HOSTILE DRONES:

THE HOSTILE USE OF DRONES BY NON-STATE ACTORS AGAINST BRITISH TARGETS

January 2016

REMOTE CONTROL
Examining changes in military engagement

open briefing
the civil society intelligence agency

The Remote Control project is a project of the **Network for Social Change** hosted by **Oxford Research Group**. The project examines and challenges changes in military engagement, in particular the use of drones, special operations forces (SOF), private military and security companies (PMSCs) and cyber and intelligence activities.

Chris Abbott is the founder and executive director of Open Briefing. He is also an honorary visiting research fellow in the School of Social and International Studies at the University of Bradford and was the deputy director of the Oxford Research Group until 2009.

Matthew Clarke is an associate researcher at Open Briefing. He is also a freelance campaigner and analyst. He has worked in business, politics and the European NGO community.

Steve Hathorn is a senior analyst at Open Briefing. He is an intelligence analyst with nearly 30 years' experience in the British Army, Defence Intelligence Staff, National Criminal Intelligence Service, United Nations, International Criminal Court and the National Crime Agency.

Scott Hickie is a senior analyst at Open Briefing. He is also a senior policy officer for the New South Wales government. He is a former political adviser and lawyer.

Open Briefing is the world's first civil society intelligence agency. Founded in 2011, its mission is to keep those striving to make the world a better place safe and informed. It provides groundbreaking intelligence and security services to aid agencies, human rights groups, peacebuilding organisations and concerned citizens. It does this so that a stronger civil society can promote alternatives to armed conflict, protect human rights and safeguard the environment. Open Briefing is a bold and ambitious nonprofit social enterprise. It is a unique international collaboration of intelligence, military, law enforcement and government professionals working tirelessly behind the scenes to make a difference.
www.openbriefing.org

Published by the Remote Control project, January 2016

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298
media@remotecontrolproject.org

http://remotecontrolproject.org

Cover image: Pieces of a Hezbollah UAV (Unmanned aerial vehicle) that was taken down by the Israeli Air Force. Wikimedia Commons, Flickr/ Israel Defense Forces

Contents

Executive Summary

Ever-more advanced drones capable of carrying sophisticated imaging equipment and significant payloads are readily available to the civilian market. Unmanned aerial vehicles (UAVs) currently present the greatest risk because of their capabilities and widespread availability, but developments in unmanned ground (UGVs) and marine vehicles (UMVs) are opening up new avenues for hostile groups to exploit.

A range of terrorist, insurgent, criminal, corporate and activist threat groups have already demonstrated the ability to use civilian drones for attacks and intelligence gathering. The best defence against the hostile use of drones is to employ a hierarchy of countermeasures encompassing regulatory countermeasures, passive countermeasures and active countermeasures.

Regulatory countermeasures can restrict the capabilities of commercially available drones and limit the ability of hostile groups and individuals to procure and fly drones. Policymakers should pass stricter regulations limiting the capabilities of commercially available drones in the key specifications affecting hostile drone operations, particularly payload capacity. Particular attention should be paid to limiting the attack and ISR capabilities of UAVs and the attack capabilities of surface UMVs. Manufacturers should be required to install firmware that includes the GPS coordinates of no-fly zones around sensitive fixed locations. Finally, civilian operators of drones capable of carrying payloads should be licenced and the serial numbers of purchased drones registered.

Passive countermeasures alert security to the presence of any drone within a no-fly zone or defensive perimeter around a static or mobile target. They limit the ability of hostile groups and individuals to guide a drone onto a mobile target or target of opportunity or take evasive action against any kinetic defences. The British government should support the research and development of commercial multi-sensor systems capable of detecting and tracking drones within a target area. The government should also make funding available to police forces and specialist units for the purchase of early warning systems and other passive drone countermeasures, including radio frequency jammers and GPS jammers. The government should also relax the regulations restricting the use of radio frequency jammers for protection against hostile drone use around defined key sites.

Active countermeasures can be deployed against drones that still represent a threat despite passive systems being employed. However, the active countermeasures currently available for use in non-military settings are limited. The British government should support the research and development of innovative less-lethal anti-drone systems, such as directional radio frequency jammers, lasers and malware, and set out clear guidelines for the police and military use of kinetic weapons against hostile drones as a last line of defence.

However, such countermeasures are not foolproof. Furthermore, there is also the very real chance that, as with drones themselves, countermeasures will be deployed in turn by some threat groups against British police or military drones. The technology of remote-control warfare is impossible to control; the ultimate defence is to address the root drivers of the threat in the first place.

Introduction

After long and frequently controversial use by the military, unmanned vehicle technology is now being widely employed in numerous civilian settings. There are unmanned vehicles (or drones) for use in the air (UAVs), on land (UGVs) and on or under the sea (UMVs). Drones are used for leisure and to monitor crops, take aerial photographs, track hurricanes, protect wildlife, monitor traffic, deliver parcels, undertake search and rescue operations and monitor disaster zones. As with many preceding technologies, civilian drones are also used for less benign purposes, including snooping and harassment, drug trafficking and smuggling contraband into prisons.

Ongoing large-scale commercial investment has led to civilian drones becoming cheaper, able to operate over longer ranges and capable of carrying ever-larger payloads. The pace of development has accelerated in recent years, with a vast range of models now available to the civilian customer. There are hundreds of models available, ranging in size from that of an AA battery to prototypes capable of carrying a person.

The legislation governing the civilian use of drones is still evolving. It is struggling to keep up with the speed at which innovative uses are being identified and new drones developed. There are growing concerns over the use of drones by private individuals with little knowledge of aviation rules. In July 2015, the US Department of Homeland Security distributed an intelligence assessment to law enforcement agencies warning of the possibility of criminal or terrorist groups using unmanned aerial vehicles.

In February 2015, the House of Lords EU Select Committee called for the mandatory registration of all civilian drones in the United Kingdom. As legislation stands, anyone can buy a drone and immediately operate it without any training or a license, as long as the drone weighs less than 20 kilograms and it is not being used for commercial purposes. While there are minimal regulations specifically governing the use of ground and marine drones, aerial versions must not be flown within 150 metres of any populated area or 50 metres of any other person, vehicle or structure. The operator is also required to keep the drone in sight, within 500 metres and below 400 feet in altitude. While these simple rules will be followed by the majority of leisure users, those with more nefarious motivations will be less inclined to adhere to them. Even if followed, the regulations cannot account for operator error or technical drone failures. The regulations surrounding UGVs and UMVs are less clear, though existing maritime navigation rules and motor vehicle regulations will likely apply and combat vehicles will likely be covered by existing import/export arms control regimes.

This report details the findings of our study into the hostile use of drones by non-state actors against British targets. While the focus is on unmanned aerial vehicles, we have examined the designs and capabilities of over 200 current and upcoming unmanned aerial, ground and marine systems in order to understand the threat these platforms pose to potential targets. The previous hostile use of drones by non-state actors is also examined. A range of terrorist, insurgent, criminal, corporate

and activist threat groups using drones for attacks and intelligence gathering are identified. The report outlines specific recommendations on the strategies available to mitigate the threat of the hostile use of drones by non-state actors in the short to medium term.

