ARPAS-UK
The UK Drone Association

Written follow-up submission to The Science and Technology Committee on the commercial and recreational drone use in the UK

The Science and Technology Committee requested a follow-up on 3 specific questions following the oral evidence given on 11th June 2019 by Anne-Lise Scaillierez, director of ARPAS-UK, on the commercial and recreational drone use in the UK. We aim to respond to these questions in this written submission to the best of our knowledge, and in a spirit of transparency, we have also included articles that we recently published to the benefit of our members on related matters.

Invitation to a session with a commercial operator

We understand the Committee's concerns and vigilance on the matters of safety, security and privacy in drone use. To support the Committee's efforts, we would like to invite its members to a practical session with a commercial operator. It would be the opportunity to demonstrate in real-life the training, authorisations required, and processes put in place before, during, and after flying a mission, in order to ensure safe and secure operations. Members would also gain a better understanding of how drones can become a powerful tool to capture data and support many businesses in their digital transformation. We invite interested Committee members to contact us at: chairman@arpas.uk

Follow-up to Q6

Q6: you stated that ARPAS are "concerned" about risks relating to privacy and security misuse because "they affect societal acceptance". Please could you elaborate on your views on both the privacy and security risks related to drones in addition to their impact upon societal acceptance.

In our written submission last April to the Committee's enquiry on the ethical and safety implications of the growing use of civilian drones, of all sizes, across the UK, we explained that "the use of drones raises implications in terms of:

- Safety in the air: risk that a drone hits another airborne vehicle, including a manned aircraft;
- Safety on the ground: risk that a drone lands or falls on the ground, damages property or injures an animal or a person;
- Citizen privacy: risk that a drone captures images of people without their consent;
- Security: risk that a drone is used to deliver drugs in prison, or plan robberies by capturing images of houses' backyards
- Enhanced security risks or terrorism: risk that a drone is used to perform a malicious attack on sensitive sites, on high profile individual targets, or on crowds."

"Having stated these risks, it is important to reassess that the drone market in the UK is a regulated industry and that the regulator implemented measures to mitigate these risks

- It is illegal to take images of people without their consent;

- Recreational flight is permitted under the terms of The Drone Code only. The vast majority of recreational drone users fly responsibly;
- Professional drone operators such as ARPAS-UK members are trained professionals. They fly smart, they fly responsibly within the framework of law. They adhere to a Code of Conduct and strive to achieve best industry practice;
- Until the Gatwick incidents in December, we were not aware of significant incidents in the UK."

Breach of citizens' privacy and security misuse are illegal. But occurrences have happened (drones on beaches, drone crashing near Angela Merkel in protest in 2013, Gatwick). Education will take time and, in absence of quantification of these risks and their probability of occurrences, the perception of risk and uncertainty will likely affect societal acceptance. As a result, the positive impact of drone adoption by businesses in terms of job creations and economic growth may be impacted.

This challenge around public acceptance was recently quantified by PwC. Its research into public and business attitudes towards drones has revealed less than a third (31%) of the UK public currently feel positive towards drone technology, and almost half (48%) are undecided.

Follow-up to Q66

Q66: you discussed swarming and stated that "currently, on the commercial market, there is no such thing". It would be helpful if you could provide some further evidence in relation to this point.

Our understanding is that swarming technology refers to the ability of multiples drones to collectively perform one mission, to communicate and coordinate among each other, and to autonomously modify their behaviours in real-time to adjust to new circumstances and continue to collectively complete the mission, like a swarm of bees would for example.

In a military context, DARPA, the U.S. Defence Advanced Research Program Agency, is working on a project called OFFSET OFFensive Swarm-Enabled Tactics programme.

A first step in that direction is that communication networks between different assets from different milieu (air, sea, subsea, land, satellites) are interconnected.

At the other end of the spectrum, in terms of commercial drones, the current regulatory framework in the UK strictly provides for "one drone, one pilot". Therefore, there are no widely commercially available solutions for "multiple UAV – one operator" flight automation, let alone swarming, because there is no commercial market.

