Andrew V. Shelley

A Framework for Counter-Unmanned Aircraft System Regulation in New Zealand

Abstract

The malicious or negligent use of unmanned aircraft systems (UAS) – usually referred to as 'drones' – gives rise to significant risks. While the risky behaviours are subject to existing legal sanctions, the apprehension of perpetrators can be difficult, and traditional regulatory controls, such as licensing drone operators, may be ineffective. 'Counter-UAS' (C-UAS) systems that defend against unmanned aerial systems are emerging internationally as a way to address the latent threat. Potential legal issues with the implementation of C-UAS in New Zealand are briefly surveyed. I propose the adoption of a licensing system for C-UAS similar to that already adopted in civil aviation regulation.

Keywords Drones, unmanned aircraft systems, counter-UAS, C-UAS, regulation, New Zealand

Andrew Shelley is a PhD student in the School of Economics and Finance, Victoria University of Wellington, and Chief Executive of Aviation Safety Management Systems Ltd, a company that provides training to drone pilots.

Recent research suggests that there may be over 280,000 New Zealand-resident drone users, with another 200,000 overseas visitor users each year (Colmar Brunton, 2017).[1] Behind these statistics, drones seemingly have an ever growing number of uses, but they also give rise to potentially significant risks that may not be managed well by our existing regulatory framework. A malicious actor could easily fly a drone into the path of an airliner, deliver contraband to prisons or drop an improvised explosive device over a sports stadium without ever being at risk of detection by authorities. A significant risk also exists that an individual who is negligent or reckless, rather than malicious, could also cause harm by flying into the path of an aircraft, or crashing at a public event. While all of the activities identified are subject to existing legal sanctions, the identification and apprehension of perpetrators can be difficult, and traditional regulatory approaches, such as licensing drone operators, may be ineffective. This article considers the beneficial role of 'counter-UAS' – systems intended to counter or defend against unmanned aerial systems – and proposes the adoption of a licensing system to enable counter-UAS (C-UAS) to be adopted in New Zealand.

The threat

In 2015 a small drone carrying radioactive material was flown onto the roof of the Japanese prime minister's residence (BBC, 2015). In the years since then unmanned aircraft have increased in sophistication: drones manufactured by DJI, the most popular brand of drone worldwide, have object avoidance technology, allowing them to be flown close to structures with minimal risk of collision. The Syrian civil war and the subsequent war against ISIS in Syria and Iraq has seen the use of small drones to drop improvised explosives and grenades (Gibbons-Neff, 2017; Watson, 2017). However, the planned use of drones by non-state insurgent groups predates the Syrian civil war. For example, Ballard et al. (2001) report that in early 1994 the Japanese cult Aum Shinrikyo attempted to use a remote-control helicopter to deliver the nerve agent sarin against a target; however, the helicopter crashed during testing (Bunker, 2015). Small drones have not, to date, been used in terror attacks in the West, but authorities are concerned that attempts will be made (Hughes, 2015).

Small drones have been used to deliver contraband – particularly drugs, weapons and mobile phones – to prisons in both the United Kingdom (Glanfield, 2015) and the United States (Brandes, 2015). In the United Kingdom it was reported that 120 drones were seized flying contraband into prisons over a 23-month period (Drury, 2017). Drones have also been used to aid criminal activity, such as as reconnaissance for potential burglaries (Barrett, 2015). These concerns are equally relevant to New Zealand as they are to the United Kingdom and United States.

New Zealand has seen five recent incidents where the presence of drones closed airports and required manned aircraft to divert or enter a holding pattern. On 6 March 2018 a drone was observed in airspace near the approach path for aircraft landing at Auckland International Airport. Approximately 20 aircraft entered a holding pattern while air traffic control halted operations for 30 minutes, and a Boeing 777 aircraft arriving from Japan diverted 500km to Ohakea airbase to refuel (New Zealand Herald, 2018a). Less than three weeks later, on 25 March, a drone approached to within approximately five metres of another Boeing 777 landing at Auckland International Airport (Lawrence, 2018). On 6 April 2018 a drone was seen at 1,200ft above ground three nautical miles from Auckland International Airport, resulting in seven flights being delayed (Boyle, 2018). Three days later, on 9 April 2018, operations at Whenuapai air force base were suspended when a drone came within 60m of a helicopter flying at 3,000ft above ground (New Zealand Herald, 2018b). On 23 April a passenger flight was delayed at Tauranga because of a drone seen 1.6km from the end of the runway (Motion, 2018).

