National Security Journal

http://nationalsecurityjournal.nz

Published by:
Centre for Defence
and Security Studies,
Massey University

ISSN: 2703-1926 (print) *ISSN: 2703-1934 (online)*

A Counter-Drone Strategy for New Zealand

Author: Shelley, Andrew. V.

To cite this article: Shelley, A. V. (2022). A Counter-Drone Strategy for New Zealand. *National Security Journal*. Published 18 May 2022. doi:10.36878/nsj20220518.02

To link to this article: https://doi.org/10.36878/nsj20220518.02

View CrossRef data: https://search.crossref.org/?q=10.36878%2Fnsj20220518.02

Journal Article published 18 May 2022 in National Security Journal.

A COUNTER-DRONE STRATEGY FOR NEW ZEALAND

Andrew V. Shelley[1]

A recent article in this journal provides a quantitative assessment of the threats from drones in New Zealand.[1] The present article builds upon that risk assessment to develop a counter-drone strategy for New Zealand. Selected literature is reviewed to identify the key elements of a security strategy. The approaches adopted to countering drones by New Zealand and its Five Eyes partners are then reviewed. Australia and Canada have adopted limited measures that allow radio jamming of drones by Federal police. The United Kingdom has published an explicit strategy that will allow for organisations other than law enforcement to act against drones. The United States does not have a published strategy but has enacted legislation allowing counter-drone action. The Civil Aviation Bill recently introduced in New Zealand proposes counter-drone powers for law enforcement. The strategy developed in this article is compared with the provisions in that Bill and recommendations are provided for improving that legislation.

Keywords: Civil Aviation Bill, counter-drone, drones, Unmanned Aerial Systems, risk analysis, security strategy

INTRODUCTION

Drones, also known more formally as "unmanned aircraft" or unmanned aerial systems (UAS), are aircraft intended to operate with no pilot on board.[2] A drone may either be piloted remotely, in which case the broader system of which the drone is a part includes a command and control (C2) link,[3] or the drone may follow a pre-programmed path and be fully autonomous.[4] Drones have a wide range of potential beneficial applications including photography, movie making, survey, asset inspection, package and medicine

1 Dr Andrew Shelley is Managing Consultant of Andrew Shelley Economic Consulting, and Chief Executive of the drone training school run by Aviation Safety Management Systems Ltd. His research focusses on the regulation of drones and counter-drone systems. This article is derived from a research report prepared in partial fulfilment of the requirements for the degree of Master of International Security through the Centre of Defence and Security Studies, Massey University, supervised by Terry Johanson. Corresponding author: Andrew.Shelley@xtra.co.nz.

delivery, and agrichemical application. However, as demonstrated by Shelley in his recent review of drone-related threats to New Zealand, drones can also be used in a range of criminal and malicious activities.[5] The threat posed by drones is not just theoretical: globally a range of incidents have occurred which demonstrate most hypothesised threats can be readily implemented. A key problem with countering the threat from drones is that it is extremely difficult to identify the operator of the aircraft. The standard regulatory prescription by regulatory authorities to require registration of drones and licensing of operators will be ineffective if the operator does not comply with legal requirements.[6] In addition, some threats from drones require an immediate response to stop the drone, not just an attribution of liability after the fact. Legal and regulatory systems struggle to keep pace with emerging technologies,[7] including drone technology,[8] and as demonstrated in this study often do not allow appropriate counter-drone action to be taken.

Counter-drone provisions are included in a comprehensive Civil Aviation Bill (CA Bill) recently introduced to the New Zealand Parliament.[9] While several documents were proactively released when the CA Bill was introduced to parliament,[10] none of those documents demonstrate that the CA Bill is part of a comprehensive strategy. Changes to legal and regulatory systems should not be made on a piecemeal basis but should be a deliberately made as part of an overall counter-drone strategy linked to national security objectives. This study develops a counter-drone strategy for New Zealand and develops recommendations for improvement of the provisions proposed in the CA Bill.

METHODOLOGY

This article describes the nature of the threat potentially posed by drones, and summarises the different means of countering drones. Identification of threats could be informed by both interviewing appropriate people from within New Zealand's security agencies and by textual analysis informed by relevant literature. Due to the difficulty of interviewing appropriate people, this article relies on a textual analysis that has been published in a recent article in this journal.[11] A summary of the key findings of that article are presented here.

A central question in developing any strategy is identifying the critical components of a strategy. Selected literature on corporate and security strategy is reviewed to identify the core elements that should be included in a security strategy. That review identifies that a strategy should start with a statement of strategic objectives and then identify potential threats to the achievement of those objectives. A risk assessment should then be conducted to establish the relative significance of the threats.[12] Policy should then be established to specify what actions will be taken to address the identified threats.[13]

Development of strategy potentially benefits from consideration of the approaches adopted by others. This article therefore reviews the approaches adopted to countering

drones by New Zealand and its Five Eyes (FVEY) partners. Australia and Canada have a piecemeal approach that enables a particular aspect of counter-drone action but, based on this review, neither appears to have a coherent strategy. The United Kingdom has a formal counter-drone strategy document[14] and is proceeding to implement the steps in that strategy. The United States has what could be described as an emergent strategy[15] that is enabling a coherent counter-drone response. The presence of a counter-drone strategy in both the United Kingdom and the United States enables these states to use counter-drone operations to protect critical national infrastructure, to an extent that is not generally possible in Australia, Canada, or New Zealand. New Zealand has recently introduced legislation that will provide some counter-drone powers to police and appointed personnel, but some important gaps will still remain.

A counter-drone strategy for New Zealand is then proposed, which has been developed utilising the critical components identified. Strategic objectives are identified based on New Zealand's *National Security System Handbook*.[16] The analysis of strategy identifies that a key aspect of establishing a strategy is identification of strategic threats, establishing the risk of those threats, and identifying appropriate controls for those risks. Identification of threats and risk analysis is informed by the recent article.[17] The path of this research then explores the question of how the identified threats in New Zealand could be effectively addressed or mitigated. The proposed mitigations are compared with the measures proposed in the recently introduced CA Bill. Recommendations for improvement of that legislation are developed. Guidance on implementation of the counter-drone strategy is provided, including recommendations for the Civil Aviation Authority and Radio Spectrum Management to be directed to develop and promulgate a process for relevant people and organisations to receive the appropriate approvals.

BACKGROUND

The Threat Posed by Drones

The key security-related threats from drones in New Zealand are described in a recent article by Shelley published in this journal.[18] The assessment in that article attempts to express all risks as an economic cost so that (a) the relative size of different threats can be established, and (b) the estimates provide a guide to the level of resources that should be expended to counter the threat. The full methodology is described in the source article, but in essence consists of the following components:

1. A threat occurs at an assumed frequency (daily, weekly, monthly, annual, once-per-decade), which corresponds to a range of values;
2. When the threat occurs, there is an assumed probability of success (low, medium, high, certain), which again corresponds to a range of possible values; and

3. The consequence of a successful event may include fatalities, injuries, disruption, delay to travel time, damage to aircraft, interruption to power supplies, all of which can be expressed in dollar terms.

Multiplying the data from these three components provides an expected annual economic cost. The word "expected" is used in the statistical sense, which means that it is the average that will occur over time.

The most important results from the risk assessment in that article are:

(a) The expected annual economic cost of collisions with aircraft is only $0.6m, using parameters that are arguably high given the historic record. The cost of disruptions, imposed as a mitigation against possible midair collisions between drones and airliners, is higher than the cost of the problem it is seeking to solve.

(b) The largest cost is from the delivery of contraband to prisons, with an aggregate expected annual cost of $10.0m. The likely frequency and success of contraband deliveries across the prison network as a whole are assessed on the basis of news reports. Contraband deliveries that might result in a fatality are assessed to be attempted monthly with only a low probability of success and have an expected annual cost of $2.7m. Contraband deliveries that result in other harm (such as serious injury from drug-related harm) are assessed to be attempted daily across the prison network, but again with a low probability of success, and have an expected annual cost of $7.3m. If such deliveries were only attempted weekly then the expected annual cost reduces from $7.3m to $1.0m, and the total cost of contraband deliveries is $3.7m.

(c) A combination of four different types of "terror" threats from drones (IED attacks, incendiary attacks, CBR attacks, and inert noise makers inducing panic) have an aggregate expected annual cost of $2.1m, some 44 percent higher than the aggregate cost of aviation-related risks.

(d) Disruption to electric power supply has an expected annual cost of $0.9m based on the cost of "lost load" including lost production during outages.

(e) Diversion to enable other direct action to occur, such as disruption of a Police or other law enforcement operation, has an expected annual cost of $0.8m.

In addition to the threats described above, Shelley notes but does not quantify threats of surveillance in areas of commercial or national security sensitivity, delivery of electronic listening devices, and surveillance prior to or during burglary. Drones have allegedly been used to identify targets for burglary. In addition to providing a visual surveillance capability, drones can also be used as a listening device or to deliver electronic listening devices to otherwise impossible to reach locations.

Means of Countering Drones

The two main ways of countering drones are detection and interdiction. Detection of drones allows action to be taken to protect the potential target, and may in some circumstances allow information about the operator of the drone to be obtained. Drones can be detected by way of radar, analysis of noise signatures, or with automated optical recognition.[19] None of these methods is perfect, and subject to both false positives (something that is not a drone being identified as a drone) and false negatives (an actual drone not being detected), so a combination of detection systems may be required.[20] A further detection method is interception of the C2 link that may be used to control the drone. A drone can be characterised as a flying computer; often that computer is controlled remotely via C2 signals transmitted over a radio link, but it may also be flying a pre-programmed flight path between GPS waypoints and undertaking a pre-programmed action.[21] If the drone is being controlled remotely then interception of the C2 link is possible, and in some instances may reveal the location of the transmitter. However, if the drone is flying a pre-programmed flight path then this method will not work.

