G4S Academy

DETECTING AND COUNTERING DRONE INTRUSIONS

PART TWO

TABLE OF CONTENTS

1. INTRODUCTION

We have created two guides on Detecting and Countering Drone Intrusions. This guide is part 2 and focuses on the different technologies, threats and risks as well as neutralisation. This guide is a more complex and in depth look at the topic, so for a simpler introduction and overview please see part 1.

Unmanned Aerial Vehicles (UAV) - Drones - are one of the major growing technologies that offer huge benefits when used in the manner in which they were intended; however, they also pose a significant threat to our safety, security and privacy if used inappropriately and in the wrong hands. This guide presents an overview of the UAV technology as well as the threats presented by inappropriate use. We look at various prevention measures through Detection, Delay and Response.

Rising incidences of security violation by unauthorised drones, long lasting air traffic disruptions and increased acts of terror worldwide is primarily driving the demand for counter measures.

There are many terms that are used interchangeably to describe a drone. These include: remotely piloted vehicle (RPV), remotely piloted aircraft (RPA), unmanned aircraft (UA), unmanned aircraft system (UAS), unmanned combat aerial vehicle (UCAV). For the purpose of this paper, we will use the term Drone to include this entire group of vehicles.

Our general definition of a drone is as follows:

An Unmanned Aerial Vehicle (UAV) that can operate without a pilot being on-board that can be controlled by a ground control system (GCS) which allows the pilot to remotely control, pre-programme and/or monitor the operation of the drone. Most drones will have a bi-directional link to the GCS which provides control, status and sensor/imagery information. HALE (high altitude long endurance) drones are not considered in this document, as they fly in the airspace already monitored by the national Air Traffic Control.

2. THE THREAT FROM UNWANTED DRONES

The threat from unwanted drones presents itself in three ways: to our privacy, to our safety and to our security. Looked at another way, drones can be used to obtain, damage or destroy our assets be that: People, Information, Property, Reputation and Values.

PRIVACY

Drones now offer an unprecedented capability to acquire information from locations that were previously unreachable for most people. Drones are capable of recording and streaming live video in 4K resolution. Possible threats to privacy include:

- Eavesdropping
- Voyeurism
- Stealing IP
- Hostile reconnaissance

SAFETY

Threats to our safety range from an honest accident to miscalculations whilst using drones for malicious means.

- **Accidental Harm** - Accidental harm can come from drones that are out of control, have malfunctioned in some way. There is a clear correlation between the size of the drone and the amount of harm it could cause.
- **Harm from Miscalculation** - Harm from miscalculation could occur when a nefarious act, not intended to cause harm, goes wrong for example a protest group looking to disrupt aircraft on their approach and takeoff make a miscalculation and cause damage to the aircraft.
- **Kinetic Attack** - Drones can be used as an aerial platform to deliver weapons explosives or as a kinetic weapon themselves and be deliberately crashed into something, e.g. a building or aircraft.

SECURITY

Drones can be used as a platform to steal sensitive or protected data either through cyber means such as hacking or from video streaming/photography.

The capabilities of commercially available drones are ever expanding and include:

- **Range under Control** - A Radio Frequency control range up to 5 kilometres using mostly known protocols.
- **Range One way** - Have an actual flight range of 10 kilometres and as battery technology increases, so too does range and flight time/endurance.
- **Payloads** - Payloads are increasing. Payload is a tradeoff between range and endurance, i.e. the more carried, the shorter range/flight time.
- **Navigation Resilience** - Some drones now use more than one global positioning system for location and navigation, which means greater resilience for the honest user but also greater capability for the nefarious user too.
- **Automation** - Some drones can be pre-programmed to follow GPS coordinates alloying them to fly autonomously without a controller.
- **Speed** - Drones are getting faster every year, however pure physics dictates that a rotary winged drone could never exceed 140 knots (161 mph, 259 kph).

Commercial and recreational use of drones are governed by regulations; the opportunities for inadvertent, unthinking and malicious use of drones are however expanding, including:

- Interference with Police and Rescue operations
- Airspace violations
- Disruption of events
- Drug smuggling
- Delivery/collection of contraband to/from prisons
- Threat or embarrassment to VIPs
- Privacy intrusion
- Theft of data
- Weapons delivery platform

Detection and disruption of low and small drones is rapidly becoming a critical factor for effective maintenance of security. Recreational and commercial drones are progressively becoming more sophisticated, resulting in the emergence of diverse new threats that need to be optimally dealt with by physical security systems of the future.