There is no doubt that unmanned vehicles are here to stay and will have a considerable impact on society, both beneficial and detrimental. Although there is still a large gap between the capabilities of military and civilian drones, commercially available drones are giving hobbyists, companies and hostile groups access to capabilities previously only available to the military. Law enforcement agencies and policymakers are struggling to respond appropriately to this development. This report is a contribution to countering that threat.

Assessment of commercially-available unmanned vehicles

Unmanned aerial vehicles

The civil and commercial market for unmanned aerial vehicles has grown significantly over the last five years. The increasing uptake by the commercial sector is clearly evidenced in the growing numbers of US Federal Aviation Administration (FAA) exemptions for drone operators to fly UAVs in the National Airspace System (NAS),[1] with the exemptions list showing a broad range of UAV technologies, uses and capabilities.[2] The UK Civil Aviation Authority (CAA) also has a similar licensing regime for operators using UAVs for commercial aerial work and equipped for data acquisition. As of 11 September 2015, the CAA has issued 1,036 current UAV licences, with an estimated 37% of licences for models in the 7-20 kilogram weight class.[3] The civil or hobbyist market is also showing significant growth. Some estimates have the global civil and commercial UAV sector valued at €563.7 million (£418 million).[4]

UAVs are commercially available as off-the-shelf Ready to Fly (RTF), Bind and Fly (BNF – with customisable transmitter) and Plug and Fly (PNF – with customisable transmitter, receiver, battery and charger). Users with no prior UAV flying experience can procure RTF models, and more experienced and knowledgeable users can purchase fully-customisable PNF models. Most commercially available models are rotary multicopter UAVs coming in quadcopter (four propellers), hexacopter (six propellers) and octocopter (eight propellers) variants. Fixed-wing UAVs are more frequently used for commercial deployments in agriculture, public safety, emergency response and ISR. Many UAV manufactures sell individual components, enabling customers to build fully-customised drones. This allows users to achieve specific capabilities, such as flight time, payload capacity, programmable flight, maximum speed and weather hardening. Table 1 lists the most popular and readily-available commercial UAVs across three price points (low end, mid level and high end) and provides basic specification information.

Our analysis of the 202 commercially-available drones listed on the product comparison site SpecOut.com reveals that the listed drones have an average flight time of 18 minutes, an average range of 1,400 metres and median price of $600 (£390).[5] Our analysis of FAA Section 333 exemptions indicates that in the United States the agricultural and film sector are using UAVs with the largest capacity for heavier payloads, most likely a result of needing to carry larger sensor and imagery equipment. The public safety, emergency response and infrastructure inspection sectors appear to be relying upon UAVs with greater capacity for all-weather conditions.

---

1 Section 333 FAA Modernization and Reform Act of 2012 (FMRA).
2 https://www.faa.gov/uas/legislative_programs/section_333/333_authorizations/ and http://auvsilink.org/advocacy/Section333.html.
3 https://www.caa.co.uk/docs/1995/SUA%20Operators%2011Sep15.pdf.
4 INEA Consulting (2014), Global Commercial and Civil UAV Market Guide 2014-2015.
5 http://drones.specout.com.

Specifications affecting hostile UAV operations

A number of specifications are critical to the capabilities and uses of aerial drones. Users seeking greater payload capacity, flight time and range will most likely build customised drones from individual components to specification, requiring some basic technical knowledge. The specifications most relevant to UAV operations include:

Payload

Most RTF and BNF UAVs have a limited payload capacity beyond that required for a gimbal, camera and battery. Those with larger capacity payloads are UAVs aimed at carrying a broader range of imagery capture hardware, such as LiDAR or infrared camera, or other environmental sensors. Despite some high-profile interest, such as Amazon's nascent Prime Air service, logistics and transport companies have not embraced the use of UAVs because many commercially available platforms have insufficient carrying capacity for goods.

Range

Commercially available UAVs are generally limited in range by signal transmission and image relay distance and battery power (flight time). This means a pilot must be within a particular proximity of the UAV and that flights cannot span a significant distance. Flight time due to power constraints can be partially managed by interrupting flights for battery changes.

Table 1. Select list of commercially available UAVs

Model	Weight	Payload	Flight time	Range	Max speed	Camera	Operating conditions	Price
Parrot BeeBop	0.4 kg	0 kg	12 mins	250 m (extendable)	29 mph	Yes (14MP)	Dry conditions only	£700-900 (RTF)
Blade 350 QX2	1 kg	0.2 kg	10 mins	1,000 m	32 mph	Yes	Dry conditions only	£200-300 (RTF)
3DR IRIS+	0.9 kg	0.2 kg	16 mins	800-1,000 m	40 mph	Yes	Dry conditions only	£500-600 (RTF)
DJI Phantom 2 Vision +	1.2 kg	0.2 kg	25 mins	600 m	33 mph	Yes (14MP)	Dry conditions only	£800-1,200
DJI Phantom 3 Professional	1.2 kg	0.3 kg	28 mins	1,900 m	35 mph	Yes (12MP)	Dry conditions only	£1,000-1,200
Walkera Scout X4	1.7 kg	0.5-1.0 kg	25 mins	1,200 m	40-50 mph	Yes	Dry conditions only	£700-900
Yuneec Q500 Typhoon	1.1 kg	0.5 kg	25 mins	600 m	54 mph	Yes (12MP)	Dry conditions only	£900-1,100 (RTF)
SkyJib-X4 XL Ti-QR	15 kg	7.5 kg	15 mins	3,000-25,000 m	24 mph	Yes	Wind	£7,500-8,000
Altura Zenith ATX8	3.1 kg	2.9 kg	45 mins	1,000 m	44 mph	Yes	Light rain/ snow	£15,000-20,000
MicroDrones MD4-1000	2.65 kg	1.2 kg	88 mins	5,000 m	26 mph	Yes	Light rain/ snow	£20,000-30,000

Weather proofing

Most low-end and mid-level commercial UAVs have limited operating conditions. The ability to operate in a broader range of weather conditions, such as high winds, rain and snow, is generally found in the more expensive commercially available drones, as weather hardening adds weight, which has cost implications. Compared to military-grade UAVs, such as AeroVironment's Puma AE (All Environment) model, commercial UAVs have a limited ability to operate in harsh, unpredictable and extreme climatic environments. Commercial UAV users could retrofit weather hardening to drones, though the extra weight would likely reduce flight time and payload capacity unless power or the number of rotors was also increased.

Imaging

Most UAVs have medium- to high-resolution cameras (at least 12 megapixels) and the ability to capture both stills and video. The use of a gimbal can allow manual and electronic camera rotation, providing greater situational awareness. Civilian UAV operators can install LiDAR and infrared cameras on UAVs.

