ADS Policy Paper
Counter-drone technologies

After the Gatwick drone incident prior to Christmas 2018, there has been considerable political interest, including Parliamentary inquiries, in the use of technologies to counter the improper use of drones at airports and other key sites to defend against such intrusions in future.

There has also been some public confusion as to why such technologies were not already in place. But not all counter-drone technologies are the same, and authorities in the UK face restrictions or challenges in their usage.

By looking at typical, everyday examples where counter-drone technology might be needed, it's possible to identify the counter-drone systems that might be needed and factors that can helpfully support quick decision-making.

An overview of technologies for countering the improper use of drones

There are a wide range of counter-drone technologies on offer in the UK, which broadly can be categorised into detector and effector systems. Detector systems enable the operator to detect, track and identify (DTI) drones in an area, even going so far as to track down the drone operator in some circumstances. In turn, effector systems can either be physical kinetic, electronic or high energy.

There are a range of CUAS solutions in the marketplace, some of which are produced by UK manufacturers but then exported, as they are not legal for deployment in the UK (the highlighted electronic effectors below).

Current technologies and solutions include, but are not limited to:

Detectors (Detect, Track and Identify)

a. Radio Frequency (RF) detectors
b. Microwave detectors
c. Optical scanning (cameras)
d. Radio monitoring
e. Drone-specific radar sensors
f. Electro-optical infrared systems
g. Acoustic sensors

Effectors

a. Ground-based net launchers, either shoulder-mounted or via a platform
b. Hunter/killer drones (e.g. armed with net launchers)
c. RF jammers
d. GPS jammers
e. Directed energy (including laser) systems
f. Trained birds of prey

Individual counter-drone technologies cannot respond to every kind of malicious, or inadvertent, drone threat. For instance, while one system may be able to effectively deal with a single drone intrusion, it may struggle to deal with a swarm of drones. In other cases, they may be inappropriate for use in built-up areas, because of concerns about the impact on third parties. For that reason, the deployment of counter-drone technologies should not be done on a generic basis, as the risks arising from civilian drones and the effectiveness of a response will vary in each case. Indeed, in some circumstances it may simply not be worthwhile for reasons of cost to deploy counter-drone technologies, if the drone intrusion poses no threat to life and limited battery life means it may only last a short while. ADS therefore believes a risk-based approach that determines the appropriate measures, including response procedures, to be used in each case.

Effective counter-drone systems should provide a layered defence, with detector and effector systems integrated to provide a complete response (Detect, Track, Identify, and if necessary, Destroy). Integrated responses can also then minimise the risk of collateral damage in the surrounding area, for instance to stop a drone falling on people and property nearby using a combined jammer and net launcher with an in-built parachute.

It is worth noting that there are a range of legal issues hindering the use of effector systems.

First and foremost, it is currently illegal to interfere with a flying aircraft in the UK, as per the Air Navigation Order 2016, and drones are counted as such. Also, it is illegal to jam commercial RF bands and GPS under the Wireless Telegraphy Act without a licence. There are also legal restrictions on interception systems that may be considered a form of wiretapping.

As such, legal powers to use jamming technology are currently only held by the police, military and intelligence agencies, all in limited circumstances (generally, a direct threat to life). This means that while there are a range of counter-drone technologies that can effectively mitigate the risk of civilian drones, many of these systems cannot currently be used in the UK except in certain circumstances.

Case study Airports

The current risk

As was seen during the Gatwick incident, drones are being used to maliciously fly over restricted airspace to force airports to suspend operations. The wider risk is from accidental drone flights near airfields, often by hobbyists.

In the worst-case scenario, a drone could be piloted into a plane on takeoff or landing, causing major damage and a potentially fatal crash. It is worth noting that this hasn't yet happened, and there is only one documented incident of a drone hitting a flying plane (a 737 in Mexico in 2018), but no lives were lost.

The current response

The UK government has extended the exclusion zone around airfields from 1km to 5km. This will only affect drone flights conducted legally, so determined malicious operators will simply ignore the exclusion and likely circumvent any geofencing software, but it will help to reduce the number of accidental incursions by hobbyists.

Prior to the Gatwick incident, the roll-out of counter-drone technology to airports had been limited, in part due to the legal restrictions on using effector systems and a lack of guidance issued by CPNI, the UK's technical authority for physical security. However, after the Gatwick incident most airports in the UK have been purchasing drone detector systems following advice from CPNI and other authorities.

The current use cases for counter-drone technology

Drone DTI systems are in use at airports to provide confidence to their operators that no drones are flying in their airspace, posing a risk to inbound and outbound traffic.

