EPE
Trusted to Protect

White Paper

RPAS, Evolving Threats & Counter RPAS Technology

June 2019

www.**epequip**.com

Contents

Please Note: This white paper presents information that is accurate at the time of release. It captures the legislation in Australia and is reflective of principles in New Zealand.

Introduction

This White Paper has been produced to assist in the understanding and consideration of technology options to counter the threat posed by Remotely Piloted Aircraft Systems (RPAS) / Unmanned Aerial or Aircraft Systems (UAS) / Unmanned Aerial Vehicles (UAV) / Drones. The paper provides an initial introduction to RPAS and Counter RPAS (C-RPAS) also know as Counter UAS (C-UAS) characteristics and briefly outlines current leading technologies, for readers that have had limited exposure to this threat domain. It should be read in the context of the current threat, and with the understanding that technological aspects of both RPAS and C-RPAS systems continue to change and develop. This paper will enable the reader to understand current C-RPAS capabilities and technologies with consideration to strengths, weaknesses and constraints, which may be functional, technical, legislative or some combination of the three.

Agencies and organisations should consider how each of the general RPAS / C-RPAS considerations listed may affect their operational environment in the development of their C-RPAS strategy as well as ways in which they may want to encourage and influence areas such as emerging technologies, amendments to legislation, training as well as possible integration of capabilities.

RPAS Characteristics

1. **RPAS Types.** RPAS categorisation informs C-RPAS type and employment considerations:

    a. **Fixed wing.** Static wings; greater speed; longer range; longer loiter; cannot hover (always forward movement); more difficult to control.
    b. **Rotary wing.** Single or multi-rotor; vertical take-off / landing; hover well; easier to control; have reduced endurance & range compared to fixed wing.
    c. **Power lift / hybrid.** Combine benefits of fixed and rotary systems; complexity means these RPAS are (currently) less common.
    d. **Airship (aerostat).** Low speed; extended loiter; low power usage; poor vertical manoeuvrability.

2. **RPAS Classes.** RPAS classification impacts threat assessment, in particular for detection thresholds and payload options. Classification by gross mass (ie includes payload) is as follows:

    a. **Micro.** 100 grams (g) or less;
    b. **Very small.** 100 g and less than 2 kg;

c. **Small.** 2 kg and less than 25 kg;
d. **Medium.** 25 kg and less than or equal to 150 kg; or
e. **Large.** Greater than 150 kg.

3. **Communications Link.** RPAS require a communication link between the control station (usually on the ground) and the RPAS when under operator control; and select C-RPAS systems can target this interface. Primary targetable links include:

   a. **Radio Frequency (RF).** Radio waves propagate from both a control transmitter/ antenna and RPAS in a specific radio frequency bands. Both the RPAS and Controller have a radio receiver set to this specific frequency bands in order to receive the operating signal.
   b. **WiFi.** The RPAS and its control station communicate over a wireless signal via an extended range WiFi protocol. The RPAS will include a wireless adapter that translates data that is transmitted, via an antenna, to the controller.
   c. **Global Navigation Satellite System (GNSS) spectrum.** The RPAS accesses satellite navigation systems that provide autonomous geo-spatial positioning with global coverage. This term includes GPS, GLONASS and other regional systems.

4. **Autonomy.** Autonomy refers to the RPAS's ability to operate independently of the communications link. C-RPAS systems need to be able to mitigate autonomous aspects of RPAS operation, which can include:

   a. **Frequency Hopping.** This function (eg LightBridge) switches between frequencies to avoid congested communications environments or to counter frequency interdiction. (Note: Frequency hopping is not really autonomy. It is the RF link for the RPAS and Controller that finds a solution to the connection disturbance without controller input).
   b. **Return to Home.** This function enables the RPAS to return to the control station location if the communications link / frequency is interrupted. It requires a GPS capability.
   c. **Pre-programmed flight.** This function utilises GNSS and enables the RPAS to operate in a designated area without interaction with the control station. This is important as the RPAS can fly out of the operator's line of sight and negates the ability to target the communications link.
   d. **Inertial Guidance.** This function utilises an electronic system that continuously monitors the position, velocity, and acceleration of a vehicle and thus provides navigational data or control without need for communicating with a base station.
   e. **Artificial Intelligence / Machine Learning.** This function allows the RPAS to respond autonomously to in-flight interference utilising multiple sensors. Certain drones can utilise this and other functions to enhance capability and effectiveness through machine learning algorithms, making them increasingly difficult to defeat as they learn from their own environment.

