AIRSPACE SECURITY INSIGHTS REPORT

MIDYEAR 2017

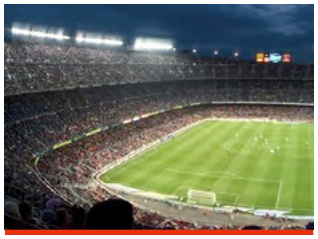
AIRSPACE SECURITY INSIGHTS REPORT

EXECUTIVE SUMMARY

Drone detection has never been a more urgent issue. This report is a recap of drone physical and cyber security and safety-related activity for the first half of 2017, and includes insights on current applications of drone technology, new incidents, and emerging regulations which unfolded in various industries and across the world.

INDUSTRY UPDATES

Oil and gas facilities are using drones for infrastructure inspection, but also are understanding the costs of a shutdown due to a rogue drone.



Stadiums and arenas are integrating drone shows for audiences, but also are seeing hobbyists crashing into spectators.

Airports across the world are seeing drones fly dangerously close and crashing into passenger flights, prompting runway closures, flight delays and implementation of heightened security measures.

Public event coordinators are using drones to monitor spectators, but are also concerned with drones threatening crowds.

Data centers and corporations are protecting themselves against espionage and hackers, who can use drones as a tool to infiltrate vulnerable networks.

VIPs and homeowners are seeing an increase in drones near their airspace, compromising their privacy and physical safety.

Federal agencies and militaries are seeing a rise in drones used for terrorism and destruction, and are also investing significant resources to advance their unmanned aerial surveillance and civilian protection programs.

Local governments are increasingly relying on drones to monitor events and respond to disasters, and they also understand the need for proactive detection of unauthorized drones to prevent interruptions and enable first responders to focus on life-saving efforts.

LEGAL AND REGULATORY ROUNDUP

Industry use cases are continuing to unfold as more drones enter the market. Whether a drone is used for commercial, military, or personal use, U.S. and global regulators are reacting to drone incidents with a slew of new proposed legislation and regulations. Drone industry advocates are being asked to advise legislators to ensure that laws address the needs of drone users, while also protecting civil liberties.

DRONE SAFETY AND SECURITY PREDICTIONS FOR SECOND HALF OF 2017

The drone security conversation is new, and there are emerging topics yet to be explored. Drone manufacturers and enthusiasts will continue to outpace regulators, as they struggle to keep up with an increase in drones on the market, and enforce new laws. As more incidents occur, and drone detection technology is integrated, there will be an entirely new set of data and information to inform regulators, insurers, and the general public of the risks to airspace. As this data unfolds, local governments and private citizens will have to carry the burden of enforcing anti-drone measures, and there will be an increase in criminal and civil legal actions against pilots who enter unauthorized airspace.

911 Security UPDATES

911 Security, a leading integrator for the world's leading drone security platform, brought on additional investors, retained partners, and announced a market expansion and new hires in the first half of 2017. The company integrated their drone detection solution individuals around the world.

CONCLUSION

Drones are here to stay. Whether a drone is used for entertainment, commercial applications, or malicious activities, there are no barriers in our airspace to prevent interruptions or attacks. Laws are emerging, but those with injurious intent and motivation to cause harm can easily circumvent them. However, detection technology cannot be avoided once implemented and is being advanced every single day to provide warning of the presence of unauthorized drones.

ENERGY AND UTILITIES

INTRODUCTION

Energy, oil, and gas manufacturers are beginning to implement drone programs around the world, providing engineers an early opportunity to use smart sensors to "sniff" out leaks, locate faults with precision, inspect facilities, equipment, drilling rigs and pipelines, and assess structural health or damage. Drones are quick to get into the air and don't require safety nets, and provide live imaging and surveying. Dangerous and cost-inefficient detection tactics, such as scaffolding or deploying helicopter operations, can be a second-response solution.

Safety is top of mind for all utility operators. Spills and leaks have been of extreme concern throughout the history of the industry, with safety of the environment and people the most critical part of a manufacturer's infrastructure. Combined with the rise and availability of drone technology, these organizations have taken note of how to advance their facility and risk programs, and integrate drone maintenance to help prevent disasters and avoid costly interruptions to their operations.

Energy corporations are investing in drones for maintenance and surveillance, and are also considering the unique risks drone hardware poses to the physical infrastructure of their facilities. Wherever a drone operates to support a structure's safety program, there must also be a security procedure to ensure proper use and entry of drones in the airspace.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE IN OIL, GAS AND PUBLIC UTILITIES

Currently, the oil and gas sector relies primarily on road vehicles, helicopters, and other manned aircraft to detect damage and threats to pipelines, at a significant financial cost. Such organizations need to consider how rogue drones fit into their security equation. Energy providers and utility operators experienced multiple drone incidents firsthand in the first half of 2017, and were affected by following activities:

- The State of Texas' legislature proposed H.B.A No.A1643, bill that could attach jail sentences to any pilot found guilty of flying a drone over oil and gas drilling facilities. The bill was passed and will go into effect September 2017.
- A drone crashed into a Con Edison power plant in New York City. The drone broke into several pieces after striking the building.
- Drone crash knocks out power to 1,600 in Mountain View: The hometown of Google, a hobby pilot crashed his drone in a power line, shutting off the city's electricity, which prompted the evacuations of government buildings and a local library.
- Oil & Gas UK released the 2017 UAS Operations Management Standards and Guidelines: The publication aims to guide the growing use drones in offshore oil and gas, to achieve consistency with the high safety and operating standards already adopted for production and helicopter flight operations.