Drone effector systems are not in use at airports due to legal restrictions, but they were deployed at Gatwick under the jurisdiction of the police due to the exceptional circumstances.

Case study Prisons

The current risk

Drones are used at prisons to deliver contraband (e.g. drugs) and for reconnaissance purposes. However, it is worth noting that around 70% of contraband in prisons come in through the 'front door'.

Drones at prisons do not currently pose a threat to life but they are being used to facilitate criminality within prisons and could be used to aid break-outs.

The current response

HMPPS prisoner officers 'shall have all the powers, authority, protection and privileges of a constable'. However, the constabulary powers available to a public sector 'prison officer' are not available to a private sector 'prison custody officer'. In terms of offensive capability prison officers are still often dependent on a police response.

Many prisons are installing nets on the perimeter fence to deter contraband delivery. Moreover, prisons are generally included as restricted sites in geofencing software installed on commercial and civilian drones. Finally, the Prisons (Interference with Wireless Telegraphy) Act 2012 enables Prison Governors to give authority to use jamming equipment within prisons, primarily to prevent the of use of mobile phones by prisoners

In April 2017 the MoJ announced that a specialist squad of prison and police officers has been formed to tackle the threat drones pose to prison security. However, their task is to inspect drones that have been recovered in a bid to identify the operators. To date, there have been at least 28 sentences imposed relating to drone activity at prisons, with those convicted serving a total of more than 80 years in prison.

The current use cases for counter-drone technology

HMPPS is working on the development of counter-drone technology with the Home Office and others. Legislation was approved by HMG to enable a prison (Les Nicolles) in Guernsey to deploy a detector and electronic effector system (SkyFence, which projects a defensive jamming field around the walls of a prison to prevent entry by drones over its airspace). This legislation extended existing powers for prison officers to interfere (jam) with mobile phone signals in the vicinity of a prison.

In the rest of the UK electronic effectors cannot yet legally be used by prison officers, but in December 2018 the Prisons Minister indicated that the government is considering rolling out the technology used at Guernsey to England. Following this, there is an active call for DTI technology for countering the threat of drones.

Case study Major events

The current risk

Drones could be used as stand-off delivery platforms for any type of dangerous substance (for example CBRNE) or simply to cause panic at a crowded event via a simulated attack (for example an innocuous white powder). Drones could also be used for surveillance to help support criminal activity or a ground-based terrorist attack at a major event.

There are no documented examples yet of threats to life from drones at major events, but during the Euros 2016 a drone was used to deploy an Albanian flag during a match with Serbia, intended to stir political tensions. There have also been several incidents where drones have been used to capture "action shots" which could have caused injury or worse.

The current response

Private security managers do not have the authority to act against drones at major events and HMG proposals to extend such powers to them last summer have been quietly dropped.

Police are the only authorities with the power to interfere with drones, if a threat to life is posed or if a serious crime will be committed. Major events are therefore dependent on paying for an appropriate police presence where there is a high security threat and the response may include deployment of counter-drone capabilities.

The current use cases for counter-drone technology

At events such as New Year's Eve in London companies have worked with the Metropolitan Police to deploy integrated sensor-effector systems to provide protection against drone incidents. Japan's National Police Agency also intend to deploy drone 'jammers' at a wide range of upcoming major events, including the G20 Summit in June, Rugby World Cup in the autumn, and the 2020 Olympics. Finally, France has put out a call for counter-drone technologies for use in the Paris 2024 Olympic Games.

Case study Nuclear power plants

The current risk

Nuclear power plants are hardened but high-impact targets for drones, which could either be piloted to crash into the power plant or else be used for stand-off delivery of explosives.

Drones can also be used for surveillance purposes at nuclear power plant sites, to either aid serious criminality or a ground-based terrorist attack, although given their flight range limitations and the size of power plant sites this may offer limited utility.

There is a separate but connected risk posed by the spent-fuel pools that are also stored at nuclear sites, which tend to be less protected than reactor cores. There is also a risk from protest groups – in France in 2018 Greenpeace piloted a UAV into a nuclear power plant to highlight their vulnerability to attack.

While drones do pose a risk to nuclear power plants, conventional threats such as parachuting infiltrators, mortar attacks and rocket attacks will remain the simplest and most effective way of damaging a power plant, given their hardened nature.

The current response

In the UK the Civil Nuclear Constabulary (CNC) are responsible for the security of UK nuclear sites, and as with other police they have the legal power and capability to act against drone incursions. Most CNC officers are also Authorised Firearms Officers. However, there are issues with using firearms at nuclear sites, not only due to the risk to nearby third parties, but also to the site itself if a firearm is discharged.

