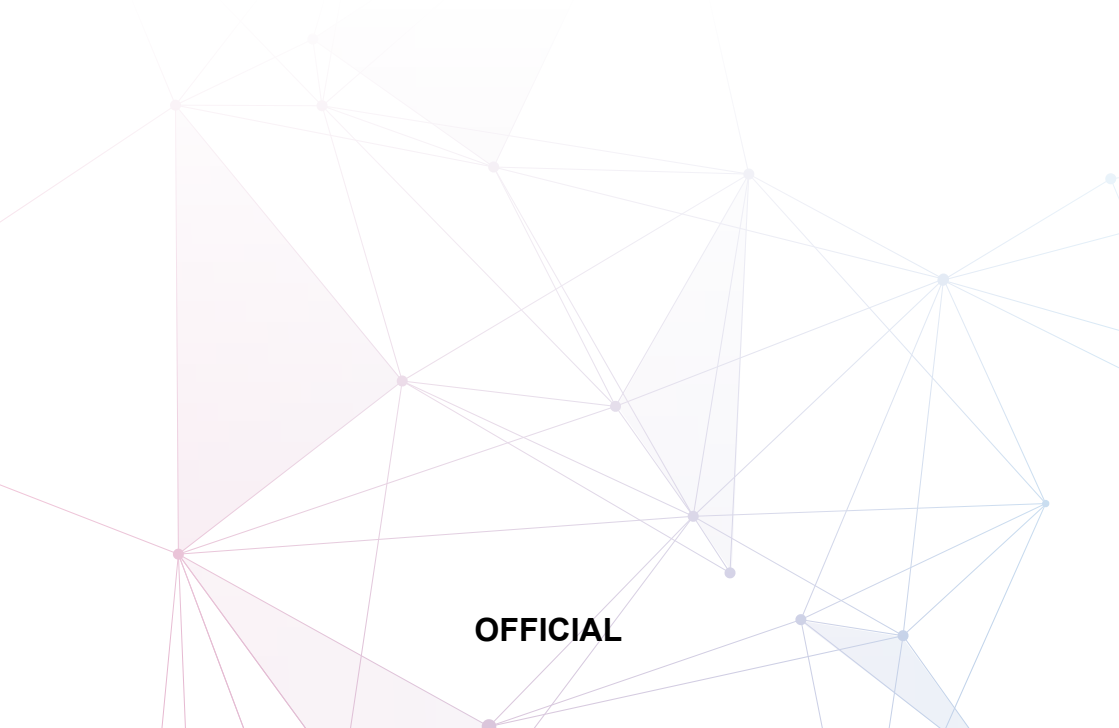
AUSTRALIAN DEFENCE FORCE

CONCEPT FOR ROBOTIC AND AUTONOMOUS SYSTEMS

Version 1.0
Reference: DPN BN9939583



AUSTRALIAN
DEFENCE FORCE

CONCEPT FOR
ROBOTIC AND AUTONOMOUS SYSTEMS

Version 1.0
Reference: DPN BN9939583

Considered: Joint Warfare Council
Date: 11 November 2020

Version	Date	Drafted by	Description
0.1	08 Oct 19	SQNLDR Vine	Idea Level Outline
0.2	10 Feb 20	SQNLDR Vine	First Draft for Workshop 1
0.3	15 May 20	SQNLDR Vine	Workshop 1 Outcomes Incorporated
0.4	29 Jun 20	SQNLDR Vine	Draft for engagement. Workshop 2 and 3 Outcomes incorporated
0.52	06 Aug 20	SQNLDR Vine	Draft for experimentation
0.62	07 Oct 20	SQNLDR Vine	Draft for 1 and 2 star engagement.
0.9	16 Oct 20	SQNLDR Vine	Submitted to JWC
1.0	16 Nov 20	SQNLDR Vine	JFA Approval

Lead Author:
Squadron Leader Robert Vine
Staff Officer Grade Two –
Joint Concepts (Air/Space)
Joint Futures and Concepts Directorate
Force Exploration Branch
Force Design Division
force.exploration@defence.gov.au

Lead Analyst:
Ms Elizabeth Kohn
Wargaming and
Experimentation Analyst
Strategy and Joint Force Branch
Joint and Operations Analysis Division
Defence Science and Technology Group

FOREWORD

Joint Concepts are published to increase warfighting effectiveness, and link strategy to the development and employment of Future Force capabilities. They are the method by which the Australian Defence Force develops ideas that can embrace the opportunities and confront the challenges that we will face in the Future Operating Environment. Joint Concepts inform future iterations of the Integrated Investment Program to design a Joint Force that will fight and win.