Having said that:

- In the entertainment industry, there are solutions for a "choreography" of drones. This was showcased for example by Intel during the Winter Olympic Games PyeongChang in 2018 with 1200 drones carrying lights.
- For use outside of the UK, there are "multiple UAV – one single operator" mission management software that automates the flight paths of a drone fleet to perform a mission, surveying an area for example.
- Research is ongoing as demonstrated by Cranfield University's announcement on 8th July that "researchers have developed a smartphone app which can connect with off-the-shelf drones and send them to autonomously inspect multiple locations using coordinates received by SMS text message. Controlling drones in this way could be useful for a variety of applications in the future including the collection of crop health data in specific locations and searching for missing persons. The goal of the

> CASCADE project is to accelerate the exploitation of unmanned aerial vehicles (UAVs) across a range of science and industry applications by automating control and facilitating communication between multiple drones so they can work on tasks together.”

Follow-up to Q83

Q83: you discussed your work on medical drone delivery – we welcome any further comments on this subject.

Using drones to deliver vital medical products in emergency situations in cities for a 24/7 service, or in difficult to reach areas in rural Europe or in Africa, offers a compelling value proposition. A number of experiments and even routine operations are taking place, some with the support of Unicef. Zipline, a California company, has set-up a programme with Rwanda and now Ghana to deliver blood units to hospitals. Matternet, another California-based company, has set-up a pilot programme in Switzerland with Swiss Post.

Why not a UK-based solution? Anne-Lise Scaillierez is a partner at The Drone Office, itself member of ARPAS-UK, and has been working on developing a medical drone delivery service in the UK/Europe to:

- Give better access to medicines and medical products to patients and better working conditions to medical teams
- By offering a sustainable alternative mode of transportation as a last-mile/last-leg delivery resource where existing infrastructure is inadequate or costly, in remote areas as well as in cities.

The preliminary phase of building a multi-disciplinary team is well under way. Teams at the Institute of Pharmaceutical Science, King’s College, London, at the Centre of Autonomous and Cyber-Physical Systems, Cranfield University, Milton Keynes, as well as at Barnard Microsystems, London, have confirmed their interest in principle to participate in the project. The next step is to engage with medical/pharmaceutical/local communities to ensure that we address real needs, to formalise the project’s terms of reference and deliverables, and eventually seek funding.

Articles (3) recently published by ARPAS-UK to its members on related matters

10 July 2019: ARPAS-UK talks to DJI about data security

On 11th June 2019, the Science and Technology Committee were joined by the Defence Committee to continue their Inquiry into Commercial and Recreational Drone Use in the UK. DJI presented oral evidence, along with other key stakeholders in the drone industry, including ARPAS-UK. DJI's representative, Brendan Schulman, Vice President for Policy & Legal Affairs, was repeatedly asked about DJI's data security.

Afterwards ARPAS-UK spoke with DJI to reinforce the message that commercial drone operators are being asked by their clients about data security too. In the light of this, the following interview was arranged between Graham Brown, CEO of ARPAS-UK, and Christian Struwe, Head of European Public Policy at DJI, with the aim of establishing the facts.

Graham:

Hi Christian, thanks for speaking to us today. We're hoping to get some further information after DJI's Vice President for Policy and Legal Affairs, Brendan Schulman, appeared in front of a parliamentary committee last month to answer MPs' questions about drones. He was asked repeatedly about the data security of DJI drones, and it would be really helpful for our members to also get some further clarification on this topic.

Christian:

Thanks for inviting me. The UK is one of DJI's most important markets and we see a lot of fantastic drone applications. We recognise that in order for this to continue, users need to be reassured that they can have complete confidence in our products and the security of their data.

Graham:

So, what actually happens to the data that our drones create? Where does it go and who controls it?

Christian:

DJI drone operators maintain absolute control over their data – at all times. DJI drones do not share flight logs, photos or videos whatsoever unless the drone pilot deliberately chooses to do so. In other words, your data will remain solely on the drone itself and on your mobile device unless you actively choose to share it with DJI, for instance in case of a repair service that a user requires. On top of this, all of our products are protected by embedded passwords and data encryption features.

Graham:

And what would you say to those who still remain yet to be convinced about data security of DJI drones, in spite of this?

