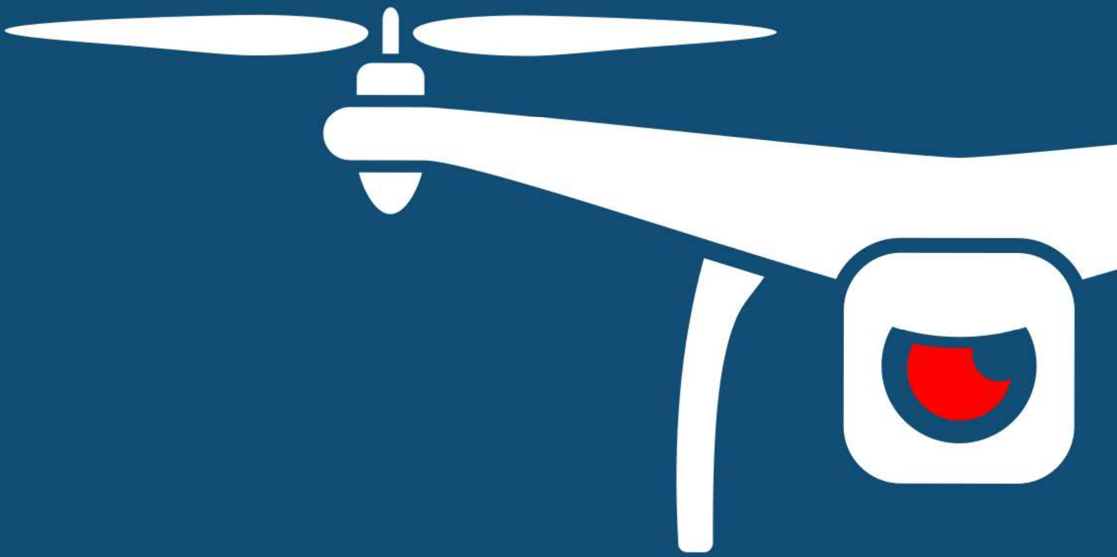
DRONESEC SUBMISSION

NATIONAL AVIATION POLICY ISSUES PAPER (DOITRDC)

31 October 2020



UAS HACKING, HARDENING AND DEFENCE

UAS PENETRATION TESTING
COUNTER-UAS CONSULTING
FORENSICS & INCIDENT RESPONSE
AERIAL THREAT SIMULATIONS
DRONE SECURITY MANAGEMENT PROGRAMS

SUMMARY

DroneSec is a fully Australian-owned, independently operated drone security consulting and advisory company specialising in cyber-physical systems, threat intelligence and counter-unmanned system services. We encourage, support and invest in the drone ecosystem and industry through the implementation of safe and secure drone programs. As an organisation, we provide early-adoption of unmanned aviation safety skills to children in both primary and high school, tertiary and adult-age.

We have relentlessly advocated for and developed drone security frameworks through both unmanned, aviation and cyber-security forums on a national and international scale. Our commitment to the industry is to ensure both hobbyist and commercial drone ecosystem have longevity and the minimisation of risk in the form of incidents. We have proactively identified, responsibly disclosed and helped remediate vulnerabilities and security issues in major airlines, UTM vendors, major drone manufacturers and drone software and C-UAS vendors since 2016.

DroneSec ("We") acknowledges the forward-thinking and safety-prioritisation approach of the Department of Infrastructure, Transport, Regional Development and Communications ("the Department"). We believe there is no greater time or need for this type of policy approach within the unmanned industry in Australia than right now. Whilst the paper has many varying topics, we have provided a position on this paper that is entirely through the lens of drone safety and security.

We thank you for the opportunity of being able to have our voice heard and look forward to future developments in this space. We use a number of references within the submission. Counter-Drone otherwise defined as (C-UAS) for Counter-Unmanned Aerial System, Unmanned Aircraft System Traffic Management (UTM), Commercial Off The Shelf (COTS), and Standard Operating Procedure (SOP).

1. DISCUSSION QUESTIONS

Do you agree with the proposed core principles for the National Emerging Aviation Technologies policy?

We agree with the proposed core principals and great need for this policy to ensure the innovation of drones is protected by embedding safe and secure drone operations in from the very start.

Drone security is made up of three sectors; the protection of friendly drones, the protection of the systems/infrastructure supporting drone operations (UTM) and the protection against rogue drones (C-UAS). This encompasses measures undertaken to enhance physical and cyber defence, incident management and response, training and education. The outlined Drone Security Framework has covered all these areas, however, was not clear on identifying the specific bodies that would enforce or govern the regulations once complete. Furthermore, specific Federal or State bodies should be identified that may be involved in the creation of the policy; for example, regulation changes behind Counter-Drone systems may involve various points of law including the Cybercrime Act 2001, CASA, ACMA and Federal and State Police.

