Corporate Risk Services

Intelligence Bulletin

Risk Consulting · Software & Technology · Systems Integration · Security Personnel

Drones: Threat from Above

EXECUTIVE SUMMARY

Recent operations in Iraq and Syria clearly highlight the viability of unmanned aerial systems as a legitimate terrorist tactic and one that should be a focus for law enforcement, especially during special event planning. The threat is significant enough to motivate world leaders to address it at the 2016 Nuclear Security Summit in Washington, D.C. Additionally, echoing that concern, is testimony by senior military commanders to Congressional leaders in March 2017.

Commonly referred to as "Drones," these systems may truly be programmable, self-directing fixed-wing or rotary aerial vehicles. However, they are most commonly not true Drones, but small unmanned piloted vehicles which provide positive control and retargeting. Collectively, the term "Drone" is popular mainly due to media coverage of U.S. military operations.

Drone platforms have developed as a significant tool and benefit for public safety and commercial businesses. Likewise, they have also developed as a significant threat. With the increase in use by citizens and private sector, the costs for drones has continued to decrease, making it a viable tool used by criminals and terrorists.

A video released by ISIL's Salah Al-Din province in Iraq in February 2017, showed fighters learning how to weaponize drones in a class. (MEMRI)

The State of Iraq and the Levant (ISIL) formally announced its Drone program in January 2017 on an online propaganda channel. These operations focus mainly on reconnaissance of Iraqi and Kurdish forces. ISIL also uses Drones offensively in attacks with improvised explosives. In Syria and Israel, Hezbollah uses Iranian-supplied vehicles that have greater capability and logistic support. Other terrorist groups and "lone wolves," from jihadists to anarchists and drug cartels, could also use Drone tactics. It is not beyond possibility for legal demonstrations to turn deadly by "black bloc" factions and anti-constitutional infiltrators.

Technology improvements made by manufactures to gain a greater audience now allow for drones to be flown by anyone with little or no experience in aerial flying. Where an active shooter targets crowds that are contained within a set enclosure, a Drone attack can target a wide area of open space.

BACKGROUND

The internet and social media provide unlimited access to motivation, tactics, techniques and procedures for planning several types of terrorist attacks, including aerial Drone attacks. *Inspire Magazine*, the English-language publication of Al-Qaida in the Arabian Peninsula (AQAP), is a major media venue for several recent terrorist attacks in Europe and the United States. Following in the footsteps of its parent Al-Qaida, ISIL has also proven effective in their use of the internet and social media. ISIL main messages have been to join the battle in Iraq and Syria, or kill westerners in the home country and encouraged "lone wolf" operations.

Expanding its online media channels, on July 19, 2016, a channel titled "Inspire the Believers!" on the Telegram encrypted application was used to motivate Drone attacks at the 2016 Rio Olympics. In September 2016, ISIL began internet publishing of Rumiyah Magazine, the online version of ISIL's glossy magazine Dabiq and a mirror of Al-Qaida's Inspire. However, where Inspire provided guidance and motivation, Rumiyah has shown that it builds upon lessons learned from recent attacks and provides more specific tactical details for attack planning and execution. On Jan. 24, 2017, ISIL formally announced its Drone program with a picture on Telegram and continues to use it as an additional online propaganda channel.

Although not always related to terrorism, the following timeline of incidents for use and attempted use of Drones illustrates a developing and growing understanding of the feasibility for their weaponization:

Drone-Use Timeline

- Pre-June 1994, Japan. Aum Shinrikyo, using Remote Controlled Helicopters, attempted Spray Chemical Agent (Sarin). It crashed during testing.
- Pre-July 2001, Genoa, Italy. Osama bin Laden, al-Qaida Leader using Remote Controlled Airplanes for improvised explosive device (IED) attack on G8 Summit Leaders. Considered Only; Not Attempted (Alleged).
- Pre-February 2002, Pakistan/UK. Moazzam Begg, an al-Qaida terrorist, planned to use a Drone launched from Suffolk, UK with Anthrax against House of Commons. Sent to Guantanamo Prison and released in January 2005.
- June 2002, Not Specified. Al-Qaida using Remote Controlled Airplanes for IED attack on Passenger Airliners. Considered Only; Not Attempted (Alleged).
- August 2002, Colombia. FARC maintained nine Remote Controlled Airplanes for unknown, possibly weaponized IED use. Recovered by Colombian army unit at a remote camp.
- December 2002, Jerusalem, Israel. Fatah maintained hundreds of Model Airplanes for IED attacks on Jewish sections of Jerusalem. Conducted flight tests only.
- August and December 2003, Gaza, Palestine. Hezbollah Cell linked to Al Aqsa Martyrs Brigades; Fatah planned a UAV for IED attack on Jewish settlers in Gaza. Interdicted by Israeli Security Forces.
- Nov. 7, 2004, Nahariya, Northern Israel. Hezbollah Iranian Mirsad-1 Drone conducted a 20-minute reconnaissance mission. The vehicle either crashed in the sea near Lebanese shore or returned to the Hezbollah Base.
- April 11, 2005, Acre, Northern Israel. Hezbollah Iranian Mirsad-1 Drone conducted an overflight of Israeli communities (Stated as a Protest of Lebanese Airspace Violations). Successful Operation; Returned to the Hezbollah Base.
- Sept. 13, 2005, North Waziristan, Pakistan. Al-Qaida using a Chinese made Remote Control Model Airplane conducted a reconnaissance of Pakistani security forces prior to attack. Also, a weaponized (IED) Model Airplane was seized by the Pakistani Army in a raid of an al-Qaida hide site.
- Sept. 14, 2005, Fairfax County, Virginia. Ala Asad Chandia (Abu Qatada), trained by Lashkar-e-Taiba, obtained an MP 1000SYS Electronic Automatic Pilot System for Model Aircraft in April 2002 for Lashkar-e-Taiba terrorist group Drone use in Pakistan. He was indicted and subsequently convicted.
- Aug. 13, 2006, near Tyre, Lebanon, Haifa, Israel and Western Galilee, Israel. Hezbollah used three Ababil Drones, each with a 40-50-kilogram warhead attacked "Strategic Targets." All three were shot down by Israeli F-16 jets.