Simulation results suggest that a 3.6kg drone could fracture the turbine blades of a jet aircraft, rapidly destroying the entire engine (Mackay, 2015; Wasserman, 2015). Known as an 'uncontained engine failure', such an event can cause significant structural damage to the aircraft (Australian Transportation Safety Bureau, 2013) and even a catastrophic fire, as occurred to a British Airways Boeing 777 in Las Vegas in 2015 (Gates, 2015). On 17 April 2018 a mid-air uncontained engine failure on a Boeing 737 aircraft in the United States resulted in the death of a passenger and injuries to eight others (National Transportation Safety Board, 2018).

Drones are also of concern to light aircraft, including helicopters. Helicopters have characteristics that make them particularly vulnerable in the event of a collision with a drone: many have turbine engines subject to the same risk of destruction as airliner engines; main rotor blades can fracture on impact with a drone; and tail rotors are likely to be destroyed on impact with a drone, which could result in severe spinning of the helicopter. Helicopters also often operate at low level, in the same airspace as small drones, including for rescue and firefighting purposes. Due to the high risk of collision, and potential severity of the outcome, helicopter firefighting operations are suspended if a drone is seen close to the firefighting operations (Stuff, 2017).

On a purely economic front, electric power infrastructure, particularly overhead power lines and outdoor switchyards, is vulnerable in the event of a drone crash. Careless rather than malicious use of small drones has resulted in power outages of varying severity. Drones have crashed into overhead power lines, causing power outages affecting hundreds of people (Farivar, 2015; Serna, 2015; Green, 2017) and even starting a fire and damaging vehicles (Brilbeck, 2017). In New Zealand, a drone caused a power outage affecting 200 homes in 2015 (Stuff, 2015). While more power outages are currently caused by cars crashing into power poles than by drones, the potential for a drone to fly into the switchyard of a major substation or power station means that the potential effect of a drone is much greater than that of a car.

On a purely economic front, electric power infrastructure, particularly overhead power lines and outdoor switchyards, is vulnerable in the event of a drone crash.

Existing regulatory provisions

Drones are regulated as aircraft under the Civil Aviation Act 1990, and subject to the provisions of the Civil Aviation Rules (2015), part 101. Part 101 specifies restrictions such as not flying higher than 400ft above ground level, not flying over people without their consent, not flying over property without the consent of the occupier or owner, not flying within 4km of an aerodrome without the agreement of the aerodrome operator, and not flying in controlled airspace without the approval of air traffic control.

Research conducted for the Civil Aviation Authority found that 56% of New Zealand-resident drone users and 55% of overseas-resident drone users in New Zealand self-identified as being aware of the rules and having at least a basic knowledge of those rules (Colmar Brunton, 2017). For New Zealand-resident drone users, awareness of specific rules ranged between 56% and 78% of users, with only 35–59% always complying with those rules.

As with most issues of human safety, prevention of harm is generally preferable to allowing the harm to occur and then compensating the victims' families or punishing the perpetrator.

Need for further measures

Drone users may cause significant harm, whether through ignorance, negligence, recklessness or intentional acts. Licensing may help solve the problem of ignorance, and may reduce negligence, but is unlikely to solve the problem of recklessness or intentional acts.

From a law and economics perspective, the law (and the attendant penalties for breaking the law) results in individuals internalising the social costs of their actions, and generally making more socially efficient decisions as a result. However, the characteristics of drones are such that it may be extremely difficult to identify and locate the operator of an errant drone; hence, laws may often be unenforceable against a drone operator. It is impossible to enforce a law if the perpetrator cannot be found.