It is also recommended that a central reporting body is nominated, that will oversee malicious drones' threats, receive reported incidents and model appropriate risk and threats for both industry and government. If law enforcements are to fulfil this function, they will require cooperation from cyber-security organisations and counter-drone vendors in the reporting of drone incidents to provide evidence-based review and policy adoption. Currently, there is no requirement for Counter-Drone vendors to report detection or mitigation of malicious drone events; this may prevent Government from valuable threat intelligence and adoption to new technologies, threats and threat actors. As the drone industry expands in the next 30 years, it will require regular reviews of what attacks or infringements have taken place against friendly drones (or drone supporting systems) or the threats assessed by Counter-Drone systems. This will help shape future policy and measure risk on an evidence-based approach. Similar to a centralised Cyber Security function within government, Australia may require a body that focuses on the digital and physical threats posed to and by drones.

Will the proposed approach to policy development adequately allow for the future direction, operations and investments of your business/organisation?

Currently, we have a number of organisations that are apprehensive of utilising drones in their commercial operations because of the risks posed. They are unsure who to look to for guidance on ensuring their systems are secure or if they follow the same cyber-security compliance requirements as the rest of their IT/OT infrastructure. In some cases, organisations are unsure if drone operations fall within their IT department or a new branch; often, this results in a lack of data security and privacy assessments resulting in loss of video, audio, telemetry data and in some cases, company secrets. Having a Government department form this National Policy and provide guidance on the aforementioned concerns will allow our organisation and others to minimise risk within our drone programs.

Another perspective is various drone manufacturers who are wary of their systems (with heavy payload capabilities) being purchased and used for malicious actions, such as contraband delivery or for terrorism. They seek guidance on how to vet their customers with this technology or, in the case one of their systems are used for malicious purposes, how to identify the operator and/or owner. In some cases, they seek both hardware (laser-etched) and software (certificate-based) mechanisms for identification purposes. National guidance and advice in relation to the Threat Assessment may provide these manufacturers with the confidence to sell knowing protections are adequately in place or their concerns are addressed with potential solutions available to them.

For organisations developing drone, UTM or C-UAS software technologies, there is an observed lack of safety and security process in their Software Development Life Cycle (SDLC). Sometimes, this can be due to the systems not being made for the 'aviation' sector, seeing emerging technologies such as drones in a different perspective. However, these systems will in fact eventually be part of, or affect, airspace operations. As a result, with the ability for COTS [1]drones to be both close-proximity to humans (<1m) and in upper airspace (<2500m), cyber-security vulnerabilities have a much higher impact than static, standalone digital systems that exist on the ground. In some cases, UTM vendors are building systems that can control over 500 autonomous, unmanned systems around populated areas; these systems are released without independent assurance activities taking place such as penetration testing, vulnerability assessments and secure code review practices. Simple policy guidance in this area from Government may provide long-lasting resilience to the sector in the form of safety and security.

Overall, the compounding feedback we receive from industry is that they are 1) not aware of the risks, 2) receive no Government guidance of handling those risks and 3) are not compelled by standards, compliance or regulation to identify, address and mitigate those risks. We believe that a Drone Security Framework would greatly minimise potential drone incidents, reducing the risk of knee-jerk reactions and providing proactive guidance to vendors creating and supporting drone systems, software and hardware.

What level of service and regulation do you expect from the Government?

For service, providing an on-going forum for listening to industry use cases and adopting the policy based on continued feedback. Given the autonomous, unmanned sector, it is likely the context of this environment will change very quickly. Creating long-lasting, systemic plans that allow for subtle but coherent change is important. Government is in the best position to identify what security or safety risks may exist within each environment, utilising their network of departments and resources.

For regulation, Government should create policy but clearly identify who and how it will be enforced. For example, if a vendor is developing a software that will manage or control multiple drones in airspace, it may be required to abide by testing guidelines of its product before commercial use in Australia. Government should clearly identify who would assess the process (whether Government or independent industry appointees), who would identify if the process was not followed, and who would enforce it in the case it is deliberately ignored.

[1] COTS: Commercial-Off-The-Shelf (can be bought at an easily accessible store by the public)

What are the most significant barriers to realising these opportunities?

As with many other countries, when large incidents occur with new technologies, the technology is often restricted until regulations or comprehensive compliance frameworks are able to 'catch up'. This unfortunately has occurred when drones have interfered with airport operations, been used for planning or carrying out terror attacks, or where sensitive vision from drones has been mistakenly leaked due to cyber-vulnerabilities.

Incidents will continue to occur if the drone industry is not provided leadership in the form of well-balanced regulation, which could result in restrictions and the stifling of innovation within the sector. Currently, the root cause of incident such as these include 1) a lack of cyber-security hygiene in developing drone systems and infrastructure, and 2) a lack of adaptable C-UAS laws regarding who can use counter-drone technology, when and how. For C-UAS, incorrect use of systems or unlimited use by the public may result in complete removal of the technology; however, that would increase the risk to Critical Infrastructure and areas that require adequate protection against drones. A framework should outline specifically who should be able to access, trial and use C-UAS systems, whilst maintaining the authority and privacy of authorised and legitimate drone users. This policy has the potential to be a world-first in setting precedent for C-UAS use that allows growth for the industry in reducing malicious drone use whilst ultimately powering the drone industry forward.