Drones: Threat from Above

Corporate Risk Services

- 2006-2007, Columbus, Ohio. Christopher Paul, trained by al-Qaida, using a five-foot long model helicopter, conducted Drone research for terrorism purposes. Arrested by FBI and convicted on a Plea in 2008.
- January 2009, Kent, United Kingdom. A Drone carried narcotics into Elmley Prison in Sheerness.
- February 2011, Moscow, Russia. A Drone carrying heroin was captured going into a prison in the Tula region.
- Sept. 28, 2011, Ashland, Massachusetts. Rezwan Ferdaus (al-Qaida radicalized), in an FBI sting operation to acquire scale Models of F-86 Sabre and F-14 Phantom Jets with GPS capability and C-4 Explosive for IED attack on the Pentagon and US Capitol Buildings. Arrested by FBI and convicted on a Plea in 2012.
- November 2011, Spain. A Drone was used to carry drugs coming across the Strait of Gibraltar into Spain.
- May 19, 2012, Helmand Province, Afghanistan. Taliban recovered a NATO Desert Hawk Drone for unknown use/possible reconnaissance. System was found with IED materials captured in a raid.
- Oct. 6, 2012, Dimona, Israel. Hezbollah Iranian Ayoub Drone conducted reconnaissance of Israeli nuclear weapons complex and military exercise preparation. Shot Down by Israeli F-16 jet.
- January-December 2013, Quebec, Canada. Drones going to various prisons flew narcotics into prisons.
- April 22, 2013, 10 kilometers over the sea west of Haifa, Israel. Hezbollah flew an unspecified unmanned Drone on an unknown mission. Shot down by Israeli F-16 jet at an Altitude of 6,000 feet.
- October 2013, West Bank, Palestine. Hamas plot centered at Hebron University to place explosives on a UAV and fly into Israel to engage unknown target(s). Palestinian Authority arrested plotters prior to launch.
- November 2013, Calhoun, Georgia. A Drone was used for smuggling cigarettes into a U.S. prison. Other contraband and drugs are suspected.
- March 2014, Melbourne, Australia. A Drone flew narcotics into a prison.
- May 2014, Kaliningrad, Russia. A Drone was successfully used to smuggle cigarettes into the region.
- July 14, 2014, Ashdod, Israel. Hamas flew a five-foot-long homemade Drone aircraft with small rockets into Israel to engage unknown target(s). Shot down by Israeli Patriot missile.
- Aug. 23, 2014, near Raqqa Province, Northern Syria. Islamic State flew a DJI Phantom FC40 Quadcopter on reconnaissance of Syrian Army Military Base 93 prior to a ground assault. Successful Operation. Imagery was provided via IS propaganda video on YouTube.
- Aug. 30, 2014, Falluja, Iraq. Islamic State flew an unspecified Drone for propaganda purposes. Successful Operation with video of attacks in the city.
- Sept. 12, 2014, Kobani, Northern Syria. Islamic State flew an unspecified Drone for propaganda purposes. Successful Operation with video of suicide and ground attacks.
- Sept. 21, 2014, near Arsal, Northeastern Lebanon. Hezbollah armed Drones attacked and killed 23 al-Nusra Front (al-Qaida linked) fighters at a Base, followed by ground assault. Successful Operation.
- Jan. 20, 2015, Tijuana, Mexico. A Chinese-made "Spreading Wings 900" Drone was found by Tijuana Municipal Police near the San Ysidro, California crossing with a payload of heroin.
- Jan. 26, 2015, Washington, D.C. At 03:00 am, a commercial quadcopter piloted from an apartment building several blocks away, crash landed on the White House grounds.
- March 16, 2015 (approx.), near Fallujah, Iraq. Islamic State flew an unspecified Drone on a possible reconnaissance or propaganda mission. Operator and Drone destroyed in a car by U.S. Coalition air strike.