Even if the perpetrator could be found and apprehended, appropriate incentives require a willingness by the courts to impose sanctions that reflect the seriousness of the harm or potential harm. In the realm of workplace safety, the New Zealand courts have considered it 'abhorrent to calculate in dollar terms' the value of a life,[2] and reparations ordered by the courts have only been a small fraction of the $4.21 million value of a statistical life calculated by the Ministry of Transport (2017).

If the courts did award a sum reflective of that value, properly adjusted for probability of detection (Polinsky and Shavell, 1992), the amount would be so high that perpetrators would essentially be judgment proof and there would still be insufficient deterrence against operating a drone in a dangerous manner. In such circumstances some form of ex ante regulation is appropriate to reduce the likelihood of harm occurring (Shavell, 1984). For drones, relevant measures include licensing and C-UAS.

Licensing is insufficient

Licensing is common to a number of activities that are considered to pose a hazard to third parties. For example, licenses are required to drive cars, fly aeroplanes and possess firearms, even if the relevant activities are to be performed privately. Licensing is typically coupled with a knowledge test, and consequently could eliminate the knowledge deficit evident in the Colmar Brunton (2017) survey.

However, licensing, even when coupled with surveillance and enforcement, does not prevent unlicensed individuals from engaging in the activity, or licensed individuals from undertaking the activity in an unsafe manner. For example, both cars and drivers are licensed. In a random survey of 746 vehicles being driven in Auckland, 79% of drivers elected to participate in the survey, and of those drivers 1.1% were unlicensed (Blows et al., 2005). Notwithstanding the prohibition on using a hand-held cell phone while driving, in the 2017 calendar year the New Zealand Police recorded 23,412 offences of using a hand-held device for calling or texting while driving (New Zealand Police, 2018).

Thirty five per cent of New Zealand drone users do not consider that drones pose a risk to aviation safety (Colmar Brunton, 2017), which suggests that they would also view enforcement of the relevant Civil Aviation Rules as lacking legitimacy. Watling and Leal (2012) report statistically significant negative correlations between the likelihood of violating specific driving laws and the perceived legitimacy of enforcement of that particular law. It therefore seems likely that licencing of drone operators would not solve the problem of compliance.

Licensing also does not change the fact that the casual bystander will not be able to determine who is flying a particular drone, let alone whether the pilot is licensed or unlicensed. There is, therefore, likely to be an ongoing problem of potentially hazardous use of drones, and this problem is likely to persist regardless of any licensing regime that may be proposed.

Counter-UAS technology

Against this backdrop it would seem to be common sense that action should be taken to restrict the ability of drones to operate in certain circumstances. As with most issues of human safety, prevention of harm is generally preferable to allowing the harm to occur and then compensating the victims' families or punishing the perpetrator. Thus, in the health and safety arena the best control is considered to be elimination of a hazard, and the next best control is to isolate the hazard so that people are physically separated from it. The use of explicit regulatory controls is particularly relevant when private parties are incapable of paying for the full magnitude of harm done (Shavell, 1984).

In an ideal world, therefore, we might envisage the use of a force field to exclude drones from an area where there was a high risk of harm being caused, thus meeting the health and safety requirement to isolate people from the hazard. While force fields remain the realm of science fiction, technology exists that can take control of errant drones, forcing them to land in a safe area or potentially destroying the intruding drone.

One option is the use of radio or GPS jamming. Radio jamming involves the use of 'a radio transmitter ... to disrupt or prevent the reception of radiocommunications' (New Zealand Gazette, 2011). This basic principle can be applied to disrupt the control signal from a transmitter or ground control station to a drone. A number of commercial jammers are available for drones, such as the Battelle Systems 'Drone Defender' shoulder-mounted radio 'gun' (Matyszczyk, 2015), the hand-held 'Dronebuster' by Radio Hill Technologies (Blighter Surveillance Systems, 2016), and the DroneShield 'DroneGun' deployed by Australia at the 2018 Commonwealth Games (Cooper, 2018).

The Blighter Surveillance Systems 'Anti UAV Defence System' (AUDS) is a much larger, military-grade C-UAS which utilises radar to detect drones at a range of up to 10km for larger drones, and smaller drones at a range of up to 3.6km (Blighter Surveillance Systems, 2017). Another large-scale detection and jamming system has been developed by Airbus Defense and Space (Airbus, 2015).

