Drone Risks in Aviation

Summary

The security risks that drones pose to aviation are a growing threat to the industry. In our view, security should be considered an integral part of safety in the Committee's deliberations and our submission focuses on that narrow but important perspective.

The development of drone technology has outpaced, and the evidence suggests it will continue to outpace, the development and deployment of anti-drone solutions. We have seen considerable innovation and many improvised methods by those with the capability and intent to attack aviation assets including passengers and crews. Their use of drones is in its infancy but our assessment is that this will evolve and increase. We are concerned that disruptive drone activities will become a tactic of choice for airport expansion protesters too.

The challenge for regulators is to achieve the balance between allowing the nascent industry to develop at a pace for commercial and leisure applications, and ensuring adequate levels of safety and privacy.

We believe this regulatory balance should be risk-based as proposed in the European Union (EU) draft Commission regulation 'Laying down rules and procedures for the operation of unmanned aircraft', and as the UK government has practised in aviation safety and aviation security for many years. The government and Civil Aviation Authority have strongly promoted a performance-based regulatory regime in aviation safety and a similar outcome-focused risk-based regime in aviation security.

A multi-faceted approach using different technologies is expected to provide the greatest level of mitigation against security threats. In our view, it is essential for authorities responsible for developing and maintaining drone-interference prevention policies to be as innovative and agile as the would-be attackers. To that end, more insight into the drone-interference prevention regime of the future could be gained from a wide-ranging analysis of industry intelligence and research, including drone, aviation, information technology, other industries and initiatives such as "All one in the sky". In view of the growing Artificial Intelligence and Cybersecurity threats, ethical hackers may also make a valuable contribution.

The ethical implications of civilian drones on citizen privacy and safety in the UK

In terms of privacy, if a drone has a camera installed then, according to the UK Information Commissioner's Office, it has the potential to be covered by the Data Protection Act and GDPR as there could be privacy risks.

It is not only the capturing of the images that can be an issue but how they are then used. In social media publishing, the originator loses control of image distribution and the drone privacy issue is intricately bound with social media privacy issues.

In terms of safety, the distinction between safety and security is artificial and unhelpful: there is a tendency to ignore security issues when considering safety. In our view, security should be considered an integral part of safety in the Committee's deliberations, although for some specific issues we have singled it out where the distinction is helpful.

'Civilian drones' may be a misleading term. There is evidence of weaponisation of what would be considered civilian drones, albeit mostly in conflict zones overseas to date. An incident in Venezuela in August 2018 highlighted the potential risks to citizen safety, when two weaponised drones detonated explosives in Caracas, where President Maduro of Venezuela was addressing the Bolivarian

National Guard. The Venezuelan government claims the event was a targeted attempt to assassinate the president.[1]

In designing preventive measures and powers of intervention, there is an ethical consideration in terms of possible collateral damage and unintended consequences. Granting of any powers should involve a weighing up of the risks of unintended consequences against the severity of current and future safety and privacy risks.

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

Built-in safety features are likely to be effective in mitigating risks caused by normally law-abiding drone-flyers without sinister intent, for example by reducing accidental incursions.

However, these are unlikely to be effective against organised crime groups (OCG), protestor groups, terrorists and others with criminal or disruptive intent who will be willing and able to bypass such technology. The technology is also ineffective against those who build their own drones. Open source reporting warns that hackers are offering software to drone owners who want to bypass “no fly zone” technology and other features deployed to help ensure drones operate safely.

The effectiveness of anti-drone technology in mitigating the risks of civilian drones

The development of drone technology has outpaced, and the evidence suggests it will continue to outpace, the development and deployment of anti-drone solutions.

To date, the most notable unlawful activity seen in the UK has been the employment of drones as a means to transport drugs into prison environments, and what appear to be deliberate acts to cause disruption at UK airports.

