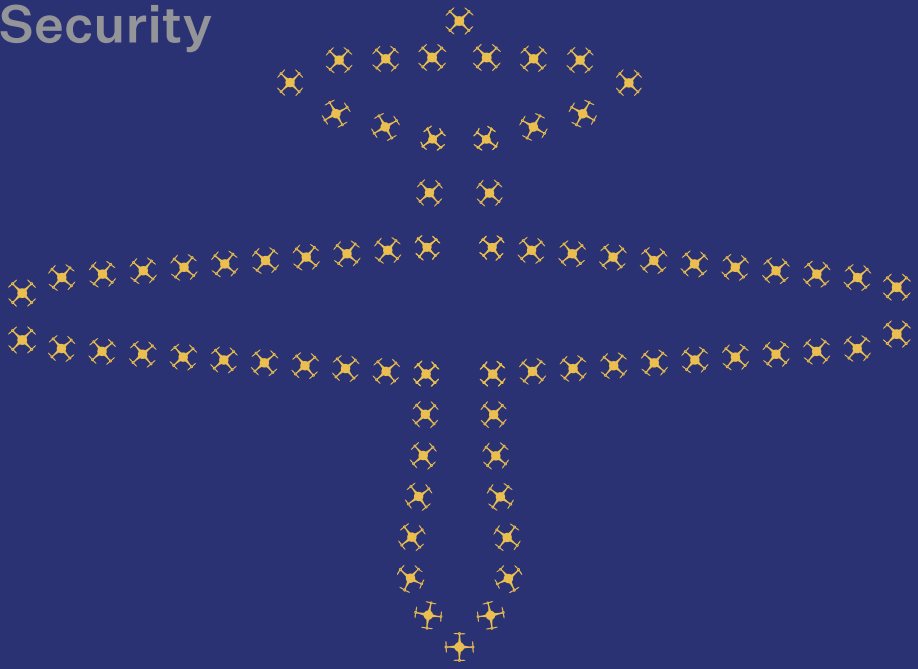
The Institute for Regional Security

Kokoda Paper No. 23



Countering Unmanned Aerial Systems

Rear Admiral Simon Cullen AM CSC (Ret'd)

About The Institute for Regional Security

The Institute for Regional Security is a registered charity and not-for-profit organisation. Its research is independent and non-partisan. The Institute For Regional Security does not take institutional positions on policy issues nor do sponsors have editorial influence. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the authors.

Published: September 2019 by The Institute For Regional Security

ISBN: 9780646809052

Cover Illustration: Inklab

Published and distributed by:

The Institute For Regional Security
2/10 Kennedy Street
(PO Box 4060), Kingston ACT 2604

Tel +61 2 6295 1555
Fax +61 2 6169 3019
Email info@ifrs.org.au
Web www.regionalsecurity.org.au

NATIONAL LIBRARY OF AUSTRALIA

A catalogue record for this book is available from the National Library of Australia

Kokoda Paper No. 23

Countering Unmanned Aerial Systems

By Rear Admiral Simon Cullen AM CSC (Ret'd)

The Institute
for Regional
Security

regionalsecurity.org.au

About the Institute

The Institute for Regional Security seeks to improve the quality and content of strategic thought and debate in Australia, with a focus on issues affecting Australian and regional security, stability and prosperity. The objectives of the Institute are to develop insights, ideas and impact through strategic dialogue, congresses, workshops, research papers, a peer-reviewed journal, and a Future Strategic Leaders program.

About the Author

Rear Admiral Simon Cullen AM CSC (Ret'd)

Simon Cullen is Deputy Chairman of the Institute for Regional Security. Simon retired from the Royal Australian Navy in late 2014, following a 38-year career. His career highlights included command at sea and ashore, extensive operational service and appointments to key senior military positions in the United States. Simon is now pursuing a portfolio of new challenges, ranging from consulting to working in the not-for-profit and charity sectors. He resides in Canberra.

Research and Editorial Assistant

Jack Ayoub

Jack Ayoub is a Research Officer at the Institute For Regional Security.

About our Sponsor

The Joint Counter Improvised Threat Task Force

The Institute For Regional Security is extremely grateful to the Joint Counter Improvised Threat Task Force (JCIT TF) for agreeing to sponsor this project and actively engage in all three workshops. Without the backing of the JCIT TF, this project would not have been possible. The JCIT TF assesses, plans, coordinates and executes Defence actions to counter improvised threats in order to ensure ADF operational freedom of action and force protection. JCIT TF maintains a deep understanding of current and emerging improvised threats and associated technology, contributes to counter threat network effects, and addresses gaps in current capability, whilst identifying and exploiting opportunities to counter emerging improvised threats.

