ASMS
Aviation Safety Management Systems

Enabling Counter-UAS and UAS-Detection Systems in New Zealand

19 November 2018

Andrew Shelley
Aviation Safety Management Systems Ltd

Contents

1 Introduction

This report proposes legislation to address the threats posed by unmanned aerial systems (UAS), commonly known as “drones”.

At the outset it is helpful to clarify nomenclature. An unmanned aircraft is any aircraft that does not have a pilot on board. An unmanned aerial system is the combination of the unmanned aircraft, any ground control station, and the command and control (C2) links between the ground control station and the aircraft. Another term frequently used is “Remotely Piloted Aerial Systems” or “RPAS” – these are UAS that are actively piloted by a remote pilot and are a subset of UAS. It is possible to have a UAS that is entirely autonomous and not remotely piloted. Finally, the term “drone” is popularly used as a synonym for UAS or RPAS.

The report is structured as follows:

- Section 2 summarises the threats posed by UAS;
- Section 3 summarises a range of available counter-UAS technologies;
- Section 4 describes the prohibitions which prevent the use of UAS detection systems and counter-UAS systems in New Zealand;
- Section 5 discusses the need for a positive right to take defensive action against UAS;
- Section 6 describes relevant aspects of the Civil Aviation Authority rule-making process;
- Section 7 summarises the proposed legislative changes.

A draft Counter Drone Bill is provided as an appendix.

2 Threats

The potential threats from UAS are detailed elsewhere, but include:[1]

- Danger to aircraft, including stopping or destroying the engines of jet aircraft;
- Potential damage to the cockpit windows of jet aircraft;
- Debris on airport runways causing damage to jet aircraft, including crashes while jet aircraft are travelling at high speed after landing;
- Contraband, weapons, and other prohibited items being delivered to airport operational areas;
- Contraband, weapons, and other prohibited items being delivered to prisons;
- Harm to crowds at mass events including sporting fixtures;
- Airborne delivery of hazardous substances (radioactive material, 1080, poisons, nerve agents) to political targets; and
- Surveillance and harassment of law enforcement operations.

In June 2018, in a statement before the Senate Homeland Security and Governmental Affairs Committee, the FBI Deputy Assistant Director Scott Brunner said:[2]

> *UAS technology renders traditional, two-dimensional security measures (such as perimeter fences) ineffective, enabling criminals, spies and terrorists to gain unprecedented, inexpensive, and often unobtrusive degrees of access to previously secure facilities.*

At a recent more briefing to the Senate Homeland Security and Governmental Affairs Committee, FBI Director Christopher Wray stated:[3]

> *The FBI assesses that, given their retail availability, lack of verified identification requirement to procure, general ease of use, and prior use overseas, UAS will be used to facilitate an attack in the United States against a vulnerable target, such as a mass gathering. This risk has only increased in light of the publicity associated with the apparent attempted assassination of Venezuelan President Maduro using explosives-laden UAS.*

While the immediate risk to New Zealand may be lower than the risk to the United States, the threat still exists and reasonable action can be taken to counter that threat.

---

1 For more details on a number of these threats see: Andrew Shelley "A Framework for Counter-Unmanned Aircraft System Regulation in New Zealand", *Policy Quarterly*, Vol 14 No 3, August 2018.

2 Scott Brunner, "Countering Malicious Drones", Statement Before the Senate Homeland Security and Governmental Affairs Committee, Washington, D.C., 6 June 2018. https://www.fbi.gov/news/testimony/countering-malicious-drones

3 Christopher Wray, "Threats to the Homeland", Statement Before the Senate Homeland Security and Governmental Affairs Committee, Washington, D.C., 10 October 2018. https://www.fbi.gov/news/testimony/threats-to-the-homeland-101018

3 UAS Detection and Counter-UAS Technologies

The threat of UAS can be mitigated (although not completely eliminated) by the use of appropriate technologies. These technologies can be divided into three broad categories:

1. UAS detection systems that provide information on the location of the UAS, and potentially its speed and direction, but no information on the location or identity of the operator. Radar-based systems belong to this category, and are currently the only systems that are fully compliant with New Zealand legislation.