The *Concept for Robotic and Autonomous Systems* is the amalgamation of research activities from scientific and academic communities, the concepts of partner nations and the ideas of critical thinkers from within the Department of Defence. This concept has been tested by the Defence Science and Technology Group to confirm that the alternate models of capability and thought it proposes is fit for purpose.

This Concept is to guide the acquisition of capabilities, employment of the Joint Force, and education and training of our people. However, Joint Concepts must be subject to continual improvement, as the nature of the operating environment evolves we must reconsider the design of the Future Force. Your feedback is critical to the continued relevance of our capability.

DL Johnston, AO
Vice Admiral, RAN
Vice Chief of the Defence Force

25 November 2020


AUSTRALIAN SUBMARINES

SECTION 1 - EXECUTIVE SUMMARY

1.1 Joint Concepts enable the ADF to test alternative theoretical models of capability and measure their effectiveness in supporting Defence Strategy. The role of Joint Concepts is to describe potential models of Joint Force capability that, following testing through Joint Experimentation will provide the justified confidence that enables investment decisions.[1] Defence considers new models of capability when it identifies catalysts for change such as new strategic direction, changes in the operating environment or new threats and opportunities. The catalyst for this Joint Concept is the emergence of Robotic and Autonomous System (RAS) technologies that represent both a threat and an opportunity for Defence.

1.2 RAS have been utilised by Defence in one form or another for a number of decades but recent developments in Platforms, Payloads, Control Systems, Artificial Intelligence and supporting technologies are converging to create more advanced and capable systems that will disrupt current methods of warfare. This concept determines how Defence will adopt the next generation of RAS technologies to embrace these opportunities and mitigate the challenge of the future operating environment.

1.3 Defence requires a concept to identify how it can utilise RAS to achieve strategic disruption. By analysing the potential opportunities and challenges of this technology, the concept details the capabilities that the Future Force requires to embrace RAS. This concept mitigates against RAS technologies being used to disrupt Defence activities by outlining potential approaches to counter adversary RAS. The central idea, capability requirements, principles and characteristics contained within provide the basis from which to analyse and develop options for achieving advantage with RAS.

1 JFA Directive 03/2018, The Joint Concepts Framework

1.4 This concept answers the military problem of:

> How will Defence's future force exploit RAS to gain advantages throughout the spectrum of conflict, and how can Defence counter threats posed to the future force by RAS?

1.5 **What are RAS?** RAS is an accepted term used by academia and the science and technology community to highlight the physical (robotic) and/or cognitive (autonomous) aspects of a system (or platform).[2] Defence uses this term to describe systems that perform a function on their own by being either physically remote from a human operator, performing cognitive-like functions on behalf of a human operator or, increasingly, both. A RAS may not always be capable of physical autonomy and could be a software agent that is authorised to act on behalf of a human to conduct non-physical, or cyber, tasks.

1.6 This concept presents separate ideas for how to embrace the opportunities and mitigate the potential challenges presented by RAS. To embrace RAS:

> Defence will enhance its combat capability within planned resources by employing RAS in human commanded teams to improve efficiency, increase mass and achieve decision superiority while decreasing risk to personnel. Defence will develop RAS that are optimised to roles which enhance, augment or replace current capabilities.

2 US Joint Chiefs of Staff, Joint Concept for Robotic and Autonomous Systems, 19 Oct 2016

1.7 To mitigate the challenge of RAS:

> Defence will counter adversary RAS through attacks on their environmental perception and control systems, information warfare activities and platform destruction.

1.8 RAS provides Defence the opportunity to achieve greater combat power within its planned budget by increasing its physical and non-physical mass.[3] It challenges an assumption that Australia cannot achieve mass compared to regional competitors as RAS offer the potential for Defence to increase the scale of effect that can be employed within planned resources. RAS provides the opportunity to fundamentally alter the structure of Defence from a force of a few large and expensive platforms to one of many small and cheap platforms.[4]

1.9 Defining how Defence will Command and Control RAS is critical to exploiting the potential of this technology. This concept expands upon Defence Concept For Command and Control of the Future Force (Future C2 Concept) to achieve '*Hierarchical Command – Agile Control*'.[5] The Future C2 concept considers Command and Control to be separate functions; RAS may assist humans to Command while RAS may conduct Control.

