Response to Commons Science and Technology Committee

Inquiry: Commercial and Recreational Drone Use in the UK

On behalf of the UK Computing Research Committee, UKCRC.

Prepared by: Professor Chris Johnson,
School of Computing Science, University of Glasgow, Glasgow, G12 8RZ.
http://www.dcs.gla.ac.uk/~johnson

The UK CRC is an Expert Panel of all three UK Professional Bodies in Computing: the British Computer Society (BCS), the Institution of Engineering and Technology (IET), and the Council of Professors and Heads of Computing (CPHC). It was formed in November 2000 as a policy committee for computing research in the UK. Members of UKCRC are leading researchers who each have an established international reputation in computing. Our response thus covers UK research in computing, which is internationally strong and vigorous, and a major national asset. This response has been prepared after a widespread consultation amongst the membership of UKCRC and, as such, is an independent response on behalf of UKCRC and does not necessarily reflect the official opinion or position of the BCS or the IET.

Executive Summary

We argue that:

- legislation must take into account the likely changes in "drone" technology with increases in the range, performance and autonomy supported by on-board software;
- legislation must take into account changes in the sensing capability of on-board systems including listening technology, night vision and enhancements to remote 3D scene capture within the wider privacy concerns of sensor integration through the Internet of Things;
- legal requirements, which in other countries tend to be based simply on the mass of the drone, are insufficient to account for the privacy concerns raised above;
- legislation on registration, location tracking and geo-fencing must account for the growing "cottage industry" in drone manufacture using 3D printing and avionics that easily subvert the mechanisms, which might be required of commercial suppliers;
- any deployment of kinetic and electro-magnetic countermeasures must take a systemic view of risks that include direct hazards to the public from the drone but also the hazards to conventional air traffic and other safety-related infrastructures influenced, for example, by inadvertent deployment;
- any legislation must be proportionate to the very small number of instances of malicious use. It must be sufficient to discourage any recurrence of these acts – with appropriate and convincing technological mitigations. It must not, however, jeopardise the tangible benefits of drones to the UK economy and to a wide range of research activities.

Response to Questions

Area 1: The ethical implications of civilian drones on citizen privacy and safety in the UK;

[1] It is important to define what is meant by drones given that any legislation is likely to persist beyond the present generation of technology and that the ethical concerns raised by these devices are likely to change as a consequence. At present, many people associated "civilian drones" with small quad-copter devices that are mainly operated within line of sight with significant, disruptive noise levels. The ethical issues associated with these devices include but are not limited to:

a) The operators' ability to observe and record private property where citizens have a reasonable expectation of privacy;
b) Even within line of sight, it is not always possible to identify, prevent and ultimately seek redress from the operators of these devices;
c) The third-party risks that arise to citizens and to private property under the flight path of these devices, compounded by the difficulty of redress in b);

[2] We envisage that in the near future these and similar devices will be equipped with increased levels of autonomy. Noise levels will likely be reduced through advances in materials and rotor design. Developments in geo-location technologies, in image analysis and on-board processing will enable drones to operate independently of continuous ground-based communications links. We also foresee increases in both the sensing capability of devices and potential miniaturisation – using technologies that are already available to the military and intelligence communities. Night vision (image intensification and infrared) as well as enhanced directional sound capture can be embedded in very small drones. At the same time, larger and more powerful devices are likely to become more widely available. These changes will exacerbate the ethical and privacy concerns identified in paragraph [1] and introduce further issues that are directly relevant to UK computing research:

a) If legislation clarifies liability for the operation of drones, it must consider the impact of autonomous modes of use. In such circumstances, the behaviour of the platform will be influenced both by the immediate operator but also by the algorithms embedded within the autonomous control system. This raises questions of whether or not the developer of an autonomous control algorithm might be liable for any consequent losses when such a vehicle is operating outside the direct control of the end user?
b) Some existing airworthiness requirements might reasonably be extended to increase public confidence in the safety of these devices. We would also encourage the CAA and industry partners to help operators actively mitigate risk from autonomous and semi-autonomous modes of operation. We are particularly concerned about situations in which responsible users might inadvertently violate privacy or safety constraints;
c) With increased acuity of on-board sensors, there will be increased potential for collateral recordings – even where a legitimate user of these devices is behaving in a responsible manner they may inadvertently record the behaviour of third parties in an unintended manner, legislation should provide for resolution and redress of these situations while respecting the owners' right to operate these systems in a controlled and safe manner.

