Pilgrims Assessment:
The Unmanned Aerial Threat

Stuart Fraser, Pilgrims Group

DJI Phantom 2 (Photo Courtesy: DJI)

Unmanned Aerial Vehicle (UAV): An aircraft or aerial vehicle (including rigid-hulled, propeller-driven and fixed-wing) which does not possess an on-board pilot. Instead, it is directed by a remotely-based operator who generally utilises a radio-signals connection to maintain active control over the vehicle. In some cases, the aircraft will be capable of acting without an operator, although generally only for simple tasks.

Also, known as remotely-piloted aircraft (RPAs), unmanned aerial systems (UAS –encompassing both vehicle and control systems), or also, colloquially, “drones”).

Overview:

UAV (**under covers**) with radioactive trace elements on top of the Japanese PM's residence following examination / containment by bomb squad.

On 22 April 2015, an unmanned aerial vehicle (UAV) landed on the roof of the personal residence of the Prime Minister (PM) of Japan, Shinzo Abe (who was overseas at the time). It was later determined that the UAVs payload, a plastic container, contained trace elements of the radioactive element Caesium, although not a sufficient amount which could generate physical harm. This incident has followed various high-profile uses of UAVs:

January 2015: At 0300, a UAV quadcopter (**pictured**) was flown into the grounds of the US White House by an inebriated member of a US government intelligence agency. Reportedly, the official lost control. He had been controlling it from a few city blocks distance.

The UAV, a DJI Phantom, was spotted by a White House staffer although could not be prevented from entering the secure perimeter.

Photo credit: US Secret Service.

September 2013: A small quadcopter UAV (circled in red) flies close to German Chancellor Angela Merkel (**circled in black**). The UAV (flown by the libertarian 'Pirate Party') crashed shortly after.

The users were reportedly aiming to emphasise concerns over spying and privacy.

Photo credit: Washington Post.

The Threat:

Small UAVs (SUAVs) of the type utilised in the above incidents represent a new, and difficult to fully counter, threat for a variety of organisations and facilities. This is a result of both the new technologies involved and the absence of a comprehensive regulatory response.

While small, remotely-controlled platforms (**left**) have been in existence since 1937, with widespread commercial availability from the 1970s; the technologies involved have only recently begun to represent a conceivable threat. This is primarily the result of advances in miniaturisation of electronics, widespread accessibility of GPS navigation and improvements in battery-life. The military usage of UAVs in the last decade (most notably for combat and reconnaissance missions, see **below right**) also undoubtedly stimulated the public perception of such systems and assisted with the development of relevant technologies.

This process has led to the development of small, difficult to detect (either visually or through the use of monitoring / surveillance technologies) aerial platforms which have the capability to penetrate (via overflight) fixed ground-based perimeters. While a fence / wall has historically offered a physical barrier to pedestrians or vehicles, it represents no obstacle for an SUAV. Consequently, the threat is that anyone with access to such a system can now (remotely) access secured facilities.

Quadcopters remain the most widely used SUAV, although 'fixed-wing' propeller aircraft (with advantages in stability) are also seeing more usage.

Advances in flight-distance / navigation / access:

Such SUAVs also possess significantly greater flight-time / range / height than their predecessors of only a few years ago. Currently, the DJI Phantom (**Front cover**, an increasingly ubiquitous model of SUAV) has (without modification) a flight-time of 25 mins / a tethered range of 300m / a max ceiling of 200m. (Higher-level SUAVs can operate up to one mile distant.)

The DJI Phantom 2 has an off-the-shelf base cost of £200.00 (including HD camera) with a range of sophisticated attachments well within the economic means of many. Availability / accessibility of such technologies is now no longer a major obstacle to individuals.

SUAV systems can also fly further (untethered) through the use of GPS 'waypoint' setting, i.e. the use of fixed GPS points which the (modified) aircraft can follow; this would enable deeper (if uncontrolled) flight penetration.

Such an SUAV could be programmed to move deep into a controlled site via using commercially-available software (such as GoogleMaps) to create waypoints.

Payloads – surveillance / destructive:

The other key evolution which has turned such technologies into a threat is the increased payload which they can utilise (and the range of advanced commercially-available technologies). The Phantom 2, as an example, has a maximum carriage-payload of 1.2kg (basic) which enables it to carry a range of attachments.