Executive Summary

Unmanned aerial systems (UAS) pose an evolving and substantial threat to Australia's national security and the Australian Defence Force. While UAS use by a state or non-state actor on Australian soil, or against Australia's interests has yet to occur, it is only a matter of time before hostile actors will possess the capability to inflict harm upon Australia, its citizens and its national interests, if this is not already the case. Rapid advances in, and the proliferation of, increasingly more affordable technology, weaknesses in existing regulatory and legislative frameworks, the lack of an international framework of rules and norms for the use of UAS and the blurring of boundaries between sovereign and online communities, present a series of significant challenges to existing capabilities designed to counter the use of unmanned aerial systems by entities attacking Australia's national interests and those of our regional partners.[1]

[1] Australia's region has come to be defined as the Indo-Pacific (see Defence White Paper 2016 p13). For the purposes of this paper, Australia's region is more narrowly defined as South-East Asia and the South-West Pacific.

The objective of this research project was to answer the following questions:

Question 1.

How will evolving commercial and military generated unmanned aerial systems technology be employed by both state and non-state threat groups in the next 10 years and what emerging technologies may be incorporated to enhance these threats and what are the likely regional security impacts?

1. Non-state actors will likely use UAS to identify targets and carry out strategic decapitation operations; disable or disrupt critical infrastructure; influence the information narrative; and to establish and grow an insurgency.
2. State actors will likely employ UAS as part of an A2/AD strategy. They will also use UAS for influence operations; to establish command and control of operations; and to take direct action against targets. To be able to overcome UAS operating within an A2/AD strategy, C-UAS capabilities must be adaptive.

Question 2.

How will regional terrorist organisations gain asymmetric advantage from the increased availability of unmanned aerial systems knowledge and capability over the next decade and how might this threat be countered?

1. Terrorist organisations are already developing and deploying cheap and lethal UAS. The development and proliferation of AI technology has the potential to make relatively primitive UAS systems more effective.
2. The flow of technology associated with UAS to non-state groups is unlikely to be stemmed.
3. In the short-term terrorist organisations will employ UAS against vulnerable nations and their assets.
4. To counter the emerging regional threat and the longer term domestic threat, Defence should:
    a. Adopt a layered defence and countermeasure response strategy to detect, characterise and defeat UAS threat capabilities.
    b. Embrace a process of continual evolution.
    c. Consider adopting a pre-emptive C-UAS strike capability.
    d. Support the development of an international legal framework for the employment of UAS and lead initiatives to develop a regional framework.

Our response should be to invest in the understanding of the development of UAS technology and the deployment of capabilities in the region. Australia's knowledge of the emerging threat should be used in making countermeasure investment decisions. This should include kinetic, electronic and cyber means.

The workshops developed the following recommendations:

1. That the ADF should undertake the following:
    a. Support and participate in a whole-of-government counter unmanned systems community of interest.
    b. Incorporate UAS and C-UAS into future warfighting concepts.
    c. Incorporate UAS and C-UAS into exercises such as Autonomous Warrior.
    d. Incorporate UAS and C-UAS into exercises with international partners, including regional capacity building training.
    e. Regularly 'Red Team' Australia's UAS counter-measures to ensure these measures remain effective.
2. That the Government, more broadly, should:
    a. Support global regulatory initiatives and consider leading regional counter proliferation initiatives.
    b. Support the development of advanced C-UAS technology as part of Australian sovereign capability.
    c. Invest in a broad range of countermeasure technologies that provides Australia with a layered response option for dealing with UAS threats.
    d. Support domestic and regional unmanned system licensing arrangements.
    e. Establish an inter-agency counter unmanned systems coordination group with key stakeholders such as the National Intelligence Community, law enforcement agencies and government departments.

Section One
Project Plan

Research Focus

Initial discussions with the JCIT TF in late 2018 were centred on initiating a research project that addressed the two questions outlined above.

Subsequent engagement with the Task Force further refined the project. Given emerging threats, the JCIT TF partnered with IFRS in order to gain a better understanding of what the threat profile of unmanned systems might look like in the medium term (5-10 years) and to brainstorm new ways of thinking with regard to countering this emerging threat.

The objective of the project is therefore to determine broad technology themes and trends, understand how these trends will affect the threat environment in the medium term, and to recommend the areas and capabilities in which Defence should invest in in order to be best placed to counter this complex and dynamic threat to Australia's national interests.

The principal focus of the project has been on countering unmanned aerial systems as these systems currently present a significant challenge to national security.[2] Land and maritime systems have not been excluded from discussion but are not central to this project.

Approach

This study was conducted through a series of three workshops that engaged a diverse audience of industry, academia, the science and technology and law enforcement communities as well as the defence and national security community.

---

[2] J. J. Stubbs et al., "Counter Unmanned Aerial System Security Education," in 2018 International Carnahan Conference on Security Technology (ICCST), 2018, 1, https://doi.org/10.1109/CCST.2018.8585651.

Section Two
The Current and Future Operating Environment

The Current Unmanned System Threat

The project confirmed that the current threat posed by unmanned systems is widespread, growing, and more advanced than many realise.

