can be networked to existing command and control systems	Many sensor do not provide precise target location Electro-optical sensors degrade during poor weather or night time operation Many systems lose track when target nears horizon or in poor lighting conditions
Identification	Identifies commercial UAS by recognizing their distinctive radio signal characteristics System does not false-detect upon encountering animals or other non-UAS flying objects Sensors can be networked to existing defense systems for integrated threat awareness	Most systems require expert operator to perform platform identification Most systems cannot identify specific types of commercial drones Traditional system do not identify the operator
Classification	Upon identification, UAS is compared to drone-related-signals library in order to properly classify the aircraft	Electro-optical and Wi-Fi based solutions cannot automatically distinguish between and among multiple aircraft
Verification	Sensors collect forensic data for threat verification and differentiation from non-threats	Typically cannot differentiate between various types of UAS In many cases, forensic data collection is not offered
Mitigation	Non-kinetic mitigation of UAS via RF methods allow for precision engagement The UAS and operator are identified and located	Many detection systems do not offer any mitigation capability Do not locate operator, slowing response for security personnel

Desired Action	SkyTracker Capability	Deficiencies of Other Counter-UAS Technologies
	System can employ multiple non-kinetic responses in parallel Mitigation is integrated into end-to-end detection, identification, tracking, and mitigation system	Most systems do not deliver precision non-kinetic countermeasures Most mitigation systems do not integrate countermeasures with the detection, identification, and tracking Typical offerings provide kinetic defeat or brute force jamming, which is non-precise and disruptive to existing legitimate communications like mobile phones and Wi-Fi

Table 1. Summary of SkyTracker capability and comparison to competitor systems.

Applications

SkyTracker is demonstrated to address a variety of UAS threat scenarios – anywhere UAS pose a potential risk to people or assets. This includes, but is not limited to:

- Agriculture
- Airports
- Aviation
- Critical Infrastructure
- Defense
- Event Venues
- Executive Protection
- Fire Departments
- First Responders
- Homeland Security
- Law Enforcement
- Media
- National Facilities
- Stadiums

Conclusion

CACI's SkyTracker system leverages precision signals detection and cyber exploitation technologies to address the evolving threat posed by the misuse of commercially available UAS platforms. The SkyTracker system exemplifies the necessity of cyber solutions to keep pace with the proliferation of commercial technologies that are increasingly cheap, available, and sophisticated, and which pose significant challenges to the safety of the U.S. – its people, assets, airspace, and critical infrastructure.

CACI advances such solutions by leveraging the full range of its cyber expertise and strategic goals. For example, the company combines niche digital signals and RF expertise with years of cyber and electronic warfare experience to deliver significant defensive and offensive platform cyber capabilities. These solutions include the passive detection and targeted exploitation of signals emitted by platforms. By levering all available resources, CACI is able to respond to rapidly emerging, non-traditional global threats with precision technologies and techniques. Now, the company is applying these solutions to addressing the safety issues posed by commercial drones in a manner that supports public safety even as it benefits responsible UAS hobbyists.

About SkyTracker's Developers

SkyTracker is CACI-proprietary technology that was developed by the company's National and Cyber Solutions (NCS) group. NCS is composed of over 1,300 engineering, data science, cyber security, and signals intelligence experts. The team delivers services and solutions for every step of the intelligence lifecycle, and leverages an agile development methodology that provides rapid prototyping of new technologies, quick reaction to customer requirements, and operational support for a diverse customer base. CACI Senior Executive Alan Kraft and Communications Specialist Kenneth Israel worked closely with NCS to develop this white paper.

About CACI

CACI provides information solutions and services in support of national security missions and government transformation for Intelligence, Defense, and Federal Civilian customers. A *Fortune* magazine World's Most Admired Company in the IT Services industry, CACI is a member of the Fortune 1000 Largest Companies, the Russell 2000 Index, and the S&P SmallCap600 Index. CACI provides dynamic careers for over 20,000 employees worldwide.

References

1. Consumer Electronics Association, “We Have Liftoff: CEA Says FAA Action on Drones Rules a Welcome Step Forward,” February 16, 2015, https://www.cta.tech/News/News-Releases/Press-Releases/2015-Press-Releases/We-Have-Liftoff-CEA-Says-FAA-Action-on-Drones-Rule.aspx.
2. Federal Aviation Administration, “Pilot Reports of Close Calls With Drones Soar in 2015,” August 12, 2015, http://www.faa.gov/news/updates/?newsId=83445&omniRss=news_updatesAoc&cid=101_N_U.
3. Michael S. Schmidt, “Airmail via Drones Is Vexing for Prisons,” *The New York Times*, April 26, 2015, http://www.nytimes.com/2015/04/23/us/drones-smuggle-contraband-over-prison-walls.html?_r=0.
4. Maïa de la Baume, “Unidentified Drones Are Seen Above French Nuclear Plants,” *The New York Times*, November 3, 2014, http://www.nytimes.com/2014/11/04/world/europe/unidentified-drones-are-spotted-above-french-nuclear-plants.html.
5. Associated Press in Tokyo, “Drone 'Containing Radiation' Lands On Roof of Japanese PM's Office,” *The Guardian*, April 22, 2015, http://www.theguardian.com/world/2015/apr/22/drone-with-radiation-sign-lands-on-roof-of-japanese-prime-ministers-office.
6. Des Bieler and Marissa Payne, “Teacher Arrested After Drone Crashes Into Stands During U.S. Open Match,” *The Washington Post*, September 4, 2015, https://www.washingtonpost.com/news/early-lead/wp/2015/09/03/drone-crashes-into-stands-during-u-s-open-match.
7. Patrick McGreevy, “Private Drones Are Putting Firefighters In 'Immediate Danger,' California Fire Official Says,” *Los Angeles Times,* August 18, 2015, http://www.latimes.com/local/political/la-me-pc-fire-officials-warn-lawmakers-about-threat-of-drones-to-firefighting-aircraft-20150818-story.html.