There are many ways that a drone can be weaponised from being a straightforward weapons platform carrying high explosives through to being used as a kinetic weapon itself. The potential risks are: assassination, dropping or embedding munitions and harmful materials, targeting sensitive sites or manned aircraft or guiding alternative attacks (reconnoitring security professionals). Fears are expressed around a "dirty bomb" style of attack.

Drones do not need to be weaponised to prompt and cause disturbances, examples include:

- Drones can be used to disrupt events or sensitive sites (airports), but also cause major fire hazards (accidental or intentional) and disrupt operations by airborne emergency services.
- The unexpected presence of one or more drones, fitted with a dropping device, could cause fear in a crowded location (stadium, festival etc.) prompting a rush to the exits and a stampede, injuring large numbers of people. Just dropping an inert white powder in a stadium would cause mass panic and harm - it does not have to be anthrax.
- Legitimate drone user markings could be duplicated or mirrored by nefarious operators to steal information, avoid prosecution or cause other harm.
- A swarm of drones could be used to distract or overwhelm security and to facilitate other crimes.

3. DRONE DETECTION IN GENERAL

There are a number of different technology types which detect drones from varying distances with varying degrees of success. Various technologies can be combined in order to achieve better detection results.

The success of the technologies deployed will depend on the area to be surveilled, the skill of the drone pilot and the prevailing meteorological conditions. The type, mix and volume of detection technology that is deployed will mainly be dictated by the criticality of the asset that is being protected combined with the ease in which a drone can be brought into close proximity of the target. For example, a cluttered urban environment will necessitate different technologies to a flat featureless desert landscape.

A recreational drone can typically travel at 35 knots, so on a still day, the equivalent ground speed will be 35 knots too (commercial drones can have significantly higher speeds). In a 10 knot wind, the air speed of the drone will still be 35 knots however, if the drone is flying downwind, the ground speed will be 45 knots. If the drone is flying cross-wind, the ground speed will be 35 knots and if the drone is flying into wind, the ground speed will be 25 knots. Equivalent ground speed is what we are interested in. A nefarious drone pilot will use the weather and the terrain to their advantage i.e. to get a faster closing speed to their target and to mask the drone from detection for as long as possible.

Speed			Distance in Meters					Ready Reckoner time in mm:ss						
Knots	mph	kph	20	40	60	80	100	150	200	250	300	400	500	1000	2000
5.00	5.75	9.26	00:08	00:16	00:23	00:31	00:39	00:58	01:18	01:37	01:57	02:36	03:14	06:29	12:58
10.00	11.51	18.52	00:04	00:08	00:12	00:16	00:19	00:29	00:39	00:49	00:58	01:18	01:37	03:14	06:29
15.00	17.26	27.78	00:03	00:05	00:08	00:10	00:13	00:19	00:26	00:32	00:39	00:52	01:05	02:10	04:19
20.00	23.02	37.04	00:02	00:04	00:06	00:08	00:10	00:15	00:19	00:24	00:29	00:39	00:49	01:37	03:14
25.00	28.77	46.30	00:02	00:03	00:05	00:06	00:08	00:12	00:16	00:19	00:23	00:31	00:39	01:18	02:36
30.00	34.52	55.56	00:01	00:03	00:04	00:05	00:06	00:10	00:13	00:16	00:19	00:26	00:32	01:05	02:10
35.00	40.28	64.82	00:01	00:02	00:03	00:04	00:06	00:08	00:11	00:14	00:17	00:22	00:28	00:56	01:51
40.00	46.03	74.08	00:01	00:02	00:03	00:04	00:05	00:07	00:10	00:12	00:15	00:19	00:24	00:49	01:37
45.00	51.79	83.34	00:01	00:02	00:03	00:03	00:04	00:06	00:09	00:11	00:13	00:17	00:22	00:43	01:26
50.00	57.54	92.60	00:01	00:02	00:02	00:03	00:04	00:06	00:08	00:10	00:12	00:16	00:19	00:39	01:18
55.00	63.29	101.86	00:01	00:01	00:02	00:03	00:04	00:05	00:07	00:09	00:11	00:14	00:18	00:35	01:11
60.00	69.05	111.12	00:01	00:01	00:02	00:03	00:03	00:05	00:06	00:08	00:10	00:13	00:16	00:32	01:05
65.00	74.80	120.38	00:01	00:01	00:02	00:02	00:03	00:04	00:06	00:07	00:09	00:12	00:15	00:30	01:00
70.00	80.55	129.64	00:01	00:01	00:02	00:02	00:03	00:04	00:06	00:07	00:08	00:11	00:14	00:28	00:56