US/Australian firm Department 13 has developed a radio-based system called 'Mesmer' that does not utilise jamming (Department 13, 2017). This system relies on what Department 13 describes as 'protocol manipulation' (Department 13, 2016), which involves intercepting the radio signals used to control the drone, identifying the protocol being used, then transmitting commands to completely take over control of the drone. The drone can then be instructed to leave the area or to land in a safe zone.

Some drones would make it through such electronic controls, so a second layer of defensive measures may also be required in some circumstances. Firearms and lasers can both be used to knock a drone out of the sky (Rees, 2018). Another option is the C-UAS grenade which releases streamers that will foul a drone's propellers, causing it to crash (Wong, 2018).

A number of alternative methods of drone interdiction have been developed which neither knock the drone out of the sky nor utilise jamming. Eagles have been trained to hunt small drones in both the Netherlands (Zhang, 2016; Cade, 2016) and France (Samuel, 2016; Roberts, 2017). Nets may also be used to entangle a drone: nets may be shoulder-launched (OpenWorks, 2016), draped from a drone (Economist, 2015) or fired from a drone (Goodrich, 2016; Goppert et al., 2017; Horiuchi et al., 2016).

International experience

Other countries have already taken steps to allow or enable the use of C-UAS. As noted earlier, Australia deployed C-UAS for the Commonwealth Games. The United States is undertaking trials of the AUDS system at selected airports (Waitt, 2016), and the United Kingdom reportedly used the AUDS system to protect against drones at the royal wedding in May 2018 (Williams, 2018). Like New Zealand, all of these countries are subject to the Montreal Convention (see below), so the convention need not prove a barrier to taking action against drones.

The United States has recently enacted legislation that explicitly allows a range of actions to be taken against drones that potentially threaten the safety or security of a broad range of assets or facilities. The National Defense Authorization Act for Fiscal Year 2018 (2017) allows action to be taken against drones that potentially threaten assets or facilities related to national security. Additional legislation has been introduced into Congress to enable the Department of Justice and the Department of Homeland Security to also take action against drones in a wide range of circumstances, including 'penal, detention, correctional, and judicial operations' and 'mass gatherings or events that are reasonably assessed by the Department of Justice to be a potential target for terrorism or other criminal activity' (the Safeguarding America's Skies Act, 2018). The actions allowed by both pieces of legislation include warning the operator, seizing control of the drone, destroying the drone, and the like. Importantly, these provisions relate to assets or facilities located in the United States or its territories, and are therefore focused on domestic security rather than security during war or war-like situations.

> The biggest difficulty with implementing [counter-UAS] in New Zealand is not the technology but the legal environment.

Legal issues

The biggest difficulty with implementing C-UAS in New Zealand is not the technology but the legal environment. The Aviation Crimes Act 1972, the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 (New Zealand Gazette, 2011) and the Crimes Act 1961 all potentially raise impediments to C-UAS.

While not all C-UAS technologies will damage or destroy a drone, many do. A drone that is executing a pre-programmed flight path may also be unresponsive to the technologies that would seek to gain control and redirect it to another location. However, a drone is considered to be an aircraft, and hence subject to the same regulatory provisions as all other aircraft. The Montreal Convention (United Nations, 1975) prohibits any person from destroying an 'aircraft in service' or causing 'damage to an aircraft in service which renders the aircraft incapable of flight'. While the Montreal Convention includes the qualification that these acts are performed 'unlawfully and intentionally', New Zealand's codifying legislation – the Aviation Crimes Act 1972 – omits this qualification and specifies a maximum term of imprisonment of 14 years. These prohibitions are clearly reasonable in respect of manned aircraft, but less obviously so in respect of unmanned aircraft operating in an area where they have potential to cause significant harm.