Recent incidents at airports worldwide have shown that there is no one reliable solution, further complicated by legal and regulatory constraints on their deployment. Some of the legal and regulatory systems do not permit counter-drone activities, e.g. signal jamming and GPS spoofing, due to the risk of collateral damage. Cost is also a factor.

A multi-faceted approach using different technologies is expected to provide the greatest level of mitigation against such threats. We are aware that the Home Office and their partner organisations are testing and evaluating the safe use of various counter-drone technologies in the UK, but further rapid development is needed. Unless existing anti-drone technology can be widely deployed, a lack of operational experience will remain an obstacle to the design of practical solutions to tomorrow’s challenges, challenges which are proliferating at an accelerating pace.

Russia's KUB-UAV Kalashnikov drone, which is capable of self-exploding on approaching a target, was unveiled in February 2019 at the IDEX-2019 arms exhibition in the United Arab Emirates. The drone, which is said to be ready for use, can travel at speeds from 80 to 130 kilometres (50-80 miles) per hour, with a payload about three kilograms (6.6 pounds) and a flight duration of up to 30 minutes.[2]

China is reported to be programming new autonomous AI-powered drones to conduct "targeted military strikes" without a human making the decision to fire. Whilst these drones are intended for “official” military use, it is not unknown for weaponry to end up in the hands of terrorists and other criminals.

---

[1] ‘Venezuela: Military figures arrested after drone “attack”’ BBC News (London, 18 August 2018) https://www.bbc.co.uk/news/world-latin-america-45190905 accessed 11 April 2019.

[2] F Wolfe ‘Russia Unveils KUB-BLA “Kamikaze” Drone at IDEX 2019’ Aviation Today (Rockville, MD, 21 February 2019) < https://www.aviationtoday.com/2019/02/21/russia-unveils-kub-bla-kamikaze-drone-idex-2019/> accessed 11 April 2019.

In Catalyst Go's recent white paper *Countering Tomorrow: The Age of Materials, Coatings and Deceptions*[3], they make a valid point about drone countermeasures. Those available to us today are primarily used to target vulnerabilities in the control systems to stabilise and navigate the drone. Tomorrow's autonomous vehicles rely on internal sensors to sense their environment and guide themselves. GPS and command links are not required, thereby nullifying the countermeasures that are available (but not widely deployed) today.

Highlighting similar concerns, a report authored by Gregory C Allen of the Centre for a New American Security, a US national security think-tank, notes that drones are becoming increasingly automated as designers integrate sophisticated AI systems into the decision-making processes for next-generation reconnaissance and weapons systems[4]. This level of technological sophistication brings with it new challenges in terms of mitigating the risk posed by drones.

A further concern is the growing ability to compromise the firmware or software of IoT devices, robot and autonomous vehicles by relatively unsophisticated means. Hijacking a substantial commercial drone and using its own weight as an attack payload would be possible by a relatively unskilled lone attacker, an attack type favoured by some terrorist groups and less easily detected by the intelligence services.

There is an urgent need to develop anti-drone technology capable of addressing such threats and ready to keep pace with future drone developments.

Risk managers need to be mindful that terrorist tactics could be exploited by UK actors to cause harm. While it is not beyond the imagination to envisage the use of UAVs to spread chemical or biological materials in public areas, in the absence of credible intelligence in our view this is more likely to be in the form of a hoax, causing mass panic. There have been many instances of stampedes by panicked crowds causing injury and death.

The economic opportunities arising from the growth of drone technology

Several prestigious companies have predicted that drones present massive economic opportunity.

In a 2016 research report, Goldman Sachs estimated that the global drone industry would be worth $100 billion by 2020. While the largest markets are defence (estimated at $70 billion) and the consumer drone market ($17 billion), the commercial/civil sector representing business and governments was identified as the fastest growing, projected to reach $13 billion by 2020.[5]

A study conducted by McKinsey & Co in December 2017 predicted the US UAV market would "have an annual impact on the country's gross domestic product" of up to $46 billion.[6]

PricewaterhouseCoopers has predicted that the drone industry, if managed correctly, could add £42bn to UK GDP by 2030.[7]

---

[3] Catalyst Go 'Countering Tomorrow: The Age of Materials, Coatings and Deceptions' (22 January 2019) <https://www.catalyst-go.com/countering-tomorrow> accessed 11 April 2019.

