Hostile drones
Supplementary risk assessment

12 January 2016

The following is provided as a supplement to the Open Briefing/Remote Control Project report *Hostile drones: The hostile use of drones by non-state actors against civilian targets*, available at http://www.openbriefing.org/thinktank/publications/hostile-drones-the-hostile-use-of-drones-by-non-state-actors-against-british-targets/.

The overall risk from the hostile use of drones by non-state actors against British targets is assessed to be **medium,** though the threat from terrorist organisations and insurgent groups is assessed as **high.** This is based on a risk assessment involving 270 individual likelihood/impact judgements taking into account the type of threat group (terrorist, insurgent, criminal, activist or corporate), the type of unmanned vehicle (aerial, ground, surface marine or submersible marine), the theatre (domestic or international), the nature of the threat (attack or intelligence) and the target (long-term static, temporary static or mobile). The risk ratings by drone type and nature of the threat are provided in Table 1 and by threat group and nature of the threat in Table 2. The full risk assessment is provided in Appendix 1, and a narrative is provided in the following pages.

Lone wolf

A lone wolf uses terrorist tactics to pursue explicitly political or ideological goals but acts without membership of a terrorist organisation or cell. The lack of group decision-making means creativity is unstifled and the lone wolf can think 'outside the box'. An innovative individual prepared to use violence is a dangerous adversary. In theory, a drone represents an excellent platform for such an individual to use in an attack, as it is able to deliver destruction without directly risking the terrorist's life and can circumvent many current security measures, such as the police searching and destroying unattended bags.

Fortunately, there has so far been very few instances of individual terrorists using drones to undertake attacks. What could be was demonstrated in April 2015 when a man landed a drone on the Japanese prime minister's office in Tokyo. The drone was carrying a bottle containing radioactive sand from Fukushima, which was emanating up to 1.0 micro Sievert per hour. In another example from the United States, a 26-year-old man with a physics degree planned to crash drones carrying five pounds of plastic explosives each into the Pentagon.

open briefing
the civil society intelligence agency

Open Briefing
27 Old Gloucester Street
Bloomsbury
London WC1N 3AX

t 020 7193 9805
info@openbriefing.org
www.openbriefing.org

Open Briefing Ltd is a non-profit company limited by guarantee.
Registered in England & Wales, No. 07649656.

Table 1. Risk rating by drone type and nature of the threat.

Drone type	Attack	ISR
Unmanned aerial vehicle	High	High
Unmanned ground vehicle	Medium	Low
Surface unmanned marine vehicle	High	Medium
Submersible unmanned marine vehicle	Low	Low

Table 2. Risk rating by threat group and nature of the threat.

Threat	Attack	ISR	Overall
Lone wolf	Medium	Low	Low
Terrorist organisations	High	Medium	High
Insurgent groups	High	High	High
Organised crime groups	Low	Medium	Low
Activists	Low	Medium	Medium
Corporations	Low	Medium	Low

It is possible to import a UAV in the United Kingdom for around £8,000 capable of flying up to 15 miles carrying a payload of 7.5 kilograms. A cheaper drone purchased in the United Kingdom could be modified to carry a 3-5 kilogram payload. It would be relatively cheap and feasible for a lone wolf to plan and undertake an attack using such a drone. The biggest obstacle the individual terrorist would have to overcome is obtaining the explosive materials. A homemade fertiliser bomb weighing 7.5 kilograms would be insufficient to cause serious damage to a building or armoured vehicle, though it would cause significant harm if directed towards an individual target or a group of people. A payload of 7.5 kilograms is roughly comparable to an rocket-propelled grenade, three pipe bombs or a suicide vest.[1] (For comparison, the suicide bombing at Domodedovo airport in Russia in 2011 had the power of 7 kilograms of TNT and caused 35 deaths and 130 injuries.)

Of course, a drone itself could also be used as a weapon if flown into an aeroplane or vehicle for example. A drone could also be weaponised with a handgun or other firearm.[2]

The lack of backing from a terrorist group able to procure explosive material limits the threat posed by lone wolf attackers. The threat can easily be further mitigated by bringing in new regulations that restrict the capabilities of commercially available drones and limit the ability of hostile individuals to procure and fly drones. However, while the overall threat is limited, the use of drones as a delivery system is increasingly likely as the price of payload-capable drones decreases.