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310

- April 2015, Calexico, California. A Drone operated by a Mexican Cartel crossed the U.S.-Mexico border. The Drone delivered a payload of 30 pounds of heroin.
- February-April 2016, Bangor, Washington. Multiple small unspecified Drones overflew Naval Base Kitsap-Bangor, during the day and night, where eight U.S. nuclear missile submarines are homeported. Investigation open with no determination.
- June 2016, Columbia, South Carolina. Multiple unspecified Drones were detected on several occasions flying over the Savannah River Site nuclear arms complex. FBI agents questioned an anti-nuclear activist about the flights. Investigation open with no determination.
- July-August 2016, Brazil. Islamic State on a Telegram Group encouraged followers to attach bombs to small Drones and attack the Rio Olympics. With assistance from the FBI, Brazilian Federal Police arrested 10 people for plotting a terrorist attack at the games. No attempted attacks in Rio were reported.
- Oct. 2, 2016, Northern Iraq. Islamic State flew an unspecified Drone to attack Kurdish forces. Kurdish forces reportedly grounded a small Drone on the battlefield and brought it back to their base to examine it. When they began to dismantle it, a small but sufficiently powerful explosive hidden inside and disguised as a battery exploded killing two Kurdish soldiers and wounding two French paratroopers.

According to the Federal Aviation Administration (FAA) there were over 2.5 million Drones purchased in 2016 in the United States. Annual sales are predicted to reach 7 million by 2020. Additionally, the Center for New American Security estimates that …"90 countries have reconnaissance/surveillance Drones, with at least 30 countries in various stages of developing armed variants ... "

In March 2017, Inc. Magazine reported that since late 2014 the FAA issued over 5500 exemptions for nonpilots to fly Drones for primarily commercial purposes. While many of these exemptions were for hobbyists, news media, commercial use (i.e. Amazon), even more people are using drones without approval by FAA.

DRONE WEAPONIZATION — TACTICS, TECHNIQUES AND PROCEDURES

The intent and effect of a Drone attack are comparable to an active shooter or wheeled vehicle attack in that they both can easily kill and injure as many people as possible unless stopped. Therefore, using a Drone would offer a wide variety of target-rich environments. This is particularly the case if coordinated with a vehicular or active shooter attack. Although procurement of an aerial vehicle is easy and relatively inexpensive, the major logistical limitation for terrorists was commonly believed to be access to appropriate explosives. However, limited only by imagination, the payload may be any dangerous chemical, poison, radiological, incendiary or explosive device within the increasing payload weight of modern Drones. Their use within a public venue can spread fear, panic and distrust of law enforcement's capability to protect the public that is more than sufficient for propaganda purposes. When combined with an active shooter scenario, it will significantly increase the effect.

On March 28, 2016, the Small Wars Journal reported government concerns of Drone use over the U.S.-Mexico border related to terrorist operations. "Of concern are future Mexican cartel UAV evolutionary potentials related to a) sensor payload use for reconnaissance and surveillance functions and b) weapons payload use for small arms and IED attack capabilities." There were an estimated 150 UAV intrusions across the border from 2012 through 2014. The implied capability is a collaboration of Cartels with transnational terrorist groups like ISIL and Hezbollah.

During the 2016, Nuclear Security Summit held in Washington, D.C., on March 31 and April 1, 2016, the threat was considered critical by leaders from 54 nations, the European Union and Interpol. Then British Prime Minister David Cameron warned attendees that "the dangers of the Islamic State of Iraq and the Levant getting a hold of nuclear material was "only too real." Prime Minister Cameron went on to warn that "Islamic State terrorists are planning on using Drones to spray nuclear material over Western cities in a horrific 'dirty bomb' attack…we have already seen Daesh (ISIL) trying to look at whether they can get their hands on low-level, crop-using [dusting]-type Drones."

The concern is driven from, not only readily available unmanned aerial systems, but also readily available nuclear material to weaponize a Drone. On April 1, 2016, Bloomberg News reported that "at least 130 countries have radiological material stored at such places as universities, hospitals, companies, and research centers," that could be used to construct a dirty bomb.

Evidence of the acquired 90 pounds of uranium from the University of Iraq would likely cause fear and panic if used more than illness, and that may be sufficient for propaganda purposes. However, of greater significance, a July 2015 report from the Government Accounting Office showed weak acquisition controls of radioactive material in the U.S. and stated, "an attack that involves relatively low-level radioactive material from a U.S. facility is more likely to be successful than an attack using imported material because the chances of detection are so much less."

In a highly unusual move for the 2016 Nuclear Security Summit, leaders took part in tabletop exercises to plan responding to such an event. One scenario U.S. officials briefed to the attendees was radioactive material taken from a medical facility by "insiders" then sold to Islamic terrorists on the "Dark Web."

Since 2010, following an Inspire article, the Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) have increasingly focused on asymmetric use of commercially acquired equipment and materials in attacks on the Homeland, especially by small cells of "clean skin" operators or a "lone wolf." Such attacks would target locations where large numbers of people congregate, including sporting events, entertainment venues, or shopping centers.