2. UAS detection systems that provide information on the location of the UAS, as well as the location and/or identity of the operator.

3. Counter-UAS systems that both detect the UAS and take action to stop or "counter" the UAS.

Counter-UAS technologies include:

- Radio and GPS jamming;
- GPS spoofing;
- Protocol manipulation;
- Firearms;
- Lasers;
- Counter-UAS "streamer" grenade;
- Trained eagles; and
- Net-based systems.

Jamming is the broadcast of high powered radio signals intended to block or "jam" another radio broadcast. Jamming can therefore be used to overwhelm the signal used to control a UAS. The behaviour of the UAS then depends on what it has been programmed to respond to a loss of the control signal: some UAS will return to where they took off from (known as "return to home"), some will hover in place, and others may continue with the last known input. A number of commercial jammers are available for UAS, such as the Battelle Systems "Drone Defender" shoulder-mounted radio "gun",[4] the hand-held "Dronebuster" by Radio Hill Technologies,[5], and the DroneShield "DroneGun" deployed by Australia at the 2018 Commonwealth Games.[6] Another system with considerable potential is the PDA Electronics "Repulse 24", which can be installed in the nose of an aircraft and "repel" a UAS at a range of up to 1km.[7] None of these systems are legal under existing New Zealand legislation.

---

4 Chris Matyszczyk, "Say welcome to the special anti-drone shoulder 'rifle'", *CNET*, 15 October 2015. https://www.cnet.com/news/say-welcome-to-the-special-anti-drone-shoulder-rifle/.

5 *Dronebuster*^{TM}, Blighter Surveillance Systems, 2016. http://vectorsolutions.us/wp-content/uploads/2017/02/Dronebuster-Data-Sheet.pdf.

6 Luke Cooper, "Security measures increased ahead of Gold Coast Commonwealth Games," *9 News*, 27 March 2018. https://www.9news.com.au/national/2018/03/27/15/58/commonwealth-games-gold-coast-drone-gun-security-measures?ocid=Social-9NewsGC

7 Repulse website, 19 November 2018. https://www.repulsedrones.com/products.php

Another technique for disrupting UAS that is similar to jamming is known as "GPS spoofing". GPS spoofing relies on transmitting a GPS signal with a false position that overwhelms the weak GPS signals received from satellites. A report in 2001 warned of the vulnerabilities of GPS to signal loss and disruption, including malicious disruption,[8] yet UAS technology remains vulnerable to attack. GPS spoofing was used by Iran to commandeer and land a United States RQ-170 Sentinel surveillance aircraft,[9] and the technique has been demonstrated as being able to be used to commandeer and potentially crash a small unmanned aircraft.[10]

Drug Traffickers are reportedly using GPS jamming and spoofing technologies to disrupt unmanned aircraft surveillance of the US-Mexico border,[11] surveillance which is conducted using military-grade unmanned aircraft. Technologies exist to protect against GPS attacks, although these are not yet practical for small UAS.

The Blighter Surveillance Systems "Anti UAV Defence System" (AUDS) is a military-grade counter-UAS system that utilises radar to detect UAS at a range of up to 10km for larger UAS, and smaller UAS at a range of up to 3.6km.[12] Another large-scale detection and jamming system has been developed by Airbus Defense & Space.[13] Airways Corporation of New Zealand has deployed the Gamekeeper 16U UAS detection radar at Auckland International Airport Ltd: this system does not include any UAS counter-measures.

US/Australian firm Department 13 has developed a radio-based system called "Mesmer" that does not utilise jamming.[14] This system relies on what Department 13 describes as "protocol manipulation",[15] which involves intercepting the radio signals used to control the UAS, identifying the protocol being used, then transmitting commands to completely take over control of the UAS. The UAS can then be instructed to leave the area or to land in a safe zone. Representatives of Department 13 demonstrated this system to New Zealand Defence Force and other New Zealand government personnel in 2017.