Important questions remain as to what C-UAS measures can legitimately be adopted. Under the Radiocommunications Regulations the jamming of radio communications is prohibited unless the person holds a licence allowing the use of radio jammer equipment. The only entity licensed to operate jamming devices is the Department of Corrections, which means that equipment that can jam drone control signals could potentially be used at prisons but nowhere else. Should this restriction remain, or should other security agencies also be able to utilise jamming devices in certain circumstances?

Protocol manipulation systems which seize control of a drone avoid the problems attendant with destroying or damaging a drone, but potentially contravene the prohibitions in the Crimes Act of interfering with a computer system (section 250) and accessing a computer system without authorisation (section 252). The vendor of such a system could potentially contravene the prohibition against making, selling or distributing software 'that would enable another person to access a computer system without authorisation' (section 251). The sale and use of such systems would therefore appear to require an explicit recognition in law that C-UAS are exempt from this prohibition.

The law generally recognises a right to the use of reasonable force in self-defence and in defence of others, with common law defences recognised by section 20 of the Crimes Act and specific defences recognised in sections 39–43 and section 48, among others. From an economic perspective, reasonableness and proportionality suggest that the cost associated with an action should not be greater than the benefit achieved from the action. This economic test requires that the expected (i.e. probability weighted) cost of any harm to third parties is included in the cost of self-defence. Self-defence that complies with this restriction will be efficient. The economics suggests that taking preventive action against drones is likely to be efficient (and thus reasonable or proportionate) in situations where a high magnitude of harm could result, such as at major airports, mass gatherings or critical national infrastructure.

Trespass … provides no assistance when the drone is operating other than above the land where the protected activity takes place, such as when operating in the approach path to an airport or in controlled airspace generally.

In the event of a shooting in defence of another, the defences in the Crimes Act have been considered sufficient to avoid police officers being charged for accidentally killing a third party who happened to be in the line of fire (Independent Police Conduct Authority, 2012). Thus, these defences might generally provide protection for any counter-UAS action taken where the party taking action believed that there was an imminent threat to people – such as when a drone is flying in the approach path of an airliner, or towards or over a mass gathering, or into a protected area around a VIP – and some harm to a third party occurs as a result of the C-UAS action.

However, there are circumstances in which the legal basis for taking action is less clear. Consider, for example, C-UAS action taken against a drone flying in the approach path to an airport, but there is no airliner approaching. In the absence of imminent harm to people the C-UAS action might not be the use of reasonable force, and might instead be considered reckless and subject to prosecution under the Crimes Act. Inter alia, recklessness requires knowledge of the type of harm that *might* occur (France, n.d., section CA20.27), but not necessarily that the risk is seen as significant or likely to eventuate (ibid., section CA20.26). Prosecutions for reckless conduct are also possible under section 47 of the Health and Safety at Work Act 2015, without any necessity for harm to have occurred.

Prosecution requires a decision by the relevant prosecuting authority that it is in the public interest for a prosecution to occur. It is possible that the prosecuting authority may decide that a particular C-UAS action not be prosecuted. However, that does not provide certainty as to future non-prosecution, and may instead simply serve to allow a pattern of behaviour to develop that strengthens the future case for a public interest prosecution. Furthermore, it is untenable for law enforcement agencies to rely on such a strategy. As Chief Justice Sian Elias stated in *Hamed v R* (2011):

> The courts cannot remedy the deficiency [of explicit legislative authority] through approval of police action taken in the absence of lawful authority without destruction of important values in the legal system, to the detriment of the freedoms guaranteed to all.[3]

It could be argued that trespass might provide an avenue for taking action against errant drones. There are, however, a number of complexities in the practical application of trespass to drones (Shelley, 2016). Trespass also provides no assistance when the drone is operating other than above the land where the protected activity takes place, such as when operating in the approach path to an airport or in controlled airspace generally.

Proposal

The legal issues described above suggest that specific legislative authority may be required for C-UAS, as has occurred in the United States. The relevant legislative changes need not be 'all or nothing'. As with other potentially hazardous activities, the ability to operate could be restricted to those who have been licensed to do so. In general terms, it is efficient to set an ex ante regulatory framework coupled with potential ex post liability (Kolstad, Ulen and Johnson, 1990). The standards specified in regulation are minimum standards, requiring less than the socially optimal level of precaution (ibid.). The threat of ex post liability, provided by the prospect of being required to defend in court the reasonableness of actions taken, then ensures an efficient outcome.