Commentary provided by the Royal United Services Institute in the United Kingdom (U.K.) highlighted that strikes against Saudi infrastructure and the shooting down of a United States (U.S.) Predator in the Strait of Hormuz indicates that the Middle East is currently the geographical area in which *"UAS technology is evolving and maturing rapidly under combat conditions."*[3]

The use of weaponised unmanned aerial systems by non-state actors is becoming a growing concern. While most evident in the Middle East, this threat could emerge in Australia's region as technology, tactics, techniques and procedures continue to proliferate.[4] Perhaps, most importantly, a 2015 report by the U.S. Army War College Strategic Studies Institute highlighted that the use of UAS technology by non-state threat groups would *"likely have great influence on the conduct of future forms of conventional warfighting… because ultimately UAS represent artefacts belonging to the ongoing informational and robotics revolutions that has been taking place for decades."*[5]

---

[3] Alexander Balas, "UAVs in the Middle East: Coming of Age," RUSI (blog), July 10, 2019, https://www.rusi.org/commentary/UAVs-in-the-Middle-East-Coming-of-Age.

[4] Robert J. Bunker, "Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications" (Carlisle, Pennsylvania: U.S. Army War College, Strategic Studies Institute, August 2015), 12, https://apps.dtic.mil/dtic/tr/fulltext/u2/a623134.pdf.

[5] Bunker, 2.

This project also found that much of Australia's domestic and offshore critical infrastructure such as electricity grids and oil-fields are particularly vulnerable to kinetic attack by UAS because their design pre-dates the rapid technological advancement in UAS technology. Indeed, the government has acknowledged that protecting critical infrastructure from UAS is a priority. In order to protect critical infrastructure the government has proposed tightening regulations relating to the use of UAS in the vicinity of critical infrastructure and has recommended that the implementation of mechanisms such as geo-fencing be actively considered as technology continues to advance.[6] However it is the view of this project that once vulnerabilities are exposed, current options for effective mitigation are time consuming and expensive.

In addition to kinetic attack, one of the most likely threats posed by UAS is a nuisance and/or disruption attack. The recent disruption at Gatwick airport in the United Kingdom, highlights just how effective UAS is for conducting these attacks. The Gatwick incident appears to have been a deliberate but relatively simple incursion into controlled airspace that nonetheless took several days to resolve and led to a significant disruption of air services that had a flow-on affect across the European continent and the world.[7]

Whilst it is important to note that there has not been an instance where an unmanned aerial system has been used to coerce a leader of a State, the project believes that UAS technology is already at a stage where it is directly possible to use these systems to do so. This is a particular risk for smaller States which do not have the resources or capacity to mitigate and/or respond to this threat. Furthermore, any security measures put in place to counteract such a threat will be costly and will likely require foreign assistance to implement and maintain.

---

[6] "Australian Government Response to the Senate Standing Committee on Rural and Regional Affairs and Transport Report: Regulatory Requirements That Impact on the Safe Use of Remotely Piloted Aircraft Systems, Unmanned Aerial Systems and Associated Systems," 6.

[7] Gwyn Topham, Matthew Weaver, and Haroon Siddique, "Runway Reopens after Days of Drone Disruption at Gatwick," The Guardian, December 21, 2018, sec. UK news, https://www.theguardian.com/uk-news/2018/dec/20/tens-of-thousands-of-passengers-stranded-by-gatwick-airport-drones.

One of the major challenges in the current operating environment is how authorities are able to determine whether UAS operating in a particular airspace are friendly or adversarial. At present, there is under-regulated access and use of unmanned vehicles, particularly air vehicles for recreation. Their proliferation in the civil sphere is making it increasingly difficult for law enforcement and security agencies to determine whether impacts caused by their use are deliberate or accidental. A recent incident in Canberra, where a private drone operator was caught operating a drone within a "no-fly" zone in close proximity to Canberra airport highlights the nature of the threat with which law enforcement and security agencies are required to deal with and/or stop.[8] Whilst there was no disruption to, or collision with air traffic, the proliferation of UAS use and technological development is outpacing regulation which could ultimately reduce law-enforcement's ability to respond to serious threats.

Current methods employed in Australia for countering the threat posed by UAS against critical targets seem effective, however this is rapidly changing.

[8] "Media Release: Drone Infringement a Timely Reminder for Community: Police," Australian Federal Police, April 9, 2019, https://www.afp.gov.au/news-media/media-releases/drone-infringement-timely-reminder-community-police.