CONCLUSION

The risk of the wrong drone near an oil or gas storage facility could be deadly and cause billions of dollars in infrastructure and environmental damages. Such drones must be detected before they enter protected airspace and cause damage. When the drone is known, and comes to work at oil and gas facilities, whether it be in the middle of an oil field in Texas, or at a refinery in Louisiana, there also needs to be an aerial protection and safety program in place.

STADIUMS AND ARENAS

INTRODUCTION

Filmmakers are always looking for a new way to tell a story, and drones with cameras provide an advanced perspective never seen before, with breathtaking views and new vantage points. They've flown in fleets at the Super Bowl, capturing close-up views of performers, and granting audiences a chance to watch as if they're onstage or on the field. However, when airspace is unprotected, rogue drones can interrupt play, threaten the safety of spectators and infrastructure. For artists and performers, spying drones may also infringe on copyrighted materials, and violate intellectual property laws.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE IN STADIUMS AND ARENAS

The risk of drones in stadium and arena airspace is becoming increasingly apparent, especially as drones become accessible to any user, carry payloads from grams to hundreds of pounds, and have limited laws barring operation. The FAA prohibits drone flights within three nautical miles of a stadium, starting one hour before and ending one hour after the scheduled time. They include Major League Baseball, National Football League, NCAA Division One Football, NASCAR Sprint Cup, Indy Car, and Champ Series races. This rule is largely ignored, and arenas and stadiums need to consider what sort of protection they want to provide their spectators and performers from aerial threats as a part of their overall security program ecosystem. Stadium, arena and public venue operators experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- Security takes down drone flying over Falcons practice facility: Ahead of their Super Bowl game, the NFL's Atlanta Falcons' security spotted a drone flying over their practices. While the pilot turned out to be a neighborhood family, many initially speculated espionage from their opposing team, the New England Patriots.

- Terrorist drone attack fears led to closure of stadium roof: The Union of European Football Associations (UEFA), decided to close the retractable roof of the Millennium Stadium in Wales over fears terrorists could fly a drone into the ground during the Champions League final.

- No drone zone for those attending the Super Bowl: The U.S. FAA implemented temporary flight restrictions within a 34.5-mile radius of NRG Stadium in downtown Houston, Texas for the Super Bowl. Drone security wasn't the only talk of the town for the Super Bowl – Intel showcased a drone light show at halftime.

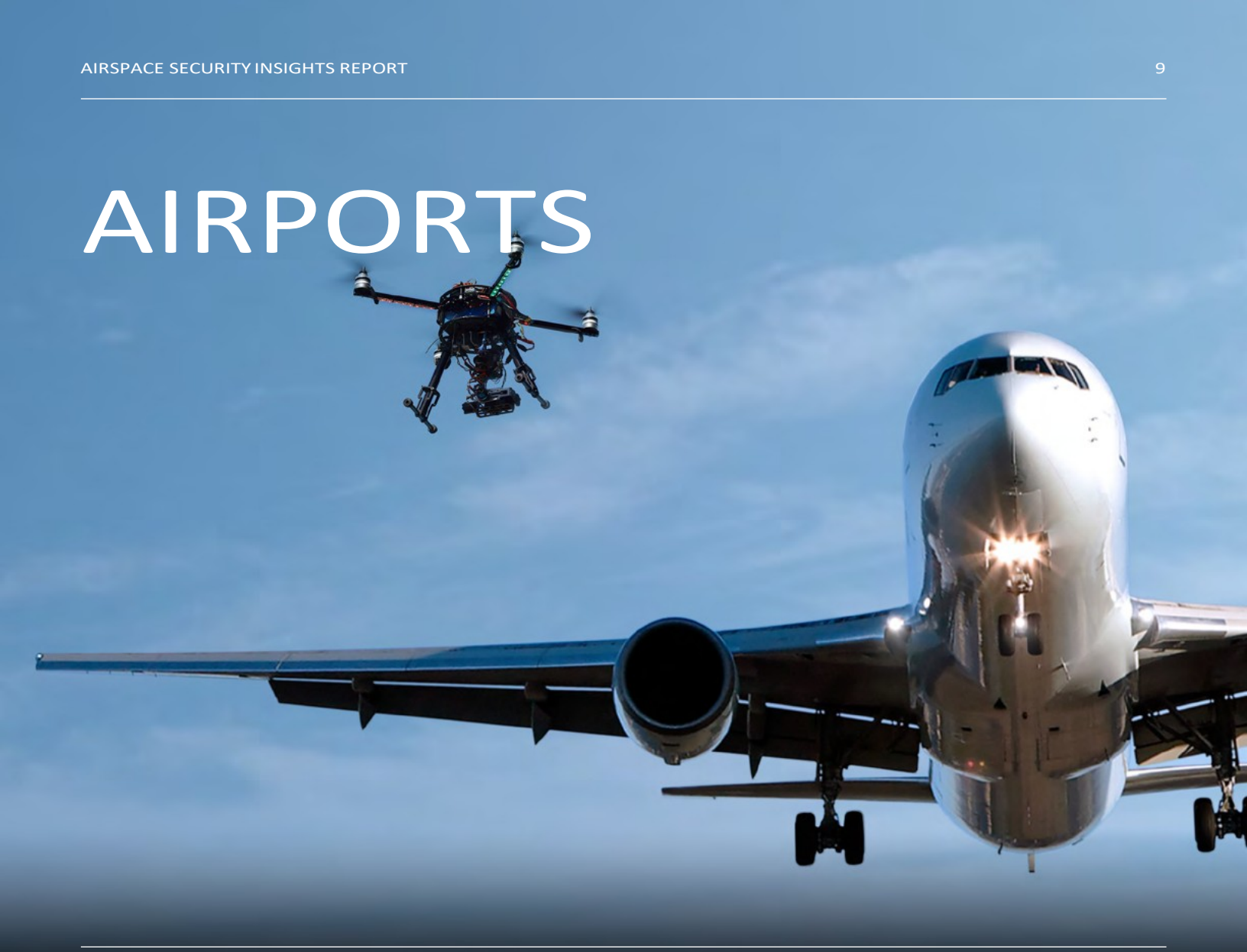
- Drone crashes into spectators at baseball game: A rogue drone flew directly inside a baseball stadium, crash landing into a group of spectators. Investigators were not able to determine if the pilot was flying with malicious intention, or if this was a case of pilot error.