Area 2: The effectiveness of built-in drone safety features, such as tracking and monitoring capabilities, in mitigating the risks of civilian drones;

[3] The effectiveness of built-in drone safety-features is determined by the motivation of the operators. It is relatively straightforward to construct drones from publically available sources on the Internet, for example using Arduino controllers for the avionics and 3-D printed structures for the control surfaces. The use of these approaches to support novel drone designs is also a key component of many undergraduate degrees and research programmes in aeronautical engineering and in computer science across the UK. Any new safety features can, of course, be embedded within these devices. However, these fabrication techniques also offer the opportunity to create drones that by-pass the features required of commercial suppliers. Malicious users are likely to be able to undermine the majority of mitigation measures.

[4] Similarly, it is increasingly possible to disable protection mechanisms when enthusiasts are motivated to reverse engineer and then publish means of gaining greater degrees of control over these devices. The nature of these protection mechanisms is such that it can be difficult, if not impossible, for police agencies to detect whether or not they have been compromised in a particular drone without attempting to actively deploy them in a controlled environment. Any legislation that permits multiple means of tracking, monitoring and denying airspace can make it even more difficult to determine the extent of any protection that may be required by future legislation and could be embedded within a growing range of heterogeneous platforms.

Area 3: The effectiveness of anti-drone technology in mitigating the risks of civilian drones;

[5] It is important to recognise that anti-drone technology can itself increase risk. Deployment of any system carries the possibility of side-effects that jeopardise safety. Electro-magnetic and directed energy systems have been used by the US military and, in all cases, concerns have been raised about the impact of those systems from errors in target identification and tracking. Other concerns focus on inadvertent deployment, for example, against conventional aircraft. It must also be possible to ensure that are emissions are focussed only on the drone without the possibility of reflection. Triggering 'return to home' functions must ensure that the drone does not then hit any objects or people en route or overfly sensitive areas such as Primary Schools under autonomous control.

[6] The consequences of deploying any countermeasure are highly dependent on the environment. Disabling a drone in flight may cause no risks if it falls onto a 'safe area'. However, changes in wind direction are sufficient to create a field of foreign object debris similar to that which led to the loss of Concorde flight 4590. This example, and those presented above, illustrate the need for systemic risk assessments prior to the deployment of any anti-drone technology.

Area 4: The economic opportunities arising from the growth of drone technology;

[6] The overwhelming majority of operators pose no risk to the public and those that do often suffer from a lack of awareness rather than malfeasance. Legitimate operators are unsure of the processes that they need to follow to comply with existing requirements. Significant criminal sentences should be associated with the deliberate use of drones in a situation that can be proven to be the result of deliberate intent. This must be coupled with a technically credible array of defensive mechanisms that do not carry significant increased risks to the public through the deployment of those mechanisms. However, these must be balanced by initiatives to simplify operating requirements and to increase awareness of operators' responsibilities.

Area 5: The success, or otherwise, of regulatory frameworks for civilian drones and what should be covered in the forthcoming 'Drones Bill';

[7] It is important that the DfT monitors the implementation of any legal provision to ensure that the interpretation of those provisions by the CAA and by other bodies does not inadvertently have a detrimental impact on UK industry and research. There is a danger that their actions will limit the well-intentioned users of new technologies while having little impact on those with the deliberate intention to harm.