Factors reducing the effectiveness of current counter-measures include:

Availability and Price

- Prices for autonomous vehicles (aerial, surface and underwater) have dropped dramatically. An outlay of AUD $10,000 can buy an unmanned aerial system capable of carrying a 5kg payload. Similarly, in 2014 an American think-tank manufactured a military-grade drone using commercial electronics, a 3-D printed airframe and open source software for a total cost of USD $2,000.[9]
- Internationally, crowdfunding is being used as a means of raising finance to fund the rapid development of new technologies. Of particular note are news reports that suggest that Ukrainian nationals are using crowdfunding to develop UAS that are capable of by-passing Russian jamming systems.[10]

Rapid Technological Advancement

- The rapid pace of development in unmanned systems means that new technology is being manufactured and becoming internationally available within six months of development.
- 'Off-the-shelf' software and technology is capable of providing a low-cost and highly effective asymmetric capability for non-state actors. An attack on Russian forces and assets operating in Syria in January 2018 is a prime example of how affordable and readily accessible components such as lawn-mower engines, scrap wood and plastic can be developed into an airframe capable of carrying munitions that threaten conventional armed forces.[11]

---

[9] "Home-Made Drones Now Threaten Conventional Armed Forces."

[10] Christian Borys, "Crowdfunding a War: Ukraine's DIY Drone-Makers," The Guardian, April 24, 2015, sec. Technology, https://www.theguardian.com/technology/2015/apr/24/crowdfunding-war-ukraines-diy-drone-makers.

[11] "Home-Made Drones Now Threaten Conventional Armed Forces," The Economist, February 8, 2018, https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces.

- There is no longer domain specificity when it comes to unmanned systems and this presents additional challenges. For example, surface and sub-surface vehicles now have the capability to launch aerial vehicles.
- There is a vast amount of information which has lowered the threshold for creating UAS capability. This had led to the development of advanced libraries of threat information[12] that are available online and readily accessible to the general public.

Legislative and Regulatory Frameworks

- Domestic and international legislative and regulatory frameworks are assessed as being inadequate for dealing with rapid developments in the use of unmanned systems, due to:
  - Regulations and legislation being effective in situations where the adversary is bound by the same rules. In the case of a non-state actor, there is no incentive or reason to comply with regulations, making regulatory mechanisms redundant.
  - Current legislation is at risk of being out-paced by rapid technological advancement and proliferation in UAS use.
  - Current legislation is unclear as to which agency has jurisdiction to respond to and mitigate UAS threats, particularly when dealing with a threat to Australian interests both on and off-shore.
  - Where ambiguity exists, there is a risk that unclear legislation could cause a delay in response to, and mitigation of an active threat.
- There is no agreed international approach to countering the threat posed by unmanned systems.

[12] This term refers to UAS threat generation from open-source information. The vast amount of information now available online has lowered the threshold for creating UAS capability.

Future Unmanned System Threats

Exponential technological development makes it very hard to predict the threat posed by unmanned systems 10 years from now. Industry advice was that there could be up to four development cycles for these vehicles over the next decade. According to Silicon Valley start-up *Toptal*, investment in drone technology is continuing to increase, prices of critical UAS components is decreasing and there has been significant technological developments in artificial intelligence and analytics.[13]

It was highlighted that the mobile telephone industry provides the impetus for development of the essential components of unmanned vehicle technology and this is advancing at a very rapid rate.

Consistent technology themes that emerged during the project included:

Swarming[14] – Swarm technology already exists and the use of multiple unmanned aerial systems concurrently against a target(s) is a very real threat. The first recorded and tactically effective swarm attack occurred in Syria in January 2018. While small and cheap, the sum of their parts provides a greater threat than any one device. There is the potential for swarm capability to be overestimated in the near-term but underestimated in the medium to long term. As Artificial Intelligence continues to develop, swarm intelligence will allow UAS to undertake and complete larger and significantly more complex tasks due to the opportunity that AI provides in terms of creating networks that act independently of human control.[15]

---

[13] Francesco Castellano, "Commercial Drones Are Revolutionizing Business Operations," Toptal Finance Blog, 2016, https://www.toptal.com/finance/market-research-analysts/drone-market.

[14] In this context, swarming refers to the use of multiple UAS to conduct an attack against a target. However, due to the rapid advancement of AI technology, the definition of swarming could evolve to include multiple systems performing certain tasks without human direction. It is expected that these systems would be able to make decisions based on the environment in which they are operating.

[15] Castellano.

Machine Vision – With regard to robotics, Australian research and product development is world-leading. However, as the capability is developed that will enable unmanned systems to perceive their environment and respond to it, counter methodologies such as the jamming technique that was recently used by U.S. Marine Corps to destroy an Iranian drone that posed a threat to an amphibious assault ship, could quickly become redundant.[16]

Machine Learning / Artificial Intelligence (AI) – There have been significant advances in the area of machine learning. At this point in time, unmanned vehicles still require a human involved in the control loop. Once AI technology becomes integrated into unmanned platforms, these systems will become truly autonomous. Whilst it is unclear when UAS will make the transition to becoming truly autonomous, this development would have significant implications for defence capabilities and national security.