ISO 28001:2007, Security Management Systems for the Supply Chain alludes to this in a supply chain threat scenario (The threat will intrude and/or take control of an asset (including conveyances) within the supply chain). Application examples include:

- Damage or destroy the supply chain asset
- Damage or destroy an outside target using the supply chain asset or goods
- Cause civil or economic disturbance
- Take hostages or kill people

On Dec. 28, 2016, addressing an operational shift in tactics (following the Berlin wheeled vehicle attack), the National Counterterrorism Center (NCTC) reported "a significant shift in terrorist tactics that requires intelligence and law enforcement agencies to locate mobile and cyber/ internet smart "lone wolf" individual attackers, not necessarily detect a detailed and complex plot." It is logical and prudent to assess that operational shift additionally applies to the use of Drones.

The report further states that, "increase of individual attacker operations coincides with the deepening and broadening of the digital revolution as well as the encouragement of such operations by terrorist groups because intensified [counterterrorism] operations have disrupted their ability to launch larger plots ... Lone actors now have greater capability to create and broadcast material than a decade ago, while violent extremists can contact and interact with potential recruits with greater ease."

NCTC analysis identifies a shift in extremist violence to "small autonomous cells" and "individual terrorism." Increasingly, thanks in part to the digital revolution, they can rely on what Syrian terrorist Abu Musab al-Suri called 'individual terrorism' and published in a training guide titled A Call to Global Islamic Resistance. Indicators show that with ISIL losing territory and al-Qaida increasingly decentralized, individuals and small autonomous cells may increasingly take the initiative in both the murderous and messaging dimensions of violent extremism."

On March 8, 2017, General John E. Hyten, commander of the U.S. Strategic Command, revealed the Drone threat in written testimony before the U.S. House Armed Services Committee:

"Of recent concern have been the unauthorized flights of unmanned aerial systems (UAS) over Navy and Air Force installations. These intrusions represent a growing threat to the safety and security of nuclear weapons and personnel." He stated that currently the Navy and Air Force are planning to deploy counter-unmanned aerial system defenses that "effectively detect, track and, if necessary, engage small UAS vehicles."

With growing technical knowledge, reduced cost and availability, Drones may become the new IED, useful in many different scenarios, and limited only by imagination for its target and weapon payload. It is a threat that is getting more complex, sophisticated and difficult to confront.

ATTACK SCENARIOS

Complicated attacks can be planned with increased time and assets. However, the more complicated the planning is, then the greater the chance of discovery and interdiction. Drone attacks are more asymmetric and scalable to the individual "lone wolf."

As with traditional violent crime, Drone attacks can be classified by major profiles of "organized" and "disorganized" that provide indicators of the nature of the individual(s) involved and extent of the support structure.

Organized

- Organized previously planned attacks against known events
- Motivation/radicalization is well developed over time within a mutual support group/ mechanism
- Security is paramount, due to the scope of planning and coordination involved
- Requires communications, logistics and detail coordination
- Study target area, route reconnaissance, timing, possible rehearsal
- Selection of aerial vehicle(s) must be made for reasons that are feasible to avoid suspicion
- Acquisition of aerial vehicle(s) requires proper timing to avoid early discovery and may be stolen prior to an attack
- Modification of Drone(s) may be required, depending on radio frequencies, the target area and route, and should be accomplished in a manner to avoid early discovery. This may require additional logistical planning for a test facility with equipment
- Additional equipment/weapons, such as body armor and firearms are desired and may be available, but must be acquired in a manner to avoid suspicion
- Legacy material (written or recorded) announcing one's allegiance is produced at a time just prior to attack to avoid early discovery
- Early discovery is possible and will result in sufficient warning and interdiction, even with individual "lone wolf" attacks

Disorganized or Impulse

- Disorganized attacks are typically unplanned events and impulsive in nature
- Conducted by an Individual "lone wolf" who may not have a previous record of arrest or troublemaking
- Psychologically or event triggered by impulse driven core beliefs of motivation/radicalization
- Little or no planning; related to being psychologically or event triggered by impulse
- Acquisition of aerial vehicle and control unit that is familiar with pilot/control experience
- Known target area, route, timing
- Possible additional equipment/weapons, based on known availability
- Possible legacy material (written or recorded)
- No warning
- Hard to identify and stop, ultimately relies on first responder direct action

Inspire and Rumiyah, enabled by the mass distribution of the internet, remains an effective groundwork for Islamic propaganda, terrorist planning, recruitment and motivation with a new focus on the "lone wolf" as an asset "to wage their individual jihad." Taken together, Inspire, Rumiyah, the Telegram channel and readily available online and academic technical expertise can provide an effective and feasible operational concept for Drone attacks.

OBJECTIVE AND TARGET SELECTION

The Inspire/Rumiyah general guidance for attacks emphasizes the importance of defining the objective. An attack may be to achieve a small to medium kill count; disrupting the financial stability of a specific nation, or simply be aimed at "terrorizing the enemies of Allah and depriving them of a peaceful sleep."

When deciding on the target, attention will be given to the target's accessibility by the Drone for inflicting maximum damage. It is not important to target gatherings restricted to government or military personnel only. If attacked, public events that have little if any U.S. Government involvement or relation to U.S. Foreign Policy would be considered would be more devastating and damaging to the morale and perception of the public in the United States.

