(DTD0013)

Written evidence submitted by Dr Anna Jackman

Written submission from Dr. <u>Anna Jackman</u>, Lecturer in Political Geography at Royal Holloway, University of London. Anna is an active drone scholar and has undertaken research with both military and civil drone communities. Anna acts as a Specialist Adviser for the Science and Technology Committee <u>inquiry</u> into Commercial and recreational drone use in the UK. This submission is in a personal capacity.

Executive summary

- Commercially-available off-the-shelf drones are increasingly available and accessible.
- Following their growing deployment on global battlefields by non-state actors, in both weaponized and surveillance capacities, consumer drones are increasingly being deployed in domestic/ homeland settings, raising a series of security concerns.
- Consumer drones have, to date, been deployed in: assassination attempts, the transporting of small amounts of hazardous material, the transport of contraband, and the capturing of imagery of sensitive sites/facilities.
- Consumer drones are evolving in capability, with notable developments in the areas of: intelligent flight, manoeuvre and speed, capabilities raising concerns around potential nefarious re-imagining and deployment with malicious intent.
- It remains important, when mapping potential drone threat/ risk, to engage with emerging communities (e.g. the DIY community) who are experimenting with drones, including the addition of weapons and non-lethal payloads, those which could be nefariously re-imagined and deployed.

Risks:

How great is the risk of a drone attack in the UK, and what types of target are most vulnerable?

- 1. Non-state actor operated drones (both commercially-available off-the-shelf, modified, and self-constructed) are increasingly present on global battlefields (<u>Rassler</u> 2016, <u>Friese</u> et al. 2016, <u>Abbott</u> et al. 2016). In such locales, drones have been deployed by groups, including the Islamic State, in the gathering of surveillance imagery, the directing of alternative forms of attack, in weaponized capacities to conduct attacks (both by dropping munitions and embedding them to later detonate), in attempts to overwhelm via the use of small swarms, and to film or feature in propaganda (<u>Rossiter</u> 2018, <u>Hambling</u> 2017, <u>Stalinsky</u> and Sosnow 2017).
- 2. Such drone deployments have both followed and inspired the use of drones in domestic homeland locales (<u>Abbott</u> et al. 2016). Concerns about the (potential) risks borne of drones became particularly salient following the events of 4th August 2018, when a commercially-available off-the-shelf drone was flown towards Venezuelan President Nicolás Maduro as he delivered a speech at a military parade. The remotely triggered C4-laden drone exploded in mid-air, marking what the press widely reported as the first assassination attempt via consumer drone (<u>CNN</u> 2019). While notable in this sense, this is by no means the first time a drone has been deployed in proximity to a political figure or sensitive sites more broadly. For example, in 2013, the Pirate

(DTD0013)

Party flew a drone towards the German Chancellor Angela Merkel in protest of surveillance legislation (Ars Technica 2013). Subsequently in 2015 a drone outfitted with a small amount of radioactive sand was landed on the roof of the Prime Minister of Japan's office, flown by an individual in protest of nuclear energy policy (The Guardian 2015). Unauthorised drones have also been flown, largely with the aim of image (or data) capture, over a range of sensitive sites, from the White House. Eiffel Tower and The Colosseum, to international embassies, and naval, submarine and nuclear bases (Abbott et al. 2016), with plants in the UK reportedly suffered 37 security breaches in 2014 alone (Michaelides-Mateou 2016). While thus far predominantly driven by the desire for aerial imagery capture, such incursions remain indicative of wider security vulnerabilities. As those who have employed drones for the transport and smuggling of contraband into prisons and across borders have demonstrated, both the drone's ability to be outfitted and mobile with items, and its carrying capacity, is notable (The Times 2018, Washington Times 2018). Further, there has been a considerable increase in reports of drone incidents to UK Police Forces, with 2,400 reports in 2018 alone (Sky News 2019).

3. Alongside such deployments of drones (as protest and image-capturing tools), they have also been used by those seeking to target and disrupt transport infrastructure. In December 2018, for example, Gatwick Airport suffered serious disruption for a period of over 30 hours following reports of a drone (or drones) over the airfield (Jackman 2018). While Gatwick have since further invested in drone counter-measures, this incident nonetheless effected 140,000 passengers, and the (potential) operator(s) continues to evade prosecution. This form of drone-incursion-disruption is also evident, albeit often at a smaller scale, across many more airports, both in the UK (e.g. Heathrow), and internationally (e.g. Chengdu, Dubai, Lisbon, Tel Aviv, Delhi, Frankfurt, Stockholm, Dublin, Cork, Wellington, Auckland, Calgary, Warsaw). The UK Airprox Board reported 125 incidents (including close-calls and drone sightings) between manned aircraft and drones in 2018, raised from figures of 93 in 2017 and 71 in 2016 (IFSEC Global 2019). Significantly, there is also a growing imagination surrounding the potential to employ drones in disruptive or potentially harmful capacities at key transport hubs. For example, in April 2019 documents reportedly authored by the climate activist group Extinction Rebellion, detailing plans to deploy drones to disrupt operations at Heathrow Airport, were covered by the press (The Independent 2019). The idea of targeting of transport infrastructure by drones also has a lengthier history, including the uncovering of plans by "Japanese apocalyptic group Aum Shinrikyo [to use] a drone [or remote control helicopter] to distribute sarin gas", an attack they later successfully conducted on Tokyo's subway system without the use of a remote control device (Rassler 2016: iv, 1).