The C2 link provides the avenue for two methods of interdiction: 'jamming' the radio link with an over-powering broadcast, and taking control of the drone by 'hijacking' the control link.[22] The response of the drone to jamming is uncertain and will depend on what actions the drone has been programmed to take: some may return to the location that they took off from or to some other pre-programmed 'home' point; others may hover in place; and a truly malicious operator could programme the drone to deliver its payload.[23] Hijacking the C2 link, on the other hand, can instruct the drone to fly to a safe location and land. Both of these methods require that the drone is being piloted remotely, but it is also possible that the drone is executing a pre-programmed flight path and will be unresponsive to any attempt to interfere with the C2 link. In this case, the only option for directly countering the drone is physical interdiction, which can range from trained eagles,[24] defensive drones armed with nets,[25] nets launched from stationery, vehicle-mounted, or shoulder-mounted systems,[26] interceptor drones that crash into the target drone,[27] or even directed energy weapons such as microwaves and lasers.[28]

Core Elements of a Security Strategy

Before assessing the strategy of others and developing a counter-drone strategy for New Zealand, it is necessary to define what is meant by the term strategy and identify the core elements of a security strategy. There are few studies identifying the essential constituent elements of a security strategy. The conventional Western approach to military strategy relies on the concept of "ends, ways, means" proposed by Lykke,[29] and taught at the US Army War College.[30] In the broadest sense, a strategy is a set of choices for achieving a particular objective,[31] and this concept of choice is reflected

in Lykke's ends-ways-means framework. However, Lykke's approach is devoid of a strong theoretical approach and has been criticised by others.[32] Stolberg compares the national security strategy development process of Australia, Brazil, South Africa, the United Kingdom (UK), and the United States of America (USA) to identify the most important elements of both the strategy development process and the security strategy itself,[33] but he advances no theoretical framework for why the identified elements are important. Du Mont proposes 10 "core elements" and three "optional elements" that should comprise a security strategy,[34] however these elements are again divorced from any theoretical basis.

Rumelt argues that the "kernel" of a good strategy "contains three elements: a diagnosis, guiding policy, and coherent action".[35] Krasner asserts that "grand strategy is a conceptual framing that describes how the world is, envisions how it ought to be, and specifies a set of policies that can achieve that ordering".[36] Krasner's approach aligns closely with the first two elements of Rumelt's kernel, with Rumelt's strategic diagnosis encapsulating both the description of the current state of the world and the vision of how it should be. The analysis that follows conducts a comparative analysis of Rumelt's kernel with the frameworks provided by Du Mont and Stolberg to establish the essential elements of a security strategy.

The first element of Rumelt's kernel is the 'strategic diagnosis', being an accurate statement of the problem or challenge to be overcome. Rumelt separates the diagnosis from objectives, positing that a strategy transforms "vague overall goals into a coherent set of actionable objectives". Other authors, however, start with objectives. Stolberg recommends that those formulating strategy should "identify and prioritize national interests",[37] while Du Mont recommends "accurate reflection of national values" and "clear articulation of national interests". Having identified national interests, Stolberg proposes the formulation of "objectives for the strategy",[38] but in this context, the objectives are broad statements of what the strategy is intended to achieve, which is in essence the same as Du Mont's "declaration of strategic vision". Ultimately, the difference between Rumelt, Stolberg, and Du Mont on this point is essentially one of semantics, caused in part by the synonymous nature of the words "goal" and "objective". Rumelt's diagnosis requires that there is a problem that requires solution, which in turn implies that there is an ideal end state and that the current situation departs from that end state. Rumelt refers to the ideal end state as a "goal", while others refer to it as an objective. The ideal end state may also be expressed as the "ends" that the strategy is intended to achieve.[39] Given the greater frequency with which the word "objective" is used in the sources reviewed, the current research uses the term "strategic objective" as the descriptor for the ideal end state. In keeping with the idea that a strategy is a set of choices, the strategic objective itself is also a choice.[40] A security strategy is a strategy concerned with achieving or addressing particular security objectives that are in the national interest, whether that is national security as a whole, or a particular element of national security.

All of the authors reviewed start with a strategic objective, albeit expressed using different terminology. This objective is merely the starting point in establishing the strategic diagnosis. With that established, Stolberg and Du Mont both propose a risk assessment, which necessarily requires identification of potential threats, and an assessment of the risk from each threat. A risk assessment thus creates "a prioritized approach",[41] ensuring that resources can be focussed on the challenges that pose the greatest risk. Taken as a whole, the strategic diagnosis thus provides a high-level view of what the strategy's authors envisage the ideal future to be, with the risk assessment identifying the most significant challenges to be overcome to attain that future state. The diagnosis "simplifies the … overwhelming complexity of reality by identifying certain aspects of the situation as critical".[42]

The second element of Rumelt's kernel is a 'guiding policy'. Just as it was important to define what is meant by "strategy", it is also important to define what is meant by "policy".[43] It is sometimes suggested that "it is difficult to define policy", which is unsurprising when the study of policy may conflate the study of decision-making processes, policy, and policy outcomes. However, Rumelt is clear that the guiding policy provides direction on the actions that will be taken to address the identified challenges, which is consistent with the practice of policy in the corporate world. Similarly, Bacchi suggests that in a public policy context, "the term 'policy' is generally associated with a program[me or] course of action".[44] Thus, for the purpose of the present analysis, the guiding policy is a statement of *what* is intended to be done to address the challenges identified in the strategic diagnosis.[45] Like Rumelt, Krasner explicitly requires a set of policies to achieve the strategic objective. Stolberg refers to "ways and means", which in the context of military strategy can be expressed as the actions, methods and process executed to achieve the strategic objective(s)[46] together with the required resources.[47] Thus, Stolberg's "ways" are entirely consistent with the concept of a set of actions, or policy, to achieve the objective. At a high level, Du Mont's 'basic implementation guidance' is a statement of *what* is to be done and is thus consistent with requiring a statement of policy.

The various authors then include elements in their strategic frameworks which are not obviously required for a strategy. The third and final element of Rumelt's kernel is 'coherent action', which is absent from the other authors' frameworks. Both Stolberg and Du Mont posit that there should be 'measures of effectiveness', which will help to ensure whether the actions being taken are effective in addressing the problems identified in the strategic diagnosis. Stolberg and Du Mont both include a feedback mechanism, with Du Mont suggesting that this is optional. A formal feedback mechanism is absent from Rumelt's kernel, not because it is not important but because strategy should never be static and should always adapt to changing circumstances, and feedback is part of that process. Finally, Du Mont also suggests that there could be a "legacy statement" essentially a political statement of what has been achieved to date and an explanation of the methodology used to develop the strategy.

Having reviewed the three frameworks, the critical aspects of a security strategy can be summarised as:

1) A strategic diagnosis, consisting of:
   a) A statement of objectives or strategic vision;
   b) A threat analysis identifying potential challenges to achieving the strategic vision; and
   c) A risk assessment of the identified threats.
2) A guiding policy which states at a high level what is to be done to address the identified threats.

FIVE EYES PARTNER RESPONSES

New Zealand is a member of the Five Eyes (FVEY) arrangement, having been admitted in 1956.[48] While the agreement that gave rise to FVEY was initially limited to intelligence-sharing, the level of cooperation engendered under the "Five Eyes" umbrella now extends far beyond that of the original agreement.[49] In recent years the FVEY countries have held a "Five Country Ministerial" (FCM) meeting for political representatives to discuss issues of mutual interest. The communiqué issued at the end of the 2019 FCM provided a joint statement in relation to five broad areas of security concern,[50] and specifically addressed drones as a threat to public safety and national security. The FCM committed:[51]

> …to create a stronger Five Country approach to [drones] informed through co-ordinated and in-depth information sharing around threat, vulnerabilities, and counter-[drone] technology.

Notwithstanding the commitment to a stronger five-country approach, the response to the threats posed by drones has varied considerably across the FVEY partners. Consider the distinction between tactical measures and the existence of a strategy. Tactical measures may enable use of any of the main methods of detection or interdiction; however, those measures may have been developed on a piecemeal basis rather than as part of an overall strategy. The responses of Australia and Canada have been tactical, allowing some counter-drone measures to be taken but without an apparent over-arching strategy. The United Kingdom is the sole member of the FVEY alliance to have published a counter-drone strategy and is in the process of implementing that strategy. The United States has what Fontaine and Burton refer to as an emergent strategy,[52] evident in the actions taken to enable counter-drone response, rather than a strategy espoused in a publicly available counter-drone strategy document. New Zealand has been the laggard of the FVEY partners, with no power for law enforcement to undertake counter-drone action. However, legislation introduced in September 2021 may place New Zealand in

a similar position to the United States. Further detail on each of the FVEY partner responses is provided below. Recommendations for change to New Zealand's proposed legislation are reserved until the development of strategy proposed later in this article.

Legal Constraints

To appreciate the extent to which some legislative changes may be part of a response to drones it is helpful to first understand some of the legal constraints that exist in each country. All five of the FVEY partners are members of various international treaties which are then codified in each country's laws. Minor wording differences in how these treaties are codified can have potentially significant implications for what counter-drone action is legally available.

Interference with an aircraft

All of the FVEY partners are parties to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, otherwise known as the Montreal Convention.[53] Article 1 of the Montreal Convention provides a person commits an offence if he or she:

> unlawfully and intentionally… destroys an aircraft in service or causes such damage to an aircraft which renders it incapable of flight or which is likely to endanger its safety in flight.