[8] 'Proportionate approaches' to risk assessment have often been interpreted to impose more stringent regulations on drones with a larger mass. This is appropriate given increasing potential for damage from these vehicles. Previous paragraphs have explained that this may not be sufficient; it neglects the risks from changing levels of autonomy, the potential velocity of future micro-drones and the privacy implications of advanced sensing technologies. Obligatory registration, geofencing or low-cost/low-power disclosure technologies – for example extensions to LoRa[1] may help to mitigate these increasing concerns from drone operation. The precise nature of these mitigations should be subject to industry and public consultation. They should be reviewed over time to ensure they reflect the latest advances in protective technologies, rather than embodied within primary legislation.

Area 6: The plans for registration of civilian drones in the UK;

[9] Many owners and operators of drones are unclear about the requirements under ANO 2016 94(3), CAP772 etc:

> "The CAA cannot provide advice on what is, or is not, a legitimate interest or whether restrictions or fees are being lawfully imposed by other authorities. However, any authority or regulatory body should be able to identify the specific laws, regulations or bye-laws that empower it to regulate the use of UAS, or more usually, the land from which they are operated, much as the CAA has set out the regulations that it applies, above. We therefore recommend that if you are unsure of whether a restriction imposed by a body legitimately applies to your flight, you request that information from the relevant authority or regulatory body".

[1] https://lora-alliance.org/lorawan-certified-products

Self-help groups have promoted the responsible operation of drones by explaining some of the inconsistencies, see for example[2]. They should be encouraged alongside more focused attempts to simplify existing (and future) requirements.

[10] Operators are also unclear about existing and future registration requirements; see for example Taylor vs FAA to illustrate the international nature of this problem. Most have grown used to what they perceive as an unregulated environment[3]. Many end users assume that it is better not to raise the issue of registration than to continue operating in an ad hoc manner. This is not only an issue for hobbyists but also affects UK research – for example, it is unclear whether specific permission/additional safeguards are required to fly vehicles with new flight control algorithms.

Area 8: International comparators with exemplary drone-interference prevention policies.

[10] The UK Computing research community has conducted a number of detailed comparisons of international policy in this area, for instance [4]. The following figure illustrates previous points, including the reliance on mass as the determinant of regulatory constraints. Many of these requirements have also changed in recent months.

PROVISION	CANADA	USA SMALL UAS	USA MICRO UAS
Definition	< 4.4 lbs (2 kg)	< 55 lbs (25 kg)	< 4.4 lbs (2 kg)
Maximum Altitude	300 ft	500 ft	400 ft
Airspace Limits	Class G only	Class G and E. Class B, C, D with ATC permission	Class G only
Distance From Obstacles	100 feet laterally from structures, 100 feet from people	Operation prohibited over any person not involved in operation	Flying over any person is permitted
Operational Area Extension	No	Yes, from a boat	No
Autonomous Operations	No	Yes	No
Aeronautical Knowledge Required	Ground school	Knowledge test	Self-certification
FPV Permitted	No	Yes, if you can also visually see UAS	No
Operator Training	Ground school	Not required	Not required
Visual Observer Training	Ground school	Not required	Not required
Operator Certificate	Not required	Required, must pass basic UAS aeronautical test	Required, no knowledge test
Preflight Safety Check	Required	Required	Required
NearAirport Operations	No	Yes	No
Congested Area Operations	No	Yes	Yes
Liability Insurance	Required, $100,000	No	No
Daylight Only	Yes	Yes	Yes
Aircraft Made of Frangible Materials	No	No	Yes

[11] The concerns raised in this submission are one example of the wider problem of "regulatory lag" that hinders UK research and industry. The application of AI/Machine Learning in safety related systems, the operation of autonomous vehicles on public roads, the privacy concerns that arise from mass data analytics in healthcare provide further examples. In each instance, there

[2] https://dronesaferegister.org.uk/register/DSR-Hobbyist-Membership
https://uav-air.com/drone-licence
[3] https://forum.dji.com/thread-129275-1-1.html
[4] http://www.dcs.gla.ac.uk/~johnson/papers/ISSC16/regulator.pdf

is a common need to provide policy support to the regulatory agencies that protect the public without damaging our nascent industries.