Some UAS 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 UAS

---

8 John A. Volpe National Transportation Systems Center (2001) *Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System*, Final Report, U. S. Department of Transportation, 29 August 2001. Retrieved from http://www.navcen.uscg.gov/pdf/vulnerability_assess_2001.pdf.

9 Scott Peterson, "Exclusive: Iran hijacked US drone, says Iranian engineer", Christian Science Monitor, 15 December 2011. Retrieved from http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video.

10 Lisa Vaas, "Drone hijacked by hackers from Texas college with $1,000 spoofer", naked security, 2 July 2012. Retrieved from https://nakedsecurity.sophos.com/2012/07/02/drone-hackedwith-1000-spoofer/.

11 Patrick Tucker, "DHS: Drug Traffickers Are Spoofing Border Drones", Defense One, 17 December 2015. Retrieved from http://www.defenseone.com/technology/2015/12/DHS-Drug-Traffickers-Spoofing-Border-Drones/124613/.

12 *AUDS Fully Integrated Counter-UAS System*, Blighter Surveillance Systems, 2017. http://www.blighter.com/images/pdfs/brochures/auds-brochure.pdf.

13 "Counter-UAV System from Airbus Defence and Space protects large installations and events from illicit intrusion", Press Release, Airbus Defence and Space, 16 September 2015. https://www.airbus.com/newsroom/press-releases/en/2015/09/counter-uav-system-from-airbus-defence-and-space-protects-large-installations-and-events-from-illicit-intrusion.html

14 *MESMER™ Counter Drone Solution*, Department 13, 2017. http://www.asx.com.au/asxpdf/20170123/pdf/43fgf068n7pkj4.pdf.

15 *Department 13 Technology*, Department 13, 2016. https://department13.com/technology/.

out of the sky.[16] Another option is the C-UAS "grenade" which releases streamers that will foul a UAS' propellers causing it to crash.[17]

A number of alternative methods of UAS interdiction have been developed which neither knock the UAS out of the sky nor utilise jamming. Eagles have been trained to hunt small UAS in both the Netherlands[18] and France.[19] Nets may also be used to entangle a UAS: nets may be shoulder-launched,[20] draped from a UAS,[21] or fired from a UAS.[22,23,24]

16 Mike Rees, " Raytheon Demonstrates Microwave and Laser Counter-Drone System," *Unmanned Systems News*, 22 March 2018. http://www.unmannedsystemstechnology.com/2018/03/microwave-laser-counter-drone-system-demonstrated-us-army-exercise/.

17 Kelvin Wong, "Singapore Airshow 2018: ST Kinetics unveils speciality 40 mm ammunition," *Jane's 360*, 7 February 2018. http://www.janes.com/article/77676/singapore-airshow-2018-st-kinetics-unveils-speciality-40-mm-ammunition.

18 DL Cade, "Watch a Trained Police Eagle Take Down a Drone," *PetaPixel*, 15 September 2016. https://petapixel.com/2016/09/15/dutch-police-demonstrate-trained-eagle-takes-drone/.

19 Henry Samuel, "French Air Force turns to eagles to fight terror drone threat," *The Telegraph*, 18 November 2016. http://www.telegraph.co.uk/news/2016/11/18/french-air-force-turns-to-eagles-to-fight-terror-drone-threat/.

20 *Skywall*, OpenWorks Engineering. Retrieved June 5, 2017, from https://openworksengineering.com/images/skywall/SkyWall%20Brochure.pdf.

21 "Copping a `copter: Dealing with rogue drones," *The Economist*, 2 May 2015. http://www.economist.com/news science-and-technology/21650071-hands-criminals-small-drones-could-be-menace-now-time.