Many of these attachments are visual systems, which could (and have) been used for malicious surveillance; these include several advanced technologies:

- Night-vision capable cameras;
- Long-range cameras (capable of reading this document at 600m);
- Infra-red (IR) & thermal cameras.

All of these technologies, especially when combined with an SUAV, could potentially provide options for individuals to conduct hostile surveillance on both residential and commercial properties. Such SUAVs configured for these roles have been documented providing reconnaissance capabilities by armed groups in the Middle East and in Ukraine.

Footage from Islamic State (IS) UAV conducting surveillance / reconnaissance in Syria (2014) prior to an attack.

Photo credit: YouTube still.

While visual technologies are the most fully developed, amateur hobbyists have sought to develop payloads which could potentially be hazardous and present a degree of physical risk. As with the UAV which landed on Shinzo Abe's roof, SUAVs can have payload / containers attached (with programmed options for release). In this case, the container carried trace elements of radioactive materials; however, incendiaries or 'white powder' payloads could also be employed to cause damage / panic.

Commercially available 'fixed-wing' SUAV.

This device can be hand-launched and requires only two metres (approx.) landing space.

There are also indications that there are (as yet immature) technologies being developed for more lethal payloads. Reporting from Ukraine indicates that at least one SUAV has been configured to carry a hand grenade (0.4kg), while US enthusiasts have begun to experiment with mounting firearms on SUAVs. The photo (**right**) shows a large-calibre handgun capable of being fired remotely by a controller. In an incident in 2011, a US al-Qaeda sympathiser planned an attack on the Pentagon through remote-controlled planes configured as bombs (although the viability of these plans was questionable).

It should be emphasised that this more lethal potential threat posed by UAVs is very much in its infancy. Currently, the maximum payload capacity for a commercial SUAV remains only around 1.2kg. As such, with the required control systems / sophisticated parts needed, the current physical limitations to UAV technologies mean that more hostile applications for actual attacks are still a future prospect rather than an immediate concern. On the basis of the current trajectory of the technologies involved, the best estimates are that this will start to become a more significant issue in around 12-24 months.

The Response:

Legislative:

To date, the response by Western governments and law enforcement to the UAV threat has been generally slow, both in regard to legislation and the development of physical counter-measures. So far, much of the response has been conditioned by the (limited) physical threat posed by such devices to critical national infrastructure (for instance, planes at airports). (Currently, plans are being considered for specific sites to be 'geofenced'– i.e. programming the software to block the UAV GPS from accessing a particular location – this could be overcome, but would signal clear illegal intent).

The response by legislators has been faster in the US than in the UK, where the primary legislation is now significantly out of date (Civil Aviation Authority: *Air Navigation Order, Jan 2010*): this specifies limits to UAV flight options and also precludes flying within 50m of a person (*Art. 166 and 167*). SUAVs are defined in legislation as less than 20kg:

http://www.caa.co.uk/default.aspx?CATID=1995

http://www.caa.co.uk/default.aspx?catid=1995&pageid=16012

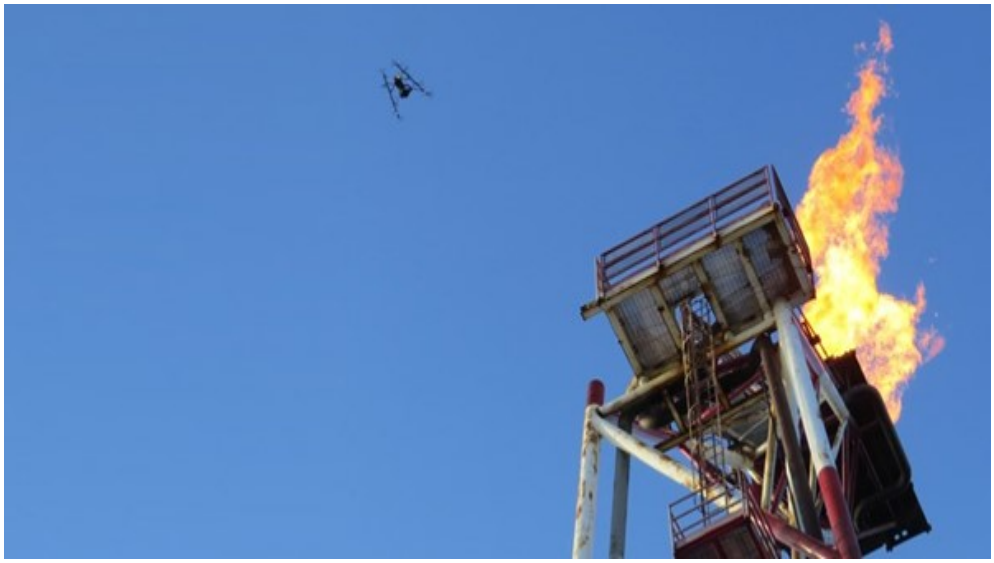
It is thought that ongoing efforts are being made to close a range of existing legal loopholes concerning the usage of SUAVs. The potential hostile functions of UAVs have not been formally (separately) defined and are covered under standard legislation.