A drone is an aircraft, so this provision applies to drones, and also applies to actions taken against drones. Of note, the action must be both unlawful and intentional to give rise to an offence. Australia[54] and the United Kingdom[55] have replicated the qualification that the action against an aircraft is only an offence if it is unlawful; thus where a party has a legal right to take action against a drone the exercise of that right will not contravene the legal prohibition. Conversely, Canada,[56] New Zealand,[57] and the United States[58] have all omitted the qualification that the action is unlawful, thus any action that might render a drone incapable of flight, or damages it, would potentially constitute an offence.

Prohibition against jamming

Each of the FVEY partners is also a signatory to the International Telecommunications Convention (ITC) and agrees to comply with the *Radio Regulations*.[59] The ITC prohibits harmful interference with the radiocommunications of *another state*, but each of the five nations has enacted national legislation that prohibits all jamming *within* their country. As discussed below, Australia and Canada have explicitly moved to allow jamming of drones by federal police forces. In New Zealand, the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011 prohibits

the "use of radio jammer equipment other than by a permitted person."[60] While there is no published process for becoming a permitted person, comments posted publicly on LinkedIn also indicate that Radio Spectrum Management (RSM), the government agency responsible for managing radio spectrum licensing in New Zealand, has granted a temporary licence to the New Zealand Defence Force (NZDF) to test counter-drone jammers.[61]

Australia & Canada: tactical responses to allow jamming

In contrast to its detailed counter-terrorism strategy[62] and associated guidance documents, Australia does not have a published counter-drone strategy. Likewise, Canada also does not have a published counter-drone strategy. However, Australia and Canada have both recognised the need to allow law enforcement officials to utilise radio jamming against drones. Both jurisdictions are federations, and the power to utilise jamming is reserved for the federal police force rather than state or municipal police forces. There is also no power for airport operators or providers of critical national infrastructure to be able to utilise jamming. In both jurisdictions the authorisation for jamming appears to be divorced from any over-arching counter-drone strategy, and as such can be considered to be a tactical measure.

In Australia, the Radiocommunications Act 1992 prohibits interference with radiocommunications, including by way of jamming.[63] Following a consultation conducted by the Australian Communications and Media Authority [ACMA], the *Radiocommunications (Unmanned Aircraft and Unmanned Aircraft Systems) Exemption Determination 2019* was promulgated,[64] authorising the Australian Federal Police (AFP) to be jamming devices against drones ("UAS Exemption Determination"). The UAS Exemption Determination authorises the use of a "radio navigation satellite service" (RNSS) jamming device,[65] but only in frequency bands used for C2 by consumer drones rather than used for RNSS.[66] Notwithstanding this drafting error, the operation of a RNSS jamming device in the frequency bands specified in the UAS Exemption Determination will still have the effect of jamming the C2 signal if sufficient power is used.

Whereas aviation and telecommunications are federal matters and addressed by federal legislation and a national regulator, interference with computer systems is addressed in the legislation passed by each State. However, the Council of Australian Governments has developed a Model Criminal Code[67] for adoption by individual States. Chapter 4 of the Model Criminal Code specifies crimes of "unauthorised access, modification, or impairment" of computer systems[68] and "unauthorised impairment of electronic communication".[69] An action is defined as unauthorised "if the person is not entitled to cause that access, modification or impairment".[70] Whether the Model Criminal Code allows law enforcement and other persons to access and impair the computer on a drone or to impair the electronic communication of a drone depends on whether those

individuals have a legal entitlement to access or cause impairment. In the absence of specific enabling legislation, an argument may be able to be made for law enforcement to exercise these powers, but there is unlikely to be a corresponding right for other entities such as airport operators and critical infrastructure providers.

In Canada, the Radiocommunications Act 1985 has a general prohibition against installing, using, possessing, manufacturing, importing, distributing, leasing, or selling a jammer.[71] However, the 'Radiocommunication Act exemption Order (Jammers Royal Canadian Mounted Police)' provides the Royal Canadian Mounted Police (RCMP) with broad powers to utilise jamming equipment for the following purposes:[72]

(a) national security;
(b) public safety, including with respect to penitentiaries and prisons;
(c) international relations;
(d) the investigation or prosecution of offences in Canada, including the preservation of evidence; and
(e) protection of property, or the prevention of serious harm to any person.

The order thus enables the RCMP to utilise any form of jamming device for any purpose related to the broad scope of their responsibilities. Unlike Australia, which has limited the AFP to only utilise jamming devices against drones, the RCMP are able to use jamming devices for a wider set of activities including preventing the activation of radio-controlled trigger mechanisms on IEDs.

The Canadian *Criminal Code* makes it an indictable offence to "intercepts or causes to be intercepted, directly or indirectly, any function of a computer system".[73] In the absence of specific authorising legislation there is no right to utilise a device that intercepts a function of the computer system of a drone, which could apply to transmissions generated by the drone. The *Criminal Code* also makes it an indictable offence to intercept a private communication,[74] which could potentially apply to the interception of transmissions between the UAV and the flight controller. The *Criminal Code* does contain various provisions for authorising interception or obtaining a warrant, but these would generally be impracticable for monitoring drone proximity and activity, and do not apply to people other than an "agent of the state". However, Police officers are granted the power of immediate interception if the "officer has reasonable grounds to believe that … the interception is immediately necessary to prevent an offence that would cause serious harm to any person or to property".[75] This provides some ability for Police to intercept the communications between a drone and the flight controller but the restriction that the interception is "immediately necessary" could be problematic for the proactive monitoring of drone transmissions in situations where a drone *might* be used to cause harm.

The United Kingdom's Explicit Strategy

The United Kingdom (UK) has a published counter-drone strategy, the *UK Counter-Unmanned Aircraft Strategy*.[76] This strategy starts with a clear statement of strategic objective, "to reduce the risk posed by the highest-harm illegal use of drones".[77] The strategy briefly touches on risk but does not include a risk assessment, instead making reference to two previous consultations that did define and analyse risks. The strategy provides four policy objectives: "develop a comprehensive understanding of the evolving risks posed by the malicious and illegal use of drones";[78] "take a 'full spectrum' approach that maximises the opportunities to deter, detect and disrupt the criminal misuse of drones";[79] ensuring counter-drone products "meet the highest security standards",[80] and "empower the police and other operational responders through access to counter-drone capabilities and effective legislation, training and guidance".[81] Specific areas of action are identified to achieve each policy objective.

The Air Traffic Management and Unmanned Aircraft Act 2021 enacts some of the key provisions required to meet the second policy objective.[82] Police are granted powers to require a person to land a drone, provide proof that competency requirements have been met, provide proof of drone registration, provide proof of pilot identity, and provide proof of consent for certain types of flight. The Centre for Protection of National Infrastructure is currently testing and evaluating technology to detect, track, and identify drones,[83] one of the steps in the UK strategy. This technology is intended to be available to national infrastructure providers and other relevant parties to protect against drones.

The United States of America's Emergent Strategy

The United States of America (USA) has implemented two pieces of legislation that enable the use of actions to counter drones. Since 2018 the National Defense Authorization Act allows action to be taken by members of the US armed forces and relevant civilian employees against drones that potentially threaten assets or facilities related to national security.[84] The Preventing Emerging Threats Act 2018 enables the Department of Homeland Security, the Department of Justice, and the United States Coast Guard to also take action against drones in a wide range of circumstances.[85] Both pieces of legislation allow actions such as warning the operator, seizing control of the drone, and destroying the drone in response to a potential threat. Despite these provisions for specified government agencies, there is no general provision for a wider private sector right to engage in counter-drone activity.[86]

New Zealand's Response to Drones

Under current legislation, law enforcement officials lack any power to require a person to land a drone that they are piloting, and lack an effective authority to require a drone

pilot to provide identifying details (such as their name and address), with the operator of an aircraft having 10 working days to provide identifying details.[87] New Zealand law enforcement agencies and the New Zealand Defence Force (NZDF) lack any legislative authority to utilise jamming devices within New Zealand (although a temporary permit to allow jamming may be obtained from RSM[88]), and lack any legislative authority to take other action to stop or destroy a drone that is causing a risk to security. Law enforcement agencies lack any legislative authority to require a drone to land or to require the immediate identification of the drone pilot. Furthermore, intercepting drone C2 signals and using them to detect, track, and identify the drone may be illegal for any person who is not a law enforcement officer or a member of the NZDF.[89]

Some of the deficiencies were to be temporarily remedied for the duration of the APEC 2021 events, with the Asia Pacific Economic Cooperation (APEC 2021) Bill providing Police with broad powers to counter drones[90] and enabling the use of "wireless electronic countermeasures" against both drones and remotely activated IEDs. However, the Bill was withdrawn when the physical visits by dignitaries to New Zealand as part of APEC 2021 were cancelled due to covid-19.

A new CA Bill, proposing comprehensive change to multiple areas of aviation legislation, was introduced to the New Zealand Parliament on 8 September 2021. The CA Bill creates the position of "response officer", being a person appointed by the Director of Civil Aviation (DCA) specifically for the purpose of responding to drones. When a constable or response officer has reasonable grounds to believe that an applicable offence is to be commissioned with a drone, or the drone will be operated in a manner that "may endanger people or property" they may:[91]

> (a) enter a place, vehicle, or other thing and search for the [drone];
> (b) prevent the [drone] from taking off;
> (c) seize the [drone] and anything being used, or that may be used, to control the [drone];
> (d) detain the [drone] and anything being used, or that may be used, to control the [drone]; and
> (e) destroy the [drone].

At face value, these powers will be similar to the powers granted by the relevant legislation in the United States and would enable effective action to be taken against drones. From the associated cabinet papers,[92] it is apparent that the measures in the CA Bill are reaction to the potential that a threat to aviation may occur and are not part of a wider strategy. The CA Bill does not include any provisions remedying the issue of not being able to request name and address details in a timely manner, reserving that power for inspectors[93] who are separate from response officers and do not respond to drone-related incidents. The CA Bill also does not remedy the inability to detect, track, and identify rogue drones.