The table above shows time in minutes and seconds against distance and speed.

4. DRONE APPLICATIONS

In order to better understand the threats that drones pose to us, it is important to look at evolving drone capabilities and how these capabilities can serve as potential challenges and/or potential leverage points for security systems designed to mitigate the effect of nefarious drone use.

Drone Capability	Capability Description	Security Challenges	Security Leverage Areas
Launch and Recovery	The ability to launch, possibly automatedly, fly a sortie and recover back to the point of take off or to another predetermined landing point, again possibly automatedly.	The landing point does not necessarily have to be the point of take off. Launch point can be a long distance from the target and out of sight. The malicious use of drones does not have to involve recovery i.e. it could be a one way trip and the drone is sacrificed.	The ability to detect at launch offers greater potential for Detection. Potential launch points can be pre-identified based on a variety of variables such as: ■ Open space ■ Accessibility ■ Escape routes ■ Remoteness ■ Privacy ■ Obstruction free ■ Wind direction Drones recovered to the controller reveal the controller's location.
Navigation	Drones must receive real time course guidance. This can either come directly from the operator via radio control or from an inbuilt navigation system such as GPS.	Drones can autonomously navigate to their target without controller intervention. Friendly drones can have their GPS feed and control guidance intentionally blocked and therefore turned into an adversary weapon.	Drones that lack autonomous capability must have a pilot within line of sight of drone and target. Energy required to block RF signals to friendly drones is detectable.

Drone Capability	Capability Description	Security Challenges	Security Leverage Areas
Sensors and Data	Drones can carry a myriad of different sensors that can detect, measure, record, store and broadcast an array of different physical properties.	A variety of different sensors can collect and store sensitive and/or protected information as well as keep the drone safe. The onboard, local storage of data does not necessarily imply malicious intent.	Some sensors are not passive and can therefore make the drone become detectable and identifiable e.g collision avoidance sensors. If the drone is beaming the data to the controller or to another location, this makes the drone detectable and identifiable too. Transmission of data can help to locate the controller.
Operating Capability	Drones come in all shapes and sizes made from varying materials and different propulsion mechanisms with varying operating envelopes in terms of speed, altitude, endurance.	Small sized drones are difficult to locate until in relatively close proximity. Through the use of onboard collision sensors and GPS, a drone can evade detection by flying behind cover to the target and only reveal itself at very close proximity to the target. The battery is the only part of a drone that reflects radar energy.	

5. THREAT ACTOR GOALS

Bear in mind that the threat actor's objectives will vary according to their grouping. A terrorist's aims will be very different to that of a subversive, however, broadly speaking all threat actor groups will use drones in the manners listed below to achieve or assist them in achieving their aims of obtaining, damaging or destroying our assets (People, Information, Property, Reputation and Values).

The table below is a guideline, its intention is not to say that the activities listed against the threat actor groups are solely related to that group but rather this is the tendency. All groups are capable of all activities

	Terrorists	Violent Criminals	Economic Criminals	Petty Criminals	Subversives
Obtain	Information by using a drone as a reconnaissance platform prior to a subsequent attack or illegal act				
Damage	Through Kinetic force against People or Property or through delivery of High Explosives or as a weapons platform		Reputation and Values through theft of Sensitive / Protected information	–	Reputation and Values through theft of Sensitive / Protected information
Destroy	Through Kinetic force against People or Property or through delivery of High Explosives or as a weapons platform		Reputation and Values through theft of Sensitive / Protected information	–	Reputation and Values through theft of Sensitive / Protected information
Disrupt	–	–	–	Used to disrupt operations for plain nuisance value or to advertise a cause	
Distract	Used as a diversionary tactic to mask an alternative attack route				
Deliver	–	–	Used as a platform to deliver or collect illegal items .e.g. drugs/ contraband into prisons		–
Deny	Friendly/legitimate communications possibly in conjunction with another form of attack by using the drone as a platform to emit Radio Frequencies at high wattage		–	–	–