- Formula One bosses fear terrorists will attack Grand Prix: Set for July 2017, event organizers are equipping themselves with massive nets to catch drones if they come too close to the racetrack, athletes or spectators.

CONCLUSION

Stadium operators and sports teams from across the globe not only want to protect their athletes, performers and spectators, but also want to ensure footage captured from drone cameras do not breach broadcast contracts or copyrights. Sports organizations such as the New York Mets and their home stadium, Citi Field, understand these risks and have taken proactive measures to secure their airspace. A drone near a stadium may be innocuous – simply a hobbyist flying around during a tailgate, or searching for a foul ball – but when stadium and arena operators are responsible for the safety of thousands of lives at each event, they can no longer operate without understanding the risks drones pose to their airspace.

AIRPORTS



INTRODUCTION

Countless stories have been appearing in the news over the years regarding drone activity in federal airspace, citing safety concerns for passenger aircraft and disruption of airline operations. These risks are clear – a drone crash into an aircraft will cause damage to both vehicles. In 2012, the FAA established The FAA Modernization and Reauthorization Act, putting into law a requirement for hobbyist drone operators to contact their local airport management and the air traffic control tower if they plan to fly their drone within five miles of an airport. The notification requirement was designed to provide the airport an opportunity to prepare for drone activity. However, since then, this rule has largely gone unnoticed by hobbyist drone users, raising concerns for airports, aircraft pilots, and passenger safety.

With this marked increase in drone sightings, airport operators are considering how to approach drone safety measures and determine the additional risks that drones pose to their overall security program. Airports are multi-faceted security centers. They have officers monitoring the airfield, tarmac and fences, people on the ground following cargo and passenger baggage, and managers of warehouses that contain fleet maintenance programs. Thousands of safety and security elements exist on a single day in the life of an airport, and each component has a different security risk. The FAA and airports are acutely aware of the dangers drones pose to their airspace. However, there is a gap of knowledge and understanding of the intention of drones within physical grounds of airports, leaving questionable security concerns.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE FOR AIRPORTS

An unauthorized drone near an airport is a serious breach of security and can ground flights, shut down runways, and alarm passengers at airports who rely on airport managers to help them travel safely. Airports around the world experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- Chinese airport experiences multiple drone incidents, prompting dramatic security measures: More than 10,000 passengers were stranded at Chengdu Shuangliu International Airport after more than 60 flights were interrupted by four drones.

- Drone in near miss with plane near Edinburgh Airport: An unmanned craft was flying about 20-30 metres away from a Loganair flight at about 4,000ft. No-one was injured and the plane successfully landed.

- FAA investigating drone that nearly struck plane at Charlotte Douglas airport: Crew members on board a Jetstream International plane spotted a drone a mile and a half from the runway as their jet was preparing to land.

- Drone pilot arrested in China for threatening safety of aircraft: A 23-year-old hobby pilot in China, who launched the drone to film the sunset, came within 50 meters of an airplane, and filmed multiple scenes including several civilian airliners passing by. He was detained by police.

- Report published, "Unmanned Aerial Systems Sightings Report": Reports of UAS sightings from pilots, citizens and law enforcement have increased dramatically, and the FAA now receives more than 100 such reports each month. The agency wants to send out a clear message that operating drones around airplanes, helicopters and airports is dangerous and illegal. Unauthorized operators may be subject to stiff fines and criminal charges, including possible jail time. This report is published quarterly. for endangering public security.