Automated and programmable piloting and Follow Me settings

Most commercially available drones can be set to fly a predetermined flight path based on GPS coordinates (fly-by-wire). Newer models also have Follow Me autopilot settings that enable the UAV to automatically follow the operator.

Unmanned ground vehicles

Unmanned ground vehicles have been available for several decades. The simplest example, as reportedly used by Islamic State (IS) in Iraq, is the familiar remote controlled car. At the other end of the spectrum, the first fully-autonomous road vehicles for the commercial market and advanced military robotics are being developed.

There are two categories of UGVs. The first are remote controlled vehicles piloted by humans who are in full control of the vehicle but driving it but from a distance. These include the Modular Advanced Armed Robotic System (MAARS) used by the US Army. The second are autonomous drones that drive themselves using algorithms, sensor inputs and pre-set waypoints. These include the Mobile Detection Assessment and Response System (MDARS) used by the US Army and Navy, and the Google Self-Driving Car Project.

UGVs have a large range of applications – from hobbyists using remote controlled cars for entertainment and leisure to the military using vehicles capable of operating in dangerous regions and environments, including for disarming explosives.

For the hobbyist, commercially available small remote controlled cars can travel up to 35 mph over rough ground, cost between £40 and £1,200, and can drive for 15 to 90 minutes over relatively short distances. They tend to have very limited payloads but could be customised to include cameras. In contrast, the military and defence sector use of UGVs is well established and increasing. This includes vehicles such as the RipSaw, a commercially available UGV the US Army equipped with weapons and used in Iraq. The Ripsaw is priced at approximately $250,000 (£165,000) and is capable of driving at up to 95 mph, carrying a 900 kilogram payload. The US Army used over 6,000 UGVs in Iraq and Afghanistan for ISR missions and counter-IED tasks.[6] South Korea is also reportedly using stationary armed surveillance 'robots' in the demilitarised zone along the border with North Korea. While there is limited commercial availability of military-grade UGVs, variants of models such as the I-Robot 110 and Mil-Sim A5 Robotic Weapon may enter a broader commercial market in the future.

Due to the wide range of variations and capabilities, it would be possible to customise or purchase a UGV capable of carrying either explosive payloads or cameras for relatively modest prices and logistical difficulty. However, it is worth noting that a comparable manned vehicle would be significantly cheaper.

6 http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=186583.

Specifications affecting hostile UGV operations

There are only a limited number of UGV specifications affecting operations that are applicable to all classes of UGV. The diversity in technological capabilities makes pinpointing operational limitations challenging.

Mobility and speed

UGVs can move across ground terrain in a range of modes and vehicle configurations. There is an important relationship between the ability of a UGV to move across diverse all-terrain environments, such as hills, obstructions, semiaquatic or flooded areas and uneven surfaces, and the speed with which a vehicle can move. For example, the average remote controlled car may have a reasonably high top speed but be unable to traverse uneven terrain very well. On the other hand, counter-IED UGVs with caterpillar tracks have a far greater capacity to negotiate diverse terrains but at much lower speeds.

Imaging

UGVs, particularly smaller vehicles that operate low to the ground, provide only limited situational awareness to operators, particularly in contrast to UAVs. Without telemetry systems, navigation based solely on video stream is likely to significantly limit the effectiveness of some UGVs. While UAVs provide superior visual situational awareness from a distance, UGVs fitted with more advanced environmental sensors, such as thermal imagers and chem-bio sensors, may offer operators a more thorough understanding of on-the-ground environments.

Payload

The payload capacity of UGVs varies widely. As with most types of unmanned vehicles, there are obvious speed and mobility to payload weight trade-offs. In most instances, a commercial UGV or remote controlled car will have a higher payload capacity than hobbyist UAVs, but the UAV operator has greater visual awareness and manoeuvrability.

Table 2: Select list of UGVs

Model	Weight	Operating environment	Range	Max speed	Camera	Components	Price
Happy Cow 777-270 i-Spy	166 g	Limited	30 m	n/a	HD video/still camera	None	£30
Jumpshot MT	n/a	All terrain	100-200 m	27 mph	No	n/a	£175
Savage XL Octane RTR	7 kg	All terrain	100-200 m	36 mph	No	n/a	£775
Mil-Sim A5 Robotic Weapon	90 kg	All terrain All weather	215-500 m	50 mph	IR/low lux with night vision	Armed with lethal or non-lethal munitions	£2,500-6,500
I-Robot 110 First Look	2.5 kg	All terrain All weather Waterproof	200 m	3 mph	4 built-in cameras (front, rear and side-facing)	Can add specialised cameras, thermal imagers, chem-bio sensors and charge deployment accessories	£13,000-£15,000
MATILDA (Mesa Associates' Tactical Integrated Light-Force Deployment Assembly)	28 kg	All terrain All weather	1,200 m	2 mph	Pan-tilt zoom camera	68 kg payload capacity with adaptable configurations: sensor, attack and manipulate	£15,000
Modular Advanced Armed Robotic System (MAARS)	136 kg	All terrain All weather	800-1,000 m	7 mph	Drive and gunnery cameras with thermal imaging	Armed with lethal or non-lethal munitions	n/a

Range

Most remote controlled UGVs have limited range, though higher end models used by special operation forces are likely to be tailored for specific missions. Ranges for counter-IED and bomb disposal operations are likely to be based on average blast radius. For models used in hazardous material inspection or site contamination, a range of one kilometre should be sufficient to protect the operator. The range a hostile operator will require is dependent on the level of risk they are willing to expose themselves to depending on the target. In reality, the effective range is also dependent on the type of terrain the vehicle has to travel over to reach its target.

Unmanned marine vehicles

Unmanned marine vehicles are available in two main classes: underwater and surface platforms. The majority of UMVs fall into the first category. These underwater vehicles are designed for two principal commercial applications: marine research and offshore oil and gas sector activities. The 2014-15 search for missing Malaysia Airlines flight MH370 demonstrated a further novel application of UMVs for search and recovery. The Association for Unmanned Vehicle Systems International (AMVSI) has identified over 745 UMV platforms, with an estimated 75% in some stage of development, manufacture or deployment.[7] In 2013, there were 115 active UMV platforms available in the United Kingdom.[8]

The market for UMVs is smaller than the UAV market, as it lacks the high levels of hobbyist uptake and is far more reliant on commercial usage. The civilian market is restricted by the very limited capabilities of lower priced entry-level models. However, expensive drones with broader capabilities are becoming more readily available. The cost of an advanced underwater UMV can reach more than £1 million. UMVs in this price range have the ability to travel at a depth of 4,500-6,000 metres for up to 28 hours and over a distance of 100 miles.[9] Market research from March 2014 estimated that the global market for remotely-operated and autonomous UMVs would be £1.08 billion that year, growing to £3.15 billion by 2019.[10]

The two key operational attributes of underwater UMVs are range and dive depth, with cheaper models requiring a cable connection in order dive below the surface. Most underwater drones have a limited payload (less than 10 kilograms) because of the need to remain buoyant, and are used for visual or sonar imaging and collection of scientific data. Surface UMVs are dependent on speed, payload and range (a 'control triangle' comparable to the naval architects' 'iron triangle' of speed, payload and endurance).[11] They are capable of carrying up to 1,000 kilograms of explosives, such as was used in the non-drone attack on the USS Cole in October 2000 in Yemen.