6. DRONE ACTIVITY MAPPING

Each risk assessment starts with understanding the threat and the assets that the threat is interested in. Drone Activity Mapping is a vital step in the threat part of a risk assessment. Maybe some drones have already been sighted, but most customers do not have a truly clear picture of the size and breadth of the problem. "Are there really drones flying over my premises? I've never seen them...". We recommend starting with a drone mapping study as the first step in any kind of risk analysis.

MAPPING DRONE ACTIVITY

- Easy to install (one single detector connected via PoE to a server/laptop).
- Reveals the magnitude of the problem and helps inform the decision to invest, or not, in additional security measures as well as inform the mitigation measures to use.
- Low cost - monthly fee.

The mapping is typically done with a single Radio Frequency (RF) sensor, detecting drone activities 360° around the antenna at a range of between 300 meters (urban environment) and up to 2-5 kilometres (rural environment).

Measuring the activities over several weeks will provide a detailed report on drone activities around the site revealing: type, quantity, duration, proximity and patterns. Reports can be prepared weekly and include useful forensic information such as:

- Date & time stamps
- Make & type of some commercial drones
- Frequency & protocol of controller unit
- Signal strength
- Unique MAC address when transmitting via Wi-Fi

The mapping will not indicate the precise drone and pilot position, as this requires multiple sensors correctly calibrated to permit a triangulation. The need to know the precise location of a pilot and drone is generally decided during the risk analysis, as it requires a substantial investment.

7. RISK ANALYSIS

The first step in preparing a drone risk management plan is to identify the potential risks that are posed to an organisation. Understanding the scope of possible risks will help develop realistic, cost-effective strategies for dealing with them.

FIRST STEP

We first need to look at what we are trying to protect. What are the assets and what is the criticality of each asset to the organisation. Assets can be broken down into People, Property, Information, Reputation and Values.

SECOND STEP

Next we need to look at what we are trying to protect our assets from. We know we are protecting from drones, but what type of drones are being used by what type of threat actor?

Threat is measured by Capability x Intent and different threat actors have different mixes of Capability and Intent. Threat actors can be classed as Terrorists, Violent Criminals, Economic Criminals, Petty Criminals and Subversives. Each threat actor group will have different levels of Intent and Capability and will therefore pose different threats to different asset types.

THIRD STEP

Finally, we need to look at how best to protect the asset. This involves looking at vulnerabilities that the threat actors can exploit in their pursuit to obtain, damage or destroy their chosen assets.

Risk is therefore a construct of
Asset Criticality x **Threat** x **Vulnerability**.

RISK IDENTIFICATION

In identifying the risk and threats, we consider:

- How could my organisation be impacted by drones?
- When did this happen; could it happen again? (the drone activity mapping)
- Why would my organisation be threatened by a drone?
- What would happen if a drone attacked/hacked my staff or organisation?
- Where are the security gaps/vulnerabilities that would allow such an attack?

Areas of impact will differ depending on the industry or type of business. Areas of impact to consider include: Human injury/wellness, operational, financial, legal, and brand reputation etc.

How a drone impacts an organisation depends on the nature of the business, but in all industries it would result in financial consequences due to disruption of operation, man hours to remedy the situation, infrastructural damage etc.

CONSEQUENCES

For many businesses, an unintentional drone accident, such as a pilot losing control of their drone and crashing it, will not cause devastating consequences.

However, for other operations - such as sporting events, stadiums, energy infrastructures - an unintentional drone crash could result in human injury, disruption to refineries or power outages.

Negligence or criminal behaviour is inevitable and it is important to consider the threats from a security standpoint. As drone capability proliferates coupled with the threat actors intent to use them, organisations should anticipate a rise in the types and number of such threats and prepare to respond appropriately.