[1] http://www.nctc.gov/site/technical/bomb_threat.html

[2] https://www.youtube.com/watch?v=xqHrTtvFFIs

Terrorist organisations

In March 2015, the UK government proscribed 67 international organisations under the Terrorism Act 2000.[3] Many of these groups have threatened or attempted terrorist attacks on British soil. Islamic State has an annual turnover of $2 to $3 billion,[4] while al-Qaeda was at one point able to carry out the worst terrorist attacks the United States has ever suffered. These organisations could purchase highly-advanced unmanned aerial, marine or ground vehicles and use smuggler routes to bypass British drone importation regulations. Alternatively, platforms weighing less than 20 kilograms could be purchased in the United Kingdom and customised or specialised platforms could be stolen from businesses licenced to operate them. Unlike the lone wolf terrorist, international terrorist organisations would also have access to explosive material capable of causing large-scale destruction.

State-sponsored terrorist organisations present a serious threat to British interests abroad because of their ability to obtain sophisticated military-grade drones. For example, Hamas and Hezbollah have access to Iranian drones, and Hamas claims to have three models of drone capable of surveillance, launching missiles and nose-diving into a target.

There are significant barriers to planning and carrying out a major terrorist attack of any sort. The intelligence work carried out by the British security services provides a robust line of defence against terrorist groups. There have been no known examples in the United Kingdom, Europe or the United States of terrorist organisations using drones for either attack or intelligence gathering. However, Islamic State is reportedly obsessed with launching a synchronised multi-drone attack on large numbers of people in order to recreate the horrors of 9/11. There is a moderate probability that such an attack will take place. The impact of single drone with an explosive payload could be high; the impact of several drones would be devastating.

Insurgent groups

The international nature of many of terrorist organisations means they are also often insurgent groups. While Islamic State may or may not be preparing drone attacks on British soil, there is already evidence of the group using drones in Iraq and Syria. In August 2014, Islamic State released a video featuring reconnaissance of a Syrian military base in Raqqa.[5] In April 2015, Islamic State released a video showing UAVs being used for reconnaissance and battlefield coordination during its assault on the Baiji oil refinery complex in Iraq.[6] In August 2015, US Central Command released a list of airstrike targets around the world, including 'an ISIL drone' near Ramadi in Iraq.[7] In December 2015, unconfirmed reports emerged that Islamic State had attempted to use small drones packed with explosives as weapons against Kurdish forces.[8]

[3] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/417888/Proscription-20150327.pdf

[4] http://www.openbriefing.org/regionaldesks/middleeast/transnational-organised-crime-monthly-briefing-islamic-states-income-from-transnational-organised-crime/

[5] http://edition.cnn.com/2014/08/24/opinion/bergen-schneider-drones-isis/

[6] http://www.longwarjournal.org/archives/2015/04/islamic-state-uses-drones-to-coordinate-fighting-in-baiji.php

[7] http://www.centcom.mil/en/news/articles/august-3-military-airstrikes-continue-against-isil-terrorists-in-syria-and

[8] http://www.popularmechanics.com/military/weapons/a18577/isis-packing-drones-with-explosives/

Insurgent groups have many of the same capabilities and intentions as terrorist organisations, but do not face the same regulatory and law enforcement barriers to attacks on British interests as groups attempting to use drones to launch attacks within the United Kingdom. Drones therefore have the potential to become significant components of insurgents' armouries. For example, larger UAVs allow insurgents to fly an IED directly to its target from miles away rather than laying it as a trap. While it is entirely possible for an insurgent group to down a military drone, they are highly unlikely to have the necessary skills and equipment to successfully re-engineer the aircraft for their own use (unlike Iran, for example, which claimed to have captured and reverse engineered a US military RQ-170 Sentinel surveillance drone in 2011).