In general, applicable targets are any outdoor attraction that draws large crowds:

- Large outdoor conventions and celebrations
- Pedestrian-congested streets (High/Main streets)
- Outdoor markets
- Festivals
- Parades
- Political rallies

Buildings normally require a significant explosive to be deadly effective. For that reason, the building target would be more for symbolism and propaganda.

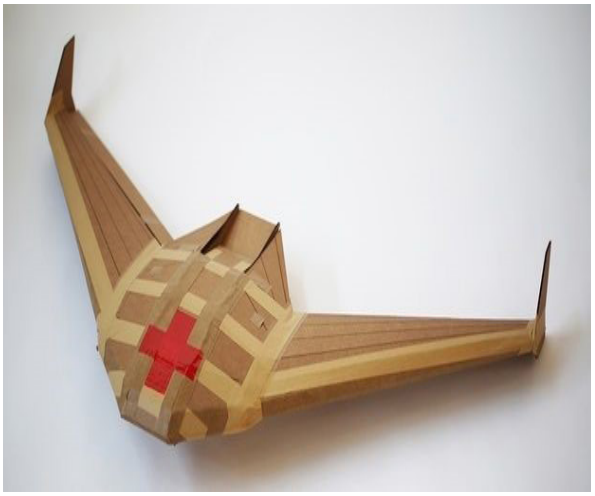
DRONE SELECTION

Based on the low-cost for drones and ease of purchasing drones, there is no need for an adversary to recover the drones after use. They are designed and configured for a single mission, a one-way trip by a radically focused operator/

pilot who may be prepared to die. Additionally, an aerial surveillance Drone may be used for recording propaganda video and conducting route reconnaissance or rehearsal prior to the attack Drone employment.

Drones can be easily purchased online or from numerous hobby or electronics stores without the need for theft. Previously, the limiting factor was believed to be payload capability, with a concentration on military grade explosives. However, as proven repeatedly, asymmetric planning and adaptability are a trademark of Al-Qaida and ISIL. Additionally, as terrain is denied to terror groups in Africa and the Mideast, reliance on radicalization and recruiting of "homegrown" cells and individual assets will increase. Multiple models are available and can be utilized by an adversary with little knowledge or training needed. The advancements in radio controlled devices, GPS, video, flight duration times, controllability and damage resistance all make current iterations of drones more reliable that previous versions over the years. Although most hobby Drones carry around 5-10 pounds of weight, payload weights of 25-30 pounds on small commercial Drones already exist and are improving. Operating times average 30 minutes, but are increasing.

The Chinese made Spreading Wings 900 Drone (pictured on left) was recovered by Tijuana Municipal Police on Jan. 20, 2015 near the San Ysidro border crossing in the Zona del Río. The model is typically used for photography, but when found, it was being prepared with a payload of approximately 20 pounds of heroin. The loss of a Drone is considered minor compared to Cartel drug profits. There are numerous rotary systems of similar design with greater capability.



The Apsara Drone (pictured on right) by Everfly, a division of Otherlab, is intended as a commercial emergency medical delivery system. Initially designed as a "disposable" glider dropped from a plane, it is constructed of corrugated cardboard and tape for field assembly. The Drone can carry a payload of two pounds but can be scaled for 22 pounds and contain tiny controls for two wing-flap motors and GPS to bring it within 50 feet of a preprogrammed landing spot. A ground-launch system is similarly possible.

Other fixed-wing and rotary models are both gasoline fueled and battery powered. Battery power will provide more stealth and possibly easier to hide and control within a congested/urban area.

PLANNING AND PREPARATION:

As possible and based on individual experience, planning will be with a military mindset, possibly based on previous military training. Selection of controller/pilot(s) will be based on technical ability, however, the main determining factor is assessed individual motivation (radicalization.) Preparations will include:

- Choosing the right drone
- Fueling or charging the drone
- Selecting the best route to fly

- Surveillance of flight route to see if there are any obstacles to be avoided, such as power lines, cranes, new construction, etc.
- Maximum effect can be achieved when coordinated with a ground attack, such as a vehicular attack or active shooter attack

Rumiyah advises that an appropriate way should be determined for announcing one's allegiance to the "Khalifah of the Muslims and the goal of making Allah's word supreme," so that the motive of the attack is acknowledged. An example of such would be simply writing on dozens of sheets of paper "The Islamic State will remain!" or "I am a soldier of the Islamic State!" and launching them from the vehicle's window during the execution of the attack.

COMMON SECURITY MEASURES

An interpretation of federal law by the FAA prevents security personnel from shooting down a Drone over a sensitive area. However, the December 2016 passage of the Fiscal Year 2017 National Defense Authorization Act included the stipulation, "if a Drone threatens any nuclear facilities, missile defense or national security space mission facilities, the Secretary of Defense has the authorization to 'use reasonable force to disable or destroy' the Drone."

Agencies are now addressing approaches to "reasonable force." Stopping Drone attacks is possible with advanced assessment and planning. While human detection of aerial vehicles has been done before, the diminished size of drones makes visual detection alone near to impossible until the drone is over a target. The best countermeasure remains electronic detections, as the use of electronics can establish processes for:

- Alert
- Acquisition
- Classification
- Neutralization

The first step is always to do a threat analysis. A rapid assessment of Drone intent and capability is required based on the potential risk to life, property and business assets or information. A Drone doesn't have to be a threat to life or causing damage but may be carrying a HD camera for surveillance or stalking.