CONCLUSION

Proactive detection solutions exist for airport security managers, and are a critical part of the overall security equation for the thousands of people travelling through and working at their operations.

PUBLIC EVENTS

INTRODUCTION

With the increase of drones being used to capture live event footage and for security, event organizers must discuss drone safety at the onset of planning, to ensure drone security measures are implemented. Event personnel must plan for rogue or malicious use of drones when they consider how to protect their security operations, attendees, spectators and athletes.

Political and government events require an advanced level of security. The 47th Annual Meeting of the World Economic Forum took place in Davos, Switzerland, and security organizers integrated a drone defense system to protect the attendees, which included world leaders in business, media, politics and the arts. Police in Canton of Graubünden, where the forum was held, were granted invaluable time to prepare for a drone threat and deploy a defense measure.

Spectators at celebrations, parades and events should enjoy the party on the ground, and not be concerned with the threats in the sky. The U.S. National Basketball Association champions, the Golden State Warriors, held their celebratory parade in Oakland, California in June 2017. Over 75 drone incidents, or the times a drone was detected within the protected airspace, were recorded, despite the City of Oakland's declaration that the area was a "no fly zone." Cities who host events must also consider the safety of landowners, tenants, building managers, and offices that may be enjoying the view of a parade or race from their home, but also be in the line of sight of a drone, without their consent to film.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE IN PUBLIC EVENTS

Incidents such as those recorded at the Warriors parade are showing a startling trend of drones being above crowded areas. As U.S. federal regulators continue to research the impact of drones on crowds, it's up to spectators and security personnel to assess the risk of physical injury a rogue drone poses, and decide if proactive detection will support event security objectives. Public event coordinators experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- Drone crashes into bike racer: A drone flying over cyclists during the Golden State Race Series in Rancho Cordova, Calif. hit a tree, crashing into a rider's front wheel. The cyclist was able to bike a bit further down the road, until the drone locked up the front wheel, causing the biker to fly over the handlebars.

- Drone agitates horse during race, injuring spectators: A horse frightened by a low-flying drone ran into a large crowd at a race in Colorado. The havoc caused three injuries and two trips to the hospital - one for a woman who suffered a gash to her head and another who suffered a hip injury.

- Man convicted in drone crash that injured woman during Seattle's Pride Parade: A woman was knocked unconscious when she was struck a small drone as she watched the annual parade in 2015. The pilot was found guilty of reckless endangerment, and sentenced to jail time.

- Report published, "The ASSURE UAS Ground Collision Severity Evaluation Final Report": The U.S. Federal Aviation Administration (FAA) commissioned research to discuss how blunt force trauma, penetrating injuries, and lacerations are the most significant threats to the public and crews operating Small Unmanned Aerial System (sUAS) platforms.

- Boston Marathon Adds Drones in New Security Push: Race organizers with the 2017 Boston Marathon integrated camera-equipped drones into their security program, allowing police to scan nearby crowds with long-distance and infrared zoom, and helping to thwart low-tech terror attacks.

CONCLUSION

It's up to drone pilots to exercise responsibility and follow laws and regulations. Even with proper authorization, pilot error occurs, which could interrupt event operations and potentially cause physical harm.

DATA CENTERS AND CORPORATIONS

INTRODUCTION

Not only do drones have the ability to discretely spy on corporate operations, risking information leaks, but also an interruption of a data center's operation can cause system malfunctions and server failures. Financial damages, including losses by customers, diminish brand image and prompt a loss of client confidence. Drones are enabling new avenues for hackers and terrorists, who can use drones to carry payloads of any kind. The FAA and other federal regulatory bodies are significantly behind in developing and enforcing regulations to protect vulnerable buildings, and drone operators can easily evade and ignore existing regulations. Data centers and organizations with critical infrastructure must proactively protect their airspace and vulnerable buildings from unauthorized drone activity.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE FOR DATA CENTERS AND CORPORATIONS

Corporations such as Volke, the world's leader in technical development in automobile design, place priority on the protection of their intellectual property. It's paramount to protect assets as they build and test concept vehicles on their outdoor tracks. After successfully integrating on-ground barriers for spies, they started seeing drones with cameras in their airspace. In addition to intellectual property and copyright infringement issues, corporations are also on alert during high-profile meetings, which small details such as identifying the attendees could compromise a business deal. Where telephoto cameras used to be the surveillance tool of choice for investigators and spies, drones are now taking their place due to their accessibility, ease of use, and discretion. Corporations and data centers experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- U.S. federal privacy laws won't necessarily protect you from spying drones: While currently there are laws to protect individuals against people stalking or spying on them in their homes, there are no federal laws in place that would protect individuals from being spied on specifically by a drone.

- Malware lets a drone steal data by watching a computer's blinking LED: An alarming hacking technique has been uncovered, which uses drones to detect vulnerabilities in computers. If a computer is infected, a drone with a camera can be deployed to hover outside a window, and collect data.