Obtaining aerial, ground and marine reconnaissance and attack capabilities would mark a step change for many insurgent groups. The greatest defence against relatively poorly-equipped and untrained insurgents has been their inability to conduct well-coordinated operations on the ground. The British solider can fight from a position of strength partly due to better intelligence on the insurgent's positions, equipment and movements. With the development of UAVs in particular, and UGVs and UMVs to some extent, modern armies lose some of their advantages. The insurgent may now have a near-equal knowledge of the enemy's deployment on the battlefield or the defensive measures being deployed against them at a targeted military base.

Organised crime groups

Organised criminal gangs are known to have used unmanned aerial vehicles to traffic illicit drugs across the US-Mexican border and trends suggest that South American gangs are likely investing in unmanned marine vehicles for similar purposes. With the ever more extensive use of security patrols and technical surveillance of most Western land borders, it is likely that criminal gangs will continue to use drones for the trafficking of drugs and other contraband until effective countermeasures are deployed. While drone use in this context continues to be probable, the low level of drone shipments to date means this method of smuggling is unlikely to play a significant part in the global drug trafficking threat in the short to medium term.

There is a role for aerial drones in providing surveillance cover for criminal groups. Camera-capable drones are both inexpensive and small. Drug traffickers could deploy drones to escort conventional shipments, providing early warning of approaching law enforcement units. A similar function could be provided to human traffickers. This would not, however, offer much additional protection for traffickers across the United Kingdom's maritime borders, as the open sea provides few hiding places to exploit even with the early warning of an approaching patrol. Groups involved in organised theft, such as the theft of cash-in-transit from an armoured vehicle, could also use drones to track the target and monitor the police response.

Beyond payload carrying and surveillance, one more application that is shared with the other threat groups is using a drone to physically attack a target. In the criminal context, this would likely be the murder of a rival or an informant. However, while this is another potential scenario, the likelihood of a criminal group undertaking such a high-tech exercise is low; there are easier and more effective ways to carry out such actions.

Activists

Drones offer force-multiplying options to activists and protesters. Although the use of drones by such groups is still low, the ability to operate at a distance from the target, with a minimised chance of disruption by security forces, will almost certainly become increasingly attractive to direct action activists.

The most likely way in which drones will be used is in undertaking publicity-seeking exercises in front of the media or filmed using onboard cameras. This may cause disruption to major events or the activities of corporations. Activities designed to embarrass a target are very possible – for example, air-dropping fake money around a campaigning politician linked to corruption. If a group's plan is innovative enough, there is the potential for footage of the event to go viral across news and social media, bringing much more attention to their cause.

Activists could also use drones to assist existing campaign efforts through reconnaissance and surveillance. Animal welfare groups are known to have used drones to monitor farms and animal testing facilities in the United States and an unidentified group has been flying drones over multiple French nuclear power stations. Direct action groups are now able to conduct support missions using drones prior to a protest action; for example, using a UAV to identify the least secure points of an establishment's perimeter immediately prior to a breach, then using it to provide air cover monitoring the security response. Anarchist groups could also use UAVs fitted with cameras to monitor police responses to large protests and coordinate counter-strategies.

Drones also offer activists a greater range of possibilities for more offensive operations against targets, with the aim of causing damage and disruption. There have been numerous incidents of over-enthusiastic leisure users flying drones near airports, which have highlighted the ability of these vehicles to circumvent conventional ground-based access controls, and their potential to cause significant disruption to airport operations is apparent. UAVs with small non-explosive payloads could easily be used to sabotage energy infrastructure. Operations are not limited to using aerial drones; unmanned maritime vehicles, especially cable-controlled submersibles, could be used against oil installations for example.

The risk to life and property from activists is assessed to be low, especially when compared to the risk from other threat actors, such as terrorist groups. The risk is potentially further mitigated by current UK legislation that restricts the use of drones near private buildings or large crowds and the right individuals and organisations have to use defensive measures to bring down unauthorised drones operating over their private property.

Corporations

There are no documented examples of private corporations using drones illegally for commercial gain. However, as in the above contexts, the potential rewards from exploiting drone technology are very apparent. The probability of offensive drone actions by companies that threaten life and property is low. It is more likely that foreign corporation might use drones to carry out intelligence gathering against British competitor companies.