1.10 **How will Defence employ future RAS?** Defence will develop RAS optimised for their role and appropriate levels of autonomy will be enabled during design. RAS will be employed in human-machine teams where human Commanders will determine the level of Control that is applied to RAS, relevant to their mission and level of acceptable risk. This concept describes a manner for employing RAS that balances the technical capability of systems against the risk of their use. Through this process humans will remain responsible for the actions of RAS and Defence will demonstrate clear lines of accountability for their use.

3 Mass is an advantageous concentration of combat power in space and/or time. '*On Tactics*' B.A. Friedman p 38

4 Layton P, *Algorithmic Warfare* p 33

5 Department Of Defence, *ADF Concept for Command and Control of the Future Force*. V1.0 13 May 19.

1.11 **How will Defence counter future RAS?** Defence will develop technical intelligence for RAS platforms so that it can identify the presence of adversary RAS in the operating environment. This will allow commanders to implement a suite of countermeasures to prevent adversary RAS from perceiving the operating environment and controlling their platforms. Defence must commence Information Warfare activities against the adversaries data and algorithms to alter the relationship between what a RAS observes and the database upon which the system makes decisions. Defence will develop kinetic counters tailored to defend against swarming attacks of numerous, small RAS.

Implementation

1.12 Section 4 of this concept identifies the abilities that Defence must possess to solve the military problem. The concept also identifies the characteristics that future RAS capabilities should possess to maximise the potential of this technology as well as the design principles that Defence RAS capabilities should adhere to.

1.13 RAS are technically complex emerging technologies and a common level of literacy cannot be assumed. There is little standardisation of terminology or standards across the S&T field pertaining to RAS. This concept is therefore intended to increase the level of RAS literacy within Defence by providing a broad description of the field and what Defence needs to do to embrace the opportunity that this technology provides. Detailed descriptions of the supporting technologies that may be utilised by RAS should be sought from researchers in the field.

1.14 Development of the concept identified a number of topics that require further analysis. The impact of RAS on operating concepts, policy, doctrine, workforce and the capability life cycle will require detailed study. Without further analysis on these topics Defence may not be able to achieve the promise of RAS.

1.15 This concept provides actionable force design requirements to allow Defence to achieve competitive advantage in the Future Operating Environment (FOE). It is intended to be used by those involved in operational planning, force design, experimentation and in the delivery of Professional Military Education (PME). It may also be used by external partners to provide context on how Defence will advance RAS.

TABLE OF CONTENTS

SECTION 2 – INTRODUCTION

Strategic Environment

2.1 The 2020 Defence Strategic Update identifies that Australia is at the centre of a dynamic strategic environment and that regional force modernisation has resulted in the development and deployment of new weapons that challenge Australia's military capability edge.[6] This environment has prompted three new strategic objectives for Defence: to shape Australia's strategic environment; to deter actions against Australia's interests; and to respond with credible military force, when required.[7]

2.2 To implement these objectives Defence will undertake a number of tasks that include growing Defence's self-reliance for delivering deterrent effects and enhancing the lethality of Defence for high-intensity operations.[8] RAS offers the potential for a middle power such as Australia to achieve these tasks by increasing the effectiveness of Defence within the constraints of Australia's resources.

2.3 **Necessity.** While Defence already deploys systems with remote or automatic operation it is not a matter of if, but when it will become necessary for Defence to adopt RAS and counter RAS capabilities to maintain Australia's military capability edge. Adversaries will utilise RAS to conduct warfare at far greater speeds, enabled by capabilities that observe, orient, decide and act at machine speed. As adversaries adopt such capabilities it will become necessary for Defence to acquire RAS that perform a broad range of roles, including the employment of lethal effects. This concept identifies the abilities that the future force requires to responsibly embrace the opportunity to employ RAS in all roles.

6 Department of Defence '2020 Defence Strategic Update' para i.

7 Ibid para 2.12

8 Ibid para 2.13

Definitions

2.4 Notwithstanding FVEY and NATO work towards standardisation, there are currently no universally agreed and recognised terms to categorise RAS. While there is ongoing work on this topic, no source can be considered authoritative. The definitions in this concept aim to provide Defence with a consistent understanding of this technology that is compatible with allies. The definitions within this document combine numerous sources to allow Defence to develop a common, foundational understanding of how a RAS works and how it can be operated in support of Defence objectives.