CONCLUSION

Drone protection for data centers and corporations is no longer theory – it's a practice in place today since any drone user is capable of causing millions in damages. Drones threaten the physical security of corporations, and consequently, their cybersecurity. With an understanding of the threat that drones pose, as well as a proactive plan in place to protect critical infrastructure, security officers at data centers and corporations will be a significant step ahead of hackers, spies, and terrorists.

VIPS AND PRIVATE PROPERTY

INTRODUCTION

A homeowner's greatest fear is an unwanted intruder and invasion of their privacy and property. Burglar alarms, fences, and locks on doors are deployed in homes across the world to prevent crime and protect families and their belongings. As more drones take the skies in neighborhood parks, playgrounds and rooftops, a homeowner's airspace is now at risk of interruptions and spying.

As much as private individuals want to protect their property, it is a federal crime in the U.S. to interfere with or tamper with a drone in flight. As a drone is classified in the same way as passenger aircraft in the eyes of the FAA, and with many other global aviation regulatory bodies, actors outside of the military cannot strike down or capture a drone. Individuals can take action against spies on their property by integrating a proactive detection program into their existing security system.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE FOR VIPS AND PRIVATE PROPERTY

For individuals whose privacy is constantly compromised, whether through stalkers or paparazzi, drones now provide what a helicopter or telephoto lens cannot - discretion and swift action. When photographs of celebrities and politicians are being monetized, a drone could not just mean a spy is in the air, but their well-being would suffer if they could not enjoy the comforts of their own home and yards. Private individuals experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- Australian television host shares live updates of paparazzi drone in her backyard: After spotting a drone hovering around her backyard, Sydney-based journalist Sam Armytage was proactive on her stance with stalking, and shared with her social media followers, "ANY women's magazines or online gossip sites who buy these creepy pictures, had better be prepared for a fight."

- Champion golfer integrates anti-drone technology to maintain privacy at his outdoor wedding: U.S. Open and PGA Champion golfer Rory McIlroy held an outdoor wedding in Ireland and installed drone detection security to proactively detect paparazzi drones, prevent interruptions, and ensure the privacy of his VIP guests.

- Paparazzi drone following Prince William nearly crashes with his rescue helicopter: Prince William's air ambulance came within half a second of a catastrophic mid-air collision with a remote-controlled drone. The near-miss happened at 1,900ft when the helicopter, with three medical staff and two pilots on board, was flying almost directly over a McDonald's restaurant filled with families.

- Fashion model Kendall Jenner spots drone near home, following a major security breach: In response to a robbery from her home, Kendall Jenner amplified security at her residence. Shortly afterwards, they spotted a 4-rotor drone spying on her and her property.

CONCLUSION

Individuals that react against drones by shooting them down or capturing them could be held liable for damages, and will also be in direct violation of federal law. Few protections exist for homeowners against spying drones, which is why proactive detection is even more critical for security programs. Closing blinds, putting up umbrellas, or moving a party indoors will deter spies and indicate that they are not only unwelcome, but also deem them incapable of capturing intimate moments that they could capitalize on.

FEDERAL GOVERNMENT SERVICES AND MILITARY

INTRODUCTION

Militaries across the world continue to invest in drone technology to survey and conduct strategic offensive measures to protect and defend. The same technology is accessible and being used by politically-motivated terror groups aimed to cause harm to innocent civilians. Because of this, government agencies are turning to drone detection to not only track their own drone traffic, but also identify when an unauthorized drone has entered their airspace.

Militaries have unique legal protections to defend themselves against malicious drones. Unlike corporations, local governments, or private individuals, militaries are able to deploy active defense measures, including jamming, spoofing, or destroying a drone. As such, drone detection can be integrated into a defense system, where if a drone is detected, a defensive measure can be automatically deployed.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE FOR FEDERAL GOVERNMENT SERVICES AND MILITARY

As recently as a decade ago, drone technology was being pioneered in the United States for military use. Today, dozens of countries manufacture and operate military-grade drones, and are developing Drone technology has been made available to private consumers around the world.

Anyone can purchase a drone off of an online retailer, and choose among hundreds of models. Federal government services organizations and global military operations experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- Use of weaponized drones by ISIS spurs terrorism fears: The terrorist group announced the establishment of a new "Unmanned Aircraft of the Mujahideen" unit, a fleet of modified drones equipped with bombs.

- Terrorist drone threat: US unprepared for growing danger, experts say: The emergence of terrorist drones flown by ISIS in Iraq has fueled interest in drone-defense technology – while raising questions about whether the U.S. is ready for potential drone terrorist attacks on the homeland.

- Report published, "A Decade Of Jihadi Organizations' Use Of Drones – From Early Experiments By Hizbullah, Hamas, And Al-Qaeda To Emerging National Security Crisis For The West As ISIS Launches First Attack Drones": The Middle East Media Research Institute (MEMRI) Jihad and Terrorism Threat Monitor Project has been monitoring jihadis' use of drones over the past decade, and has seen their advances in research and development culminating in an ISIS release of a 40-minute video showing its new weaponized drones.

CONCLUSION

Drone technology is becoming more sophisticated and efficient in breaching airspace and buildings, especially as cameras or other hacking technology that can be attached to a drone will advance along with them. There's no question of the threat that drones pose, and proactive detection must be a part of every military's safety and surveillance programs.