Law Enforcement have also had recent great success with drones in crime prevention, crash scene modelling, locating missing persons and clearing dangerous areas. However, public perception of drones shows a lack in understanding of privacy and could sway public opinion against the use of drones. Again, we believe careful addressing of these issues within a Drone Security Framework would clarify their use, identify their capabilities and also provide a forum for members of the public to share their concerns and have them addressed by a central body.

What issues or actions should the government prioritise to facilitate the growth of emerging aviation technologies?

For an immediate call to action, a methodology or maturity model should be implemented to ensure that the vendors developing drone (also: management and countermeasures) systems, software, applications or infrastructure should have their products undergo cyber-security testing. The risks of digital misconfiguration or vulnerable systems within the unmanned sector have an extremely high impact and should be reduced to prevent incidents in the sector. This will ensure minimisation of risk and longevity of the industry from a security and safety perspective.

Education should be available, supported and invested in (in some cases, required) from Government for both the public and private to undertake drone safety and security training. Training like this already takes place in primary and secondary schools, universities, and commercial organisations; however, cyber-security is hardly an inclusion of these courses. For example, when drones are used on critical infrastructure systems, their operators may undergo an additional training module highlighting the potential risks of how the data (vision, telemetry) is stored, transmitted and handled during and after. Whilst this area of risk traditionally fell within the remit of pure information-cyber-security operations, guidance from Government can help bridge the gap between industries.

To ensure the industry can mitigate the potential misuse or malicious use of rogue drones, the Government should prioritise a Counter-Drone (C-UAS) Framework that can provide guidance on applicable and legal use of both detection and mitigation options. The central aim of C-UAS should be to inhibit malicious drone use whilst supporting and enabling safe and secure legitimate operations. It is possible to have a C-UAS industry that works hand-in-hand with UTM with the right feedback from all parties involved.

To ensure law enforcement services are better equipped to forensically handle or investigate malicious drones, guidance should be provided to critical infrastructure on incident response. For example, many firms look to Government for guidance on cyber-security response capabilities even if they are legally allowed to conduct their own response actions. For critical infrastructure, they may develop their own SOP[2] based on Government advice. In the way of drone investigations, this may mean the difference in law enforcement receiving useful incident information, preventing future threats and apprehending offenders. We recommend a policy or standard on reporting malicious drone incidents or investigations similar to that of Airprox reports to further industry understanding and reaction to the threat.

To what extent should Australia's approach be harmonised with approaches taken in other countries?

On matters that are pertaining to drone registration, remote identification, counter drone systems and UTM, Australia should attempt to learn from some of the best practices from around the world.

On matters that pertaining to data security within emerging unmanned and aviation industries, both India and the United Kingdom have provided guidance on drone security measures. Several independent organisations such as the Cloud Security Alliance (CSA) have published their own guidelines as a form of a standard. Data security issues that are localised within Australia should follow existing Australian federal/state laws and expect foreign parties to abide by them.

Are there other issues that the Australian Government should consider?

Geofencing as a safety precaution rather than a countermeasure

Whilst we agree with much of the benefits of a Geo-fenced solution for UTM, we disagree it provides effective control against unauthorised drone use in designated sensitive security areas. Geofencing is a software-based capability and without secondary mitigation functions (such as C-UAS), the system can be easily bypassed by 1) Not updating a system 2) Removing the geo-fencing functionality 3) Using imported drones or systems from other countries or even 4) Spoofing geo-fenced areas to threaten legitimate drone operations.

From our experience Geo-fencing is a technique that prevents misinformed, accidental infringements and commercial systems from entering unauthorised areas. Geo-fencing as a real-time No-Fly-Zone geographic area to prevent legitimate users from entering law enforcement or first responder operations is a great preventative measure for the public. However, it better represents a barrier on a

[2] SOP: Standard Operating Procedure

highway to prevent vehicles from going off the road rather than a security system to prevent the cars leaving the road on by their own merit.

Threat Assessment and modelling

For the aforementioned 'Threat Assessment' section, the Government should consider not just a review or guidance or what systems (or configurations) can be used within critical infrastructure operations, but a policy. For example, a review might result in certain systems being 'whitelisted' for use in Critical Infrastructure operations. However, mishandling of data or a subsequent cyber-security compromise of a whitelisted drone system may undermine that selection process. As a result, regardless of the vendor make and model, steps should be followed to ensure the system and the storage, handling and transmission of data are safe and secure. This drips down through the software, hardware, applications, wireless protocols and supporting infrastructure; not just the drone system.

The Government should or should appoint a body to collate incident data and provide early-warning to critical infrastructure regarding drone threats or threats to drone ecosystems. Providing guidance on what has occurred in the past and what may occur, and how to respond, may help mitigate the effect of targeting by threat actors who utilise drones as a method of nefarious utility.