STRATEGY DEVELOPMENT

Objectives

The objectives for the counter-drone strategy proposed here can be drawn directly from the objectives of the New Zealand national security system. The *National Security System Handbook* defines national security as:

> "the condition which permits the citizens of a state to go about their daily business confidently free from fear and able to make the most of opportunities to advance their way of life".[94]

One of the key objectives underpinning New Zealand's national security strategy is "ensuring public safety", being the mitigation of "risks to the safety of citizens and communities".[95] This objective is of particular relevance to a counter-drone strategy, as many of the potential threats from drones present risks to individuals. Other relevant objectives contained in New Zealand's national security strategy are "sustaining economic prosperity" and "maintaining democratic institutions and national values".[96] Sustaining economic prosperity is defined as "maintaining and advancing the economic wellbeing of individuals, families, businesses and communities",[97] which is particularly relevant to preventing activities that could involve espionage, sabotage, or other attacks on businesses. Maintaining democratic institutions and national values is concerned with preventing actions "aimed at undermining or overturning government institutions",[98] which encompasses the counter-terrorism aspects of a counter-drone strategy.

Risk Assessment

Risk assessment is the prioritisation and management of "risks based on the likelihood and severity of their likely impact on national interests".[99] As with the *UK Counter-Unmanned Aircraft Strategy*,[100] the risk identification and assessment for New Zealand is primarily conducted in a separate document – a recent article in this journal.[101] Key results from that assessment are summarised earlier in this article. Based on that risk analysis, and utilising the expected annual cost of a threat as a quantitative measure of risk, the risks referred to previously and in order of priority are:

1. Drone deliveries of contraband to prisons ($3.7m-$10.0m), which a "[risk] to the safety of citizens and communities" and impedes activities "ensuring public safety".
2. Terror-related threats to mass events ($2.1m), which is a "[risk] to the safety of citizens and communities".
3. Surveillance and/or espionage in areas of commercial or national security

sensitivity (not valued, but assumed here to be worth at least $1.0m per year), which is a direct threat to "sustaining economic prosperity".

4. Disruption to electric power supplies ($0.9m), which threatens the "well-being of individuals, families, businesses and communities".
5. Diversion / disruption related to law enforcement ($0.8m), which impedes activities "ensuring public safety".
6. Collision with general aviation aircraft (helicopters and light aircraft), which is a "[risk] to the safety of citizens" and a threat to "the economic wellbeing of individuals, families, [and] businesses".
7. Collision with airliners, which the historical record shows happens only extremely rarely and might result in superficial damage to the aircraft. However, on the basis of theoretical simulations, there is a possibility of major damage to the aircraft which could threaten both individual safety and the economic wellbeing of the business operating the aircraft.

To place these risks into perspective, the New Zealand Ministry of Transport (MOT) uses a Value of a Statistical Life of $4.42 million per fatality for estimating the social cost of death and injury from transport accidents across transport modes.[102] Thus, the highest risk is equivalent to an average of between 0.8 and 2.26 fatalities per year. The risk from terror-related threats is equivalent to approximately 0.5 fatalities per year. Risk to aviation other than disruption of flights has an expected annual cost of $0.6m, which is equivalent to just 0.14 fatalities per year.

Disruption of flights – while included in the recent risk analysis – is a result of the policy of eliminating all risk by diverting air traffic at controlled aerodromes in the event of a drone sighting. That cost could be immediately eliminated by stopping the use of this policy. While this would likely be a controversial change, the historical record shows that (a) it is small aircraft, particularly helicopters, that are at risk in areas where air traffic control is not necessarily controlling aircraft, and (b) while drones have collided with larger aircraft, there has never been a serious incident involving such a collision between an airliner and a drone.[103]

Strategic Considerations

Compliance-based Policy Interventions will not stop criminal misuse

The MOT advances a regulatory programme focussed on a basic online licence test for drone pilots and registration of drones as key policy tools for controlling misuse of drones.[104] The CA Bill also includes provisions to criminalise unauthorised incursion into controlled or restricted airspace, and the associated cabinet paper explicitly links that provision to drones.[105] These interventions may be appropriate for the inadvertent or negligent misuse of drones, but they will not stop the deliberate misuse of drones.

A current example of how policy interventions relying on compliance will not stop criminal misuse is provided by the increasing level of firearms-related crime in New Zealand. In the aftermath of the 15 March 2019 mosque shootings, New Zealand rushed to ban military style semi-automatic firearms and assault rifles,[106] with the Prime Minister vowing "we cannot allow this to happen again".[107] Opponents of the changes noted that the mosque shootings were a criminal act, and the law changes targeted law-abiding firearms owners rather than the "problem of criminal activities with firearms going unpunished".[108] While it will be impossible to ever prove that the law changes prevented an attack that would otherwise have occurred, evidence shows that assault rifles are still in the possession of the criminal fraternity, with repeated news reports of AK-47 rifles and other prohibited firearms being recovered in Police operations.[109] [110] [111]

Furthermore, data released by New Zealand Police[112] shows that the underlying increase in firearms-related crime has continued unabated. Omitting the outlier event of the 15 March 2019 mosque shooting, total firearms-related offences in New Zealand were 901 in calendar year 2018, 1,050 in 2019, and 1,141 in 2020. There were 647 offences in the six months to the end of June 2021, suggesting a possible total of 1,294 offences for 2021. It is apparent that the firearms law changes – which rely on compliance – have not had any effect on firearms-related crime, and instead such crime requires a direct response from Police.

Strategy must be deliberate, not reactionary

New Zealand National Security System has been described as "reactive",[113] driven in part by "responses after the fact to significant events"[114] and "effectively reactionary in nature".[115] An example of this reactionary behaviour is provided by the changes to firearms legislation in the wake of the March 15 Mosque Shooting,[116] discussed above. The Mosque Shooting was not a normal event in New Zealand, but it precipitated a range of legal changes which adversely affected law-abiding firearms owners but had no effect on the level of firearms-related crime. As described above, such crime has continued to worsen.

The risk analysis implies that the same dynamic could occur in relation to drones. Events that are rare could result in fatalities, and even rare events can occur in clusters.[117] The current policy proposals from MOT[118] are based primarily on aviation-related threats which the risk analysis suggests are infrequent and relatively low risk. When those policies prove ineffective in controlling criminal misuse of drones there is a risk that alternative policies will be adopted which, mirroring the experience with firearms, curtail the rights of law-abiding drone operators while not addressing the underlying problem.

Necessity of Immediate Response

The characteristics of drones, and particularly their inherent ability to fly rapidly and undetected, means that often an immediate response will be required. When a drone is detected crossing the boundary of a prison, action to counter the drone is required then and there; in twenty minutes time – which might be the response time for Police – the drone will have delivered whatever it was sent to deliver and will no longer be on the scene. Similarly, if there is a potential terror attack at a mass event an immediate response is required to stop the threat.

Selection of potential controls

Having identified and prioritised relevant drone-related threats, and identified relevant strategic considerations, this article now examines the appropriate "risk controls" – the policies and actions that will provide an effective response to the identified threats. A five-pronged strategy is proposed:

1. Abandon policies that will not address the threat;
2. Use an intelligence-led risk-based approach to developing policy;
3. Implement legislation that empowers relevant entities to take appropriate action;
4. Utilise a flexible approach that enables a wide range of organisations to implement counter-drone capabilities; and
5. Ensure that counter-drone responders are able to take proportionate actions short of destroying the drone.

Each of these elements is discussed in further detail below.

Abandon polices that will not address the threat

First, it is necessary to abandon the notion that policies such as online pilot licensing and registration of drones – as advocated by MOT[119] – will do anything significant to counter the threats identified. There may be other reasons for adopting these policies, but they will not prevent intentional malicious use of drones. Starting from this position will ensure that wishful thinking does not dominate the policy formulation process and will help ensure that policies are justifiable on the basis of genuine benefits.

Use an intelligence-led risk-based approach to developing policy

New Zealand must also abandon a data-driven reactionary approach in favour of an intelligence-led risk-based approach to responding to drone threats.[120] As discussed earlier, the reactionary approach is evident in New Zealand's approach to firearms reforms in the wake of the March 15 shootings. The data-driven reactionary approach is also evidenced by government policy papers arguing that the pre-Christmas delays in 2018

at Gatwick Airport provide justification for regulatory proposals.[121] [122] The fact that delays happened is a data point, and that the *initial* justification for those delays was the sighting of drones is part of that same data point. However, a more fully developed picture would show (a) that military drone-detection equipment was unable to detect a single rogue drone;[123] (b) there are credible reports that at least some sightings may have been of a helicopter;[124] and (c) Sussex Police have even admitted that there might not have ever been a drone.[125] An intelligence-led approach would largely discount the Gatwick incident, and would utilise appropriate statistical analysis to determine whether changes in observed occurrences represent a change in the threat level, or whether they are consistent with the assumptions underpinning existing policy settings. As already noted, random events may occur in clusters, and those clusters do not necessarily provide a justification for changing policies.

Implement legislation that empowers relevant entities to take appropriate action

An effective response to drone-related threats requires the ability to utilise drone-detection equipment, and may, at times, require the ability to utilise signal jammers, nets, and kinetic interceptors (including drones that physically intercept the threat). As Shelley (2019) asserts this in turn means that legislation must be enacted that provides:[126]

- a positive right to undertake drone detection activity to ensure that such actions do not contravene the Radiocommunications Act 1989;
- a qualified right to undertake counter-drone activity; and
- a positive authorisation to access the computer system on board a drone when a right exists to undertake counter-drone activity.