The standard licensing model employed by the Civil Aviation Authority and by the New Zealand Space Agency is consistent with the theoretical ideal. The relevant regulations generally specify a minimum level of safety, but complying with those regulations does not absolve the licence holder from liability arising under the Civil Aviation Act 1990, the Health and Safety at Work Act 2015, or tort. Furthermore, the licence must specify how they will comply with the relevant regulations, which enables the licence holder to elect operating procedures that are most efficient for their specific circumstances.

The same approach could be adopted for the operation of C-UAS: a regulation for obtaining a licence for the operation of C-UAS could be promulgated, with potential operators of C-UAS being required to submit operating procedures for approval in order to obtain a licence. The licensing process adopted by the Civil Aviation Authority issues operator licences for a maximum period of five years, ensuring that the licensed entity is subject to regular regulatory scrutiny. As C-UAS technology matures the need for licences may be obviated, or alternatively the increasing capabilities of C-UAS may reinforce the need for such systems.

For the time being, radio jamming should be reserved to security agencies, but rather than a blanket authorisation being granted to those agencies, it may be more appropriate to require that an agency obtain an authorisation from the C-UAS regulator and from the Radio Spectrum Management group. The literature suggests that such a dual oversight model may be more efficient than a single unified regulator (Laffont and Martimort, 1999), primarily because it reduces the possibility of regulatory capture.

Conclusion

The policy issues to be addressed in relation to C-UAS are not particularly difficult. The right to peaceful use of a drone does not override the right of others to go about their daily lives free from harm, and there are circumstances in which it is clearly efficient to allow self-defence against drones. We put fences around high lookouts and along cliff edges to prevent people falling; we regulate to require isolation of dangerous machinery; we can and should implement policy now that allows relevant parties to implement systems to reduce the potential for drone-related harm by preventing drones from accessing the areas where they will cause most harm. There should never be the opportunity for drones to fly in the approach and departure paths of our major airports, major infrastructure should be protected from errant drones, and people should be able to attend events and gatherings free from the prospect of drones being an agent of harm. There are important questions about the range of measures that can and should be used for C-UAS, but a flexible licensing system may be the most appropriate way to address such questions.

1 This article is derived from material prepared for a PhD thesis in the School of Economics and Finance, Victoria University of Wellington, supervised by Emeritus Professor Lew Evans and Dr Paul Calcott. I would like to thank three anonymous reviewers for helpful comments and suggestions. All errors are my own. Address for correspondence: Andrew.Shelley@xtra.co.nz.

2 *Department of Labour v Sir Edmund Hillary Outdoor Pursuit Centre of New Zealand* [2010] DCR 26.

3 *Hamed v R* SC 125/2010 [2 September 2011] at [1].

References

Airbus (2015) 'Counter-UAV system from Airbus Defence and Space protects large installations and events from illicit intrusion', media release

Australian Transportation Safety Bureau (2013) *Inflight Uncontained Engine Failure Airbus A380-842, VH-OQA, overhead Batam Island, Indonesia, 4 November 2010,* Canberra: Australian Transportation Safety Bureau

Ballard, T., J. Pate, G. Ackerman, D. McCauley and S. Lawson (2001) 'Chronology of Aum Shinrikyo's CBW activities', James Martin Center for Nonproliferation Studies, Middlebury Institute of International Studies, Monterey

Barrett, D. (2015) 'Burglars use drone helicopters to target homes', *Telegraph,* 18 May

BBC (2015) 'Japan radioactive drone: Tokyo police arrest man', *BBC News,* 25 April

Blighter Surveillance Systems (2016) 'Dronebuster™', http://vectorsolutions.us/wp-content/uploads/2017/02/Dronebuster-Data-Sheet.pdf

Blighter Surveillance Systems (2017) 'AUDS Strategic Counter-UAS System', http://www.blighter.com/images/pdfs/brochures/auds-brochure.pdf