AI supported decision-making will be far quicker than human decision-making and while having humans involved in the decision-making loop is desirable from a western and liberal government perspective, it is not likely to be adhered to by non-state actors or terrorist threat groups. This will need to remain front-of-mind when considering, developing and implementing counter-measures.

Blurring of Boundaries – The emerging generation of technology users do not view themselves as distinct from their technology. They have only known a world connected by the World Wide Web. Consequently, the presence of online communities, at arms-length from the rule of law that transcend national boundaries and loyalties, has grown markedly. This will present new and testing challenges to governments, existing legislation, law-enforcement and security agencies and to the ADF.[17]

---

[16] Mosheh Gains, Courtney Kube, and Adam Edelman, "U.S. Marines Jam an Iranian Drone in the Gulf, Destroying It," NBC News, July 19, 2019, https://www.nbcnews.com/politics/national-security/trump-says-u-s-navy-ship-shot-down-iranian-drone-n1031451.

[17] For more information on the Blurring of Boundaries see: Brigitte Jordan, "Blurring Boundaries: The 'Real' and the 'Virtual' in Hybrid Spaces," Human Organization; Oklahoma City 68, no. 2 (Summer 2009): 183.

Globalisation and technological advances have blurred traditional state boundaries and afforded multi-national companies unprecedented power. A world where some of these companies begin to act like non-state actors is not impossible.

A potential outlier threat is an organisation or individual who, through access to open source technology, develops a system that is unique, highly capable and previously unknown to intelligence agencies.

Countering the Current Unmanned Systems Threat

The current approach to countering unmanned aerial systems involves detecting and monitoring the vehicle within an area of interest, attempting to identify it, and then mitigating the threat as required.

Current options for managing the threat include the following:

- Warning the controller.
- Denying access to a designated area using a combination of hardware and software options.
- Disrupting communication, navigation and targeting links.
- Seizing control of the vehicle through cyber means.
- Physical incapacitation.

A key factor to be considered when developing countermeasures is the definition of mission kill. For example, is mission kill the physical destruction of a vehicle or something more or less than that? Each case of a UAS incursion will present different threats and will likely require a range of response options to nullify the threat. Definitions of mission kill should be malleable depending on the sophistication, nature and urgency of the threat.

When designing countermeasures, potential second and third order effects to people and infrastructure must be considered. As reported by The Guardian, military drones currently crash, on average, twice a month in both conflict zones and civilian environments.[18] This has

---

[18] Jamie Doward, "Military Drone Crashes Raise Fears for Civilians," The Observer, June 9, 2019, sec. World news, https://www.theguardian.com/world/2019/jun/09/two-military-drones-crashing-every-month.

raised concerns about the safety of civilians and highlights that as the proliferation of UAS continues, the risk to civilian life from physical incapacitation of a drone will increase. Uncontrolled landings and/or creation of a debris field will pose safety risks to civilians. Furthermore, the use of GPS and radio frequency jamming may also impact other systems in the vicinity reliant on those systems such as civilian aircraft.

While unmanned vehicle swarms are identified as an emerging threat, they are also currently being tested and implemented as a means of protecting valuable assets. In February, Britain's Defence Secretary announced that "swarm squadrons" would be deployed by the British armed forces in the coming years. Swarming can confuse enemy sensors, provide search and rescue functions and protect expensive, human-centric defence assets.[19] Similarly, Australia has indicated its intention to develop the unmanned aerial "Loyal Wingman" concept as a mechanism for defending the Joint Strike Fighter.[20] Nonetheless, whilst countermeasures presently available to Australia were considered adequate in the workshops, they could be rendered ineffective through employment of counter countermeasures as the quality of technology continues to improve and proliferate.

The workshop participants concluded that the Australian Defence Force should practice the use of countermeasures against unmanned vehicles in all operating environments, on a regular basis.

---

[19] Thomas McMullan Lee Dave, "How Swarming Drones Will Change Warfare," BBC News, March 16, 2019, sec. Technology, https://www.bbc.com/news/technology-47555588.

[20] Christopher Pyne and Steven Ciobo, "Media Release: Australian-Designed Unmanned 'Loyal Wingman' Aircraft to Be Developed with Industry," Text, Department of Defence, February 27, 2019, https://www.minister.defence.gov.au/minister/cpyne/media-releases/australian-designed-unmanned-loyal-wingman-aircraft-be-developed.

Future Countermeasure Capabilities

Investment in countermeasure capabilities will need to be regularly undertaken to ensure they remain effective as the threat rapidly evolves. It may be hard to convince governments to invest in defeating threats that have yet to eventuate. However, in order to avoid "black swan"[21] events, the project concluded that investment in developing countermeasures in line with predicted trends and developments in technology is becoming urgent.