In addition, as noted in the discussion of interference with an aircraft, a single word change is required to the Aviation Crimes Act 1972 to allow lawful action against drones. These legislative changes will allow relevant agencies in New Zealand to exercise the same powers to utilise jamming as are available to all four of our FVEY partners and allow other actions to directly counter drones as are available in the United States. The proposals in the CA Bill provide the relevant powers, but do not address the required changes to the Aviation Crimes Act 1972 nor the Radiocommunications Act 1989.

Utilise a flexible approach

The speed of response required for the most significant drone-related threats requires that a party who is on-site has the ability and authority to respond to the threat. This means that the appropriate party to provide a response is different for each threat. The most significant threat from drones is at prisons, where Department of Corrections staff are the most logical responders. The second most significant threat is a terror attack at a mass event. The nature of the Police presence at such events will depend on the nature of the event. It is possible that Police could be the lead agency for such events, but it

might also be appropriate for contracted security personnel to provide the response capability. Any immediate response to drones engaged in surveillance and espionage at commercial facilities would be best addressed by personnel contracted or employed by the operator of those facilities. Surveillance and espionage in areas of national security sensitivity is best addressed directly by NZDF, including contracted private security if appropriate. Any threat to power supplies, particularly at an electricity substation will be best addressed by the operator of the substation. Diversion and disruption of law enforcement activities can be addressed by law enforcement or contracted security.

While threats to aviation were the least significant of the threats analysed, it may still be considered that some form of response capability is required. The Aviation Security Service (AvSec) is located at the five major airports and would be the appropriate responder at those locations. Most if not all other airports serving regular scheduled passenger flights have contracted security staff onsite, and those personnel would be the logical individuals to provide an immediate response to a drone threat.

These examples demonstrate that an effective response to drone threats requires a flexible approach that enables the most appropriate organisation, with personnel already on site, to deploy the relevant drone-detection or counter-drone capability. This is the approach adopted in the UK. The CA Bill ostensibly provides an appropriate level of flexibility, providing the DCA with powers to appoint a broad range of persons as response officers. However, there is an apparent preference for response officers to be restricted to law enforcement. The Cabinet minute associated with an earlier consultation paper stated that cabinet "agreed that the commentary document includes a section that seeks stakeholder views on options to provide *law enforcement agencies* with powers necessary to detain, seize or destroy drones" (emphasis added).[127] The Regulatory Impact Statement that accompanies the counter-drone provisions of the CA Bill acknowledges the potential relevance to the Department of Corrections of being able to undertake counter-drone action,[128] and consistent with that the CA Bill provides that a "statutory officer" may be appointed as a response officer.[129] The Regulatory Impact Statement also acknowledges the potential need for airport staff to take action against drones, but notes only that the proposed approach "does not preclude" this from happening.[130] Choosing to restrict capability to law enforcement such as Police and/or AvSec will necessarily increase response times and result in a lower level of security. In most cases analysed by Shelley (2021),[131] restricting powers to law enforcement will prevent any effective response.

Enable proportionate actions short of destroying the drone

There are also a number of actions between detecting a drone and destroying that drone that should be available to any person authorised to respond to drone threats, particularly the power to order a person to land a drone or remove it from the area of concern. These powers are common features of the strategies adopted by the United Kingdom

and United States. These powers were contained in the APEC 2021 legislation but are absent from the CA Bill. Furthermore, while these powers might normally be thought of as being reserved for identifiable law enforcement personnel – including Police, AvSec, Department of Corrections officers, Customs Service officers, and Ministry of Primary Industries officers – it is not unreasonable for security personnel at an identifiable location to have the same powers. Such a location might be a stadium, a high technology facility, an electricity substation, etc.

A minor change is required to the Radiocommunications Act 1989 to enable personnel other than law enforcement and NZDF personnel to detect, track, and identify drones.[132] [133] Such actions enable precautions to be taken against drones that stop short of destroying the drone. The CA Bill should also provide an authorisation to access and control the on-board flight controller for a drone, which would enable applications that hijack the C2 link to be used to land the drone in a safe location.

Implementation Guidance

There are three important implementation issues: which agency should be responsible for development of legislation; the Civil Aviation Authority's (CAA's) demonstrated slowness to develop processes for new regulatory authorities; and the granting of permits to operate drone jamming equipment. Legislation (both primary and subordinate) concerning aviation is prepared by the MOT and, on that basis, it might be considered that the logical choice is for the MOT to lead the development of the legislation. However, Police are the lead agency for domestic counterterrorism response, and given that the combined threat from terror related events, threats to prisons, and disruption of law enforcement significantly outweighs the threats to aviation, it would also be reasonable for Police to be the lead agency for developing this legislation. In contrast, the development of the CA Bill has been led by the MOT and reflects an aviation-centric approach.

Second, if counter-drone response is restricted to response officers designated by the DCA, then the CAA must be directed to develop and promulgate an appropriate process in a timely manner. The general tenor of the Regulatory Impact Statement[134] suggests a general ambivalence to appointing response officers outside of the CAA or AvSec, and this could be easily effected by the CAA prioritising resources to address other matters. Another drone-related rule provides an example of how slow CAA can be to develop necessary processes when it apparently does not see them as important. Civil Aviation Rule 101.202 provides for an "approved person or organisation" to undertake specified functions including issuing a pilot qualification for drones, inspecting and approving drones weighing more than 15kg, and authorising the operation of drones weighing more than 15kg.[135] As of February 2020, some four and a half years after the 101.202 rule came into force, there was "no formal procedure to apply for a 101.202 approval".[136] This meant that potential applicants did not know how to make the application nor

what criterion they would need to satisfy to become approved. To avoid a similar situation occurring with counter-drone response, the CAA must be directed to develop and promulgate a process and criteria for appointment as a response officer, and to do so in a timely manner.

Third, there is also a question over which agency should have a licencing authority for operators licenced to utilise signal jammers against drones. The two logical alternatives are (a) the CAA, which will be given the power to appoint response officers, and (b) Radio Spectrum Management (RSM), which manages and licences all matters relating to radio spectrum. Given the risk assessment described in this report, it is apparent that risks to aviation are relatively small, while the issues relating to the use of jammers are potentially more significant. In Australia it is the Australian Communications and Media Authority (ACMA) that issued the exemption allowing federal police to utilise jammers, not the Civil Aviation Safety Authority (CASA). It is also appropriate that RSM, being the New Zealand equivalent to ACMA, is the regulatory agency for jammers here in New Zealand. This is consistent with RSM being the agency responsible for the Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011.[137] Given the wide range of parties who may have a legitimate reason to operate counter-drone jamming equipment, RSM should also develop a clear process for applying for becoming a permitted person under that Notice.

CONCLUSION

The new Civil Aviation Bill contains significant new powers to enable law enforcement and (potentially) "statutory officers" to take action against drones. However, it appears that the legislation has been developed in response to high profile events (such as the discredited Gatwick event), rather than as part of a comprehensive strategy. For many of the threats analysed, restricting powers to law enforcement will be insufficient. An analysis of New Zealand's FVEY partners suggests that New Zealand is not alone in lacking a strategy to deal with the malicious drone use.

New Zealand is exposed to a range of potential threats from the misuse of drones, including delivery of contraband to prisons, terror attacks at mass events, attacks on or disruption to aviation, attacks on and disruption of critical infrastructure and energy production, and espionage. The two most critical risks in New Zealand are the delivery of contraband to prisons, and the potential for a terror attack at a mass event. There are also lesser threats from espionage (including commercial espionage), disruption to power supplies, and disruption to law enforcement operations. Setting aside the cost of disruption to airline transport that is the intended outcome of the current policy of diverting or holding flights when a drone is sighted, the risks to aviation are relatively low. To address the identified threats a five-pronged strategy should be adopted:

1. Abandon policies that will not address the threat, particularly basic operator licensing and drone registration;
2. Use an intelligence-led risk-based approach to developing policy so that interventions are focussed on the greatest risks;
3. Implement legislation that empowers relevant entities to take appropriate action;
4. Utilise a flexible approach that enables a wide range of organisations to implement counter-drone capabilities; and
5. Ensure that counter-drone responders are able to take proportionate actions short of destroying the drone.

New Zealand should follow the UK's lead in allowing a range of organisations to implement and act on drone-detection systems, and to implement and use counter-drone systems. Such organisations should not just be limited to law enforcement but should be expanded to include critical infrastructure providers and any commercial or industrial facility that has sensitive information. This can be enabled through minor changes to legislation, the introduction of a positive right to undertake drone detection, the introduction of a qualified right to undertake counter-drone action, and additional powers to require a drone operator to land the drone and provide their identifying details. The counter-drone powers provided in the CA Bill address some, but not all, of the required changes. Police should be the lead agency for developing this legislation, CAA must be directed to develop and promulgate a process for approval of response officers in a timely manner, and RSM should be directed to develop a process for organisations to become permitted persons to operate counter-drone jammers.

1 Shelley, A. V. (2021) Quantifying the Cost of Drone-Related Threats in New Zealand. *National Security Journal*, 3(3), 8 November 2021. DOI: 10.36878/nsj20211108.03.

2 International Civil Aviation Organization (2011). Unmanned Aircraft Systems (UAS), Cir 328 AN/190, p. x. Retrieved from https://www.icao.int/meetings/uas/documents/circular%20328_en.pdf.

3 International Civil Aviation Organization, 2011, above n. 2, p. 8.

4 International Civil Aviation Organization, 2011, above n. 2, p. 12.

5 Shelley, 2021, above n. 1.

6 Shelley, A. V. (2020). *Essays in the regulation of drones and counter-drone systems* (Doctoral dissertation, Victoria University of Wellington). Retrieved from http://researcharchive.vuw.ac.nz/handle/10063/8900.