22 Marcia Goodrich, "Drone Catcher: 'Robotic Falcon' can Capture, Retrieve Renegade Drones," *Michigan Tech News*, 7 January 2016. http://www.mtu.edu/news/stories/2016/january/drone- catcher-robotic-falcon-can-capture- retrieverenegade-drones.html.

23 Goppert, J. M., Wagoner, A. R., Schrader, D. K., Ghose, S., Kim, Y., Park, S, …, Hopmeier, M. J., "Realization of an Autonomous, Air-to-Air Counter Unmanned Aerial System (CUAS)," IEEE Xplore Digital Library, 15 May 2017. https://doi.org/10.1109/IRC.2017.10

24 Horiuchi, T. K., Paras, M., Cervi, T., Oursler, B., Sanz, S., Gaus, J., …, Xu, H. "An Autonomous, Visually-Guided, Counter-sUAS Aerial Vehicle with Net Countermeasure," *AIAA Atmospheric Flight Mechanics Conference*, American Institute of Aeronautics and Astronautics, 10 June 2016. https://doi.org/10.2514/6.2016-3397.

4 Prohibitions against Counter-UAS Systems in New Zealand

4.1 Aviation Crimes Act 1972

UAS are defined as "aircraft" and as such are subject to the general prohibitions in the Aviation Crimes Act 1972 against taking actions that would damage an aircraft or render it incapable of flight. The relevant provisions of s5 of the Aviation Crimes Act 1972 state:

> ***S5 Other crimes relating to aircraft***
>
> *Everyone commits a crime, and is liable on conviction to imprisonment for a term not exceeding 14 years, who, whether in or outside New Zealand,—*
>
> *(b) destroys an aircraft in service; or*
>
> *(c) causes damage to an aircraft in service which renders the aircraft incapable of flight or which is likely to endanger the safety of the aircraft in flight;*

Any action taken which renders a UAS incapable of flight, damages it, or destroys it, is prima facie contravening this section.

The wording of this clause reflects Montreal Convention (MC) but omits the MC's qualification that acts are performed "unlawfully". The inclusion of this qualification would then allow counter-UAS actions to be taken, so long as those actions were lawful.

4.2 Crimes Act 1961

Some counter-UAS systems rely on a technique called "protocol manipulation" which essentially hacks into the computer running the UAS to issue it with new instructions to either land in place, land in a safe area, or return to its origin. Taking such action would appear to contravene s250 of the Crimes Act 1961, which has a prohibition against interfering with or impairing any data or software in a computer system, and s252 of the Crimes Act 1961, which has a prohibition against accessing a computer system without authorisation. Furthermore, any person that makes or sells such a system would contravene s251, which prohibits the "making, selling, or distributing software that would enable another person to access a computer system without authorisation".

Importantly, the prohibitions in ss250 and 252 relate to a person who does so "without authorisation". Authorisation is defined in s248 as including "an authorisation conferred on a person by or under an enactment or a rule of law, or by an order of a court or judicial process". This suggests that:

- there is no need to alter the anti-hacking provisions of the Crimes Act 1961; and
- legislation is required to define when a person is authorised to utilise counter-UAS technology.

4.3 Radiocommunications Act 1989

The radio signals used to control a UAS are detected by some systems and used to identify the UAS, determine the location of the UAS, and determine the location of the transmitter that is controlling the UAS. These systems enable defensive measures to be taken, from diverting aircraft away from the UAS to enabling law enforcement officials to be dispatched to the location of the transmitter.

However, such systems appear to contravene s133A(1)(a) of the Radiocommunications Act 1989:

> ***133A Offence to disclose contents of radiocommunications***
>
> *(1) Every person commits an offence against this Act who receives a radiocommunication and who, knowing that the radiocommunication was not intended for that person,—*

> *(a) makes use of the radiocommunication or any information derived from that radiocommunication; or …*

The radiocommunication is clearly not intended for any person, but rather for the UAS that the signal is controlling. Therefore making use of that radiocommunication, or any information derived from it, is a prima facie breach of this section.