Christian:

Well, we have independently verified that DJI drones don't share data unless prompted to by the pilot, through a third-party security review of our technology by a renowned US-based cyber forensic firm at the beginning of last year. Since 2017, users of DJI drones have also been able to use Local Data Mode. This feature allows for complete disconnection between the pilot's app and any internet connection – meaning, for example, that the location of the user can't be detected by the app at all, let alone shared anywhere.

Graham:

Given recent accusations about the technology produced by Chinese companies, like DJI, being used by foreign governments to spy on countries like the UK, do you think that these provisions are watertight enough even for those conducting the most sensitive operations, such as police forces?

Christian:

We have full confidence in the security of our products, but to offer even further reassurance for the most security conscious of our customers, DJI has also made available a FlightHub Enterprise edition and a Government edition, allowing operators to feel totally confident with data backed up to their own personal servers. The Government edition even prevents users from transferring data off of the drone to other parties, whether intentional or accidental, and has restricted hardware pairing to prevent the use of any unsecure hardware or unauthorised third-party applications. The U.S. Department of the Interior has recently independently validated and approved this Government edition, confirming after 15 months of rigorous assessment with expert industry partners like the NASA Kennedy Space Center, that no data whatsoever would be transmitted outside of the system and that it was therefore safe for them to use.

Graham:

Finally, how do you keep pace with unprecedented and emerging cybersecurity risks to ensure that your drones don't become susceptible to new threats?

Christian:

We operate a global Bug Bounty Programme which has internationally renowned security researchers continuously working to identify any potential gaps so that they can be swiftly resolved. DJI's prioritisation of data security means that the company is constantly working towards further improvement.

For more information, DJI data security in the UK 090719

4 July 2019: ARPAS Statement – BBC 2 Documentary "Britain's Next Air Disaster? Drones?" – Aired Mon 1 Jul 2019

ARPAS members have expressed deep concern and criticism of the BBC Two documentary, 'Britain's Next Air Disaster? Drones?', which aired on Monday 1 July 2019 and which focussed heavily on the illegal and malevolent use of drones in UK airspace, exaggerated the risks and presented a one-sided view that has the potential to harm the livelihood of ARPAS members.

ARPAS acknowledges that mid-air collision, unauthorised flight within restricted and sensitive airspace as well as deliberate nefarious use, are the most credible causes of a serious incident involving a drone, but a balanced assessment of risk is always a combination of severity and likelihood. ARPAS believes the programme overemphasised the former and neglected to realistically assess the latter.

As a public service broadcaster, the BBC has a responsibility to provide its viewers with balanced reporting which, on this occasion, we believe it failed to do. ARPAS is the UK's trade association representing the unmanned aviation industry and we would hope that in the future, programme makers ask us to contribute in order to gain a more balanced view.

ARPAS vigorously supports the legal, safe and legitimate uses of drones and strongly believes this represents the vast majority of recreational users and all the commercial users amongst its members for whom it will continue to advocate.

ARPAS has raised a complaint with the BBC and contacted BBC Points of View. We encourage you to do the same.

25 June 2019 Key takeaways of the Defence Committee, Science and Technology Committee Oral Commission at Parliament held 12th June 2019.

ARPAS-UK was invited to testify in front of the Select Committee about “commercial and recreational use of drones in the UK”. Anne-Lise Scaillierez, Director of ARPAS-UK, testified along with Tim Johnson, Policy Director of the CAA, and Richard Parker, CEO at Altitude Angel. A second panel comprising Brendan Schulman, VP Policy and Legal Affairs at DJI, Sir Brian Burridge, CEO of the RAeS, and Prof. James Scanlan of Southampton University, took place immediately afterwards. Both transcripts are available in the Vault.

The Draft Drone Bill is about law enforcement, and members of the Defence Committee joined the session. So, understandably, the focus of the Committee was about that particular aspect. The key question was:

How effective are the contemplated measures in tackling the misuse of drones? Not only from the “careless and clueless”, but also from criminal or malicious intent?