7 Marchant, G.E., Allenby, B.R. & Herkert, J.R. (eds) (2011). *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*, Springer. DOI: 10.1007/978-94-007-1356-7.

8 Wallace, P., Martin, R. & White I. (2018). Keeping pace with technology: drones, disturbance and policy deficiency, *Journal of Environmental Planning and Management*, 61(7):1271-1288. DOI: 10.1080/09640568.2017.1353957.

9 Civil Aviation Bill. Government Bill, 61-1. Retrieved from https://www.legislation.govt.nz/bill/government/2021/0061/latest/whole.html.

10 Cabinet (2019). Civil Aviation Bill: Confirmation of Key Policy Decisions. Minute of Decision, CAB-19-MIN-0167. Retrieved from https://www.transport.govt.nz/assets/Uploads/Cabinet/2019-Civil-Aviation-Bill-Cabinet-minute.pdf. New Zealand Ministry of Transport. (2020, March 5). Impact Statement: New civil aviation enforcement powers. Retrieved from https://www.transport.govt.nz/assets/Uploads/RIS-1-New-civil-aviation-regulatory-powers-Redacted-v2.pdf. Office of the Minister of Transport (2021). Civil Aviation Bill – New Policy Proposals. Retrieved from https://www.transport.govt.nz/assets/Uploads/3.-Civil-Aviation-Bill-New-Policy-Proposalswatermark.pdf.

11 Shelley, A. V. (2021) Quantifying the Cost of Drone-Related Threats in New Zealand. *National Security Journal*, 3(3), 8 November 2021. DOI: 10.36878/nsj20211108.03.

12 Du Mont, M. (2019, February 28). Elements of national security strategy. Retrieved from https://www.atlanticcouncil.org/content-series/strategy-consortium/elements-of-national-security-strategy/; Stolberg, A. G. (2012, October). *How nation-states craft national security strategy documents*. Strategic Studies Institute, US Army War College. Pennsylvania. Retrieved from https://publications.armywarcollege.edu/pubs/2201.pdf.

13 Krasner, S. D. (2010, October 1). An orienting principle for foreign policy. *Policy Review*. Retrieved from https://www.hoover.org/research/orienting-principle-foreign-policy; Rumelt, R. P. (2011). Good strategy / bad strategy: The difference and why it matters. London: Profile Books.

14 HM Government. (2019, October 21). *UK Counter-Unmanned Aircraft Strategy*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/_le/840793/Counter-Unmanned Aircraft Strategy.pdf.

15 Fontaine, R. & Burton, B.M. (2010) *Eye to the Future: Refocussing State Department Policy Planning. Policy Brief*, Center for a New American Security. Retrieved from https://www.jstor.org/stable/pdf/resrep06259.pdf.

16 Department of Prime Minister and Cabinet. (2016, August). *National security system handbook*. Retrieved from https://dpmc.govt.nz/sites/default/_les/2017-03/dpmc-nss-handbook-aug-2016.pdf.

17 Shelley, 2021, above n. 11.

18 Shelley, 2021, above n. 11.

19 Wilson, B., Tierney, S., Toland, B., Burns, R. M., Steiner, C. P., Adams, C. S., . . . Chang, I. (2020). *Small unmanned aerial system adversary capabilities*. Homeland Security Operational Analysis Center, RAND Corporation. Retrieved from https://www.rand.org/pubs/research_reports/RR3023.html.

20 Lykou, G., Moustakas, D., & Gritzalis, D. (2020, June). Defending Airports from UAS: A Survey on Cyber-Attacks and Counter-Drone Sensing Technologies, *Sensors*, 20(12). DOI: 10.3390/s20123537.

21 For an example of commercially available software for pre-programming a flight path see Da-jiang Innovations (2018, November). *DJI GS Pro User Manual*. Retrieved from https://dl.djicdn.com/downloads/groundstation_pro/20181102/GS_Pro_User_Manual_v2.0_EN_201811.pdf; Litchi (2021, October). User Guide: Waypoint. Retrieved from https://flylitchi.com/help#waypoints-p3.

22 Lykou et al, 2020, above n. 20.

23 Many consumer drones have the option to "Return to Home" if the control signal is lost, and also allow the "home" point to be updated to a location other than that the drone took off from. The simplest method of delivering the payload in the event of a lost link occurs with a kamikaze attack, where the home point can be set to the location of the target. For an example of Return to Home see Da-jiang Innovations (2020, January). *Phantom 4 Pro/Pro+ Series User Manual*, v1.8, p. 15. Retrieved from https://dl.djicdn.com/downloads/phantom_4_pro/20200108/Phantom_4_Pro_Pro_Plus_Series_User_Manual_EN.pdf. For an example of the home point being updated see Litchi (2021, October). User Guide: General. Retrieved from https://flylitchi.com/help#general-p3.

24 Roberts, J. J. (2017). France is training eagles to kill drones. *Fortune*. Retrieved from http://fortune.com/2017/02/22/drones-eagles-france/; Samuel, H. (2016). French Air Force turns to eagles to fight terror drone threat. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/2016/11/18/french-air-force-turns-to-eagles-to-fight-terror-drone-threat/.

25 Goodrich, M. (2016). Drone Catcher: "Robotic Falcon" can Capture, Retrieve Renegade Drones. *Michigan Tech News*. Retrieved from http://www.mtu.edu/news/stories/2016/january/drone-catcher-robotic-falcon-can-capture-retrieve-renegade-drones.html.

26 See for example, OpenWorks. (2016). *Skywall*. Retrieved from https://openworksengineering.com/images/skywall/SkyWall%20Brochure.pdf.

27 Unmanned Airspace (2021, April 5). XTEND announces delivery of "dozens of SKYLORD GRIFFON C-UAS units to US Army Special Operations Command. *Unmanned Airspace*. Retrieved from https://www.unmannedairspace.info/counter-uas-systems-and-policies/xtend-announces-delivery-of-dozens-of-skylord-griffon-c-uas-units-to-us-army-special-operations-command/.

28 Rees, M. (2018, March 22). Raytheon demonstrates microwave and laser counter-drone system. *Unmanned Systems News*. Retrieved from http://www.unmannedsystemstechnology.com/2018/03/microwave-laser-counter-drone-system-demonstrated-us-army-exercise/.

29 Lykke, Arthur F. (1989). Defining Military Strategy, *Military Review*, 69(5):2-8. Retrieved from https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/504.

30 Dorff, Robert H (2001, February). A Primer in Strategy Development. In Cerami, Joseph R. and Holcomb, James F. (eds.) *Guide to Strategy*, US Army War College. Retrieved from https://www.comw.org/qdr/fulltext/01cerami.pdf, p.11.

31 Lafley, A. & Martin, R. L. (2013). *Playing to win: How strategy really works*. Boston, Massachusetts: Harvard Business Review Press.

32 See, for example: Cavanaugh, M.L. (2017, July 24). It's Time to End the Tyranny of Ends, Ways, and Means, Modern War Institute at West Point. Retrieved from https://mwi.usma.edu/time-end-tyranny-ends-ways-means/; King, Iain (2020, September 03). Beyond Ends, Ways, and Means: We Need a Better Strategic Framework to Win in an Era of Great Power Competition, Modern War Institute at West Point. Retrieved from https://mwi.usma.edu/beyond-ends-ways-and-means-we-need-a-better-strategic-framework-to-win-in-an-era-of-great-power-competition/; Webb, Andrew C. (2019). *Rethinking Strategy: Art Lykke and the Development of the Ends, Ways, Means Model of Strategy* (Master's thesis, US Army Command and General Staff College, Fort Leavenworth). Retrieved from https://nsiteam.com/social/wp-content/uploads/2019/06/Webb-Andrew-C.-Rethinking-Strategy-Art-Lykke-and-the-Development-of-the-Ends-Ways-Means-Model-of-Strategy-31-MAY-19.pdf.

33 Stolberg, A. G. (2012, October). *How nation-states craft national security strategy documents*. Strategic Studies Institute, US Army War College. Pennsylvania. Retrieved from https://publications.armywarcollege.edu/pubs/2201.pdf.

34 Du Mont, M. (2019, February 28). Elements of national security strategy. Retrieved from https://www.atlanticcouncil.org/content-series/strategy-consortium/elements-of-national-security-strategy/.

35 Rumelt, R. P. (2011). *Good strategy / bad strategy: The difference and why it matters*. London: Profile Books, p. 7.

36 Krasner, S. D. (2010, October 1). An orienting principle for foreign policy. *Policy Review*. Retrieved from https://www.hoover.org/research/orienting-principle-foreign-policy.

37 Stolberg, 2012 (above n. 33), p. 120.

38 Stolberg, 2012 (above n. 33), p. 122.

39 Lykke, Arthur F. (1989). Defining Military Strategy, *Military Review*, 69(5):2-8. Retrieved from https://cgsc.contentdm.oclc.org/digital/collection/p124201coll1/id/504.

40 Lafley, A. & Martin, R. L. (2013). *Playing to win: How strategy really works*. Boston, Massachusetts: Harvard Business Review Press.

41 Du Mont, 2019 (above n. 34), p. 4. Du Mont also proposes "identification and assessment of future challenges" as a step prior to the risk assessment; that step is by implication required as part of any risk analysis.

42 Rumelt, R. P. (2011). *Good strategy / bad strategy: The difference and why it matters*. London: Profile Books.

43 Cairney, P. (2020). *Understanding public policy: Theory and issues* (2nd ed.). Red Globe Press. Retrieved from https://www.google.co.nz/books/edition/Understanding_Public_Policy/vhC9DwAAQBAJ?hl=en&gbpv=0.