Cheaper drones and those operating nearer to the surface are controllable by Wi-Fi up to a range of 300 metres, giving a pilot direct control over the drone. However, the majority of high-end submersible models move using a GPS-based system of waypoints. It is still possible for a pilot to maintain some level of control by changing the drive-to GPS coordinates or depth levels via acoustic messages and satellite communication; however, this form of control is limited at best, and the pilot could not, for example, navigate a submersible drone through a confined space. Due to the high cost and variable commercial use, underwater marine drones tend to be highly customisable. Features such as the basic outer shell, navigation, energy and propulsion components, and payloads, such as cameras or sonar equipment, are customisable.

7 https://higherlogicdownload.s3.amazonaws.com/AUVSI/b657da80-1a58-4f8f-9971-7877b707e5c8/UploadedFiles/AUVSIUMVCoreCapabilities08-08-13.pdf. Note, the remaining 25% of platforms are either inactive (10%) or insufficient information is available to determine production or operational development (15%).

8 https://higherlogicdownload.s3.amazonaws.com/AUVSI/b657da80-1a58-4f8f-9971-7877b707e5c8/UploadedFiles/AUVSIUMVCoreCapabilities08-08-13.pdf (p. 5).

9 http://www.ths.org.uk/documents/ths.org.uk/downloads/shallowwater_auv_and_usv.pdf.

10 http://www.prnewswire.com/news-releases/unmanned-underwater-vehicles-market-worth-484-billion-by-2019-252903011.html.

11 http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR384/RAND_RR384.pdf.

Specifications affecting hostile UMV operations

There are several factors that affect UMV operations. Typically, higher-cost drones feature significantly greater payload capacity, imaging capability, range and depth than lower-cost drones.

Payload

Payload capacity is affected by two factors: internal space and the buoyancy of the drone. A payload that is above the buoyancy weight will cause the drone to sink at a rate proportional to the weight variance. A payload below the buoyancy can be offset by the drone's navigation facilities, including filling the buoyancy tanks to achieve a neutral level. Any space left in the payload chamber of underwater UMVs can be filled with high buoyancy foam to increase the potential payload weight. Higher-end UMVs will have more space for packages as well as higher natural buoyancy levels. The entry level drones may lack any payload capacity.

Speed

Speed is determined by the engine output and the shape and weight of the craft. The engine output of underwater models is very low, with top speeds in the region of 3-6 mph (similar to jogging speed). The higher end of the market is more focussed on delivering endurance rather than speed. In contrast, speed is key factor for surface drones, which can reach speeds of up to 30 mph.

Imaging

Imaging technology tends to be placed into the payload chamber in UMVs. This can range from scientific instruments measuring changes in pressure or water quality, to sonar equipment and visual capabilities. The latter allows drones to be used for surveillance or reconnaissance of critical infrastructure, such as oil rigs or offshore military equipment, including naval vessels.

Table 3: Select list of surface UMVs

Model	Weight	Payload	Fuel capacity	Max speed	Camera/ sonar	Price
C-Target 3	325 kg	0 kg	40 litres	28.7 mph	Yes	£POA
AutoNaut 3.5	120 kg	40 kg	20 litres (plus solar panels)	3.45 mph	Yes	£POA
AutoNaut 5	230 kg	130 kg	20 litres (plus solar panels)	4.6 mph	Yes	£POA

Table 4: Select list of sumbersible UMVs

Model	Weight	Buoyancy	Operation time	Range	Depth	Max speed	Camera/ sonar	Estimate price
HydroView Pro 5M	6.4 kg	0.9 kg	180 mins	0.046 miles	100 m (attached to cable)	4.6 mph	Yes	$10,000-15,000 (£6,500-9,700)
Remus-100	37 kg	1 kg	600 mins	51.8 miles	100 m	5.18 mph	Yes	$250,000 (£163,000)
Bluefin-21	750 kg	7.3 kg	1,500 mins	86.25 miles	4,500 m	3.45 mph	Yes	$2.5 million (£1.63 million)

Range

The range of a drone is not determined by controller range if the UMV is capable of satellite or GPS communication. If this is the case, provided the drone remains in contact with the GPS network, the range is determined by the fuel capacity (generally electric batteries) and optimal speed. A drone able to travel at 3 knots (3.45 mph) for 25 hours has an effective range of 86.25 miles. If GPS communication is not possible, the drone is typically limited to either Wi-Fi controller ranges (typically up to 300 metres) or a physical cable connecting it to a pilot (typically less than 100 metres long).

Depth

Due to the pressure placed on a vehicle that descends under the water and the hazards of water damage on electrical components, the shell of a drone determines the depth to which it can travel. Drones with shells made of higher strength metals, such as titanium, are able to travel deeper than those made of cheaper metals or plastics. Depth is not a factor when UMVs are deployed against surface targets, but some critical infrastructure targets have significant depth, such as oil lines and platforms or communications cables.

Assessment of known drone use by non-state actors

A review of the known use of drones by various terrorist, insurgent, criminal, corporate and activist threat groups around the world has identified two principal categories of hostile use: attack and intelligence gathering. There are particular concerns that that drones will be used as simple, affordable and effective airborne Improvised Explosive Devices (IEDs). Governments are also concerned by the decentralisation and democratisation of intelligence, surveillance and reconnaissance (ISR) capabilities made possible by the widespread availability of drones. In contrast, this is a development that is welcomed by activists working to hold governments and corporations to account. A brief summary of the review is presented in the following pages. The majority of drones used are unmanned aerial vehicles, as they are more readily commercially available and offer more options than land- or sea-based platforms.

Lone wolf

There are many examples of individuals using drones for purposes beyond authorised and accepted use, and these suggest scenarios for future lone wolf attacks.

In September 2011, a 26-year-old American man was arrested by undercover FBI agents planning to fly explosives-laden model aeroplanes into the Pentagon and US Capitol and rig mobile phones to detonate improvised explosive devices (IEDs). In January 2015, an off-duty employee of the US National Geospatial-Intelligence Agency lost control of a friend's DJI Phantom quadcopter, which then crashed onto the White House lawn. The incident raised concerns about the extent to which the Secret Service is prepared for drone activity. Four months later, a man was arrested for trying to fly a Parrot Bebop drone over the White House fence. In France, unidentified drones have been flown over the US embassy, the Eiffel Tower, the Invalides military museum, the submarine communications base at Sainte-Assise, the Place de la Concorde, the Elysee Palace and multiple nuclear power stations. In June 2014, an unidentified drone was used to monitor the French national football team during a closed training session at the 2014 World Cup in Brazil. In July 2014, an unidentified drone came within six metres of an Airbus A320 as it landed at London's Heathrow Airport, prompting the Civil Aviation Authority to issue new safety guidelines, known as the 'dronecode'. In October 2015, an unidentified drone crashed into the Sydney Opera House.