5. **Payloads.** RPAS payload options are extensive, and directly impact the threat assessment

for C-RPAS. They can include photographic, video and sound recording equipment (incl remote viewing functionality to allow the drone to be flown without operator line of sight); GPS and inertial navigation systems; imaging and detection systems; deployment mechanisms for precise release of items during flight; an expanding range of wireless communications; chemical, biological, radiological or explosive (CBRE) materials; and weapon systems (improvised and commercial).

6. **Swarming.** This is the ability to utilise multiple RPAS concurrently at one or many targets. It provides additional complexity for C-RPAS operations as detection and mitigation systems need to be able to concurrently address numerous threats and/or quickly switch from one specific threat to another.

Counter RPAS

7. **Security Risks and targets.** RPAS pose the following security risks:

   a. **Criminal activity.** For example, contraband delivery into controlled sites (eg prisons).
   b. **Espionage.** For example, standoff utilisation of collection payloads (microphones / cameras) to analyse patterns and procedures to inform covert collection on a government official.
   c. **Hostile reconnaissance/surveillance.** For example, standoff collection of information on security infrastructure, capabilities and site layout to develop an attack plan for a major event.
   d. **Propaganda / Protest.** For example, recording images of an event for public influence; or causing disruption at a protest rally.
   e. **Hoax / distraction.** For example, conducting a flight to distract / redirect response agencies from a key emergency.
   f. **Nuisance and/or disruption.** For example, intrusion into a restricted flight area which hampers safe aircraft movements.
   g. **Physical attack.** For example, attack against an individual or a site, utilising commercial weapon systems or improvised CBRE payloads.
   h. **RPAS Market Dominance and Security Threat.** While there is a current dominant player in the RPAS market, there is already evidence of drones from a range of manufacturers operating in no-fly or restricted-fly areas. History shows us there is no guarantee that market dominance will continue, particularly where rapid technological advancement is involved. This market dominance can also bring the type of national security concerns which have seen the Federal Government, and the governments of other allies, eliminate Huawei from being considered for participation in 5G infrastructure development.

8. **C-RPAS Operations.** C-RPAS operations are conducted in the following categories:

   a. **Detect and Monitor.** The ability to determine the presence and location of the RPAS within an area of interest; and to maintain / report on the detected contact.

   b. **Identify.** The ability to confirm the RPAS's type, unique identifier/s and ownership. It also includes the ability to differentiate between friendly and threat RPAS.

   c. **Effect (Mitigate).** The ability to mitigate the threat posed by the RPAS based on the Detect, Monitor and Identification analysis. Effect options are as follows:
      i. ***Defeat.*** Direct intervention resulting in physical incapacitation of the RPAS. This may result in an uncontrolled landing.
      ii. ***Disrupt.*** Interrupt the communication link to cause a response in the RPAS. This can interfere with any imagery or information being passed from the RPAS to the operator; or interfering with the RPAS control with the preferred outcome for the RPAS to undertake a controlled landing or returning to home / controller.
      iii. ***Deny.*** Combination of hardware and/or software options to prevent a RPAS from entering a designated area. This also includes the application of specific physical and personal security arrangements to reduce the opportunity for RPAS disruption to an organisation's operations.
      iv. ***Seize.*** To take over control of the RPAS in-flight for the purpose of achieving a controlled landing in a designated location.
      v. ***Warn.*** The active or passive notification to the RPAS controller of prohibited actions as a result of existing or operational constraints.