The same section does include some exceptions, most notably:

> *(b) by a constable, a Customs officer, or any other class of law enforcement official listed in regulations made under this Act for the purpose of avoiding prejudice to the maintenance of the law, including the detection, prevention, investigation, prosecution, and punishment of offences; or …*
>
> *(c) by an employee of an intelligence and security agency for the purpose of performing the function under section 10 of the Intelligence and Security Act 2017; or*
>
> *(d) by a member of the New Zealand Defence Force, in connection with any of the purposes specified in section 5(a) to (d) of the Defence Act 1990…*

There are also a number of other specific exemptions referenced in subsection (e):

> *(e) by a person acting under, and in accordance with, any authority conferred on him or her by or under—*
>
> *(i) Part 1 of the Telecommunications (Residual Provisions) Act 1987; or*
>
> *(ii) Part 4 of the Intelligence and Security Act 2017; or*
>
> *(iia) [Repealed]*
>
> *(iii) the Misuse of Drugs Amendment Act 1978; or*
>
> *(iv) the International Terrorism (Emergency Powers) Act 1987.*

None of the provisions provide a general power enabling the private sector to intercept radiocommunications used to control UAS and then utilise those signals or the information contained in the signals. Thus all of the following situations would contravene this section:

- a private security firm hired to deploy UAS-detection systems at a sports arena;
- Airways Corporation deploying these systems at airports;[25]
- Transpower deploying these systems at its major substations.

The private sector use of counter-UAS systems and UAS-detection systems would be facilitated by an additional exception under s133A(e). If there was specific enabling legislation for counter UAS systems then the additional exception in s133A(e) would refer to an authority conferred under that enabling legislation.

[25] Note that these systems are different from the drone detection radar currently being trialled at Auckland International Airport. That system is a radar system and does not rely on detection of the drone radio control signals.

4.4 Prohibition against Jamming

The Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 prohibits the "use of radio jammer equipment other than by a permitted person."

There is no general process for becoming a permitted person.

The only entity with formal permission is the Department of Corrections, with qualified permission granted by way of s189B of the Corrections Act 2004. This permission includes the qualification that there must not be "harmful interference outside prison boundaries".

The NZ Police do not have specific permission to undertake jamming, but it is understood that they have utilised the provisions of s48 of the Crimes Act 1961 to undertake jamming in particular circumstances.

The effects of jamming are potentially widespread and can have an adverse effect on a wide range of unintended targets. UAS typically use General Use Radio Spectrum, so jamming the control frequencies used by a UAS can interfere with the proper operation of other devices legitimately utilising the spectrum. It is therefore recommended that the anti-jamming provisions remain, with the power for parliament or the Secretary[26] to declare a person a permitted person for the purpose of the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011.

[26] The Secretary is defined in the Radiocommunications Act 1989 as "the chief executive of the department of State that… [is] responsible for the administration of" that Act. For the time being this is the Chief Executive of the Ministry of Business, Innovation, and Employment.

5 The Need for a Positive Right to Take Defensive Action

5.1 Self-Defence and Defence of Another

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 1961 and specific defences recognised in sections 39-43, and section 48, amongst others. Section 48 of the Crimes Act 1961 codifies the right to use reasonable force:

> ***S48 Self-defence and defence of another***
>
> *Every one is justified in using, in the defence of himself or herself or another, such force as, in the circumstances as he or she believes them to be, it is reasonable to use.*

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.[27] Thus these defences might be generally provide protection for any person taking counter-UAS action when that person believed that there was an imminent threat to people – such as when a UAS 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. It is understood that the NZ Police have indeed relied on s48 to take some actions against UAS and to utilise jamming in some instances, although the legality of these actions is yet to be tested in the courts.

5.2 Grey areas

However, there are circumstances in which the legal basis for taking action is less clear. Consider, for example, counter-UAS action taken against a UAS flying in the approach path to an airport, but there is no airliner approaching. In the absence of imminent harm to people the counter-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,[28] but not necessarily that the risk is seen as significant or likely to eventuate.[29] 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 counter-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):[30]

> *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.*

---

27 *Police shooting of Halatau Ki'anamanu Naitoko*, Independent Police Conduct Authority. April 2012.