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 microsievert per hour.

In a response to a freedom of information request by Open Briefing, the Metropolitan Police Service revealed that between January 2013 and August 2015, 20 suspicious drone related incidents had been recorded in and around London.[12] Sixty per cent of the disclosed incidents related

12 *https://www.whatdotheyknow.com/request/counter_drone_*

to air navigation orders where civil aviation requirements had been breached; the rest related to criminal or illegal activity. In one case, a UAV was used to smuggle drugs into a prison and in another case a drone was flown over 200,000 people on 20 December 2014.

Terrorist organisations

The Lebanon-based militant group Hezbollah has the longest history of drone use by a non-state group. Hezbollah reportedly maintains a small fleet of UAVs, including Iranian Ababil and Mirsad platforms and their Hezbollah derivatives.[13] Some reports estimate that the fleet includes upwards of 200 platforms for ISR and combat missions.[14] In November 2004, Hezbollah allegedly flew an Iranian UAV over parts of northern Israel before returning to Lebanese territory. In August 2006, Hezbollah launched three small Ababil drones, some allegedly carrying explosive payloads, with the intention of attacking Israeli military targets. The drones were shot down by Israeli F-16s. In October 2012, Hezbollah allegedly flew a small Ayub drone 35 miles into Israeli airspace with the intention of undertaking reconnaissance on a nuclear reactor. An Israeli aircraft shot the drone down before it returned to Lebanon.

More recently, it is possible that Hezbollah has more consistent access to Iranian UAVs, including the Ababil-3, and are using UAVs against al-Nusra Front fighters in Lebanon. In September 2014, the Fars News Agency reported that Hezbollah had achieved its first successful drone strike, killing an estimated 23 'Syrian rebels'.[15] In April 2015, IHS Jane's published evidence of a Hezbollah UAV airfield in the northern Bekaa Valley, Lebanon, that included a UAV ground command station.[16] The group is thought to be continuing to use UAVs for ISR in the border region between Syria and Lebanon.

Al-Qassam Brigades, the military wing of the Palestinian organisation Hamas, is suspected of having a small fleet of UAVs and a crude production workshop. During Operation Protective Edge in 2014, Israeli forces shot down a potentially armed Hamas-controlled Arbabil-1 UAV with a Patriot surface-to-air missile. Al-Qassam Brigades advised that the drone was only one of three that breached Israeli airspace, though the Israeli military deny this claim. In December 2014, a drone flyover of a Hamas military parade resulted in Israel scrambling fighters that returned to base after the drone did not enter Israeli airspace.

More recently, Al-Qassam Brigades announced that it had captured an Israeli Skylark 1 that came down in Gaza in July 2015. The group claimed that the drone had been repaired and was operational. Al-Qassam Brigades also claims to have developed three UAV platforms, two with combat payloads and one for surveillance.

The extremist militant group Islamic State were shown to be using DJI Phantom UAV platforms in Fallujah, Iraq, from early 2014. While the early demonstrations of commercially available drones appeared to be for propaganda purposes only, there is emerging evidence that these platforms are now providing actionable ISR and target acquisition capabilities to Islamic State.[17] There are some indications that IS used hobbyist drones to gain situational awareness ahead of the campaign to capture the Tabqa military airfield in northern Syria in August 2014. In March 2015, US military forces launched an airstrike against an IS militant who had been flying a UAV over Fallujah. 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.[18] In May 2015, the Kurdish Peshmerga shot down an IS drone that had been filming their positions. In August 2015, there were reports that Kurdish soldiers had captured a remote controlled car carrying explosives that had failed to detonate. In the

measures#incoming-702249.
13 https://medium.com/war-is-boring/this-new-airstrip-could-be-home-to-hezbollah-s-drones-bdec97ff36a8.
14 http://www.ynetnews.com/articles/0,7340,L-4457653,00.html.
15 https://www.youtube.com/watch?v=gUSGNApl9XQ.
16 http://www.janes.com/article/50922/hizbullah-airstrip-revealed.

17 https://medium.com/war-is-boring/islamic-state-has-drones-7827987c1755.
18 http://www.longwarjournal.org/archives/2015/04/islamic-state-uses-drones-to-coordinate-fighting-in-baiji.php.

same month, US Central Command released a list of airstrike targets around the world, including 'an ISIL drone' near Ramadi in Iraq.[19]

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.

Insurgent groups

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. Obtaining aerial, ground and marine reconnaissance and attack capabilities would mark a step change for many insurgent groups.

Donetsk People's Republic (DPR) militias in eastern Ukraine reportedly possess and deploy sophisticated Russian-made Eleron-3SV drones for ISR campaigns. In contrast, the Ukrainian military has been using a range of modified and tailor-made hobbyist UAVs for ISR support. There are reports that the DPR militias are using signal jamming and GPS spoofing countermeasures against some Ukrainian drones; however, more advanced autopilot software in the tailor-made models is more resilient against these countermeasures. The Ukrainians have requested US military drones, such as Reapers, and jamming equipment and radar to better intercept the Russian-made drones.

In August 2002, a Colombian Army unit allegedly discovered remote-controlled aeroplanes during a raid on a Revolutionary Armed Forces of Colombia (FARC) camp. The intended use of the aircraft remains unclear.

Organised crime groups

Mexican drug trafficking organisations (DTOs) have been documented using drones to smuggle illicit drugs across the US-Mexican border since 2010. The US Drug Enforcement Administration (DEA) has recorded around 150 drone trips across the border since 2012. Nearly two tonnes of cocaine and other drugs are estimated to have been trafficked into the United States in this way, with an average of 13 kilograms of drugs per shipment.[20] In January 2015, a drone that crashed in Tijuana, Mexico, was carrying over three kilograms of methamphetamine. In August 2015, two men pleaded guilty to trafficking 12 kilograms of heroin across the US-Mexican border in the first cross-border seizure involving a drone.

In the face of increasingly successful military and law enforcement operations against illicit drug smuggling in the early 1990s, Colombian drug cartels began to invest in producing narco-submarines as an alternate to small planes and go-fast boats. In August 2005, US authorities captured an unmanned semi-submersible in the Pacific Ocean. This was a torpedo-style cargo container, rather than a self-propelled vessel, which was towed underwater behind a boat and released if a patrol ship was spotted. The narco-torpedo would then release a buoy with a location transmitter system so that it could be retrieved later. In July 2010, the Ecuadorian police and navy found a jungle shipyard containing a 22.5-metre long narco-submarine. The advanced 'supersub' had a camouflaged hull made of Kevlar and carbon fibre and a cargo bay capable of holding over eight tonnes of cocaine. The high level of sophistication apparent in the various captured nacro-submarines and the huge resources available to the DTOs means that it is highly likely that they are now investing in remotely-piloted submersible vessels in addition to custom-made UAVs.

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

20 http://www.insightcrime.org/news-briefs/mexico-s-cartels-building-custom-made-narco-drones-dea.