2.5 Figure 1 depicts a model for understanding a RAS-enabled capability through a Technical (capability) context and a Control (use) context. This diagram creates four categories of RAS which can be used to describe platforms and systems. Definitions for each category and the context axes are given in annex B.

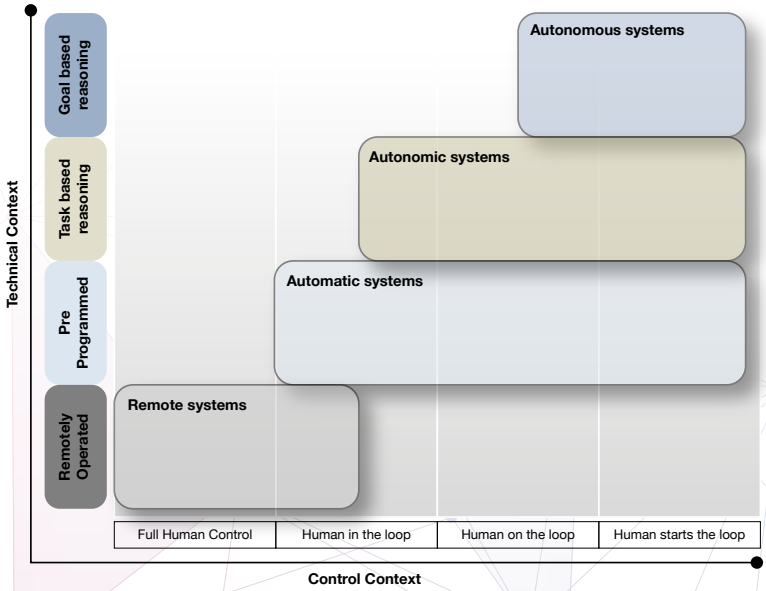


Figure 1 – Contextual Categorisation of RAS

2.6 The technical context on the vertical axis depicts levels of increasing intelligence and autonomy of a system. The bottom of this axis describes a purely robotic system that has no autonomy and is remotely controlled. The axis continues towards systems that utilise pre-programmed, deterministic behaviours to achieve automation. Finally, the axis considers systems that utilise reasoning behaviours to achieve a task in the manner determined by a human, or to self-determine how to achieve a goal.

2.7 The control context on the horizontal axis depicts types of human interaction with a system. The left of the axis describes a system that has human control of all functions. The axis continues towards systems that perform functions but require human intervention to complete the task. The final stages of control describe systems that provide a human the opportunity to interrupt the task and finally, systems whereby the human sets the start and end parameters of the task and allows the system to run to completion without further supervision, but within a defined ethical framework that adheres to Australia's legal obligations.

2.8 These two contexts are used to define the capabilities and use of a RAS through four categories:

a. **Remote Control Systems.** A system that is operated by a human via remote methods. Without the remote control element the system has little ability to operate independently.[9]

b. **Automatic System.** A system that is pre-programmed to respond to stimuli in a rules based, deterministic manner and may achieve its function without further human input.

c. **Autonomic Systems.** A system that achieves human defined tasks by operating with reference to a set of pre-defined guidelines and responds to stimuli in a probabilistic manner. Autonomic systems may require human input to complete its function or may run without further supervision.

9 Andrew Williams. *Defining Autonomy in Systems: Challenges and Solutions.* NATO ACT Publication 2017. Page 30

d. **Autonomous Systems.** A system that determines how to perform the tasks necessary to achieve a defined goal. An autonomous system responds to stimuli in a probabilistic manner and can alter how it performs tasks.