Not such an easy task for a panel that essentially deals with professional users of the airspace, who sometimes moan about regulation but certainly abide by it! It is actually encouraging that ARPAS-UK was invited to testify and that we are considered on the side of the good guys.

The CAA explained in detail the purpose of the registration scheme; the objective is to onboard all drone users for educational purposes. Also, registration is a first step towards UTM.

We mentioned other possible measures that are part of the adopted EU regulation in the Open category: direct remote identification and geo-awareness functionalities for CE marking on all drones of 250g and more.

Is the 250g threshold the right threshold?

We mentioned that it is the threshold applicable in the USA and in the upcoming EU regulation as the “harmless” threshold. The EU regulation also provides for registration of drones of any mass if they carry a camera, for privacy rights protection. The Defence Committee looked at it from a malicious perspective and questioned the virtue of any threshold. MP Stephen Metcalfe questioned the threshold as well if the point of registration is to educate the larger audience of drone users.

Why should model aircraft flyers who have a solid track record of safety, register and pay?

The CAA made its case about including all unmanned aircraft and the need to have all airspace users registered for the future management of airspace.

The option that a club, such as the BMFA, could take on the role (and legal responsibility) of operator on behalf of its pilots members and pay the fee once for all members, was discussed and confirmed. We recently heard conflicting positions, a point to follow closely.

Also, DJI made the point that the registration fee of £16.50 every year is 12 times the US fee ($5 every 3 years). It is a concern in terms of enticing drone users to register. In most other countries, the fee is 0 or as low as possible to ensure successful onboarding.

We agree with that position, but the CAA is constrained by the “users pay” policy set by Department for Transport, and the current lack of alternative sources of funding.

Why do we need a system such as UTM? How does it prevent misuse of drones?

Altitude Angel of course was the lead on the matter. Our comment on it was that we would welcome an automated system that would facilitate the use of airspace around airports. The question is the cost of it.

We mentioned the LAANC in the USA that is running with commercial UAS operators.

The vast majority of drone manufacturers are made in China. Shouldn't we engage with them to make sure that their drones and people who purchase their drones in the United Kingdom follow our regulations?

Of course, in the context of Huawei, the topic is sensitive and DJI was put on the spot by the Defence Committee, especially in terms of data protection. The answer can be complex, depending on the type of information and the options of transmission and back-up the operator has selected. We should expect some further clarification by DJI on this matter.

Societal acceptance is key to the drone community. The development of the industry can only benefit from a stronger societal acceptance. This is also true for smooth daily interactions with the stakeholders to whom we must ask for permissions to fly a specific mission.

We know that the risks raising concerns among the general public are privacy intrusion, criminal use and safety. Therefore, balanced measures that mitigate those risks are very welcome.

Education about the rules of the widest audience of drone users is essential. A high registration fee does not serve that objective well. We understand that the root cause of the high fixed annual costs for running the registration scheme are related to the required compliance with the Government Digital Services Framework, which we are looking into.

Technology-based measures could also be considered, such as registration for security as well as educational purposes; product functionalities such as remote identification, geofencing, and height limitation; enabling infrastructures such as Unmanned Traffic Management UTM. In practice, registration and electronic conspicuity, which is the CAA's name for remote identification for the purpose of airspace management, are prerequisite to develop real-time UTM.

These technologies would support both safety and law enforcement objectives and would likely address most concerns over inappropriate drone uses. They would not stop malicious users of drones who, by definition, do not intend to follow regulation.

We know that drones can be misused with malicious intent, but so can cars, smartphones and the social media…. But we still use those on a daily basis. Cybersecurity risks are probably much higher, but corporates and individuals still use the internet for all kinds of purposes without solid cybersecurity protection. If we consider the approach of other countries, the USA for example is very sensitive to security matters. US troops are subject to attacks with IED-carrying small drones in their overseas operations, and the US MoD dedicate increasing funding to counter-UAV technologies. At the same time, the USA is very much fostering innovation in the commercial field, and their ambition is likely to become leaders of both UAV and Counter-UAV technologies where they address both the risks and opportunities of drones.

The first thing is to detect and identify drones, the equivalent of primary radars, then UTM becomes useful to spot the intruders.

******* The end *******