44 Bacchi, C. (2009). *Analysing policy: What's the problem represented to be?* (1st ed.) p. ix. Pearson Australia. Retrieved from https://www.google.co.nz/books/edition/Analysing_Policy/9DniBAAAQBAJ?hl=en&gbpv=0.

45 Sometimes the guiding policy may be presented as something other than a policy. For example, the Department of Defense (DoD) *Electromagnetic Spectrum Superiority Strategy* presents a 'vision', 'guiding principles', and 'strategic goals'. The guiding principles include elements of the strategic diagnosis, presenting in an unclassified form the key challenges of Electromagnetic Spectrum Operations. The strategic goals then present the guiding policy, providing statements of what DoD intends to do in five key areas, with multiple statements of "DoD will..." and "DoD must...". As statements of what will be done, these strategic goals are clearly statements of policy. See Department of Defense. (2020, October). *Electromagnetic spectrum superiority strategy*. Retrieved from https://media.defense.gov/2020/Oct/29/2002525927/-1/-1/0/ELECTROMAGNETIC_SPECTRUM_SUPERIORITY_STRATEGY.PDF

46 Eikmeier, D.C. (2007). Ends Ways Means: A Logical Method for Center-of-Gravity Analysis, *Military Review*, September-October, , p. 63. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20071031_art009.pdf.

47 Eikmeier, D.C. (2007). Ends Ways Means: A Logical Method for Center-of-Gravity Analysis, *Military Review*, September-October, pp. 62-66. Retrieved from https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20071031_art009.pdf; Lykke, 1989.

48 London Signal Intelligence Board and United States Communication Intelligence Board (1956, October 10). UK – US Communications Intelligence Agreement (UKUSA Agreement), cl. 7 and app. J. Retrieved from https://discovery.nationalarchives.gov.uk/details/r/C11536921

49 Rolfe, J. (2020, August 03). Five Eyes: more than technical cooperation, not yet an alliance. *Incline*. Retrieved from https://www.incline.org.nz/home/five-eyes-more-than-technical-cooperation-not-yet-an-alliance.

50 FCM (2019, July 30) *Five Country Ministerial communiqué: emerging threats*, London 2019. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822816/2019-07-24_Communique_FINAL_3.pdf.

51 FCM, 2019, above n. 50.

52 Fontaine, R. & Burton, B.M. (2010) *Eye to the Future: Refocussing State Department Policy Planning. Policy Brief*, Center for a New American Security. Retrieved from https://www.jstor.org/stable/pdf/resrep06259.pdf.

53 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, 177-248. Retrieved from https://treaties.un.org/doc/Publication/UNTS/Volume%20974/volume-974-I-14118-english.pdf.

54 s 10, Aviation Transport Security Act 2004 (Cth). (2018, November 29). Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/Details/C2018C00491.

55 s 2, Aviation Security Act 1982 (UK). Retrieved from https://www.legislation.gov.uk/ukpga/1982/36/contents.

56 Government of Canada (2020, July 1). *Criminal Code*, R.S.C., 1985, c. C-46, §77. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-46/FullText.html.

57 s 5, Aviation Crimes Act 1972. New Zealand Statutes. Retrieved from https://www.legislation.govt.nz/act/public/1972/0137/latest/DLM409117.html.

58 Destruction of aircraft or aircraft facilities. 18 US Code 32, Part I, Chapter 2, §32(b). Retrieved from https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section32&num=0&edition=prelim.

59 International Telecommunications Union (2020). *Radio Regulations*. Retrieved from https://www.itu.int/pub/R-REG-RR-2020.

60 Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011. (2011, June 16). *New Zealand Gazette*. Retrieved from https://gazette.govt.nz/notice/id/2011-go4051.

61 Robinson, H. (2021, July 3). We went through our Spectrum Manager to RSM. Provided all the info required. And got the approvals. *LinkedIn*. Retrieved https://www.linkedin.com/feed/update/urn:li:activity:6816251151361564672/?commentUrn=urn%3Ali%3Acomment%3A%28activity%3A6816251151361564672%2C6816836709028896769%29&replyUrn=urn%3Ali%3Acomment%3A%28activity%3A6816251151361564672%2C6816884903158915072%29.

62 Council of Australian Governments. (2015, July). *Australia's counter-terrorism strategy: Strengthening our resilience*. Retrieved from https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/Australias-Counter-Terrorism-Strategy-2015.pdf.

63 Radiocommunications Act 1992. (2019, August 30). Federal Register of Legislation. Retrieved from https://www.legislation.gov.au/Details/C2019C00262.

64 Australian Communications and Media Authority. (2019, April 23). *Radiocommunications (Unmanned Aircraft and Unmanned Aircraft Systems) Exemption Determination 2019*. Retrieved from https://www.legislation.gov.au/Details/F2019L00623/Download.

65 The most well-known RNSS is the Global Positioning System (GPS) system operated by the United States, but there are also analogous systems operated by Europe, Russia, and China. RNSS operates in the 5,010 MHz-5,030 MHz band. See Australian Communications and Media Authority. (2016, December 15). *Australian Radiofrequency Spectrum Plan 2017*. Retrieved from https://www.legislation.gov.au/Details/F2016L02001.

66 The UAS Exemption Determination only permits RNSS jammers to be used in the 2,400-2,483.5 MHz (2.4 GHz) and 5,725-5,850 MHz (5.8 GHz) which are the frequency bands typically used for C2 links for consumer drones. See Australian Communications and Media Authority, 2019, above n. 64.

67 Council of Australian Governments. (2009, 28 May). *Model Criminal Code*. Officers Committee of the Standing Committee of Attorneys-General (a committee of the Council of Australian Governments). Retrieved from https://www.pcc.gov.au/uniform/crime%20(composite-2007)-website.pdf.

68 *Model Criminal Code*, above n. 67, §4.2.4.

69 *Model Criminal Code*, above n. 67, §4.2.6.

70 *Model Criminal Code*, above n. 67, §4.2.3(1).

71 Government of Canada. (2017, September 21). *Radiocommunication Act*, R.S.C., 1985, c. R-2, §4(4). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/R-2/FullText.html.

72 Government of Canada. (2019, July 2). *Radiocommunication Act exemption Order (Jammers - Royal Canadian Mounted Police)*. SOR/2019-269. Retrieved from https://laws-lois.justice.gc.ca/eng/regulations/SOR-2019-269/FullText.html.

73 Government of Canada (2020, July 1). *Criminal Code*, R.S.C., 1985, c. C-46, §342.1. Retrieved from https://laws-lois.justice.gc.ca/eng/acts/c-46/FullText.html.

74 Canadian *Criminal Code*, above n. 73, §184(1).

75 Canadian *Criminal Code*, above n. 73, §184.4.

76 HM Government. (2019, October 21). *UK Counter-Unmanned Aircraft Strategy*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/_le/840793/Counter-Unmanned Aircraft Strategy.pdf.

77 *UK Counter-Unmanned Aircraft Strategy*, above n. 76, p. 5.

78 *UK Counter-Unmanned Aircraft Strategy*, above n. 76, p. 15.

79 *UK Counter-Unmanned Aircraft Strategy*, above n. 76, p. 19.

80 *UK Counter-Unmanned Aircraft Strategy*, above n. 76, p. 23.

81 *UK Counter-Unmanned Aircraft Strategy*, above n. 76, p. 27.

82 Air Traffic Management and Unmanned Aircraft Act 2021 (UK). Retrieved from https://www.legislation.gov.uk/ukpga/2021/12/enacted.

83 Centre for Protection of National Infrastructure (2021, April 06). *Countering Threats from Unmanned Aerial Systems*. Retrieved from https://www.cpni.gov.uk/countering-threats-unmanned-aerial-systems-0.

84 National Defense Authorization Act for Fiscal Year 2018. (2017). H.R.2810 - 115th Congress. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/2810/text; National Defense Authorization Act for Fiscal Year 2020. (2019). S.1790 - 116th Congress. Retrieved from https://www.congress.gov/bill/116th-congress/senate-bill/1790/text.

85 Preventing Emerging Threats Act. (2018). H.R.302 - 115th Congress. Retrieved from https://www.congress.gov/115/bills/hr302/BILLS-115hr302enr.pdf.

86 Cline, T. L., Lercel, D., Karabiyik, U. & Dietz, J. E. (2020, October). The current state of counter unmanned aerial system policy in the U.S. *International Journal of Aviation, Aeronautics, and Aerospace*, 7 (3). Retrieved from https://commons.erau.edu/ijaaa/vol7/iss3/11.

87 Under s26A of the Civil Aviation Act 1990, "If a pilot-in-command of an aircraft is alleged to have committed an offence" under the Civil Aviation Act 1990 or under the Civil Aviation Rules then a constable may require the operator of the aircraft "to give all information in that person's possession or reasonably obtainable by that person that may lead to the identification of the pilot". However, the operator of the aircraft has 10 working days to comply with the request. In practice this means that a person operating a drone in contravention of the rules can be required to provide their name and address but, having 10 working days to comply with the request, can leave the immediate area and never provide the identifying details. Unless the drone operator has been observed entering a motor vehicle then there is little prospect of the pilot's details being obtained. Even relying on motor vehicle registration may be unsuccessful if the motor vehicle is registered to a person other than the drone pilot. See Civil Aviation Act 1990. New Zealand Statutes. Retrieved from https://www.legislation.govt.nz/act/public/1990/0098/latest/whole.html

88 Robinson, H. (2021, July 3). We went through our Spectrum Manager to RSM. Provided all the info required. And got the approvals. *LinkedIn*. Retrieved https://www.linkedin.com/feed/update/urn:li:activity:6816251151361564672/?commentUrn=urn%3Ali%3Acomment%3A%28activity%3A6816251151361564672%2C6816836709028896769%29&replyUrn=urn%3Ali%3Acomment%3A%28activity%3A6816251151361564672%2C6816884903158915072%29.