Blows, S., R.Q. Ivers, J. Connor, S. Ameratunga, M. Woodward and R. Norton (2005) 'Unlicensed drivers and car crash injury', *Traffic Injury Prevention,* 6, pp.230–4

Boyle, C. (2018) 'Drone delays flights at Auckland Airport', *New Zealand Herald,* 6 April

Brandes, H. (2015) 'Drone carrying drugs, hacksaw blades crashes at Oklahoma prison', *Reuters,* 28 October

Brilbeck, A. (2017) 'Drone causes power outage in Moore', *News9.com*, 29 August

Bunker, R.J. (2015) *Terrorist and Insurgent Unmanned Aerial Vehicles: use, potentials, and military implications,* Carlisle: United States Army War College Press

Cade, D. (2016) 'Watch a trained police eagle take down a drone', *PetaPixel,* 15 September

Cooper, L. (2018) 'Security measures increased ahead of Gold Coast Commonwealth Games', *9 News,* 27 March

Civil Aviation Rules (2015), Part 101: Gyrogliders and Parasails, Unmanned Aircraft (including Balloons), Kites, and Rockets – Operating Rules

Colmar Brunton (2017) *RPAS Use in New Zealand,* research report prepared for the Civil Aviation Authority, Wellington: CAA and Colmar Brunton

Department 13 (2016) 'Department 13 Technology', https://department13.com/technology/

Department 13 (2017) 'Department 13 launches MESMER™ Counter-Drone Solution', http://www.asx.com.au/asxpdf/20170123/pdf/43fgf068n7pkj4.pdf

Drury, I. (2017) 'Drones are caught flying drugs or mobile phones into jail every five days: specialist squad has seized 120 devices since the start of 2016 and convicted 17 people', *Daily Mail Australia,* 21 November

Economist (2015) 'Copping a 'copter: dealing with rogue drones', *Economist,* 2 May

Farivar, C. (2015) 'Drone downs power lines in Hollywood, hundreds affected for a few hours', *ARS Technica,* 28 October

France, S. (ed.) (n.d.) *Adams on Criminal Law: offences and defences* (online looseleaf edn), Thomson Reuters

Gates, D. (2015) 'Engine parts pierced protective case in British Airways 777 fire in Las Vegas', *Seattle Times,* 10 September

Gibbons-Neff, T. (2017) 'ISIS drones are attacking U.S. troops and disrupting airstrikes in Raqqa, officials say', *Washington Post,* 14 June

Glanfield, E. (2015) 'Drone that makes getting drugs and illicit mobile phones in Strangeways "as easy as ordering Chinese" crashes inside prison yard', *Daily Mail,* 10 November

Goodrich, M. (2016) 'Drone catcher: "robotic falcon" can capture, retrieve renegade drones', *Michigan Tech News,* 7 January

Goppert, J.M., A.R. Wagoner, D.K. Schrader, S. Ghose, S., Y. Kim, S. Park, M. Gomez, E.T. Matson and M.J. Hopmeier (2017) 'Realization of an autonomous, air-to-air counter unmanned aerial system (CUAS)', *2017 First International Conference on IEEE Computing,* Taiwan, IEEE Computer Society, pp.235–40

Green, J. (2017) 'Drone crash knocks out power to 1,600 in Mountain View', *Mercury News,* 9 June

Horiuchi, T.K., M. Paras, T. Cervi, B. Oursler, S. Sanz, J. Gaus, D. Woodbury, I. Faruque and H. Xu (2016) 'An autonomous, visually-guided, counter-sUAS aerial vehicle with net countermeasure', paper presented to the AIAA Atmospheric Flight Mechanics Conference, AVIATION Forum (AIAA 2016–3397)

Hughes, C. (2015) 'ISIS planning to use toy helicopters as bombing drones fear security chiefs', *Mirror,* 22 July

Independent Police Conduct Authority (2012) *Police Shooting of Halatau Ki'anamanu Naitoko,* Wellington: IPCA

Kolstad, C.D., T.S. Ulen and G.V. Johnson (1990) 'Ex post liability for harm vs. ex ante safety regulation: substitutes or complements?', *American Economic Review,* 80 (4), pp.888–901