PROBABILITY

Data surrounding the likelihood of a drone attack should also be analysed. This is not just limited to the drone activity study, if this was performed, but can also include:

- The study of the local area and analysing potential takeoff and recovery points based on the principles stated in the Drone Application table above (page 5)
- Speaking with neighbouring sites
- Speaking with local authorities

8. SECURITY APPROACHES

Detection encompasses all human and technical means to detect threat actors as early as practically possible in order to raise the alarm and afford as much time as possible to respond. The Delay function's aim is to provide enough time for an effective response to an attack. The Response function is a set of measures for stopping and/or neutralising attackers.

Since drones can be a potential means of either attacking a site or smuggling contraband materials to or from a site, the same 'detect, delay and respond' approach should be developed to neutralise the threat posed by them.

In the next section, we look at the technical measures that can be used for each step of this approach. In order for the Detect, Delay and Response approach to be considered successful it will have to Detect an attack early enough, the Delay will have to slow down the attack long enough such that the Response force can neutralize it. Put another way, if the adversary's timeline outperforms the friendly forces timeline, the adversary wins!

The recipe for success with regards to countering drones is therefore to increase the ability for the facility to detect as far out and as soon as possible. To increase the amount of delay that can be imposed upon the drone both above and in close proximity to the facility and finally to speed up the response force reaction time by moving the response force closer to the target(s).

In considering the potential drone threat, we evaluate how these three approaches to improving security at facilities might be accomplished.

9. COUNTER MEASURES

When designing counter measures the security strategy is based on the G4S Principal Security Effects of Detect, Delay and Respond.

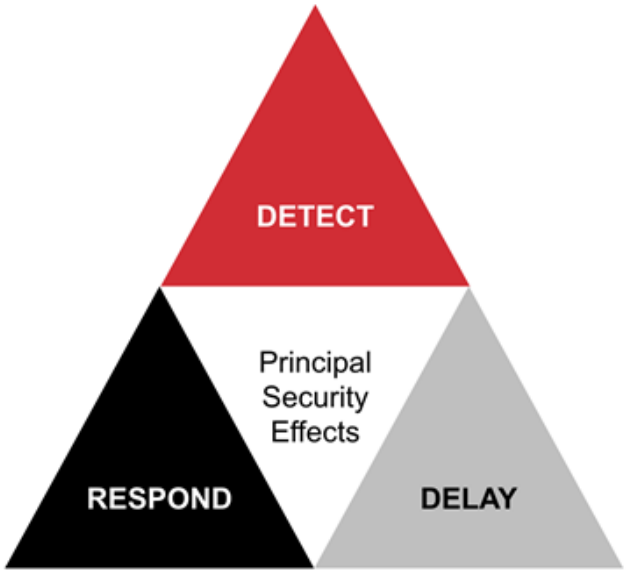
DETECT

Given what we have said above around drone capability and how a nefarious drone operator would pilot or programme the drone to evade detection it is easy to understand that we cannot reply upon a single detection capability. The ever expanding array of technological capabilities offered by drones necessitates the use of a combination of Detect mechanisms in order to guarantee greater levels of success. These detection capabilities range as follows:

- Radar
- Electro-Optical
- Radio Frequency (RF) Emission
- Acoustic
- Magnetic
- Visual

Incorporating two or more detect mechanisms increases the chances first of all of detection but once the target has been detected, with multiple systems working in tandem, there is a greater chance of keeping the target acquired and tracked.

Detection should not only detect the presence of an unwanted drone or drones, detection should also be able to pinpoint the location of the drone and track it.



Using a combination of the methods described below, this is entirely possible as we know where in space the detection devices are, locating the drone(s) is simple trigonometry and or a simple time, distance speed calculation - all of this is automated. Ideally we would want to be able to locate the drone pilot too, this really depends upon the amount of energy they are emitting, their location and proximity to the target location, amount of cover etc.

Time is the key to detect, raise awareness and enable correct decision making. False alerts - false positives and false negatives - should be avoided at all times in order to advance decision making and start in due time the appropriate standard operating procedures.