The next step is to select countermeasure solutions for Drone detection, classification, and neutralization (interception). Due to the stealth and speed of Drone systems, the process must be rapid with positive control and reporting. Procedures similar to an "Active Shooter Alert" are both appropriate and required.

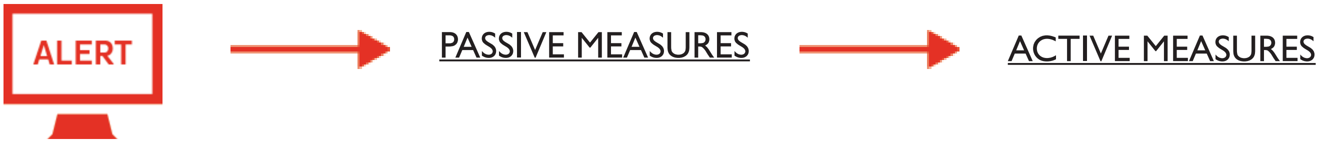
After a Drone incident, it is important to investigate the background of the incident and to share the incident data with appropriate authorities and interested parties.

Indicators

A single indicator may not be suspicious; however, multiple indicators can indicate a Drone attack is being planned. A Drone attack can be conducted with little to no warning. Examples of potential indicators are:

- Unusual modifications to aerial vehicles.
- Unease by purchaser when buying drone or asking detailed questions not normal for a hobbyist
- The use of drones over non-photographic areas, industrial or offices
- Attempts to overfly or infiltrate closed areas where traffic usually moves, but where crowds are gathered, such as for street festivals or farmers' markets.

Drone countermeasures are classified as "passive" and "active."



ALERT → PASSIVE MEASURES → ACTIVE MEASURES

Passive Measures: Personnel are the likely target. If possible, remove them from the Drone's targeting and weapon acquisition while the Drone is being classified as friendly or hostile. Typically, the type of weaponization of the drone will be unknown and/or discovered afterwards, therefore safe zones should be established that are hardened with self-enclosed HVAC systems. If a drone is spotted over your facility, the following steps should be taken immediately:

- Inform security immediately
- Lead people to safety as quickly as possible
- Block the view of the Drone
- Lock doors and gates until the situation is stabilized
- Search site for dropped objects

Active Measures: Commence neutralization (interception) by electronic and/or physical interdiction means. These measures include:

- Jammers
- Electromagnetic Pulse
- Lasers
- Physical Measures
- Investigate what was being surveilled

Counter Drone Systems

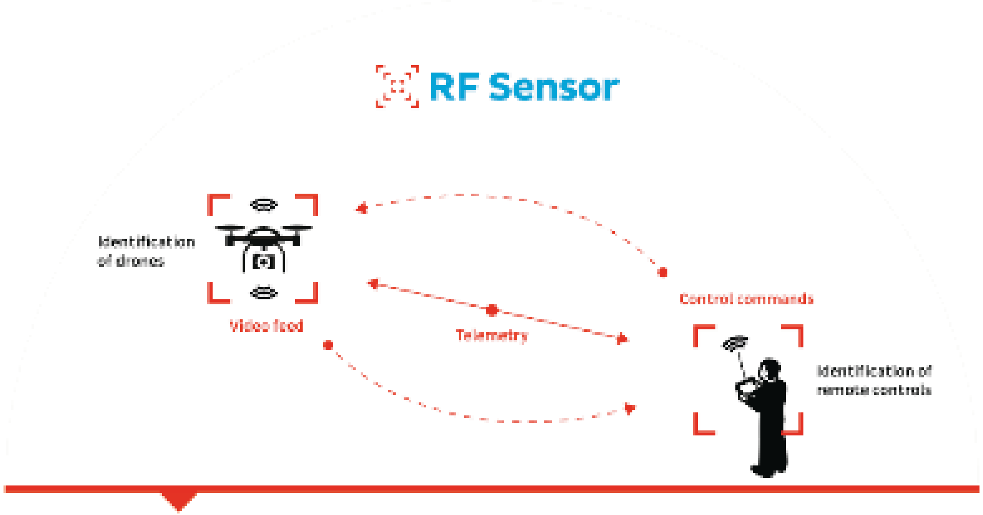
Regardless of whether measures are passive or active, the "Alert" involves identification and acquisition and classification for targeting and eventual neutralization. Typically, a counter Drone system has several electronic components.

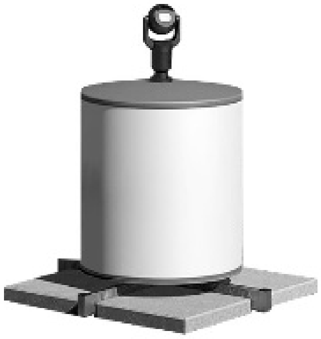
RF Sensor

RF sensors constantly search a wide frequency band and classify and decode signals, so users get early warnings, often before Drones are even in the air. There is a capability to recognize specific Drone radio signatures so that a large number of Drones can now be identified according to their manufacturers and even individual models.