As for other aspects of warfare, the project considers that a layered defence system will provide the best solution for defence against unmanned vehicles. This will entail longer range detection, improved identification, and soft and hard kill response options. While threat platforms may be relatively cheap to acquire and operate, defence systems will be much more expensive. In addition, these systems, such as Israel's "Drone Dome", are mostly still in the development stage and are not yet operational.[22]

Advice provided during the workshops suggested that Defence's objective should not be to develop and operationalise the ideal future proof technology. Rather, Defence should adopt a process of continual evolution with regard to counter UAS systems and technology in order to keep pace with the rapidly evolving threat environment. This may require that no single solution receive a majority of investment. Defence needs to remain agile in its ability to respond to changes in technology in order to safeguard against Australia's countermeasure capabilities being rendered redundant by changes in technology.

---

[21] For the purposes of this paper a black swan is an unpredictable event that is beyond what is normally expected of a situation and has potentially severe consequences. Black swan events are characterized by their extreme rarity and their severe impact.

[22] "Multi-Layered Dome System to Combat Drone Threat," Australian Aviation (blog), February 25, 2019, https://australianaviation.com.au/2019/02/multi-layered-dome-system-to-combat-drone-threat/.

The employment of techniques such as pre-emptive strikes on unmanned aerial systems before they are launched and supporting the development of an international legal framework for regulation of unmanned vehicles and proliferation of technology will also be important. Indeed, as a middle power, Australia may wish to consider leading the regional effort to develop a legal framework for the identification, detection and use of UAS at a time when existing rules and norms are being challenged by state and non-state actors alike.

Section Three
Regional Scenarios

During the workshops four table-top scenarios were exercised to further explore the use of unmanned systems by non-state actors and regional terrorist groups in order to identify countermeasures that could be employed. Scenarios were situated in the South West Pacific, South East Asia, Australia's Sea Air Gap and the broader Indo Pacific.

In a regional context in the medium term, unmanned vehicles could be used by non-state actors or terrorist groups to:

- Act as a communications node.
- Disrupt and/or destroy technology networks and transnational communications networks (including undersea cables).
- Gather intelligence
- Identify targets for kinetic attack.
- Assassinate key State/Military leaders
- Influence and shape the information narrative.
- Create counter narratives to discredit the ability of governments to provide security for its citizens.
- Implicate third parties. (false flags)
- Disable critical infrastructure.
- Provide logistical support in order to sustain an attack or insurgency.

In response, unmanned vehicles could be used by regional governments to:

- Establish situational awareness and gather intelligence.
- Detect, identify and defeat adversaries.
- Provide communications relay.
- Support command and control.
- Prevent incident escalation.
- Provide logistic support.
- Assist in restoring capabilities, assets and critical infrastructure that has been damaged.

If Australia was invited by a regional friend or partner nation to provide support to counter non-state actors or regional terrorist groups, a suite of countermeasures adaptable to the operating environment would be needed by the ADF, including:

- Mobile and fixed solutions that provide a depth of response options. These systems will have to be adaptable in order to deal with a wide variety of threats.
- Systems that protect and allow valuable assets to operate at a safe distance from the threat itself.
- An ability to capture, examine and repurpose enemy UAS.

There may be regional and global implications if Australia was to develop an advanced counter unmanned vehicle capability. These include:

- The increased risk associated with regional partners who are less aware of threat capabilities.
- Australia being considered a partner of choice in providing this niche capability which could lead to an over-commitment of C-UAS assets.

- Some nations may consider advanced countermeasure capabilities to be offensive weapons as they may be able to overcome Anti-Access/Area Denial (A2AD) systems. If these systems are not clearly defensive in nature, there is potential for misperception and miscalculation amongst Australia's regional neighbours.
- The need to deal with fully autonomous threats without human involvement, presents significant legal, ethical and legislative challenges.
- The need for forensic attribution. Evidence collection to expose potential adversarial activity will be vital in order to avoid miscalculation or a misunderstanding of the nature of the threat.
- Australia potentially assuming the lead amongst Five Eyes partners for certain countermeasure capabilities. This could have significant budgetary and resourcing implications but it has the potential to generate export revenues.

The project considered that it was not possible to prevent the proliferation of unmanned vehicle technology to non-state and terrorist actors, due to its availability through global supply chains.

Suggested Areas for Research

Collaboration between Defence, industry and academia will be critical as the ADF seeks to counter future unmanned vehicle threats. While collaboration exists now through programs such as the Asymmetric Threat Response Program and the Next Generation Technologies Fund Initiative of the Counter Improvised Threat Grand Challenge, it needs to become an embedded process across all environments. Existing hurdles to expedient collaboration need to be removed. To achieve favourable outcomes, there should be a three-way dialogue where issues of Intellectual Property (IP) protection, competition for research funding and probity issues do not impede the discussion. Consequently, appropriate ICT architecture needs to be implemented in order to make three-way collaboration secure. Currently, there is too great a lag between initial research and development of a capability, and its deployment on operations.