28 France, S. (Ed.) (2018) *Adams on Criminal Law – Offences and Defences*, section CA20.27 (online looseleaf ed., Thomson Reuters). Retrieved 3 June 2018.

29 Above n. 28, section CA20.26.

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

5.3 The Preventing Emerging Threats Act 2018 (United States)

The United States has passed two pieces of legislation granting relevant authorities the positive right to take action against UAS.

The National Defense Authorization Act for Fiscal Year 2018,[31] allows the United States' military to action to be taken against UAS that potentially threaten assets or facilities related to national security. Importantly, these provisions relate to assets or facilities located in the United States or its territories, and are therefore focussed on domestic security rather than security during war or war-like situations.

The second piece of legislation is the Preventing Emerging Threats Act 2018.[32] This Act grants the Department of Homeland Security, Department of Justice, and the United States Coast Guard the right to take action against UAS in a wide range of circumstances.

The actions allowed by both pieces of legislation include warning the operator, seizing control of the UAS, destroying the UAS, and the like. The specific provisions are:

> *(A) During the operation of the unmanned aircraft system, detect, identify, monitor, and track the unmanned aircraft system or unmanned aircraft, without prior consent, including by means of intercept or other access of a wire communication, an oral communication, or an electronic communication used to control the unmanned aircraft system or unmanned aircraft.*
>
> *(B) Warn the operator of the unmanned aircraft system or unmanned aircraft, including by passive or active, and direct or indirect physical, electronic, radio, and electromagnetic means.*
>
> *(C) Disrupt control of the unmanned aircraft system or unmanned aircraft, without prior consent, including by disabling the unmanned aircraft system or unmanned aircraft by intercepting, interfering, or causing interference with wire, oral, electronic, or radio communications used to control the unmanned aircraft system or unmanned aircraft.*
>
> *(D) Seize or exercise control of the unmanned aircraft system or unmanned aircraft.*
>
> *(E) Seize or otherwise confiscate the unmanned aircraft system or unmanned aircraft.*
>
> *(F) Use reasonable force, if necessary, to disable, damage, or destroy the unmanned aircraft system or unmanned aircraft.*

Both Acts also include privacy protections. These are unlikely to be required in New Zealand given our existing privacy legislation and the Privacy Bill (2018) currently before Parliament.

---

31 National Defense Authorization Act for Fiscal Year 2018, §1692. H.R.2810 – 115th Congress. https://www.congress.gov/bill/115th-congress/house-bill/2810.

32 Preventing Emerging Threats Act 2018. H.R.2810 – 115th Congress. https://www.congress.gov/115/bills/hr302/BILLS-115hr302enr.pdf.

6 Civil Aviation Regulation

The operation of counter-UAS systems will require regulation. The most appropriate regulator is the Civil Aviation Authority, which already has regulatory oversight of UAS.

6.1 The Civil Aviation Act Review

The Civil Aviation Act 1990 has been undergoing a process of review by the Ministry of Transport for a period of several years:[33]

- In 2014 the Ministry of Transport issued a consultation document seeking public feedback on the Civil Aviation Act 1990 and Airport Authorities Act 1966.
- Feedback received informed advice provided to Cabinet in 2016 on changes to improve both Acts.

No changes have yet been made as a result of the above process. However, it is understood that this remains a "live" project. Therefore, any changes made to the Civil Aviation Act 1990 which would introduce a positive right to take defensive action against UAS could potentially be "lost" with the introduction of a new Civil Aviation Bill intended to replace the existing Act. It is therefore recommended that the legislative changes to allow for UAS detection and counter-UAS systems should be embodied in a stand-alone Act. This Act can be incorporated into the new Civil Aviation Act if and when it is eventually introduced.