Corporations

There have been isolated examples of drones being used to obtain commercially sensitive information, such as drones flying over the filming of Game of Thrones in Ireland, Apple's new campus site being built in Cupertino in the United States and the BAE Systems facility in northern England that builds submarines for the Royal Navy. However, there have been no documented examples of corporations using drones for commercial advantage or espionage. However, there is a broad range of threat scenarios whereby drones are integrated into corporate espionage operations alongside cyber offensives and spear phishing campaigns. A likely scenario involves using drones as a means to deploy a malware payload over specific Wi-Fi networks. The leaked emails of Italian spyware vendor Hacking Team suggest that early concept plans for using drones for airborne malware delivery over Wi-Fi networks were being discussed with Insitu, a division of Boeing.[21]

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'.22 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.

Activist groups

Although clearly not presenting a threat of the same type or magnitude as the other threat groups discussed in this briefing, activists have employed drones to support their political campaigns on a number of occasions. In September 2013, the German political party the Pirate Party flew a Parrot quadcopter towards the German chancellor, Angela Merkel, during a campaign rally in Dresden.[23] The stunt was in protest against the German government's surveillance policies. In October 2014, Greater Albania activists flew a drone carrying the Greater Albania flag over an Albania-Serbia football match.[24] Greater Albanian's claim territory from Albania's neighbours, including Serbia. In July 2015, Women on Waves delivered pregnancy termination pills by drone from Germany to Poland to highlight restrictive abortion laws in Poland. Animal rights activist groups have used UAVs to remotely capture farming, animal husbandry and animal testing practices in the United States. In April 2015, a man protesting over the Japanese government's nuclear energy policy landed a drone containing radioactive sand on the roof of the Japanese prime minister's office in Tokyo.

Although the use of drones by activists is still uncommon, the most likely way in which drones will be used by such groups in future is in undertaking publicity-seeking exercises in front of the media or filmed using onboard cameras. Activists could also use drones to assist existing campaign efforts through reconnaissance and surveillance.

21 https://theintercept.com/2015/07/18/hacking-team-wanted-infect-computers-drone/.
22 http://www.desert-wolf.com/dw/products/unmanned-aerial-systems/skunk-riot-control-copter.html.
23 https://www.youtube.com/watch?v=WcFiMCMbUHo.
24 https://www.youtube.com/watch?v=hJSQf737Agw.

Drone countermeasures

There are two theatres in which non-state actors could use drones as either an offensive weapon against the United Kingdom and its interests or as an intelligence gathering tool:

1. **The international theatre**, consisting of all British military operations, embassies and commercial sites and operations abroad. These are vulnerable to attack by terrorist or insurgent groups or to being targeted by activist groups protesting against government policy or the actions of British corporations.
2. **The domestic theatre**, consisting of critical national infrastructure, military sites, government buildings and tourist sites within the United Kingdom. These are vulnerable to terrorist attacks, disruption by activist groups or corporate espionage.

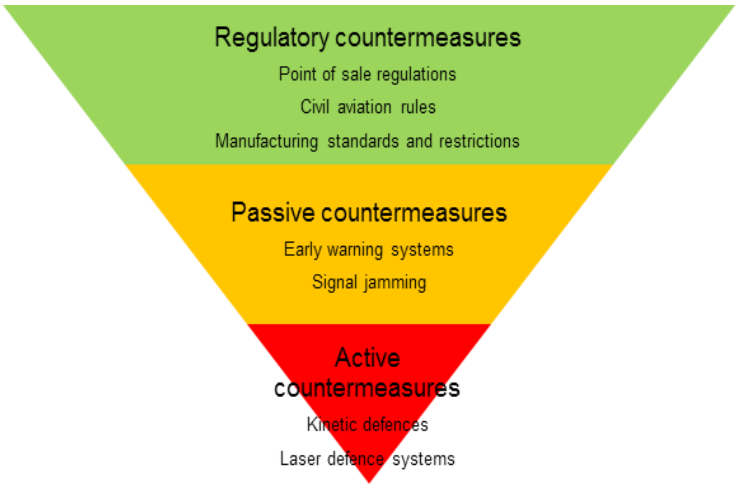
There are three key defence scenarios, which range from easier to target/easier to defend to harder to target/harder to defend:

1. **The long-term static target**, such as a foreign embassy or nuclear power station.
2. **The temporary static target**, such as a G7 summit or a speech by a politician.
3. **The mobile target**, such a military supply convoy or the prime minister's car.

The UK government, police, military and security services will need to introduce countermeasures to reduce or mitigate the risk of commercially available drones being used for attack or ISR operations. These countermeasures need to be proportionate to the risk, economically and operational sustainable and balance interests relating to privacy, individual freedoms, safety and commercial interest.

Drones are a unique technology providing users with significant capabilities. Defence system against illegal or harmful use of unmanned

Figure 1: The hierarchy of countermeasures



vehicles should provide for 'all hazard' scenarios and multiple threat environments. However, time and resource investments should be prioritised for countermeasures that respond to the scenarios with highest risk (high likelihood/high impact).

No single countermeasure is completely effective at limiting the hostile use of drones by non-state actors. The best strategy is therefore to employ a hierarchy of countermeasures encompassing regulatory countermeasures, passive countermeasures and active countermeasures. A high-level evaluation of the various countermeasures that are available is provided in the following pages. The focus is on unmanned aerial vehicles, as they present the greatest threat, but many of the countermeasures can be applied to unmanned ground and marine vehicles too, and where applicable countermeasures specific to these vehicles have also been considered.

Regulatory countermeasures

Domestic regulations can put in place a range of measures targeting the full supply chain and life cycle use of drones. Regulations would need to proportionate and balance a range of competing safety and commercial demands, including establishing procurement barriers for threat actors while at the same time encouraging innovative commercial use and maintaining easy access to suitable platforms for hobbyists. Specific regulatory countermeasures may include:

- Point of sale regulations, including identification requirements for the purchase and sale of drones above a certain level of capability.
- Civil aviation rules and licensing regimes to regulate the use of drones, with harsh penalty regimes for flying near critical national infrastructure and sites of national security importance.
- Manufacturing standards and restrictions for UAVs, including no-fly zones built in to firmware and limits on carrying capacity and controller range.

Procurement and import regulations

The main international regulation relating to drones is the 1987 Missile Technology Control Regime (MTCR). The regime currently has 34 members, and the UK government is a founding member. The MTCR aims 'to restrict the proliferation of missiles, complete rocket systems, unmanned air vehicles, and related technology for those systems.' It is a voluntary association of countries that share the goal of 'non-proliferation of unmanned delivery systems capable of delivering weapons of mass destruction.'[25]

Regulations to stop the procurement and import of drones to the United Kingdom only cover those weighing more than 20 kilograms or are equipped to undertake any form of surveillance or data acquisition at time of purchase. Heavier drones require airworthiness approval and those capable of surveillance are more stringently regulated. This limited regulation means that drones weighing less than 20 kilograms can be imported without license, despite many drones weighing 5-20 kilograms being capable of carrying explosives or camera equipment; for example, the SkyJib-X4 XL Ti-QR weighs 15 kilograms and can carry a payload of 7.5 kilograms.