9. **C-RPAS Technologies, considerations and limitations.** Effective C-RPAS requires the ability to employ multiple effects to target RPAS and deliver a proportionate and timely response across the operational categories. Each technology has limitations that need to be considered, and this underpins the requirement to assess the effects of each system, to achieve the most appropriate C-RPAS solution for respective environments.

   a. **Detect, Monitor and Identify.** Can be achieved utilising radar (electromagnetic), LIDAR (laser), radio frequency (RF), electro-optical (EO) for enhanced vision, infrared (IR) thermal detection, hyperspectral and electronic identification, or a combination of numerous sensors. Heightened identification assurance is delivered through protocol manipulation systems that employ software defined algorithms against a known library of RPAS types to confirm specific operating details, IP addresses and RPAS type.

      Considerations and Limitations. Radar generally achieves the best detection over greater ranges and under challenging environmental conditions, although detection of small RPAS is difficult and can result in false positives. "Identification" is also limited to basic results ("it's a drone") and needs to be supported by other technologies to effect RPAS identification by size, shape, and visual markings (LIDAR, RF detection, electro-optical, IR). Greater fidelity is provided with protocol manipulation system overlay.

The physical ability to employ these technologies is greatly affected by the environment, other systems (operation or interference), siting, power, system mobility (either operating on a mobile platform or timely movement between operating sites), and legislative constraints (see below). They are also subject to counter C-RPAS threats (physical sabotage or electronic attack).

b. **Effect – Kinetic.** Kinetic effect is delivered by physical interdiction of the RPAS. This includes employment of friendly 'attack' RPAS to engage with threat RPAS; launching net systems to capture the RPAS; engaging conventional surface to air weapon systems; or employment of energy weapons (eg directional laser).

Considerations and Limitation (kinetic). The key limitations are the inability to control the unintended consequences of RPAS interdiction; and the safety risk of such systems when employed in the domestic environment. RPAS usually crash as a result of this interdiction, potentially resulting in public injury and/or the actuation of malicious payloads (eg explosives, CBRE material etc). Kinetic options are also costly and require additional logistic support for operation and resupply.

c. **Effect (Mitigate) – Non-Kinetic.** Non-Kinetic effect is delivered by targeting the operational or communications cyber interface. It includes GNSS (GPS) Jammers, Radio Frequency (RF) Jammers, area denial systems (eg Geofencing), electronic attack and Protocol Manipulation. Non-Kinetic effect may be further assured by combining systems in a layered approach, although this would come at a significant increase in commercial cost.

Considerations and Limitations (non-Kinetic). Jamming technologies have significant constraints under Australian State and Federal Legislation (see below). They can also affect other operating systems in the area of application; and are not able to discern between types of RPAS that are interdicted. This can be partially mitigated through operating with lower power (reduced effect range) or by operating on frequencies that do not affect the surrounding systems. Safety assurance can be reinforced by declarations of emergency and defined / designated areas of use utilising Geofencing (virtual barrier) technologies where the RPAS has GPS – thus minimising (or at least notifying) the impact parties likely to be affected and denying virtual access.

Protocol Manipulation technologies do not affect operating systems in the area of application and are therefore safer to employ. However, only RPAS that have had algorithms developed for their system manipulation can be interdicted. This is generally mitigated by manufacturers by them developing RPAS algorithms as new RPAS are introduced to market.

d. **Multiple Effects.** Most current technologies are only capable of producing one or two of these effects. There are currently very few technologies capable of producing all these effects from the one system.

C-RPAS Legal Considerations

10. General. There are several pieces of Commonwealth and State legislation that affect the ability to Identify and Effect (Mitigate) the RPAS threat. Interim options do exist for Major Events, where special consideration for the employment of Identify and Effect technologies is granted for designated areas for specific times. However, these are complex and difficult to establish in a timely manner.