Let us look at the range of detection sensors:

- **Radio Frequency Sensors** - The RF Sensor is the foundation of the detection solution, providing early warning of malicious activities - even before airborn of the drone. It detects the communication between drones and remote controllers (Wi-Fi and RF). A combination of several RF sensors allows establishing a bearing on the drone and pilot. RF sensors are available as a mobile unit that can be worn as personal equipment on a person/security professional.

  Drone manufacturers also produce a RF-based drone detector which captures the information from the remote control, and can provide accurate information on drone and pilot position up to 5 kilometres away (under ideal conditions over 20 kilometres). A downside for the moment is that the system can only provide information if remote controllers are used.

- **Video Monitoring Camera (Video Monitoring Systems)** - Upward facing HD cameras can be used to detect drones, in addition to the RF sensors. Using video analytics, 10 x 8 pixels of image is necessary to positively identify a drone. The type of cameras can be "wide angle" to detect drones nearby in a wide angle, or "wide range" to detect drones for a greater distance, but in a narrow beam. A PTZ-camera could track the drone to check payload, follow the flight path and allow better decision making (friend / foe / ignore).

  Ideal for the detection and confirmation of small low / slow flying drones during the day and against a clear background (sky), less efficient during dark nights or for drones flying against a complex background. A combination with a thermal camera will give even better images at night and in poor weather conditions (rain, snow, fog, etc.) Cameras can be guided by information from a radar and provide faster visual confirmation of a detected drone.

- **Radar Technology** - Whereas RF Sensors and Cameras are passive devices, (i.e. they do not emit radiation), radars are active devices and emit strong radio signals and so require an official authorisation to operate.

  A Radar installation is subject to an in-depth Health & Safety analysis and cannot be installed in the immediate proximity of places where persons are at work. Radars can detect even smaller drones at a larger distance - small drones up to 5 km, larger ones up to 15 km - and additionally the height. The effective distance of a radar is limited by surrounding trees, building and terrain. Once detected, the radar software will allow it to track the drone and follow its path.

  Radars do not allow the detection of pilots. However, radar isn't only about range; the elevation of the signal is also important, i.e. the angle above the horizon that is scanned. Drones can be taking off a few kilometres away and flying at height in an attempt to avoid detection systems. Therefore 3D

radars – looking in all directions not just sideways – are preferred.

- **Acoustic Sensors** - We do not recommend the use of acoustic sensors, especially in an urban environment. The drones must be very close for a positive identification and the likelihood of false alarms is relatively high.
- **Software Tracker** - Most important is the "drone tracker" software that integrates the signals from the various sensors. The software should deliver the following:
  - Pre-alarm when a drone is detected
  - Alarm in case of intrusion
  - Send alarm notifications (sms, mail, integration with other security systems)
  - To track the drone and possibly the pilot
  - To view the images from the Video Monitoring Camera or radar
  - Provide path of flight
  - To store the information from a sensor in a secure manner, so they can be used for forensic purposes
  - Provide easy reports

DELAY

We typically achieve delay by incorporating physical or procedural barriers that will slow down the progress of the threat actor's mission to obtain, damage or destroy an asset. The longer the delay time, the more time there is for a response force to reach the location and neutralise the threat.

The greatest fundamental challenge which drones pose to any location or facility's security is the inability to delay them. Traditional barriers to delay adversary access to any type of facilities (e.g., fences, barriers, ditches, locks) are ineffective against drones.

One obvious way to achieve 'delay' is to Detect further away from the target, this in turn buys the response force more time. There are however some traditional physical measures that can assist in delaying as well as some procedural measures.

The traditional physical measures involve the placing of obstacles such as netting, wire and other physical objects that would slow down the course of a drone and/or possibly cause a collision.

Procedural measures involve the enforcement of a geo-fence and whilst this will clearly not stop a determined adversary, it may well have an effect on some of the less sophisticated adversarial groups who are using shop bought drones that will bounce off protected geo-fenced air space. Geo-fencing is manufacturer specific and will not stop a determined malicious threat actor; however, it is useful for helping sites identify intent and reducing negligent and reckless use.

Airspace restriction is another procedural method to assist delay. This may include Prohibited Areas, Restricted

Areas or Danger Areas (military ranges etc.). It is also possible to place a temporary restriction on airspace, either as a result of a longer term pre-planned event, or in reaction to a short notice occurrence, such as an emergency incident. Organisations should contact their relevant country Aviation Authority to understand what type of airspace their site sits under and whether it is possible to apply for Airspace restrictions/geo-fencing.