6.2 Civil Aviation Rules

The Civil Aviation Authority is empowered to make rules under Part 3 of the Civil Aviation Act 1990.

The major areas covered by Civil Aviation Rules are:[34]

- Personnel licencing to ensure that people performing particular functions in the civil aviation system have an appropriate level of skill and expertise (for example, pilots and engineers).
- Maintenance and airworthiness to ensure that aircraft are safe to fly.
- Conduct rules, including the General Operating and Flight Rules (Part 91), specific rules for UAS (Part 101), microlights (Part 103), gliders (Part 104), parachuting (Part 105), and hang gliders (Part 106).
- Operator certification rules, which specify the requirements that an operator of aircraft must meet in order to be authorised to conduct operations for hire and reward. Operator certification rules include carriage of passengers and goods for hire and reward (Parts 119/121,125,135), adventure aviation (Part 115), agricultural aviation (Part 137).
- Organisation certification rules, which specify the requirements that other organisations in the civil aviation system must meet to perform a particular function. Organisation certification rules include aviation security (Part 140), training organisations (Part 141), maintenance organisations (Part 145), and others.
- Provision of airways services (Parts 171, 172, 173, 174, 175).

[33] Ministry of Transport website, "Civil Aviation Act 1990 and Airport Authorities Act 1966 review". Retrieved 31 October 2018 from https://www.transport.govt.nz/air/caa-act1990-aa-act1966-review-consultation/.

[34] For a full list of Civil Aviation Rules see https://www.caa.govt.nz/rules/civil-aviation-rules/.

6.3 Part 100 Safety Management Systems

A recent innovation for operator certification and organisation certification has been to require most entities to comply with Civil Aviation Rule Part 100 Safety Management Systems, which requires a documented system for safety management. This rule and the attendant certification requirements are, to a degree, flexible, but still require systems with a relatively high level of complexity.

One of the few organisations not required to comply with Part 100 is the Aviation Security Service, certified under Rule Part 140.

6.4 Part 102 Unmanned Aircraft Operator Certification

Civil Aviation Rule Part 102 Unmanned Aircraft Operator Certification provides the basis for UAS operators to be certified to conduct operations outside the limitations specified in the Part 101 rules. As with other certification rules, the operator is required to maintain a manual of procedures ("exposition") which details how they conduct their operations.

The privilege to operate outside specific constraints of the Part 101 rules is granted if the Civil Aviation Authority is satisfied that the operator's procedures will sufficiently manage the risk of operating outside those constraints.

Part 102 operators are not required to comply with Rule Part 100 because of the elements of safety management built into Rule Part 102. For example, the Rule Part 102 requires a hazard register, and risk assessment and mitigation procedures are required.

6.5 Proposed Approach for Counter-UAS Systems

Aviation Safety Management Systems Ltd has prepared expositions for approximately 30 UAS operators, has prepared the necessary exposition amendments for three operators to gain Part 100 certification, and is working with a further three operators to gain Part 100 certification. In our experience the approach adopted by Rule Part 102 is more flexible than that in Rule Part 100, better accommodating the needs and constraints of small organisations, while still allowing the Civil Aviation Authority the scope to require appropriate risk assessment be conducted. On the basis of our experience, it is recommended that:

- Part 100 compliance is not required for operators of counter-UAS systems; but
- A certification rule for organisations utilising counter-UAS systems adopts the risk-based approach currently incorporated in Civil Aviation Rule Part 102.

7 Summary of Proposed Legislative Changes

7.1 Enabling Legislation: the Counter Drone Act

Enact new legislation that provides:

- a positive right to undertake UAS detection activity;
- the right to undertake counter-UAS activity subject to certification by the Civil Aviation Authority.

7.2 Aviation Crimes Act 1972

In section (5), replace the words “whether in or outside New Zealand,—” with “whether in or outside New Zealand, unlawfully —”

7.3 Crimes Act 1961

No changes required.

Positive authorisation for accessing computer systems is required, and this is provided by the enabling legislation.