How feasible are drone attacks using chemical, biological, radiological or nuclear agents?

4. As discussed in paragraphs 2 and 3, the Japanese context is perhaps most telling regarding instances of both small-scale drone outfitting with hazardous material, and wider plans to equip remote control devices as such. Concerns have nonetheless been raised internationally regarding this form of (potential) threat. While acknowledging that a "chemical attack is not necessarily an easy thing to do" (Cohen in Rassler 2016: 22), drone researchers have nonetheless expressed concerns regarding drones equipped with, for example, chlorine gas, being deployed over a "political rally in a Western state" (Zwijnenburg & van Hoom 2015: 7). These concerns are echoed by both global military forces and political leaders alike. In developing an aerial threat

(DTD0013)

- assessment at the 2012 London Olympics, the British Army stated that it would be "feasible" that a consumer drone could be laden with poison and deployed as a "biological weapon in the capital" (Condron 2012: n.p). Similarly, concerns around the transport via drone of radioactive and nuclear materials into major urban areas has been referenced at a gathering of global leaders, with then UK Prime Minister David Cameron expressing concern of a "dirty bomb" style attack (Riley-Smith 2016: n.p).
- 5. It may also be valuable to consider here both the changing culture of outfitting drones with alternative payloads, and the drone's history as a precision farming device. Drones are increasingly being outfitted with a growing range of payloads. While the 'do it yourself' (DIY) outfitting of drones in discussed in paragraph 7, it should be noted that within a range of commercial and civil sectors drones are being equipped with notable payloads. Alongside cameras and sensors, some policing and border force drones have been equipped with pepper spray/ tear gas (e.g. in India and Israel), drones charged with waste clearance off power lines have been outfitted with flamethrowers (e.g. in China), and industry-developed drones in Japan have been equipped with grabbling claws. When considering the changing imagination of the drone, it should also be noted that the non-military drone has an important lineage as a precision farming device, one long-deployed as an agricultural tool to both visualise large crop areas, and to distribute and disperse pesticides/ fertilizers (Mogili 2018). Thus, there is a precedent for using drones as dispersal devices, one which arguably harnesses a potential to be re-imagined, weaponized and nefariously employed.

Is the threat posed by drones increasing, and are they a unique threat requiring bespoke countermeasures?

- 6. Drones are increasingly available and accessible. As this submission has thusfar demonstrated, there remains a changing deployment of drones, one bound to different forms of risk. It remains important to understand not just drone threat as evolving, but also drones themselves as evolving platforms. For example, higher-end commerciallyavailable off-the-shelf drones boast advancements in 'intelligent flight'. Referring to types of flight mode, global drone market leader DJI advertises drones capable of locking onto and following particular points/ objects/ persons, as well as the ability to increase speed or ascend/ descend rapidly. While marketed as cinematographic techniques, concerns have been raised around the potential for such techniques to reimagined, weaponized, and nefariously deployed (National Academies of Sciences, Engineering, and Medicine 2018). These drones are also increasingly being equipped with the ability to live-stream or broadcast footage to social media (e.g. Facebook), an innovation potentially significant in propaganda terms. Lastly, and related to drone manoeuvring more broadly, the increasingly popular aerial sport of drone racing (see British Drone Racing Association) features small drones capable of travelling at between 60 and 160 miles-per-hour (FPV drone reviews). Such drones arguably present a potential threat in terms of disrupting or seeking to overwhelm a site, defensive cordon, or security provision.
- 7. Looking instead to the alternative evolving space of the 'do it yourself' (DIY) drone community, enthusiasts have developed a range of notable drone modifications and adaptations. Enthusiasts seeking to play and experiment with drones have, for example, added functioning <u>fireworks</u>, <u>flamethrowers</u>, <u>handguns</u>, <u>chainsaws</u>, <u>graffiti</u> cans, <u>paintball</u> guns, and <u>tasers</u> to drones. While not designed as malicious applications, these experimentations remain notable developments in both providing a

- "firmer baseline" of understanding around improvised innovation, and in mapping potential drone threat more widely (Rassler 2016: iv).
- 8. Such spaces highlight that the drone represents an evolving (potential) threat, one which is marked by distinct qualities, spanning: The accessibility/ availability of drones (both commercially-available off-the-shelf, second hand, or self-assembled drones), mobility, speed, the potential distance of operator (remote operation or preprogrammed flight), ambiguity of what the drone may be carrying/ doing, and anonymity/ attempts to circumvent being known operator factors collectively marking the drone as a challenging object to police and govern.

4 July 2019