Geo-fencing technologies will more than likely only deter accidental intrusions and potential attacks by unsophisticated operators. Sophisticated operators capable of hardware assembly and firmware modifications will, more than likely, be able to overcome geo-fencing limitations.

Where the neutralisation of the drone is not authorised, the identification and arrest (civilian arrest) of the pilot is the most recommended measure. The drone protection measure should:

- Allow to locate the pilot on a map from the moment he switches on the remote control. This will permit the response team to identify and possibly detain the pilot until law enforcement arrives on site. This could also include a drone to spot the pilot and provide pictures of him and/or his car as evidence.
- Follow the positions of the pilot and drone, while the response team is underway.
- Capture unique drone data (MAC address) to be used as evidence when prosecuting.

RESPOND

Respond can be a difficult thing since drones are in the air. Response can be achieved in two ways:

- Countermeasures - In many countries the use of countermeasures is strongly regulated, only special police forces or army units can employ these measures. Counter-measures tend to neutralise the drone either by affecting its controls or physically destroying (parts) of the drone.
- If the drone pilot can be identified that response team can respond directly to the pilot.
- Protective measures - A wide range of protective measures can be designed to alert the staff on site and take first precautionary measures. For example; as part of the detect strategy there can be mounted acoustic alarms for the staff working outside. Acoustic alarms can for example be used at Research And Development labs to alert them to drones in the vicinity that are trying to steal their IP.
- Automatic closing of shutters in meeting rooms, to avoid any sensitive information being displayed (including the identity of visitors) that could be observed by a drone.
- Fog (Interactive Security Systems) to hide any prototypes (fashion, cars and more) being shown/ tested outside.

It is always a good idea to post clear signage that the site is a “No Drone Zone”.

Details on the possible neutralisation technologies are provided in this guide.

10. NEUTRALISATION

Which technologies exist - What are we authorised to use?

Legislative issues aside however, defeat options broadly fall into two categories: the "Radio Frequency Effects" and "Kinetic Effects".

RADIO FREQUENCY EFFECTS

- Signal Jamming - Transmitting noise on frequencies 1.5 GHz, 2.4GHz and 5.8GHz that drones use for communications and video transmission to generate RF interference. It will either force the drones to land or maintain its position (hover) until it reconnects with the control unit (pilot). For drones that fly autonomously, signal jamming could affect if the GPS signal is jammed.
- Signal Spoofing - Mimicking the drone control signals to 'take over' the drone and redirect it. Also called Drone Hacking.
- GPS Spoofing - Deceiving the GPS receiver by broadcasting incorrect GPS signals, causing the receiver to estimate its position to be somewhere other than where it actually is and deviating the drone from its programmed route. GPS spoofing will not only affect the drone but all users within the area, including emergency services, (police) helicopters etc.
- High Power RF Techniques - Such as Lasers, Electromagnetic Pulse Guns and High Energy Microwaves which disrupt the electronic circuits within the drone to bring it rapidly to ground. These devices must be used with extreme caution, as they can also affect nearby airplanes etc.

IMPORTANT

Most commercial drones are programmed to return to their take-off position - RTH return to home and land - in case of loss of signal, however cases are known where drones have crashed as a consequence of signal jamming; creating a hazard to persons and objects on the ground. Signal jamming must be avoided for flying drones over crowded places like festivals, sports events etc.

KINETIC EFFECTS

Besides shooting at or throwing objects at the drone – which we really do NOT recommend, (especially in crowded/urban environments) there are a few possibilities to disable drones:

- Nets - Shooting nets from a ground gun or using larger drones carrying a net (Drone Swapper). The effectiveness of these measures will greatly depend on the skills of the pilot/shooter. For the capturing net, the shooter must anticipate the flight path and take into account the limited distance over which the net can be actively used. The Drone Swapper can be evaded by a skilled drone pilot as the net-carrying drone is slower in response due to the effects of the net.
- Birds - Although spectacular, the counter measure using birds of prey to attack drones and take them out of the air did not provide the expected long term results.