11. Specific Legislation – Detect and Monitor. Key legislative considerations for Detect and Monitor are as follows:

a. **Radiocommunications Act 1992**
   - ***i.*** Operation of radio communications without licence s46.
   - ***ii.*** Possession of radio communications device without authority or a licence s47.
   - ***iii.*** Use and/or possession of nonstandard devices without ACMA licence ss157, 158.
   - ***iv.*** Operations of a prohibited device ss189, 190.
   - ***v.*** Use to interfere with radio communications where likely to prejudice safe operation of aircraft s192.
   - ***vi.*** Use likely to interfere with specified radiocommunications (Police, rescue etc) s193.
   - ***vii.*** Use likely to interfere, disrupt or disturb radiocommunications so to endanger safety of another person or cause … loss or damage s194.
   - ***viii.*** Use recklessly to cause interference, disruption or disturbance of radiocommunications s197.

b. **Surveillance Devices Act 2004.** Does not create offences, however, regulates use of surveillance devices at Commonwealth level and will prevail over inconsistent State legislation. Also covers use of surveillance devices without warrant.

12. Specific Legislation – Identify

a. **Radiocommunications Act 1992.** Part 4.2 Offences relating to radio emission.
b. **Surveillance Devices Act 2004.** Does not create offences, however, regulates use of surveillance devices at Commonwealth level and will prevail over inconsistent State legislation.
c. **Privacy Act 1988.** Regulate collection, use, disclosure and security of personal information.

13. Specific Legislation – Effect (Mitigate)

a. **Radiocommunications Act 1992.** Use of nonstandard devices to interfere with radio

communications where likely to prejudice safe operation of aircraft is prohibited s192.

b. **Criminal Code.** Unauthorised impairment of electronic communication (being a communication of information in any form by means of guided or unguided electromagnetic energy) s476.1(1); s477.3.
c. **Telecommunications (Interception & Access) Act 1979.** Sect 7 prohibits interception of telecommunications except under warrant or specified exemptions.
d. **Civil Aviation Act 1988.** It is an offence to interfere with or threaten the safety of an aircraft s24.
e. **Aviation Transport Security Act 2004.** Unlawful interference with aviation is prohibited s10.
f. **General Civil Law.** May be liable under civil law in negligence (personal injury, damage to property), trespass or nuisance.
g. **General Criminal Law (States / Territories).** May be subject to criminal liability (eg property damage, misappropriation of aircraft, unlawful taking control of aircraft) if there is no lawful authority for particular action.
h. **Defence Act 1903.** Part IIIAAA utilisation of Defence Force to protect Commonwealth, State & Territory interests.

C-RPAS Way Ahead

14. Amended Legislation. The Commonwealth Department of Home Affairs has commissioned several investigative pieces of work to address these challenges at the Commonwealth level, with significant input from the Civil Aviation Safety Authority (CASA), Air Services Australia (ASA) and the Australian Communications and Media Authority (ACMA). A Senate Report (June 2018) generated findings and determinations to provide initial guidance and input into this work. These can be found in the 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 dated November 2018.

15. Threat, Integrated C-RPAS Technology and Commercial considerations. Organisations need to assess the likely threat of RPAS to their operation, considering the C-RPAS Operational Categories. This analysis will most likely confirm that the RPAS threat needs to be addressed by a combination of C-RPAS technologies to ideally allow Detection, Monitoring, Identification and Effect (Mitigation) in a layered and scalable response.

However, whilst the “penultimate” C-RPAS solution may involve layering different technologies – which could still have some vulnerabilities – end users will need to offset the potential reduction in threat with the additional commercial cost of acquisition and operation. As such, select systems achieving maximised C-RPAS capability may be the organisational end-state.

16. **Training.** Staff at all levels need to be made aware of the nature of RPAS threats and understand the C-RPAS options available (now and post-legislative amendment). They also need to be informed of basic personal and physical security considerations that apply to their particular organisation and apply these to reduce the ability for RPAS systems to impact on their operation.

17. **Technological developments.** There needs to be a focus and specific Sovereign capability developed in Australia to assess future RPAS threats; and to assess/develop technologies to counter those threats. This should be reinforced by a requirement (government and commercial) for a standing overwatch of emerging RPAS threats and C-RPAS capabilities.