Almost all commercially available drones typically use radio signals to send and receive electronic commands from the radio receiver. Some systems have significantly improved the performance spectrum of their RF sensors to detect these radio signals. The greatest benefits for operators are:

- Increased detection range
- Early detection of switched-on remote controls
- Reliable detection and identification of Drones





Drone Detection Radar

The Drone Detection Radar (DDR) is specifically designed to detect drones in both low visibility and city environments. The radar system should cover a full 360 degrees' view. It detects larger fixed-wing targets at a range of 5-6 miles (9.5 km), and smaller multi-rotor Drones detected at up to 2 miles (3.2 km). However, completely securing an area requires more than just range detection. It requires flexibility, reliability and provides unlimited coverage through its ability to combine multiple radar devices into an integrated sensor network. The output from multiple sensors is incorporated into one unambiguous picture.

Modular UAV Jamming System

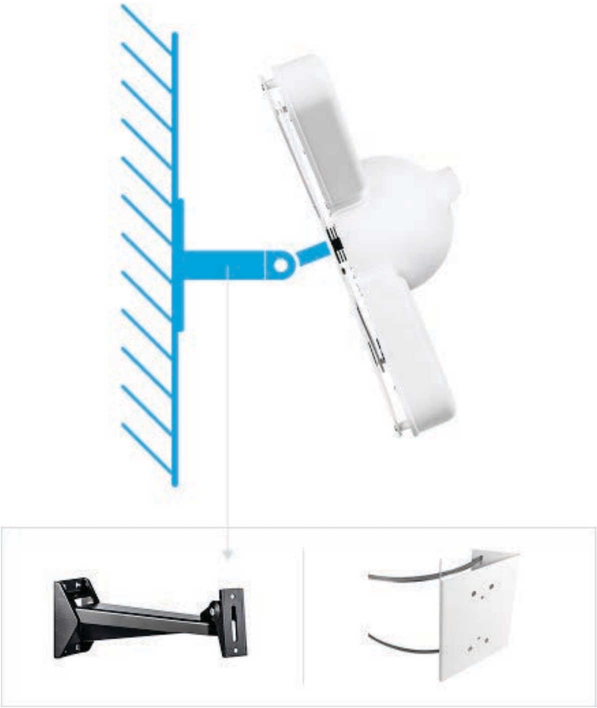
The jammer system uses a direct digital synthesis (DSS) sweep and dedicated software enabling the operator to program the system quickly using a Windows-based notebook or USB stick in order to adapt to any given threat scenario or use the system as tactical jammer. The jammer system should jam Drones using GPS, GLONASS, Galileo, WLAN 2.4 GHz and from 5000-6000 MHz.

Accessories:

- Omni directional antenna set
- Modular system (Upgradable)
- Notebook computer
- DDS controller software for dedicated system programming

Multi-Sensor

A multi-sensor component collects different types of electronic signatures. It is mounted permanently to facades of buildings or special poles, in order to survey a defined section of the sky. For mounting the multi-sensor, there are different mounts.



Typically installed for the permanent use at:

- Prisons
- Industrial facilities
- Government facilities
- Embassies
- Nuclear power plants
- Private buildings

The Sensor Suite should include:

- Audio/Ultrasonic

Acoustical sensors
Microphones have a reach of 50-80m. Civilian UAV's have typical acoustic characteristics that can be used for their reliable detection.

- WLAN

Wi-Fi sensor
An integrated Wi-Fi-sensor detects the WLAN signals of Drones. It also allows the identification of certain Drone models and even individual devices.

- Near Infrared

Optical sensor (night)
The system can be equipped with an infrared camera. The data is interpreted by means of enhanced image analysis methods.

- Video / 10°–90°

Optical sensor (daylight)
Each system is equipped with a daylight camera. Enhanced image analysis functions should be used to analyze the live video feed.

CCTV and Video

Additional closed circuit TV and video capture of a Drone target can be added in target acquisition and identification. Drone detection, identification and countermeasures platforms are customizable. Cameras should be pan-tilt-zoom (PTZ) capable.

Mobile Event Kit

An Event Kit packages the component system for mobile temporary use to provide early Drone detection at VIP visits, public conventions, concerts, sporting events, etc. An Event Kit normally comprises tripods to which you can flexibly mount a multi-sensor tracker or RF sensor and scan anywhere. Several of the mobile Event Kits were deployed for security support during the 2016 U.S. Presidential Debates and 2017 Presidential Inauguration.

Man-Portable Systems

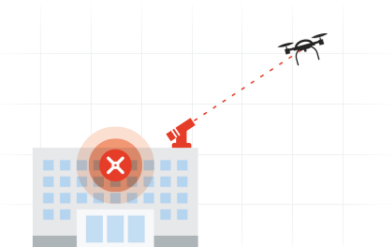
A manned portable Drone jamming system in a shotgun configuration is designed to beam radio linkage between a UAV and the operator with consequent safe landing of the intercepted Drone. There are several versions, however, the main operational characteristics are the portability, accuracy, and ease to handle of the "point and shoot" gun. The systems are deployed in Iraq against ISIL.