Civil aviation regulations on UAV licensing and use

There are currently 32 countries using regulations to control the use of drones domestically, particularly unmanned aerial vehicles. The scope and scale of the regulations range from altitude or weight limits to a complete ban on all unmanned aerial vehicles. Regulation in the United Kingdom is limited. Drones of any size or weight are permitted, though they must be used within the visual sight line of the pilot. In general, UAVs cannot be flown above 400 feet in altitude without special permission and must remain clear of controlled airspace without Air Traffic Control permission. Commercial operation requires a license, which is given to an operator for a particular class of UAV (small fixed wing or small multirotor).[26]

25 *http://www.mtcr.info/english/.*
26 *https://www.caa.co.uk/default.*

In contrast, some countries maintain a complete ban, while others have stringent rules similar to those in effect in South Africa. South Africa has a well-developed series of regulations on UAVs, with some of the strictest rules in the world short of an outright ban. The operators of drones must have a valid remote pilot license and drones cannot be operated without a letter of approval from the director of the South African Civil Aviation Authority, which is valid for 12 months. Drones must not be flown near nuclear power plants, prisons, police stations, crime scenes, law courts, critical national infrastructure or strategic installations. Regulations also prohibit drones from being flown in formation or swarm, flown directly overhead or within a lateral distance of 50 metres of a person or crowd, or within 50 metres laterally of any structure or building.[27]

There is a vigorous debate between the innovators, users and regulators. The former argue for a more laissez faire approach to allow the rapid development of the civilian drone market. They argue that if the rules of use become restrictive now, this could smother the sector before it properly established. Conversely, others argue that if the rules are too relaxed there is a high probability of misuse with potentially disastrous consequences. As usual, a compromise needs to be found.

Firmware limitations

The Chinese UAV producer DJI has built safety features into the firmware (the permanent software programmed into read-only memory) used by its drones. The firmware maintains several No Fly Zones based on the GPS coordinates of the pilot's location. There are around 350 No Fly Zones worldwide.[28] These zones are primarily designed to keep drones away from airports. Furthermore, within eight kilometres of a no-fly zone, the pilot is unable to set an automatic fly-to waypoint, forcing them to remain in manual control of the drone near these zones.

The No Fly Zone is currently a limited-use tool implemented to protect airports; however, legislation could be implemented to extend the measure to protect other key sites. In January 2015, DJI reported that it is considering implementing such a zone over Washington DC after one of their drones crashed onto the lawn of the White House. In theory, the firmware updates to protect these sites could be hacked and bypassed, but this would require specialist knowledge not likely to be held by most solo attackers at least. The company is also working to prevent criminals from using workarounds to circumvent such security features.

This would make it very difficult for individuals without the technical knowledge of computer programming and the criminal links to illegally import drones to be able to acquire and fly drones near sites that have been marked as needing protecting. In effect, this limits the lone wolf terrorist, and sends a clear message to activists and businesses of what the legal and illegal uses of drones are.

Passive countermeasures

Early warning systems

There are several early warning systems that can identify a drone within a defined area. Traditional technology such as radar and CCTV can be effective, but new commercial systems are being developed that specifically alert operators to the presence of drones. Such commercial systems include:

DroneShield is developing a system that contains a database of common acoustic signatures unique to drones. If a drone is detected, DroneShield instantly alerts security officers via text message, email or through an existing alarm system. The system was deployed at the 2015 Boston Marathon. DroneShield technology is also available for cars and vans, allowing a VIP convoy to implement such a detection system.

Domestic Drone Countermeasures is developing personal and commercial detection systems that can detect radio frequency transmitters and triangulate moving transmitters. The system

aspx?catid=1995&pageid=16012.
27 http://www.thedroneinfo.com/south-africa-drone-regulations/.
28 http://theuavdigest.com/uav036-no-fly-zones-for-uavs/

consists of a primary command and control module that can communicate with radio frequency sensor nodes up to 60 metres away, with each node typically able to detect drones within 15 metres in all directions.

Dedrone has developed the DroneTracker multi-sensor detection system, which uses an array of sensors to detect civilian drones in real time. The system uses microphones, a daylight camera and an infrared camera to track drones within a 100 metre radius, which can be extended by deploying the units in series.

Although commercial systems have the potential to be very effective against civilian drones, military-grade systems include electronic warfare and radar capabilities that make them far more effective against advanced drones. As the counter-drone market grows, defence companies may begin offering scaled down versions of their military systems for use by businesses and high-net-worth individuals.

A comprehensive early warning system would use a combination of acoustic detectors, thermal imaging sensors, cameras and radar. This would allow a drone to be detected, tracked and identified by target sites. However, many sites lack sophisticated detection capabilities, such as radar, and it would be costly to install them. Companies such as a Dedrone are developing cost-effective and drone-specific alternatives. In some high-value targets, such as military bases or Whitehall, radar could be installed, but investing in commercial systems alone would be sufficient for most sites.

Signal jamming

Once an early warning system detects a drone, popular drone control frequencies can be blocked around the target using a radio frequency jammer, such as the RCJ40-D or PRO45 High Power (civilian) or JAM201 or GM20 (military). It is also possible to block these frequencies at all times, though this would make mobile phone communications in and around the site difficult. However, a drone user can use a wireless intrusion prevention system to alert them to attempted jamming. Advanced radio receivers can use a multi-spectrum frequency set that alternates through little used frequencies meaning that the receiver is harder to block. Military-grade jammers can block a wider spectrum of frequencies. However, frequency jamming is illegal in the United Kingdom without permission.

By implementing no-fly zones around critical infrastructure, any drone detected can be assumed to be malicious and the controller frequencies could be blocked. However, if a threat actor is able to hack the firmware to override the inbuilt no-fly zones, they could place GPS waypoints within the defensive perimeter. If the drone was detected and controller frequencies were blocked, the drone operator would be unable to change the coordinates or have any control over the aircraft; however, the drone would continue along its pre-determined route and still be able to strike a static target. What controller frequency blocking does is remove the threat actor's ability to guide the drone onto a mobile target or target of opportunity or to take evasive action against any active defence systems. GPS jamming is also needed in order to interfere with the GPS radio signal or undertake a spoofing attack to change the drone's perceived coordinates and either take control of the vehicle or cause it to crash land.

A possible alternative method for taking control of a drone was revealed in January 2015 when a security researcher claimed to have developed the world's first drone malware: Maldrone. The Python script is loaded to the drone over a local Wi-Fi network and can turn off the drone's autopilot system and take control remotely.[29] However, drone malware is currently very limited, and requires the specific model of the targeted drone to be known. The Maldrone demonstration does offer an idea of what might one day be possible though.