Nuclear sites are restricted sites and thus illegal to fly a drone near, as per the Air Navigation (Restriction of Flying) (Nuclear Installations) Regulations 2007. This deters legal hobbyist users but would not stop a malicious drone operator.

Nuclear power plants are hardened targets, intended to stand up to an impact by a fixed-wing aircraft – for instance, studies carried out for the Sizewell B public inquiry concluded that, in a worst case scenario, if a military aircraft were to strike its reactor building there would be a 3-4% chance of uncontrolled release of radioactive material.

The current use cases for counter-drone technology

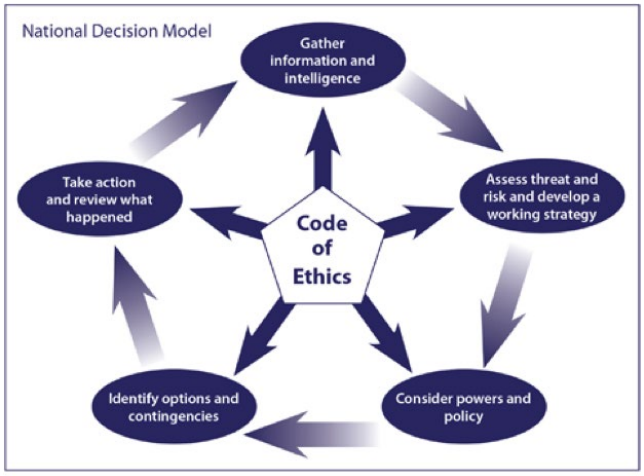
Given the highly sensitive electronic safety systems in place at nuclear power plants, there are technical challenges with deploying electronic effectors at nuclear sites. The CNC is therefore purchasing a kinetic effector system to use at its operational sites in partnership with Openworks Engineering. However, drone detector systems are in use at UK nuclear sites.

Counter-drone technology as decision-making support

As the use cases have illustrated, counter-drone technologies (both DTI and effector systems) can play a vital role in a wide range of live scenarios to combat malicious drone incursions.

However, the scope for action in each use case is variable. Given the central role that UK policing has, and is likely to retain for the foreseeable future (barring any significant changes to the role of the military and other actors such as private security managers) in countering the drone threat, the police's approach towards counter-drone technology will define how it matures within the UK market.

The College of Police's National Decision Model (NDM) sets out a clear process for police decision making in urgent situations:



Integrated counter-drone systems can support the implementation of the National Decision Model in four out of the five areas above (powers and policy being the only exclusion). An integrated system with both DTI and effector capabilities can support the police by gathering intelligence, delivering the assessment of the risk, providing response options, and acting to deal with a drone threat.

In responding to any drone threat, the police's (or other relevant actors) decision making will be informed by the context, their knowledge and the timescale of the threat. This will then affect the ethical, and potentially legal, considerations for taking direct action. For instance, a threat to life at a major event will give much greater legal and ethical scope for immediate, direct action than attempted transportation of contraband at a prison.

It is therefore important that the police (or other relevant actors) are armed with the right information, in part delivered by an integrated counter-drone system, in order to conduct good decision-making under pressure. The relevant factors for consideration include, but are not limited to, the following:

1. Whether the drone in question appears on the UK's drone registration system;
   a. If it does, whether this information can be accessed quickly by decision-makers;
2. What the size of the drone is;
3. Whether the drone is carrying a payload, and if so, what that payload is;
4. What the speed and direction of travel of the drone is
5. What the potential flight time (i.e. battery life) of the drone is;
6. Whether the drone can function beyond the line-of-sight of the operator;
7. What effector capabilities are available on-site, or nearby.

As these factors illustrate, there are a wide range of factors that can helpfully support decision-making if made available in a speedy and accessible fashion. ADS therefore supports the view that integrated, layered counter-drone systems must be a vital aspect of decision-making support to policing and should not simply be seen as a technological solution.

adsgroup.org.uk

About ADS

1. ADS is the trade association advancing the UK's Aerospace, Defence, Security and Space industries. ADS has over 1,000 member companies across all four sectors, with over 950 of these companies identified as Small and Medium Size Enterprises (SMEs).
2. The UK is a world leader in the supply of aerospace, defence, security and space products and services. From technology and exports, to apprenticeships and investment, our sectors are vital to the UK's growth – generating £74bn a year for the UK economy, including £41bn in exports, and supporting around 1,000,000 jobs.
3. ADS operates the Drone Platform and Counter-Drone (DPAC) Special Interest Group, which represents around 60 organisations who are engaged in all aspects of remotely operated and autonomous platforms operating across the land, sea and air environments, including build and operational technology, legislation, training, and countermeasures.