Physical Systems

Many facilities with access to dedicated water cannon or fire truck-mounted water systems, such as airports, use them for close-in counter Drone contingencies. The Drone collides with the end of the spray from a water cannon.

The French Air Force and Netherlands National Police are the first in the world to use birds to hunt and catch Drones that are being used illegally. Eagles are trained to attack Drones that fly near nuclear power plants, airports, and official government buildings.

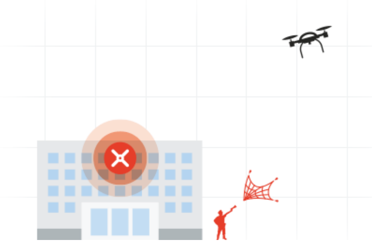
For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310



Other Systems

Fire Arms, Electromagnetic Pulse (EMP) and Lasers, although effective, have significant disadvantages. All are effective only at low range, subject to approval, and Drone crash poses risks, especially in cities. Firearms are not recommended for neutralization, especially in urban, residential and highly populated areas. Both safety and legal restrictions apply and accuracy can be questionable.

A Net Cannon/Gun shoots a net over the Drone from the ground to drag it down. The disadvantages are it is only effective at short range/low altitude. It has a low success rate.



SECURITY RECOMMENDATIONS

The shape of terrorism has changed since Sept. 11, 2001. Al-Qaida and ISIL have adapted tactics from necessity and have tapped into a virtual unlimited talent pool for recruiting jihadists. Not only can they recruit fighters for the conflict areas of the Middle East and North Africa, but also expand globally to bring the war to formerly denied regions and conduct propaganda operations for psychological warfare. Within the context of global Islamic radicalism, terrorism is now becoming more individual in nature.

The new paradigm is one with few boundaries, where small cells can form wherever resources permit and circumstances allow. Technology permits active militants to become individual terror promoters who provide a motivational path to terror and instruction to others in tradecraft and tactics. Additionally, some militants have been allowed migration into Western societies for politically naïve and humanitarian reasons without means to investigate and assess their backgrounds. The modern terrorist is, therefore, hard to detect, much like the truck terrorists in Nice and Berlin in July and December 2016.

He will hide in a closed community, use personal resources, strike in an unexpected way and then may try to disappear into society, but will be radicalized and motivated to the extent he will be willing, if not desire, to die in martyrdom. This potentially puts every citizen on the frontlines of a war that has come to them.

Additionally, the vast and growing availability of Drone technology adds an aerial dimension to a threat that has not been seen since the high-jacked commercial aircraft of Sept. 11, 2001.

To protect against this new paradigm, the following basic security measures are recommended for consideration:

- Conduct background checks and social media checks of all controllers/pilots and employees who have access to unmanned aerial vehicles and control technology
- The public must have a basic understanding of the psychological mindset of a dedicated attacker. Especially with radical Islam, the attacker is prepared for or looks forward to dying
- Reassess the daily work environment based on the geographic location and developing events.
- See something, say something/report it
- Businesses should review and rehearse emergency and security plans. Many businesses operate Drone fleets as part of their core business to supply and deliver goods and conduct emergency and geological surveys. Given the terrorist

attacks in the Mideast and published direction to radicalized individuals, the security of aerial vehicles, equipment and control frequencies and the safety of the operators and technicians must be considered.

- Businesses should coordinate information sharing and local safety/security measures with Public safety agencies to prepare for events and guard against criminal and suspicious activity
- Businesses should verify the identity of persons controlling, piloting and maintaining company aerial vehicles and their documents and use E-verify where appropriate. Additionally, businesses should include situational awareness as a component of company safety orientation with periodic updates to all persons with access to aerial vehicle equipment and technology
- Conduct risk assessments and select pre-determined lowest threat routes for aerial missions
- Geo-fence all pre-planned routes to provide alerts at the monitoring center whenever an aerial vehicle varies from its designated route
- Aerial vehicles should be equipped with GPS tracking equipment
- There should be a redundant policy and plan, such as GPS, communications, and capability for the monitoring center to communicate with an operator or pilot
- The GPS/Security monitoring center should have the capability to remotely activate disabling equipment
- Monitor parking areas for possible surveillance and/or operations by a hostile controller/pilot

If sighting a flying Drone in an unauthorized area or conducting suspicious operations:

- Notify law enforcement.
- If possible, make a note and provide:
  - Location - direction the Drone is flying, where it is coming from
  - Date and time of sighting
  - Detailed description of the Drone (i.e. size and color, number of propellers, color of lights, etc.)
  - If possible, take a photograph or video

If present during a Drone attack:

- Give immediate warning to surrounding pedestrians and notify law enforcement at first opportunity
- Immediately move out of the line of movement. Run at a right angle away from the Drone and try to put objects such as buildings, trees, powerlines between yourself and the attacker
- Do not run with the crowd. Attacking Drones intend to target large groups
- Seek hardened shelter until "all clear" is announced
- Provide emergency medical care, if possible

For more information:
corporaterisk@usa.g4s.com • www.g4s.us • 1-800-275-8310