LOCAL GOVERNMENTS AND FIRST RESPONDERS

INTRODUCTION

Local governments are taking a crucial role to lead the conversation about integrating technology into city programs, and to create local guidelines on safe and proper use of drones. Municipalities and counties are not only the first resource for creating rules for residents, but also are the leaders of regional airports, prisons, and stadiums. Their concerns for drone safety reach every person and building within their city limits, and it's up to them to decide how and when to integrate drone safety regulations.

Fire and police departments are increasingly relying on drone surveillance to help map out critical situations, search for victims, survey damage, and even apprehend fugitives. These organizations need to ensure that only authorized drones are in their airspace, and civilian onlookers who may want to be a part of the action are promptly identified and alerted to ground their flights.

Local prisons are seeing an increase in contraband deliveries to their property. Even with elaborate security provisions on the ground, including high walls with razor wire and security cameras, the dropping of contraband into inner courtyards during the day or night poses a serious threat to other inmates and prison employees.

TOP NEWS, RESEARCH & ACTIVITY FOR DRONE USE FOR LOCAL GOVERNMENTS AND FIRST RESPONDERS

Local governments are the front line for drone safety and enforcing regulations. The FAA does not have safety inspectors at the local level and depends on law enforcement or private citizens to alert federal authorities to unsafe or potentially unauthorized drone operations. Cities and towns experienced multiple drone incidents firsthand in the first half of 2017, and were involved with the following activities:

- Report published, "Cities and Drones: What Cities Need to Know About Unmanned Aerial Vehicles (UAVs)": The National League of Cities published municipal action guide for local officials, providing insight into federal rules relating to drone operation, as well as offering suggestions for how local governments can craft their own drone ordinances to encourage innovation while also protecting their cities.

- Inmates fly mobile phones, drugs, and porn into jail via drone: While smuggling contraband into prison through any method violates federal law, no statute currently bars drones from flying near correctional facilities.

- Report published, "Domesticating the Drone": Developed by the Institute for National Security and Counterterrorism, this report is a primer of drone rules for local governments throughout the United States, and overview of how different cities are developing drone regulations.

- Drone impedes Arizona firefighters' efforts to battle wildfire: As crews were battling a fire, officials say a drone's presence delayed air crews from putting out the blaze. The National Interagency Fire Center reports that there were 41 drone incursions in the U.S. last year while aerial fire fighting was underway.

CONCLUSION

Local police forces in Hempstead, NY coordinated security for the 2016 presidential debate of Hillary Clinton and Donald Trump at Hofstra University. When VIPs are in town, it's up to the local police force to ensure roads are blocked, emergency services are readily available, and now with the rise of drone activity, make certain their airspace is cleared from drone threats. The City of Hempstead needed all security measures signed off by the United States Secret Service and Federal Bureau of Investigation. The local Nassau County Police Department coordinated the deployment of more than 1,000 police officers. Local sheriff and police departments, such as Suffolk County Corrections, also provide drone detection to their local prisons, as they have seen an increase in contraband deliveries onto their grounds. A single gun, cell phone, or supply of drugs delivered through prison walls could mean the difference of life or death to corrections officers and inmates.

DRONE REGULATORY AND LEGAL NEWS ROUNDUP

INTRODUCTION

An influx of laws and regulations for drone safety have been discussed, proposed, and implemented across all levels of government in the U.S. and globally. The first half of 2017 marked the beginning of groundbreaking proposals for legislation to protect citizens from the unauthorized use of drones and the damage they cause.

- FAA Drone Advisory Committee holds Q1 and Q2 meetings

  In 2016, the U.S. Federal Aviation Administration (FAA) established the Drone Advisory Committee (DAC) to advise the FAA on the needs of new and expanding users of the National Airspace System (NAS). With more drone users in the market, this group, which consists of corporate, academic, public, and government stakeholders in the drone industry, will help develop strategic regulatory priorities and structures that will promote innovation, safety, efficiency, and rapid integration of Unmanned Aerial Systems into the NAS.

  In the Q1 and Q2 meetings of the DAC, an enduring issue was regulating drones that operate Beyond Visual Line of Sight (BVLOS). They are looking to create regulation to protect aircraft and highly populated urban and suburban areas. BVLOS operations are used for drone package delivery, mapping, agriculture, search and rescue, among other applications, and currently require a waiver from the FAA if a pilot wants to operate a drone at such a distance. Due to their size and weight limitations, most drones have limited range and endurance. Significant safety concerns for UAS operations BVLOS include flights over people, detecting and avoiding aircraft, and collision with hazardous or high-risk infrastructure.

- U.S. Circuit Court of Appeals overturns ruling that requires hobby drone pilots to register aircraft with the FAA

  The FAA announced in December 2015 that it would require every person who wished to fly a drone in US airspace pay a small fee and provide their contact information. Failure to do so could result in fines as well as potential criminal penalties. Many hobby drone owners did not agree that the government should put in place such a registration system and sued the FAA. In a win for hobbyists, the U.S. Court of Appeals in Washington, DC found that the FAA's rule forcing registration of drones under 55 lbs is unlawful.