Example scenarios include surveillance of a competitor testing products, such as cars, weapons or racing yachts. In the latter example, submersible UMVs could be used to monitor vessel design and performance (multiple incidents of espionage have been reported in the America's Cup for example). Existing off-the-shelf technology has long enabled communications and computer network activity to be monitored remotely, and drones could also be used by a company to drop monitoring hardware on a competitor's premises. Such operations would be low-risk to the operator, with little chance of identification even if the drone was seized, but could provide valuable intelligence on a competitor's activities.

Many companies, especially those operating in the more technologically-advanced and competitive sectors, already take considerable measures to secure their intellectual property. It will not be long before companies will need to seriously consider the role drones might play in corporate espionage. It is very likely that the counter-surveillance industry will grow as companies routinely deploy passive countermeasures in order to protect their highly-valuable data and products from corporate espionage using drones.

One offensive scenario is the use of crowd control drones by British companies against strikers or demonstrators threatening foreign operations. An example of such a drone is the Desert Wolf Skunk, which is equipped with four high-capacity paint ball barrels that can fire a variety of ammunition, including pepper spray balls and plastic balls. The drones can be flown in formation by a single operator. In what the South African company calls a 'life threatening situation', each drone can fire 80 balls per second, allowing for 'real stopping power'.[9] Desert Wolf reportedly sold 25 Skunks to an international mining company after a photo of the drone was featured on a military news website in May 2014.

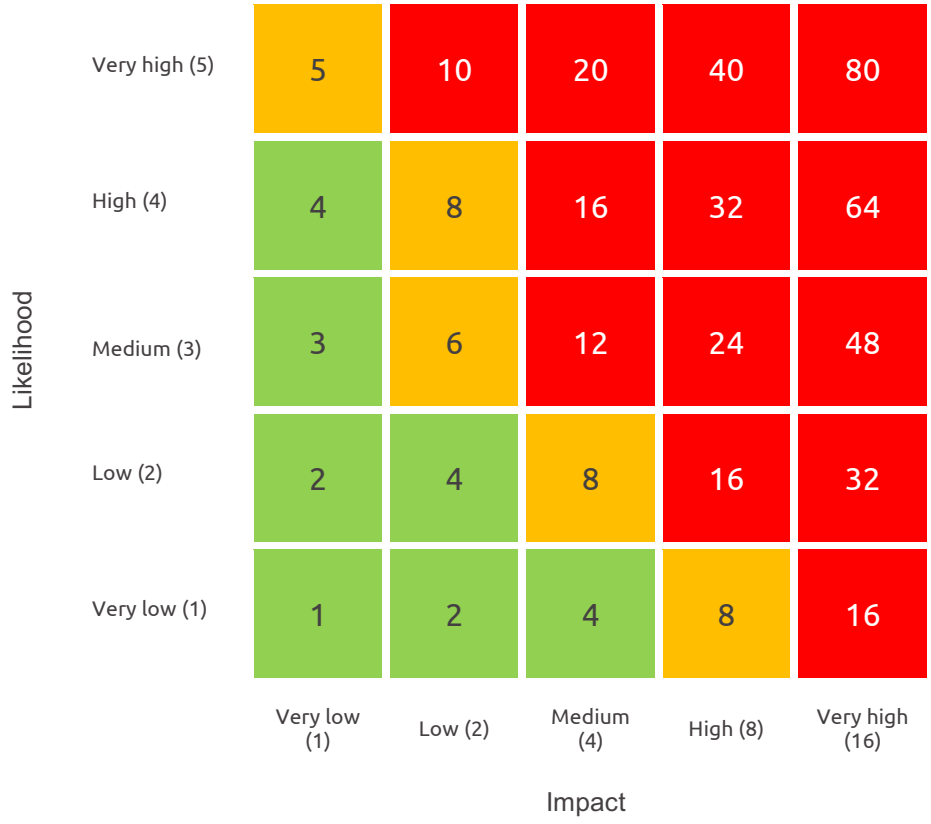
[9] http://www.desert-wolf.com/dw/products/unmanned-aerial-systems/skunk-riot-control-copter.html

Appendix 1: Risk assessment

A **threat** is a function of **capability and intent. Risk** is a function of **likelihood** (taking into account **threat and vulnerability**) and **impact** (taking into account **mitigation** measures) of the threat occurring. Impact takes into account a range of physical, financial, psychological, reputational and operational factors as well as level of vulnerability and any mitigation measures already in place.