89 Shelley, A. V. (2020). *Essays in the regulation of drones and counter-drone systems* (Doctoral dissertation, Victoria University of Wellington), pp. 238-239. Retrieved from http://researcharchive.vuw.ac.nz/handle/10063/8900.

90 ss82-87, Asia-Pacific Economic Cooperation (APEC 2021) Bill. (2019, November 14). Government Bill. Retrieved from http://www.legislation.govt.nz/bill/government/2019/0187/8.0/LMS180841.html.

91 s318, Civil Aviation Bill. Government Bill, 61-1. Retrieved from https://www.legislation.govt.nz/bill/government/2021/0061/latest/whole.html.

92 See, for example, Office of the Minister of Transport (2021). Civil Aviation Bill – New Policy Proposals. Retrieved from https://www.transport.govt.nz/assets/Uploads/3.-Civil-Aviation-Bill-New-Policy-Proposalswatermark.pdf.

93 s293, Civil Aviation Bill. Government Bill, 61-1. Retrieved from https://www.legislation.govt.nz/bill/government/2021/0061/latest/whole.html.

94 Department of Prime Minister and Cabinet. (2016, August). *National Security System Handbook*, p.7. Retrieved from https://dpmc.govt.nz/sites/default/_les/2017-03/dpmc-nss-handbook-aug-2016.pdf.

95 *National Security System Handbook*, above n. 94, p. 8.

96 *National Security System Handbook*, above n. 94.

97 *National Security System Handbook*, above n. 94.

98 *National Security System Handbook*, above n. 94.

99 Du Mont, M. (2019, February 28). Elements of national security strategy. Retrieved from https://www.atlanticcouncil.org/content-series/strategy-consortium/elements-of-national-security-strategy/.

100 HM Government. (2019, October 21). *UK Counter-Unmanned Aircraft Strategy*. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment data/_le/840793/Counter-Unmanned Aircraft Strategy.pdf.

101 Shelley, A. V. (2021) Quantifying the Cost of Drone-Related Threats in New Zealand. *National Security Journal*, 3(3), 8 November 2021. DOI: 10.36878/nsj20211108.03.

102 New Zealand Ministry of Transport. (2021b, June). *Social cost of road crashes and injuries 2020 update: June 2020*. Retrieved from https://www.transport.govt.nz/assets/Uploads/Social-Cost-of-Road-Crashes-and-Injuries-2020_final.pdf.

103 Shelley, 2021, above n 101.

104 New Zealand Ministry of Transport. (2021a, April 6). *Enabling Drone Integration: Discussion Document*. Retrieved from https://www.transport.govt.nz/assets/Uploads/Discussion/EnablingDroneIntegration.pdf.

105 Office of the Minister of Transport (2021). Civil Aviation Bill – New Policy Proposals. Retrieved from https://www.transport.govt.nz/assets/Uploads/3.-Civil-Aviation-Bill-New-Policy-Proposals-watermark.pdf.

106 Ardern, J. and Nash, S. (2019, March 21) New Zealand bans military style semi-automatics and assault rifles. Releases, New Zealand Government, https://www.beehive.govt.nz/release/new-zealand-bans-military-style-semi-automatics-and-assault-rifles.

107 Arden, J. (2019, March 19) PM House Statement on Christchurch mosques terror attack. Releases, New Zealand Government, https://www.beehive.govt.nz/release/pm-house-statement-christchurch-mosques-terror-attack.

108 See comments of Richard Munt, reported in Walters, L. (2020, August 14) Why changing gun laws isn't that simple. *Newsroom*. Retrieved from https://www.newsroom.co.nz/nzs-ongoing-fight-over-gun-laws.

109 Kirkness, L. (2020, July 2). Police confiscate AK-47, submachine gun, and meth in North Shore drug bust. *NZ Herald online edition*. Retrieved from https://www.nzherald.co.nz/nz/police-confiscate-ak-47-submachine-gun-and-meth-in-north-shore-drug-bust/TOLUWGAVIVQ7CUBXCJLARH-6C2I/.

110 NZ Herald (2021, August 16). Multiple police cars respond to firearms incident in Mangere. *NZ Herald online edition*. Retrieved from https://www.nzherald.co.nz/nz/multiple-police-cars-respond-to-firearms-incident-in-mangere/K5AYVH27TZ6GGUV44KOI3CYS7E/.

111 TVNZ (2021, June 30). AK-47 with 1500 rounds of ammo among items seized during Auckland meth labs raid. *1 News*. Retrieved from https://www.tvnz.co.nz/one-news/new-zealand/ak-47-1500-rounds-ammo-among-items-seized-during-auckland-meth-labs-raid.

112 New Zealand Police. (2021, July 5). Firearms Information Summary as at 5 Jul 2021. Retrieved from https://www.police.govt.nz/sites/default/files/publications/firearms-information-summary-5july2021.xlsx.

113 Webb, Sheridan (2021) From Hijackings to Right-Wing Extremism: The Drivers of New Zealand's Counter-terrorism Legislation 1977 - 2020. *National Security Journal*, 3(1). doi:10.36878/nsj20210409.04.

114 Webb, 2021, above n. 113.

115 Johanson, T. (2017) New Zealand's national security coordination. In: Hoverd W, Nelson N, Bradley C, editors. *New Zealand national security: challenges, trends and issues*. Albany: Massey University Press; p. 237–253.

116 Webb, 2021, above n. 113.

117 Downarowicz, T., Lacroix, Y. & Léandri, D. (2010, October 29). Spontaneous clustering in theoretical and some empirical stationary processes. ESAIM: *Probability and Statistics*, 4, pp. 256-262. DOI: 10.1051/ps:2008032.

118 New Zealand Ministry of Transport. (2021, April 6). E*nabling Drone Integration: Discussion Document*. Retrieved from https://www.transport.govt.nz/assets/Uploads/Discussion/EnablingDroneIntegration.pdf.

119 MOT, 2021, above n. 118.

120 Note that in its *Statement of Intent* the Civil Aviation Authority claims to use "intelligence-led, risk focussed activities to improve the effectiveness of aviation system regulatory policy and practice." See Civil Aviation Authority of New Zealand (2021b, June 17). Civil Aviation Authority 2021-2026

Statement of Intent, p. 12. Retrieved from https://www.aviation.govt.nz/assets/publications/statements-of-intent/CAA-Statement-of-Intent-2021-2026.pdf.

121 Office of the Minister of Transport (2021). Civil Aviation Bill – New Policy Proposals, p. 15. Retrieved from https://www.transport.govt.nz/assets/Uploads/3.-Civil-Aviation-Bill-New-Policy-Proposalswatermark.pdf.

122 MOT, 2021, above n. 118.

123 Leonardo (2019, March 04). *Focus on Falcon Shield*. Retrieved from https://uk.leonardocompany.com/en/news-and-stories-detail/-/detail/focus-on-falcon-shield; Shackle, Samira (2020, December 1) The mystery of the Gatwick drone. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

124 Shackle, Samira (2020, December 1) The mystery of the Gatwick drone. *The Guardian*. Retrieved from https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone.

125 Shackle, 2020, above n. 124.

126 Shelley, A.V. (2019, August 28). Enabling Counter-UAS and UAS-Detection Systems in New Zealand. Working Paper. Aviation Safety Management Systems Ltd. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3469332.

127 Cabinet (2019). Civil Aviation Bill: Confirmation of Key Policy Decisions. Minute of Decision, CAB-19-MIN-0167, para. 20. Retrieved from https://www.transport.govt.nz/assets/Uploads/Cabinet/2019-Civil-Aviation-Bill-Cabinet-minute.pdf.

128 New Zealand Ministry of Transport. (2020, March 5). Impact Statement: New civil aviation enforcement powers, pp. 19-20. Retrieved from https://www.transport.govt.nz/assets/Uploads/RIS-1-New-civil-aviation-regulatory-powers-Redacted-v2.pdf.

129 s334(1)(b), Civil Aviation Bill. Government Bill, 61-1. Retrieved from https://www.legislation.govt.nz/bill/government/2021/0061/latest/whole.html.

130 New Zealand Ministry of Transport. (2020, March 5). Impact Statement: New civil aviation enforcement powers, p. 39. Retrieved from https://www.transport.govt.nz/assets/Uploads/RIS-1-New-civil-aviation-regulatory-powers-Redacted-v2.pdf.

131 Shelley, A. V. (2021) Quantifying the Cost of Drone-Related Threats in New Zealand. *National Security Journal*, 3(3), 8 November 2021. DOI: 10.36878/nsj20211108.03.

132 Shelley, 2019, above n. 126.

133 Shelley, A. V. (2020). *Essays in the regulation of drones and counter-drone systems* (Doctoral dissertation, Victoria University of Wellington). Retrieved from http://researcharchive.vuw.ac.nz/handle/10063/8900.

134 New Zealand Ministry of Transport. (2020, March 5). Impact Statement: New civil aviation enforcement powers. Retrieved from https://www.transport.govt.nz/assets/Uploads/RIS-1-New-civil-aviation-regulatory-powers-Redacted-v2.pdf.

135 Civil Aviation Authority of New Zealand (2021, February 8). Civil Aviation Rules Part 101: Gyrogliders and Parasails, Unmanned Aircraft (including Balloons), Kites, and Rockets – Operating Rules. Retrieved from https://www.aviation.govt.nz/assets/rules/consolidations/Part_101_Consolidation.pdf.

136 C. Boorman, personal communication, 2020.

137 Radiocommunications Regulations (Prohibited Equipment – Radio Jammer Equipment) Notice 2011. (2011, June 16). *New Zealand Gazette*. Retrieved from https://gazette.govt.nz/notice/id/2011-go4051.