Currently, the legal advice to anyone in the UK who witnesses an unknown UAV which they feel is a concern or may be engaged in illegal activities to report it to local police.

Physical countermeasures:

The physical options for response to SUAVs as a commercial threat are extremely limited. While high-end military grade capabilities do exist for counter-UAV efforts, these are generally very sophisticated (and exceedingly expensive) electronic warfare systems. These include the use of radio-waves to saturate the electromagnetic space around the UAV (disrupting / disabling its remote-link to its operator), attempting to gain control of the platform via alternative frequencies ('spoofing') or even through the application of directed energy (i.e. lasers). For self-evident reasons, such technologies generally are not viable for protecting UK facilities from SUAV intrusions.

Kinetic counter-measures, i.e. physically attacking the system with projectiles to damage / destroy the SUAV, are generally not recommended. Testing has generally demonstrated that legally-available responses have little chance of physically succeeding in this regard. This is primarily the result of the lack of visibility: SUAVs often fly at 200m height and possess a low IR/radar signature.



The photo shows a larger SUAV (commercially designed for long-flight times) than is usual at 50m height.

An intrusive SUAV could be less than half the size and could be between four and eight times higher up than the model shown with correspondingly reduced visibility.

Photo credit: Astec

Nor do options generally exist for countering the operators themselves. No commercially available technology currently exists which can identify the radio-frequency signature / identify the location of the user (teleoperator). As users may be significantly removed from the location being intruded upon (including within private property), it is generally considered non-viable to respond to the UAV by targeting the operator.

Threat Assessment:

The nature of the SUAV threat is currently primarily of concern for the potential use of such platforms for either hostile surveillance or nuisance factor. Currently, there are a range of widely-accessible commercial visual systems which can transform an equally accessible UAV kit into a highly capable surveillance option. Such a system could conceivably access secured premises and view either sensitive business processes (such as supply chain / manufacture) or even identify sensitive documents if left on display.

The level of risk to companies / organisations would primarily be equivalent to the existing risk posed by corporate espionage (i.e. theft of intellectual property (IP) or confidential information potentially leading to a fall in revenues). However, there also exists a level of reputational risk, particularly if holding sensitive client / supplier information. Either of these elements (and others) could represent significant consequences.

While the nature of the UAV threat is clear and growing; in fundamental terms, the threat itself should not necessarily be thought of as insurmountable. The reality is that the threat of corporate espionage and hostile surveillance is an established threat which predates the growth of UAV technology. While the methods previously adopted (individual infiltration / ground-based or covert cameras / theft) may have been more basic, the response required is generally the same:

Surveillance:

- Whether or not the camera is carried by a person or a UAV, the issue is what materials / information the surveillance can physically identify / record and how damaging such access could be.
- In this regard, the counter-measures for personal surveillance and UAV surveillance are generally identical (i.e. keeping confidential documents secure, avoiding potential line of sight to such documents – through curtains / blinds / tinted film – and generally ensuring that any sensitive processes / materials are restricted from general view).
- Similarly, with residential accommodation, blinds / curtains provide effective mitigation to potential intrusive surveillance (as with the standard response to non-UAV surveillance).

Nuisance:

- As with surveillance, standard security recommendations (threat awareness, manned guarding of sites, use of CCTV) remain standard mitigation measures for limiting the nuisance factor posed by UAVs (primarily as deterrence).
- Due to the absence of physical counter-measures, no practical response (beyond reporting, below) may be achievable. However, facilities / security should be aware that any active nuisance (which would require direct control / teleoperation) would be limited to only a few minutes (less than thirty) and would be unlikely to disrupt operations for more than a very short period of time.

Physical Harm:

- It is assessed that the technology required to enable SUAVs to present a threat of physical harm is not yet advanced enough to require any new response.