To get the attention of government, industry and academia will need to demonstrate how unmanned vehicles can make a positive contribution to productivity and innovation.

Future unmanned vehicle capability and technology requirements include:

- The need for a counter swarm capability. Existing counter unmanned aerial system strategies work for a one-on-one situation, but are not as straightforward in a one-to-many scenario.
- Swarms that can communicate with one another and then adapt to a given situation without human intervention.
- Use of unmanned vehicles as part of future counter-unmanned vehicle systems.
- A variety of detection, characterisation and response techniques and options for responding to lower-level threats. For example, behavioural analysis of these vehicles is one mechanism that could enhance identification, enable a timely process for establishing the nature of the threat, and ultimately, determining the most effective response.
- Improved command and control systems that enhance situational awareness and the quality of decision-making in the operational theatre.
- Detection capabilities that stretch beyond the range of existing sensors in order to provide early warning.
- Improved sensor integration.
- Use of quantum navigation for improved accuracy and reduction in dependence on GPS systems.
- Inclusion of UAS in the Common Operating Picture.

The advances identified above have significant military applications. For example, being able to undertake discrete, persistent surveillance, think faster than your opponent or achieve collective lethal effects over a wide area, offer significant tactical, operational and strategic advantages.

Leaders of small and medium enterprises working in the field believe that Australia has the potential to develop the required UAS technologies locally. Australia has a wealth of technological expertise, has a number of universities and research institutions that are among the best in the world, and has a growing demographic of younger-generations to whom the use of advanced technology is second-nature. In addition, developing a domestic manufacturing base could reduce Australia's reliance on other states for components and hardware and software updates for countermeasure capabilities. This would strengthen Australia's ability to respond emerging UAS threats.

In addition to these operational and technical suggestions for research, there is a need to examine the policy questions, some of which have been raised in this report, more comprehensively and in more detail. These include:

1. Clarity in departmental responsibilities relating to the regulation of UAS and C-UAS activities that involve Australian interests.
2. Examination of domestic and international legal issues, particularly with respect to jurisdiction and powers to:
    a. Protect responders
    b. Gather and disseminate intelligence
    c. Conduct C-UAS activities.
3. Lead responsibility to ensure collaboration amongst regional neighbours.

Section Four
Recommendations

In conclusion, the unmanned and autonomous vehicle threat is developing at a rapid rate. It is only a matter of time before the threat extends into Australia's region. Careful investment now in a broad range of countermeasure technologies that can be tested and trialled over the next decade will lead to optimal solutions for the Australian Defence Force. These technologies can be provided by Australian industry if appropriate policies regarding sovereignty, investment and R&D are put in place.

The workshops developed the following recommendations:

1. That the ADF should undertake the following:
    - **a.** Support and participate in a whole-of-government counter unmanned systems community of interest.
    - **b.** Incorporate UAS and C-UAS into future warfighting concepts.
    - **c.** Incorporate UAS and C-UAS into exercises such as Autonomous Warrior.
    - **d.** Incorporate UAS and C-UAS into exercises with international partners, including regional capacity building training.
    - **e.** Regularly 'Red Team' Australia's UAS counter-measures to ensure these measures remain effective.

2. That the Government, more broadly, should:

   a. Support global regulatory initiatives and consider leading regional counter proliferation initiatives.

   b. Support the development of advanced C-UAS technology as part of Australian sovereign capability.

   c. Invest in a broad range of countermeasure technologies that provides Australia with a layered response option for dealing with UAS threats.

   d. Support domestic and regional unmanned system licensing arrangements.

   e. Establish an inter-agency counter unmanned systems coordination group with key stakeholders such as the National Intelligence Community, law enforcement agencies and government departments.

Section Five
Further Reading and References

"Australian Government Response to the Senate Standing Committee on Rural and Regional Affairs and Transport Report: Regulatory Requirements That Impact on the Safe Use of Remotely Piloted Aircraft Systems, Unmanned Aerial Systems and Associated Systems." Canberra, Australia: Department of Infrastructure, Regional Development and Cities, November 2018. https://www.infrastructure.gov.au/aviation/publications/files/Government-Response-RPAS-UAS-regulatory-requirements.pdf.

Balas, Alexander. "UAVs in the Middle East: Coming of Age." RUSI (blog), July 10, 2019. https://www.rusi.org/commentary/UAVs-in-the-Middle-East-Coming-of-Age.

Borys, Christian. "Crowdfunding a War: Ukraine's DIY Drone-Makers." *The Guardian*, April 24, 2015, sec. Technology. https://www.theguardian.com/technology/2015/apr/24/crowdfunding-war-ukraines-diy-drone-makers.

Bunker, Robert J. "Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Implications." Carlisle, Pennsylvania: U.S. Army War College, Strategic Studies Institute, August 2015. https://apps.dtic.mil/dtic/tr/fulltext/u2/a623134.pdf.