About EPE

EPE provides innovative solutions to protect military and emergency response personnel, critical infrastructure and high profile public events from current and emerging threats. We are force protection specialists with real world operational experience. Our solutions include Counter Drone, Unmanned Ground Systems, Counter IED (Improvised Explosive Devices, including Radio Controlled Devices), and Chemical, Biological, Radiological and Nuclear Defence (CBRND).

EPE has scanned the globe to identify and compare the most effective and appropriate counter-drone technology solutions available. This is an exercise EPE initiated in 2014, when it was engaged to provide a threat assessment for the G20 in Brisbane; and continues to review on behalf of clients in response to the evolving threat from drones. We have completed site assessments and installations of C-RPAS Systems for a number of Australian clients, delivering ongoing monitoring and monthly reports quantifying detections and identifications.

As an Australian veteran owned and managed small business, EPE's strength has always been our unique ability to be agile and responsive to our customers' requirements while delivering world-leading solutions, supported by Integrated Logistics Support (ILS) and specialist training.

EPE's Technical Team

Scott Corrigan, Strategic Capability Manager, EPE

Scott is a highly regarded senior executive with over 28 years of proven leadership experience in the design, development and implementation of solutions to complex threat environments.

Scott's expertise is derived from key leadership appointments spanning 22 years in the Australian Army—most notably the development of specialist EOD, IED and CBRNE capability whilst Commander of the Special Operations Engineer Regiment (SOER) during the high operational tempo period 2009 to 2012; and key contributions to the Iraq and Afghanistan theatres of operation during attachment and deployment with the US Joint IED Defeat Organisation (JIEDDO) and the Australian Counter IED Task Force (CIEDTF) (2007-2009). He also gained extensive experience as a specialist capability advisor to the UAE (2013-2016) and Counter Terrorism threat advisor to the NSW Department of Justice (2016-2018).

Keith Mollison GM, Counter Drone & ECM Manager, EPE

Keith is the Project Lead for EPE's C-RPAS installations for Australian clients. He served in numerous operational, training and command appointments within the UK Army EOD and Improvised Explosive Device Disposal (IEDD) community. Working closely with UK Police Forces, he provided IEDD and other specialist support to major events including the Commonwealth Games and VVIP protection. Keith commanded the UK's principal EOD unit (11 EOD Regiment RLC) from 2001-2003. His final appointment in the British Army was as a Deputy Director of Intelligence within the UK's Defence Intelligence Staff (DIS).

In 2008, Keith transferred to the Australian Army, where he served as the Chief of Staff to the Australian Defence Force Counter Improvised Explosive Device Task Force (ADF CIEDTF).

Grant Phillips, Principal Technical Advisor, EPE

Grant served for 15 years in the Australian Army and was involved in maintenance support of advanced electronic and communications systems. His final posting was as the Artificer Sergeant Major of the Army's largest field deployable hospital. During his employment as an Electronics Technician, Grant specialised in communications equipment, ECM, Fire Control Systems and Bio-medical equipment.

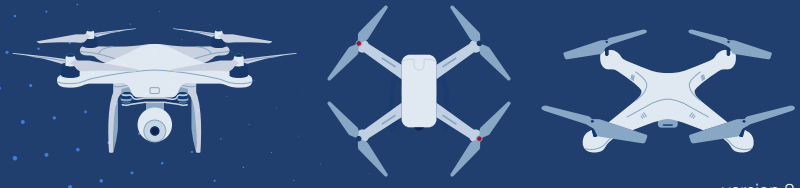
Currently, as the Through Life Support Manager at EPE, Grant has travelled globally leading in all technical related matters with EPE's Drone and Counter Drone solutions. He is one of a very select group of people in Australia to have performed complete implementation of Protocol Manipulation Counter Drone Systems including site assessment, installation, training, monitoring and ongoing reporting.

EPE
Trusted to Protect

Brisbane, **Australia | ABN: 46 003 083 609**
Wellington, **New Zealand | NZBN: 9429046847416**

For more information

scott.corrigan@epequip.com
keith.mollison@epequip.com
grant.phillips@epequip.com
+61 (0) 7 3308 9300



www.**epequip**.com

version 2