Threat = Capability x Intent
Risk = Likelihood (Threat + Vulnerability) x Impact

The risk ratings in this report range from Low to High. The ratings are based on the risk matrix below.[10] This gives more weight to risks with a high impact by doubling the numeric value each time on the impact scale. This means a low probability/high impact risk is assessed as much more severe than a high probability/low impact risk. This avoids any averaging out of serious risks.



[10] https://www.jisc.ac.uk/guides/risk-management/qualitative-risk-analysis

Table 3. Qualitative risk analysis.

Threat	Attack			ISR			Overall risk rating		
	Likelihood	Impact	Overall	Likelihood	Impact	Overall	Likelihood	Impact	Overall
Lone wolf	**Low** (2)	**Medium** (3)	**Medium** (6)	**Low** (1.25)	**Low** (2.75)	**Low** (3.4)	**Low** (1.6)	**Low** (2.9)	**Low** (4.6)
Unmanned aerial vehicle	Medium (3)	Medium (4)	High (12)	Low (2)	Low (2)	Low (4)	Medium (2.5)	Low (2)	Medium (5)
Unmanned ground vehicle	Low (2)	Low (2)	Low (4)	Very low (1)	Very low (1)	Low (1)	Low (1.5)	Low (1.5)	Low (2.25)
Surface unmanned marine vehicle	Low (2)	Medium (4)	Medium (8)	Very low (1)	Medium (4)	Low (4)	Low (1.5)	Medium (4)	Medium (6)
Submersible unmanned marine vehicle	Very low (1)	Low (2)	Low (2)	Very low (1)	Medium (4)	Low (4)	Very low (1)	Medium (3)	Low (3)
Terrorist organisations	**Medium** (2.5)	**Medium** (5)	**High** (12.5)	**Low** (2)	**Medium** (3.25)	**Medium** (6.5)	**Low** (2.25)	**Medium** (4.1)	**Medium-High** (9.2)
Unmanned aerial vehicle	High (4)	High (8)	High (32)	High (4)	Medium (4)	High (16)	High (4)	High (6)	High (24)
Unmanned ground vehicle	Low (2)	Low (2)	Low (4)	Very low (1)	Very low (1)	Low (1)	Low (1.5)	Low (1.5)	Low (2.25)
Surface unmanned marine vehicle	Medium (3)	High (8)	High (24)	Low (2)	Medium (4)	Medium (8)	Medium (2.5)	High (6)	High (15)
Submersible unmanned marine vehicle	Very low (1)	Low (2)	Low (2)	Very low (1)	Medium (4)	Low (4)	Very low (1)	Low (3)	Low (3)
Insurgent groups	**High** (3.5)	**Medium** (5.5)	**High** (19.25)	**Low** (2.25)	**Medium** (4.25)	**Medium-High** (9.6)	**Medium** (2.9)	**Medium** (4.9)	**High** (14.2)
Unmanned aerial vehicle	Very high (5)	High (8)	High (40)	Very high (5)	High (8)	High (40)	Very high (5)	High (8)	High (40)
Unmanned ground vehicle	Very high (5)	Medium (4)	High (20)	Very low (1)	Very low (1)	Low (1)	Medium (3)	Low (2.5)	Medium (7.5)
Surface unmanned marine vehicle	Medium (3)	High (8)	High (24)	Low (2)	Medium (4)	Medium (8)	Medium (2.5)	High (6)	High (15)
Submersible unmanned marine vehicle	Very low (1)	Low (2)	Low (2)	Very low (1)	Medium (4)	Low (4)	Very low (1)	Medium (3)	Low (3)
Organised crime groups	**Low** (1.25)	**Low** (2.5)	**Low** (3.1)	**Low** (2)	**Low** (2.75)	**Low-Medium** (5.5)	**Low** (1.6)	**Low** (2.6)	**Low** (4.2)
Unmanned aerial vehicle	Low (2)	Low (2)	Low (4)	Very high (5)	Medium (4)	High (20)	High (3.5)	Medium (3)	High (10.5)
Unmanned ground vehicle	Very low (1)	Low (2)	Low (4)	Very low (1)	Very low (1)	Low (1)	Very low (1)	Low (1.5)	Low (1.5)