7.4 Radiocommunications Act 1989

In section 133A(e), replace “Part 1 of the Telecommunications (Residual Provisions) Act 1987” with “Part 1 of the Counter Drone Act”.

Note: The Telecommunications (Residual Provisions) Act 1987 was repealed, on 1 October 2012, by section 341 of the Search and Surveillance Act 2012. There is therefore no longer any need to retain the reference to it in s133A(e)(i) of the Radiocommunications Act 1989.

Appendix: Counter Drone Bill

This appendix contains the text of proposed legislation that containing the minimum provisions required to enable the use of UAS detection systems and counter-UAS systems in New Zealand

Counter Drone Bill

1 Title

This Act is the Counter Drone Act.

2 Interpretation

In this Act, unless the context otherwise requires, —

aircraft has the same meaning as in the Civil Aviation Act 1990

aviation document has the same meaning as in the Civil Aviation Act 1990

Civil Aviation Authority means the Civil Aviation Authority established under Part 6A of the Civil Aviation Act 1990

counter drone system means a system that includes both a drone detection system and the ability to take action to alter or control the flight path of the drone or to stop the drone

drone means any unmanned aerial system including remotely piloted aircraft systems, including both the aircraft, control systems, and command and control radiocommunication links

drone detection system means any system that which uses a drone's radio control link, noise emitted by the drone , radar, or optical methods to detect the presence of a drone without taking any action to alter or control the flight path of the drone or to stop the drone

rule means a rule made under Part 3 of the Civil Aviation Act 1990

3 Application of Act

This Act applies to all acts undertaken in New Zealand.

Part 1

Right to Undertake Counter-Drone Activities

4 Right to Operate Drone Detection Systems

4.1 Every person has the right to operate a drone detection system.

5 Aviation Document Required to Operate Counter-Drone Systems

5.1 No person may operate a counter-drone system except in accordance with the terms of an aviation document issued by the Civil Aviation Authority.

5.2 Rules for the granting of the aviation document required by section 5.1 of this Act shall be made by the Civil Aviation Authority as if the requirement in section 5.1 was a requirement in section 7(1) of the Civil Aviation Act 1990.

5.3 If any rule is made for an organisation to hold an aviation document for the purpose of operating a counter-drone system, that rule should not require compliance with Civil Aviation Rule Part 100 Safety Management Systems, but must include measures for assessing the safety and risk of the counter-drone systems to be operated.

6 Authorisation to Make Use of Radiocommunication Signal

Every person operating a drone detection system is authorised to make use of any radiocommunication signal associated with the drone for any purpose associated with:

(a) identifying the drone or operator of the drone; or

(b) establishing the location of the drone or operator of the drone.

7 Authorisation to Access Computer Systems

Any person operating a counter-drone system under the authority of an aviation document granted under section 5 of this Act is authorised to access the computer system of the drone to the extent necessary for the operation of the counter-drone system and for the proper maintenance of the law.

Part 2

Amendments to other enactments

8 Amendment to the Aviation Crimes Act 1972

In section (5) of the Aviation Crimes Act 1972, replace the words “whether in or outside New Zealand,—” with “whether in or outside New Zealand, unlawfully —”

9 Amendment to the Radiocommunications Act 1989

In section 133A(e) of the Radiocommunications Act 1989, replace “Part 1 of the Telecommunications (Residual Provisions) Act 1987” with “Part 1 of the Counter Drone Act”.

About the Author

This report draws on research conducted by Andrew Shelley for a PhD thesis in the School of Economics and Finance, Victoria University of Wellington.

Andrew is also Chief Executive of Aviation Safety Management Systems Ltd, a company that provides training to UAS pilots, assists UAS operators with obtaining certification under Civil Aviation Rule Part 102, and assists manned aircraft operators with certification and with the implementation of Safety Management Systems.

Andrew may be contacted at:
email: andrew@asms.co.nz
mobile: 021 549 045