- The Trump administration proposes new rules expanding the powers of the federal government to protect themselves against rogue drones

  It is currently legal for the government to track drones, and this proposal would make it legal for certain government organizations to seize and destroy the drone, as well as search or destroy any data on the drone, without a warrant. The law also expands these rights beyond the military, and extends it to police, firefighters and agencies protecting "covered" areas such as sites of search and rescue operations, wildfires, police investigations, and many other government activities. Agencies would set more specific regulations and procedures, which are supposed to "appropriately protect" privacy and civil liberties.

- A bi-partisan U.S. bill, Drone Federalism Act, is introduced to U.S. Congress

  The Drone Federalism Act would establish a process for federal, state, local, and tribal governments to work together to manage the use of recreational and commercial drones. Under this Act, local municipalities will be able to decide how hobbyists and businesses can operate their drones below an altitude of 200 feet, but also seek assistance from the FAA. It is the latest attempt to make rules that balance between letting people enjoy technology while ensuring public safety.

- E.U. aggressively developing drone regulations to enact by 2019

  Drone-related laws are different across EU countries, and the European Aviation Safety Agency (EASA) is working with member states and the industry to create a common low-level airspace that covers altitudes of up to 150 meters. This space would be governed by a system similar to existing air traffic control management, which will be automated using tools like e-identification and geo-fencing so that the information can always be accessed even by autonomous drones.

PREDICTIONS AND ANALYSIS

OF DRONE DETECTION AND SECURITY FOR THE SECOND HALF OF 2017

INTRODUCTION

Drone safety and detection are two topics that began to rise to the front lines of all concerned drone users, security providers, legislators, and citizens throughout the world. While the first half of 2017 kicked off meaningful conversations, there is a significant amount of data and research needed to inform multiple stakeholders of the risks drones pose. The second half of 2017 will reveal more information on drone incidents and damages, and provide direction to law enforcement, regulators, and legislators on how to best protect high-risk and high-value infrastructure from drone threats.

1 Drone manufacturers and DIY drone enthusiasts will continue to evade and outpace regulators.

The FAA 2017 Aviation Forecast projects:

- Small model hobbyist UAS fleet will triple in size from an estimated 1.1 million vehicles at the end of 2016 to more than 3.5 million units by 2021.
- Commercial, non-hobbyist UAS fleet is forecast to grow from 42,000 at the end of 2016 to about 442,000 aircraft by 2021, with an upside possibility of as many as 1.6 million UAS in use by 2021.
- Pilots of these UAS vehicles are expected to increase from 20,000 at the end of 2016 to a range of 10 to 20 times as many by 2021.

Concerns have been raised across the U.S. regarding the FAA's ability to fund drone programs and support the timely integration of new drone regulations. In the first half of 2017, the FAA was preparing for 2018 and 2019 budgets, but government disruptions, such as sequestration, can impact the FAA's budget and programs. In the second half of 2017, issues related to the FAA's ability to advance drone safety and security-related policies will continue to cause concern, unless they can approve a budget for 2018 that provides robust resources for the rise of the commercial and hobby drone industry.

2 New methods of data collection will further inform the previously unknown risks to unregulated airspace.

As more drone tracking sensors are installed around the world, in line with an increase in sales of consumer drones on the market, there will be an increase in drones being detected and recorded. This information will further advise which industries and individuals are at the highest risk for drone interruptions. Protection starts with an understanding of previously undetected drone traffic. Security officers and individuals will start with the most basic assessment of their risk by integrated drone detection programs on their properties, With new data, business service providers, specifically, insurance companies, will be able to assess the risk of drone threats from a factual, rather than theoretical, basis.