[4] GC Allen 'Understanding China's AI Strategy: Clues to Chinese Strategic Thinking on Artificial Intelligence and National Security' (Centre for a New American Security, 6 February 2019) <https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy> accessed 11 April 2019.

[5] Goldman Sachs 'Drones: Reporting for Work' (March 2016) <https://www.goldmansachs.com/insights/technology-driving-innovation/drones/> accessed 11 April 2019.

[6] P. Cohn, A. Green, M. Langstaff and M. Roller 'Commercial drones are here: The future of unmanned aerial systems' (McKinsey & Co, December 2017) < https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems> accessed 11 April 2019.

[7] PricewaterhouseCoopers 'The impact of drones on the UK economy' (29 May 2018)

<https://www.pwc.co.uk/dronesreport> accessed 11 April 2019.

There are many legitimate and valuable uses of civilian drones, particularly in the fields of policing, firefighting, and search and rescue. Other uses include delivery of blood samples within hospital campuses, delivery of automatic external defibrillators, hurricane hunting, mapping and surveying, wildlife protection, farming, and building inspections. Network Rail uses drones to assess and improve their rail network, and Altitude Angel have partnered with Manchester Airport and the National Air Traffic Services to demonstrate an unmanned traffic management system with a programme called Operation Zenith.

Use of drones for parcel delivery and other innovative uses will be a significant part of this growth, but the potential for other innovations, particularly when enhanced by other technologies such as AI, is enormous.

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

The challenge for regulators is to achieve the balance between allowing the nascent industry to develop at a pace for commercial and leisure applications, and ensuring adequate levels of safety and privacy.

We believe this regulatory balance should be risk-based as proposed in the European Union (EU) draft Commission regulation 'Laying down rules and procedures for the operation of unmanned aircraft'[8], and as the UK government has practised in aviation safety and aviation security for many years. The government and Civil Aviation Authority have strongly promoted a performance-based regulatory regime in aviation safety and a similar outcome-focused risk-based regime in aviation security.

The challenge in taking this approach with civilian drones is determining how industry and individuals would assess their risks and implement mitigating measures. Who would be responsible, what powers would they have and how would they be regulated?

In terms of the regulatory framework's coverage, one area that has received scant attention to date is the human factors. Our work constantly shows that humans are not uniform in skills, conscience and conscientiousness, and that each individual is not consistently reliable, rational and level-headed. Add to that any risk of coercion, illness or greed affecting someone's behaviour, and it becomes clear that the variability of human behaviour is a factor that should be addressed. Flying, driving, gun ownership and many other privileges are subject to conditions and tests of basic understanding and skill, through the granting of a licence. We believe that users and owners of all but the smallest drones may have to be similarly licensed, probably using the mass of a drone as a criterion for applicability or thresholds of regulation.

The plans for registration of civilian drones in the UK

Registering civilian drones will help regulate the majority of law-abiding drone community but OCGs, protest groups, terrorists and those with criminal or disruptive intent are unlikely to comply with any such requirement.

Aligning with government policy discussed in paragraph 29, we would expect registration to be part of the risk-based regulatory regime. To compare with the example of another technology: we control the use of guns very tightly because the risks to society are rightly thought to outweigh the constraints on individual gun owners, no matter how responsible some may be. In the case of drones, the same principles apply: protection of society requires reasonable and justifiable constraints on the individual, determined by risk assessments.

[8] European Union Aviation Safety Agency 'draft Commission regulation: laying down rules and procedures for the operation of unmanned aircraft' (Cologne, Germany, 2018) <https://www.easa.europa.eu/document-library/opinions/opinion-012018> accessed 11 April 2019.