Early in 2018 the Police in the Netherlands were ready to deploy a team of eagles to take down rogue drones. Now the police say they've stopped using the birds because training them is more expensive and complicated than they anticipated.

11. NEW DRONE TECHNOLOGIES

Which changes can we expect in the near future?

Drones will continue to develop and the next generation will be lighter, smaller, more complex and equipped with artificial intelligence, which requires a quantum leap in our detection capabilities.

First tests have been done controlling drones with 5G technology, making the classic RF detectors obsolete. 5G technologies enable more autonomous operations for drones, with swarms of drones communicating with each other via 5G, and sending real-time data amongst themselves and to controllers and users.

There are already sensors detecting 5G signals but these are still very expensive and will require further testing to filter the specific drone signals once many other applications are connecting to the 5G networks.

Within modern military operations, studies and tests on airborne jamming and drone interception by other drones are also being conducted.

12. CONCLUSION

When considering measures to protect staff and premises from accidental or intentional drone damage, we propose a phased approach:

- Measure the drone activity in a cost efficient manner,
- Evaluate the risks for the company and its personnel,
- Implement the best counter-measures

The software platform where the various types of detectors can be plugged in, is at least of similar importance than de sensors.

Measures taken must be a combination of (automatic) protective measures and, where legally allowed, active defense. The best active defence against LSS drones (low, small, slow) currently is disabling the drone signals, kinetic measures do not yet deliver the expected results.

In the future, with 5G technology, signal perturbations will only be permitted in very exceptional cases as many other legitimate and vital systems could be affected.


72%
54%
96%
82%

POSTSCRIPT

This guide Detecting and Countering Drone Intrusions was written and produced by the G4S Academy.

This guide may contain forward-looking statements including statements regarding our intent, belief or current expectations with respect to the physical security services businesses and operations. Readers are cautioned not to place undue reliance on these forward-looking statements.

The intention of this guide is not to present a complete and all-encompassing view on Detecting and Countering Drone Intrusions, but to elaborate and provide qualitative insights from G4S experts as a thought-starter for the creation of the security future of your organisation.

The information provided by G4S in this guide is for general informational purposes only. We make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability or completeness of any information. Under no circumstance shall we have any liability to you for any loss or damage of any kind incurred as a result of the use of or reliance on any information provided in this presentation.

Following our G4S Academy approach "Knowledge Created Together" and "Value Created Together", we would appreciate your feedback and insights on this guide. Together we know more. Please email us your thoughts, agreements, and disagreements to this address info@G4SAcademy.com.

This guide and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of England and Wales. The courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with this document or its subject matter or formation.

G4S

G4S is the world's leading global, integrated security company. We offer a broad range of security services delivered on a single, multi-service or integrated basis across six continents.

Our growing focus on integrated, technology-enabled solutions creates additional security and efficiency benefits to customers and increases our ability to differentiate G4S's offering in the security market, which in turn supports our goal of accelerating profitable growth.

Our businesses are segmented into four core services – Secure Solutions, Cash Solutions, Risk Consulting Services and Care and Justice Services.

Please note that the solutions mentioned in this guide are not available in G4S North America or G4S Latin America.

G4S ACADEMY

The G4S Academy is a platform within G4S that allows us to work more collaboratively with our customers, suppliers, partners and other stakeholders to create knowledge and value together.

The G4S Academy's mission is to create and share knowledge based on our global expertise that will reinforce how we provide safety, security and enhance value for our customers

Security and safety has become a fundamental component of business operations. Many of our traditional customers are changing their focus from managing safety and security to fuelling business growth. This is one of the biggest challenges that executives in the security industry face today and this is forcing all of us to communicate our value in a completely new way.

Through the G4S Academy, we are able to create a culture that challenges traditional security thinking, embraces technological change and predicts future security demands by leveraging our knowledge and expertise and sharing it with security professionals. We're committed to providing relevant, up-to-date content across a variety of media.

Find out more about the G4S Academy at **https://www.g4s.com/what-we-do/g4s-academy**

VALUE CREATED TOGETHER

CONTACT

GET IN TOUCH WITH THE G4S TEAM – VISIT WWW.G4S.COM

V1 MARCH 2021