Threat	Attack			ISR			Overall risk rating		
	Likelihood	Impact	Overall	Likelihood	Impact	Overall	Likelihood	Impact	Overall
Surface unmanned marine vehicle	Very low (1)	Medium (4)	Low (4)	Very low (1)	Medium (4)	Low (4)	Very low (1)	Medium (4)	Low (4)
Submersible unmanned marine vehicle	Very low (1)	Low (2)	Low (2)	Very low (1)	Low (2)	Low (2)	Very low (1)	Low (2)	Low (2)
Activists	**Low** (2)	**Low** (2)	**Low** (4)	**Low** (2.25)	**Low** (2.75)	**Low-Medium** (6.2)	**Low** (2.1)	**Low** (2.4)	**Low-Medium** (5)
Unmanned aerial vehicle	Medium (3)	Medium (4)	High (12)	High (4)	Medium (4)	High (16)	High (3.5)	Medium (4)	High (14)
Unmanned ground vehicle	Low (2)	Very low (1)	Low (2)	Very low (1)	Very low (1)	Low (1)	Low (1.5)	Very low (1)	Low (1.5)
Surface unmanned marine vehicle	Low (2)	Low (2)	Low (4)	Medium (3)	Medium (4)	High (12)	Medium (2.5)	Medium (3)	Medium-High (7.5)
Submersible unmanned marine vehicle	Very low (1)	Very low (1)	Low (1)	Very low (1)	Low (2)	Low (2)	Very low (1)	Low (1.5)	Low (1.5)
Corporations	**Low** (1.25)	**Low** (2.25)	**Low** (2.8)	**Low** (1.75)	**Medium** (3.5)	**Low-Medium** (6.1)	**Low** (1.5)	**Low** (2.9)	**Low** (4.4)
Unmanned aerial vehicle	Low (2)	Medium (4)	Medium (8)	Medium (3)	Medium (4)	High (12)	Medium (2.5)	Medium (4)	High (10)
Unmanned ground vehicle	Very low (1)	Low (2)	Low (2)	Very low (1)	Low (2)	Low (2)	Very low (1)	Low (2)	Low (2)
Surface unmanned marine vehicle	Very low (1)	Low (2)	Low (2)	Low (2)	Medium (4)	Medium (8)	Low (1.5)	Medium (3)	Medium (4.5)
Submersible unmanned marine vehicle	Very low (1)	Very low (1)	Low (1)	Very low (1)	Medium (4)	Low (4)	Very low (1)	Low (2.5)	Low (2.5)

Open Briefing is the world's first civil society intelligence agency. Founded in 2011, our mission is to keep those striving to make the world a better place **safe and informed.** We provide **groundbreaking intelligence and security services** to aid agencies, human rights groups, peacebuilding organisations and concerned citizens. We do this so that a stronger civil society can **promote alternatives to armed conflict, protect human rights and safeguard the environment.**

Key services we provide include:

- Responding to **requests for intelligence, security or training** from NGOs and journalists.
- Issuing **regular intelligence briefings and risk assessments** for the general public.
- Developing **innovative policy solutions** and promoting them to government.
- Providing **expert consultancy services** to the third sector.

Open Briefing is a bold and ambitious nonprofit social enterprise. We are a **unique international collaboration of intelligence, military, law enforcement and government professionals** working tirelessly behind the scenes to make a difference.

We are challenging the status quo. We are *your* intelligence agency.

www.openbriefing.org