Castellano, Francesco. "Commercial Drones Are Revolutionizing Business Operations." Toptal Finance Blog, 2016. https://www.toptal.com/finance/market-research-analysts/drone-market.

Doward, Jamie. "Military Drone Crashes Raise Fears for Civilians." *The Observer*, June 9, 2019, sec. World news. https://www.theguardian.com/world/2019/jun/09/two-military-drones-crashing-every-month.

Gains, Mosheh, Courtney Kube, and Adam Edelman. "U.S. Marines Jam an Iranian Drone in the Gulf, Destroying It." NBC News, July 19, 2019. https://www.nbcnews.com/politics/national-security/trump-says-u-s-navy-ship-shot-down-iranian-drone-n1031451.

"Home-Made Drones Now Threaten Conventional Armed Forces." *The Economist*, February 8, 2018. https://www.economist.com/science-and-technology/2018/02/08/home-made-drones-now-threaten-conventional-armed-forces.

Jordan, Brigitte. "Blurring Boundaries: The 'Real' and the 'Virtual' in Hybrid Spaces." *Human Organization; Oklahoma City* 68, no. 2 (Summer 2009): 183.

Lee, Thomas McMullan, Dave. "How Swarming Drones Will Change Warfare." BBC News, March 16, 2019, sec. Technology. https://www.bbc.com/news/technology-47555588.

"Media Release: Drone Infringement a Timely Reminder for Community: Police." Australian Federal Police, April 9, 2019. https://www.afp.gov.au/news-media/media-releases/drone-infringement-timely-reminder-community-police.

"Multi-Layered Dome System to Combat Drone Threat." *Australian Aviation* (blog), February 25, 2019. https://australianaviation.com.au/2019/02/multi-layered-dome-system-to-combat-drone-threat/.

Pyne, Christopher, and Steven Ciobo. "Media Release: Australian-Designed Unmanned 'Loyal Wingman' Aircraft to Be Developed with Industry." Text. Department of Defence, February 27, 2019. https://www.minister.defence.gov.au/minister/cpyne/media-releases/australian-designed-unmanned-loyal-wingman-aircraft-be-developed.

Stubbs, J. J., C. G. Kouhestani, B. L. Woo, and G. C. Birch. "Counter Unmanned Aerial System Security Education." In *2018 International Carnahan Conference on Security Technology* (ICCST), 1–5, 2018. https://doi.org/10.1109/CCST.2018.8585651.

Topham, Gwyn, Matthew Weaver, and Haroon Siddique. "Runway Reopens after Days of Drone Disruption at Gatwick." *The Guardian*. December 21, 2018, sec. UK news. https://www.theguardian.com/uk-news/2018/dec/20/tens-of-thousands-of-passengers-stranded-by-gatwick-airport-drones.

Annex A

Strengths, Weaknesses, Opportunities and Threats (SWOT) Analysis

During project workshops, a SWOT analysis was undertaken to assess Australian capabilities to counter unmanned systems. The outcomes were as follows:

Strengths

- Membership of the Five Eyes' network and the sharing of intelligence and technologies.
- The Australian intelligence system and community.
- Bipartisan support for engagement in Australia's region.
- Whole of government coordination.
- Enduring ADF focus on force protection.
- Establishment of the Defence Cooperative Research Centre for Trusted Autonomous Systems.
- Capability of Australian SME currently working in the counter unmanned systems field, and
- A highly skilled and educated Australian workforce.

Weaknesses

- Scale of the problem – It is difficult to decide what to protect and how to protect it.
- Lack of international regulation and continued proliferation of technologies.
- Likelihood of limited warning time of attack.
- General weaknesses in Australia's manufacturing industry.
- Expensive ADF assets are vulnerable to attack from low cost systems.
- Australia has a significant investment problem. Currently, Research and Development is primarily funded by foreign firms.

Opportunities

- Designate the Vice Chief of the Defence Force (VCDF) as the ADF champion for countering unmanned systems.
- Leverage technologies arising from the U.S. Fourth Offset Strategy.
- Encourage and foster Australian innovation through Defence grant programs.
- Build counter unmanned system capacity in Australia's region.
- Support, and consider leading, international efforts to regulate proliferation of unmanned system technology.
- Support international efforts to develop a code of conduct for incorporation of artificial intelligence into weapon systems for unmanned aerial systems.
- Increased experimentation, and
- The growth of small start-up communities which present viable opportunities for investment with a view to encouraging big primes to integrate solutions.

Threats

- Rapid advancement of unmanned vehicle technology and proliferation in Australia's region.
- High potential lethality of unmanned systems.
- The acquirement of capabilities is often a slow process. This will challenge Australia's ability to effectively respond to changes in the nature of the threat posed by unmanned aerial systems.
- Lack of engagement in the region. Regional partners may not want Australia to engage for a variety of reasons, and
- Any effective counter unmanned system capabilities that Australia deploys in the region will generate a response.