Overall, the primary threat posed by SUAVs is that of hostile surveillance. However, existing control measures are generally sufficient to mitigate this threat although Pilgrims also proposes the following additional recommendations.

Recommendations:

1. It is recommended, as a new measure, that the identification of a UAV / SUAV by site personnel should immediately be reported to facilities / security (and also to law enforcement) as a standard procedure (as well as logging the date / time / location). While the response is limited, awareness of the existence of hostile surveillance may enable awareness of the target and enable a more efficient future response / legal effort. As UAVs have a generally short flight time, immediate response may enable an effective police response against culprits.

2. Active threat awareness / liaison with law enforcement is continued to determine the level of hostile intent faced by particular sites / organisations. This will enable an appropriate preparation / response to the SUAV threat.

Now what?

The forecast for UAV and SUAV technologies is for rapid technological development and increased refinement of tactics, techniques and procedures (TTPs) by various hostile users due to the open sharing of such TTPs online.

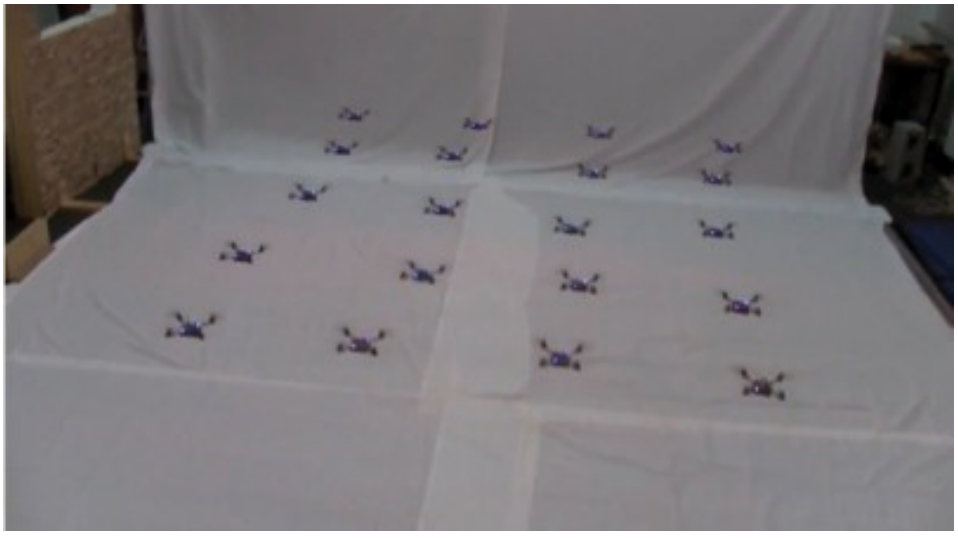
The key technological trends are all likely to be evolutionary rather than revolutionary (i.e. extensions of current trends rather than disruptive technologies emerging in place) although such developments will generate TTPs which represent a greater threat.

These evolutions include:

- Miniaturisation / increased efficiency: SUAVs will become smaller and more capable for their size, as will the existing payloads. This will generate longer flight-times, better surveillance capabilities and the emergence of more hostile applications (including physical harm). **Timeframe: Short term.**

- 'Swarm' based attacks / improved artificial intelligence (AI): Advances in AI for SUAVs continues to improve and adaptive behaviour to surroundings will become increasingly viable. This will extend their utility for users to program activities (and reduce the current UAV limitations / vulnerabilities). It will also enable increased usage of 'swarm' tactics: the use of multiple, synchronised UAVs capable of functioning together without multiple users. This will enable one user to significantly increase activities. **Timeframe: Medium term.**

- Physical attacks: The usage of UAVs to conduct attacks has been seen, but in minute levels. In the future, as the technology enables such usage and becomes publicised, such attacks are likely to become an increased factor and will represent a more substantial (if generic) risk. **Timeframe: Long term.**



UAV 'swarm' program currently under development by Royal Aeronautical Society.

These SUAVs are able to interact (without human input) to maintain relative flight position / prevent collisions.

Photo credit: Royal Aeronautical Society.

Pilgrims has compiled this report, drawing on information from a variety of media, open and privileged sources. Any feedback on this report is most welcome and should be addressed to the Information and Intelligence Department.

(Email: intcel@pilgrimsgroup.com or telephone: +44 (0) 1483 228785).