There is also a need for clarity about the legal definition of a drone. Very small drones, including some with cameras, and some with a very small range (time, distance or altitude) do not pose any significant privacy, safety or security threat. We believe the definition must be very specific and clear as to which devices are not subject to the regulations. The risk of unintended consequences is high, especially as this technology is developing quickly.

The current state of drone safety education and research in the UK

According to Nesta's 'Flying High' report[9], UK policy responses to drones are behind those of leading countries. The US, EU and Singapore are said to have taken bigger steps towards reforming regulations, creating testbeds and supporting businesses with innovative ideas.

In a risk management context, we see much discussion in drone and other aviation incidents whether it is a safety or security issue. Arguing over whose responsibility it is should not be the key area of focus and we believe that the regulatory regime should promote a collaborative approach between all stakeholders. Education is needed not only for drone users, but for authorities, regulators and the practitioners called on to deal with an event.

International comparators with exemplary drone-interference prevention policies

Drone interference extends across a spectrum from mischievous nuisance and privacy invasion to hostile attacks including terrorists, protestors and state actors.

We are aware of very few examples of excellent prevention policies, even in respect of only a part of this spectrum. We know of no policies that cover the entire spectrum comprehensively.

Approaches vary greatly, and those that we have seen are incomplete or still in early development. For example, the current US approach is limited. The Federal Aviation Administration has a prescriptive set of rules on registration and where it is permissible to fly, including on-board sensors to prevent operation beyond line of site. The only public information on the Transportation Security Administration website discusses the transporting of drones in passengers' baggage.

There appears to have been little consideration given to the types of attack and how to prevent or respond to them, such as:

- Aircraft strike
- Airport disruption
- Runway debris from exploding drone/multiple drones/drone dropping payload
- Radar interference/reflective drone
- Street disruption
- Physical attack on individuals
- Road obstruction/driver distraction
- Contaminated payload – real or hoax
- AI-controlled autonomous drone swarm
- Direct targeting of people e.g. VIP assassination (by drone adapted with firearm or payload of explosives)
- Mass fatality attack in crowded places
- Attacks targeting airport infrastructure and key sites.

[9] Nesta 'Flying High: The future of drone technology in UK cities' (23 July 2018) <https://www.nesta.org.uk/report/flying-high-challenge-future-of-drone-technology-in-uk-cities/> accessed 11 April 2019.

The collaborative industry initiative "All one in the sky"[10] has made some useful proposals. 15 associations of airlines, aircrew, airports, air navigation service providers, controllers and general aviation joined forces in mapping the areas of action that would pave the way to safe drone integration. They jointly called to accelerate the implementation of 6 key measures:

- Extensive public awareness campaign
- Mandatory training and licensing
- Airport protection from drone intrusions
- Incident reporting
- Increase in the effectiveness of enforcement
- Situational awareness of all manned aircraft
- Traffic management for drones

In our view, it is essential for authorities responsible for developing and maintaining drone-interference prevention policies to be as innovative and agile as the would-be attackers. To that end, more insight into the drone-interference prevention regime of the future could be gained from a wide-ranging analysis of industry intelligence and research, including drone, aviation, information technology, other industries and initiatives such as "All one in the sky". In view of the growing AI and cyber threat, ethical hackers may also make a valuable contribution.

3DAssurance Ltd

3DAssurance Ltd is a consulting firm dedicated to aviation security and risk management founded by the two authors of this paper, Andy Blackwell and John Wood. Both have many years of security and risk management experience and were deeply involved in developing the government's risk-based approach to aviation security management, the Framework for an Aviation Security Management System (SeMS)[11] . The firm continues to promote this internationally as the best practice for managing the interaction between regulatory compliance and autonomous risk management by aviation operators.

[10] https://www.eurocockpit.be/news/we-are-all-one-sky

[11] Civil Aviation Authority publication CAP1223