29 *http://garage4hackers.com/entry.php?b=3105.*

Active countermeasures

Kinetic defence systems

For those drones that remain a threat after the controller frequency and GPS have been blocked, the last barrier of defence in the hierarchy of countermeasures are systems capable of destroying hostile drones. This includes kinetic weapons, such as missiles, rockets and bullets.

Israel's Iron Dome air-defence system has been tested for its counter-UAV capabilities, and according to some sources can destroy armed drones before they are in attack range. Less-advanced kinetic defences use rockets or bullets and require line of sight, meaning a drone can get much closer to the target. All kinetic systems present a risk of collateral damage if deployed in a populated area. Missiles and rockets fired at UAVs could cause catastrophic damage if they miss their target. If the drone is hit, shrapnel and wreckage could still cause casualties on the ground. The blast radius from a missile or rocket fired at a UGV could include civilians near the targeted drone, and bullets fired at UGVs could easily strike passersby.

Less risky commercial options include non-lethal projectile weapons that fire blunt force rounds, such as bean bags or rubber bullets, or small portable net guns that can ensnare drones. A consortium of British companies called Liteye has developed the Anti-UAV Defence System (AUDS) system that can detect and track drones using electronic scanning and radar then disrupt its operation with a brief, focused broadcast of directional radio frequency jamming.

Laser defence systems

Laser defence systems are being developed that have less chance of causing causing collateral damage than kinetic systems. For example, a Chinese consortium of companies, led by the China Academy of Engineering Physics, has developed a weapon system that can shoot down light drones at low altitude using a 10 kilowatt high energy laser. It has a 1.2-mile range and is effective against aircraft travelling at up to 112 mph and at a maximum altitude of 500 metres. It can destroy the drone within five seconds of locating its target. Boeing is developing the truck-mounted High Energy Laser Mobile Demonstrator for the US Army and the Compact Laser Weapons System, which can be assembled in 15 minutes and destroy a drone in 15 seconds.

Laser defence systems are still in development. However, once deployed and combined with an early-warning system, directed energy weapons could provide a useful counter to a hostile drone, particularly if radio frequency jammers and GPS jammers have also been deployed to remove the pilot's ability to operate the drone. In this situation, the laser defence system would be working against an autonomous vehicle, making it easier to lock-on to and destroy. However, such systems might be of limited use in built-up areas, as they can only engage drones during times of line of sight, which may not be enough time to destroy the drone before it reaches its target. The fastest commercially available drones can travel at around 50 mph, meaning a drone could travel 112 metres in the five seconds a laser would take to destroy it. In a domestic, urban setting, this makes such systems most suited to the defence of static targets with clear lines of sight.

Conclusions and policy recommendations

It is estimated that around 200,000 civilian-use drones are being sold worldwide every month.[30] Although they are currently expensive, ever-more advanced drones capable of carrying sophisticated imaging equipment and significant payloads are readily available to the civilian market. Unmanned aerial vehicles currently present the greatest risk because of their capabilities and widespread availability, but developments in unmanned ground and marine vehicles are opening up new avenues for hostile groups to exploit.

A range of terrorist, insurgent, criminal, corporate and activist threat groups have already demonstrated the ability to use civilian drones for attacks and intelligence gathering. The best defence against the hostile use of drones is to employ a hierarchy of countermeasures encompassing regulatory countermeasures, passive countermeasures and active countermeasures.

Regulatory countermeasures can restrict the capabilities of commercially available drones and limit the ability of hostile groups and individuals to procure and fly drones. However, any new regulations controlling drones should be targeted and proportionate to the threat. The key specifications affecting drone operations are payload capacity, range, speed, depth (for UMVs), weather proofing, imaging and autopilot settings. Policymakers should pass stricter regulations limiting the capabilities of commercially available drones in the key specifications affecting hostile drone operations, particularly payload capacity. Particular attention should be paid to limiting the attack and ISR capabilities of UAVs and the attack capabilities of surface UMVs. Manufacturers should be required to install firmware that includes the GPS coordinates of no-fly zones around sensitive fixed locations. This would automatically shut down drones approaching these sites, thereby restricting malicious use. Finally, civilian operators of drones capable of carrying payloads should be licenced and the serial numbers of purchased drones registered.

Passive countermeasures alert security to the presence of any drone within a no-fly zone or defensive perimeter around a static or mobile target. They limit the ability of hostile groups and individuals to guide a drone onto a mobile target or target of opportunity or take evasive action against any kinetic defences. The military has advanced systems that can track and destroy drones using radar, lasers and electronic warfare; however, the market for commercial and civilian early warning systems is at a nascent stage of development. The British government should support the research and development of commercial multi-sensor systems capable of detecting and tracking drones within a target area. The government should also make funding available to police forces and specialist units for the purchase of early warning systems and other passive drone countermeasures, including radio frequency jammers and GPS jammers. Radio frequency jammers are heavily restricted in the United Kingdom; however, such equipment could provide additional protection and security to vulnerable locations and individuals by blocking command signals to drones. Therefore, the government should relax the regulations restricting the use of radio frequency jammers for protection against hostile drone use around defined key sites.

30 *http://dronelife.com/2015/01/24/drone-sales-figures-2014-hard-navigate/.*

Active countermeasures can be deployed against drones that still represent a threat despite passive systems being employed. However, the active countermeasures currently available for use in non-military settings are limited. Kinetic weapons – missiles, rockets or bullets – can be very effective, but present considerable risks of collateral damage if used in urban civilian areas. Less risky defences include laser systems or non-lethal projectile weapons and net guns, but these may not successfully destroy a hostile drone and require line of sight, which may be difficult in heavily built-up areas. Despite these limitations, the British government should support the research and development of innovative less-lethal anti-drone systems, such as directional radio frequency jammers, lasers and malware, and set out clear guidelines for the police and military use of kinetic weapons against hostile drones as a last line of defence.

With active countermeasures still under development or presenting a high risk of collateral damage, the focus should be on the swift adoption of appropriate regulatory and passive countermeasures and increased funding for the research and development of effective active countermeasures. The most effective and cost efficient measures should be prioritised. The implementation of more expensive countermeasures for low likelihood/high impact events involving drones will depend on the government's risk appetite with regards to specific potential civilian, government or military targets. Combined with high-quality intelligence on the present threat of the hostile use of drones by various threat groups, the recommendations outlined in this report represent the best chance of countering the new and evolving threat from the hostile use of drones by non-state actors.

However, such countermeasures are not foolproof. Furthermore, there is also the very real chance that, as with drones themselves, countermeasures will be deployed in turn by some threat groups against British police or military drones. The technology of remote-control warfare is impossible to control; the ultimate defence is to address the root drivers of the threat in the first place.

Remote Control Project
Oxford Research Group
Development House
56-64 Leonard Street
London EC2A 4LT
United Kingdom

+44 (0)207 549 0298
media@remotecontrolproject.org

www.remotecontrolproject.org

Open Briefing
27 Old Gloucester
Street London
WC1N 3AX
United Kingdom

+44 (0)20 7193 9805
info@openbriefing.org

www.openbriefing.org