Laffont, J-J. and D. Martimort (1999) 'Separation of regulators against collusive behaviour', *Rand Journal of Economics,* 30, (2), pp.232–62

Lawrence, M. (2018) 'Civil Aviation Authority statistics show small percentage of drone complaints result in disciplinary measures', *New Zealand Herald,* 27 March

Mackay, S. (2015) 'Engineering researchers seek remedies for threat posed by drones to commercial airliners', *Virginia Tech News,* 28 October

Matyszczyk, C. (2015) 'Say welcome to the special anti-drone shoulder "rifle"', *CNET,* 15 October

Ministry of Transport (2017) *Social Cost of Road Crashes and Injuries 2017 Update,* Wellington: Ministry of Transport

Motion, S. (2018) 'Drone delays police divers en route to Omanawa Falls search', Newstalk ZB, 23 April

National Transportation Safety Board (2018) 'Southwest Airlines engine incident: 5/3/2018 investigative update', https://www.ntsb.gov/investigations/Pages/DCA18MA142.aspx

New Zealand Herald (2018a) 'Drone at Auckland Airport diverts flight, causes delays', *New Zealand Herald,* 6 March

New Zealand Herald (2018b) 'Drone nearly hits Air Force helicopter at Whenuapai Air Force Base', New Zealand Herald, 9 April

New Zealand Police (2018) 'Road policing driver offence data – January 2009 to December 2017', http://www.police.govt.nz/about-us/publication/road-policing-driver-offence-data-january-2009-march-2018

OpenWorks (2016) 'Skywall', https://openworksengineering.com/images/skywall/SkyWall%20Brochure.pdf

Polinsky, A.M. and S. Shavell (1992) 'Enforcement costs and the optimal magnitude and probability of fines', *Journal of Law and Economics,* 35 (1), pp.133–48

Rees, C. (2018) 'Raytheon demonstrates microwave and laser counter-drone system', *Unmanned Systems News,* 22 March

Roberts, J.J. (2017) 'France is training eagles to kill drones', *Fortune,* 22 February

Samuel, H. (2016) 'French Air Force turns to eagles to fight terror drone threat', *Telegraph,* 18 November

Serna, J. (2015) 'Drone knocks out power to hundreds of West Hollywood residents', *Los Angeles Times,* 27 October

Shavell, S. (1984) 'Liability for harm versus regulation of safety', *Journal of Legal Studies,* 13 (2), pp.357–74

Shelley, A. (2016) 'Proposals to address privacy violations and surveillance by unmanned aerial systems', *Waikato Law Review,* 24, pp.142–70

Stuff (2015) 'Drone flies into Whangarei power lines, causes outage', *Stuff,* 17 September

Stuff (2017) 'Drone use impacts firefighting efforts on Christchurch's Port Hills', *Stuff,* 22 February

United Nations (1975) 'Convention for the suppression of unlawful acts against the safety of civil aviation (with Final Act of the International Conference on Air Law held under the auspices of the International Civil Aviation Organization at Montreal in September 1971). Concluded at Montreal on 23 September 1971', United Nations – Treaty Series, 974, pp.177–248

Waitt, T. (2016) 'FAA US airport trials Anti-UAV Defence System', *American Security Today,* 31 May

Wasserman, S. (2015) 'Personal drones getting sucked into jet engines could be disastrous', *Engineering.com,* 3 November

Watling, C.N. and N.L. Leal (2012) 'Exploring perceived legitimacy of traffic law enforcement', paper presented to the ACRS 2012 national conference, Sydney, 9–10 August

Watson, B. (2017) 'The drones of ISIS', *Defense One,* 12 January

Williams, P. (2018) 'SAS to use "drone destroyer" to stop terrorists at Royal Wedding', *Daily Star Sunday,* 11 March

Wong, K. (2018) 'Singapore Airshow 2018: ST Kinetics unveils speciality 40 mm ammunition', *Jane's 360,* 7 February

Zhang, M. (2016) 'Eagles are now being trained to take down drones', *PetaPixel,* 1 February