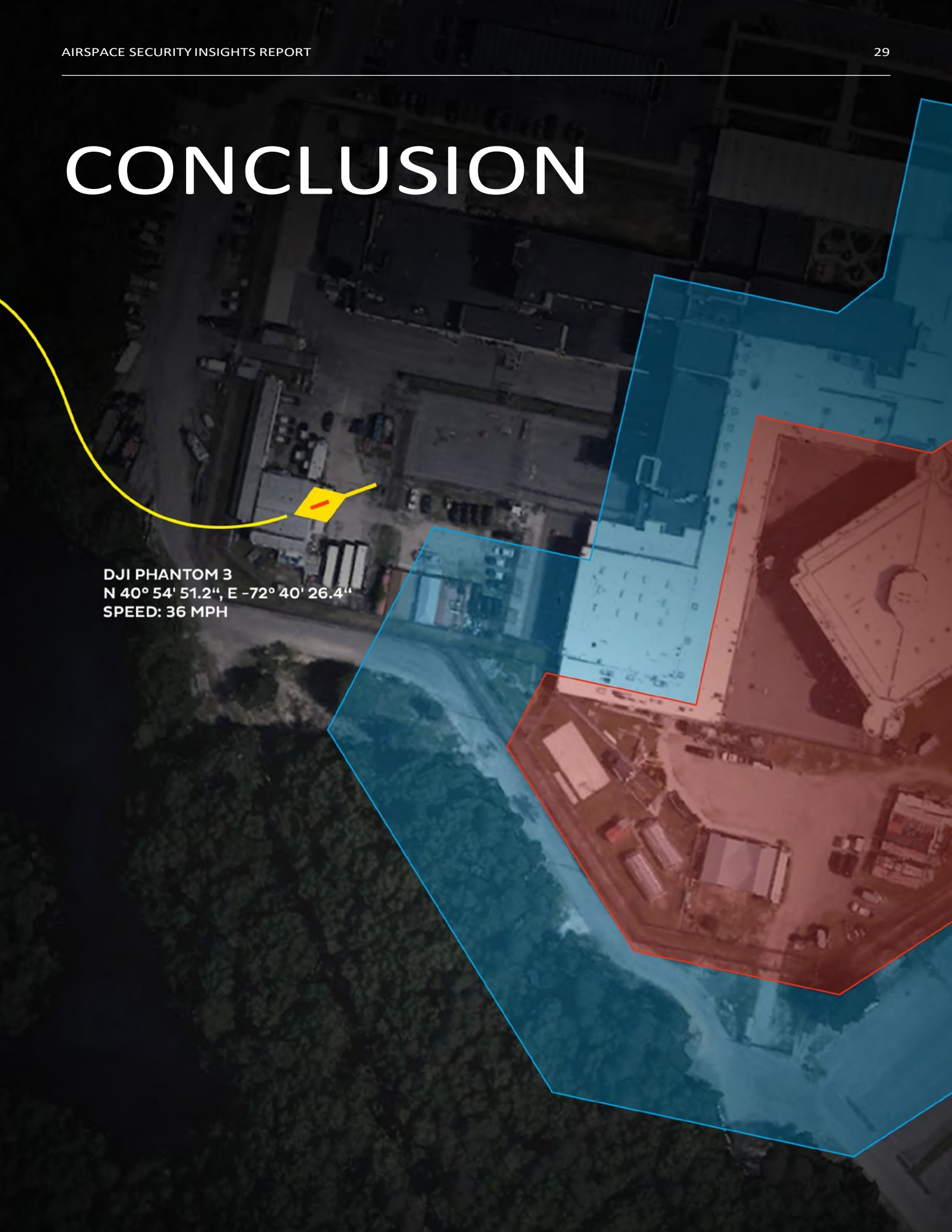
3 New data will inform insurance companies and define the direction of new drone damage and protection programs.

As high-risk individuals and properties are identified through proactive drone detection, insurance companies will be the first to lead the conversation on the costs associated with different types of damages inflicted by a rogue drone. At the top of the list of the risks that insurance providers will consider are data and cyber security. A potential hacker drone could disarm servers, crash into data centers, or otherwise harm and suspend operations. As more drones are detected, and new data appears in the second half of 2017, insurers will have a clearer vision and product offering for corporations, data centers, individuals and other high-risk or high-value infrastructure.

4 Local governments will increasingly enforce anti-drone measures, and there will be an increase in criminal and civil legal actions against pilots who enter unauthorized airspace.

Cities and towns throughout the world are implementing drone guidelines, advising the best places pilots can operate their drones within their jurisdiction. As these local governments continue to roll out new drone regulations, there will also be an increase in enforcement, and they will be highly publicized, to inform the public of the consequences of their actions. In the first half of 2017, pilots have been charged with reckless endangerment at local courts, leading to fines, jail time, and opening the door to civil lawsuits. Personal injury lawsuits will also see an increase in the latter half of 2017.

CONCLUSION



DRONES ARE HERE TO STAY

Drone detection and safety is an emerging market, and is becoming a prominent issue as new regulations and drone incidents unfold.

Drones were first introduced to the public as a military resource, and the technology has since been adapted for widespread commercial and personal use. With the introduction of any new technology, a learning curve exists, and new applications outside of their initial intention unfold as they become more prominently used. Today, drones are continuing to be employed by the military, as well as for agriculture and land surveying, wildlife monitoring, search and rescue operations, for arts and entertainment.

The rise of drones on the market will only open the door for more incidents to occur. In the first half of 2017, the world saw drones carrying contraband into prisons, interrupting firefighters during wildfires, and crashing into people and buildings, causing physical harm and damage. Drones were also being used as surveillance to apprehend fugitives, inspect oil and gas refineries, and locate victims of natural disasters. What was once a technology only accessible to the military, can now be in the hands of any consumer, whether for good or bad.

Use cases for drones are being discovered every day, and regardless of the intention of a drone pilot, a rogue drone can cause catastrophic damage. While laws and regulations can be created, pilots with malicious intent can easily circumvent them. Drones are here to stay, and the U.S. FAA expects millions of more drones to enter the market over the next few years. A fence on the ground has been the default to protect valuable assets, people and buildings. Now, with proactive detection technologies on the market, an aerial equivalent exists. It's up to security personnel, local governments, and private citizens to determine how they want to protect their airspace from drone threats.

Global Headquarters
10874 Plano rd # B
Dallas, TX 75238

Chicago
321 N Clark st
Chicago IL6065

For more information, visit www.911security.com
Contact us drones@911security.com

Published July 2017