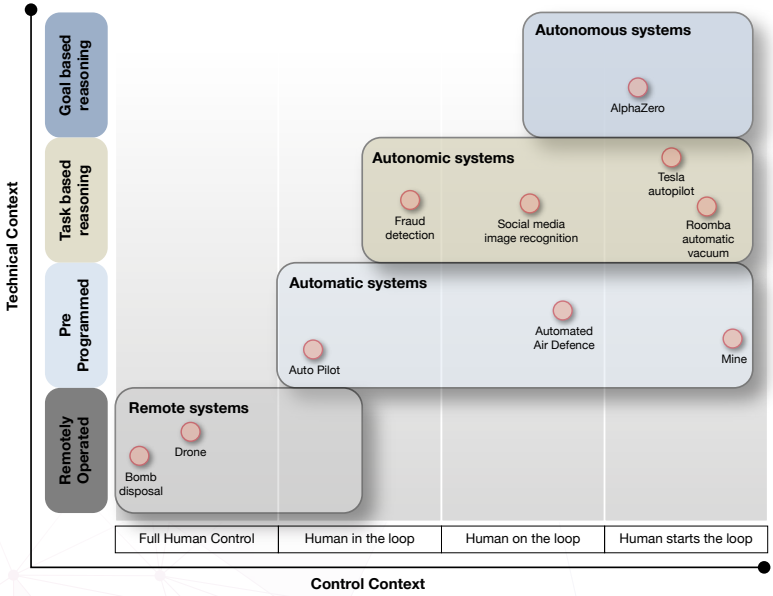


Figure 2 – Example Categorisation[10]

2.9 Figure 2 uses examples of current RAS to demonstrate use of the categorisation model.

a. A bomb disposal robot is an example of a remotely operated system as it is fully controlled by a human that is located a safe distance away. A human is in real time control of all behaviours of the robot.

10 Placement within the model represents the opinion of the author and is intended to demonstrate how current systems could be categorised. It should not be considered authoritative.

b. Certain self defence modes of air defence systems are an example of an automatic system. They are pre-programmed to automatically engage targets that meet a predetermined set of criteria. Once the system is activated it will engage targets that meet the criteria unless a human operator over-rides it.

c. The image tagging function used by some social media sites is an example of an autonomic system. When an image is uploaded, the service uses a probabilistic method to analyse if there are faces in the image. If the face matches data of those already known by the system it will apply the identity to the image. The operator may monitor the tagging process and override the automation if a match is incorrect. New images are then used by the system to learn the features of an individual so that higher confidence matches may be used in the future.

d. An example of a fully Autonomous System that meets this definition may not exist yet. The AlphaZero computer system developed to beat human players at specific board games such as Go and Chess is perhaps the closest that has been achieved at the time of writing.[11] This system was given the rules of the game, and did not rely on human expertise to learn how to play. AlphaZero then taught itself how to play, achieving a high level of mastery within four hours. AlphaZero was able to demonstrate novel strategies not previously considered by human players. However, AlphaZero operates only within a very highly-structured, fully-visible, regular and symmetric game environment.

11 AlphaZero is an evolution of the AlphaGo system, early AlphaGo systems were given records of human matches to analyse and developed their play from this data.

Assumptions

2.10 This concept assumes that collaboration between Defence, academia and industry can reduce the size and cost of RAS. Commercial use of RAS is already reducing the size and cost of RAS, Defence should leverage the developments made by the commercial sector. In addition, by defining the requirement for RAS to be smaller and cheaper than the capabilities that they replace, the concept assumes that it can drive development in this direction.

2.11 It is assumed that defining a requirement for smaller, cheaper RAS will result in platforms that can only perform a single role. Therefore, Defence will require a larger number of RAS to achieve the same capability currently provided by multi-role platforms.


BLUEFIN
ROBOTICS

SECTION 3 – MILITARY PROBLEM AND CENTRAL IDEA

Military Problem

3.1 This concept has been developed to answer the military problem of:

> How will Defence's future force exploit RAS to gain advantages throughout the spectrum of conflict, and how can Defence counter threats posed to the future force by RAS?

3.2 **Convergence.** The future capabilities of RAS will not be influenced by a single technology but by the convergence of advances in multiple technological areas including, but not limited to:

a. **Power Generation & Energy Storage.** Future platforms may be able to generate and store sufficient power and energy to enable them to persist in a battlespace for long periods without refuelling.

b. **Computation.** The continuing miniaturisation of systems and increasing capability of computers will allow RAS to conduct data processing on-board, as well as becoming smaller and more capable.

c. **Materials.** Advanced materials may allow for small, light but strong platforms that are able to withstand harsh environments and survive battle damage.

d. **Nano Explosives.** Miniaturisation of explosive compounds will enable smaller, lighter platforms that are able to produce magnified but controllable effects.

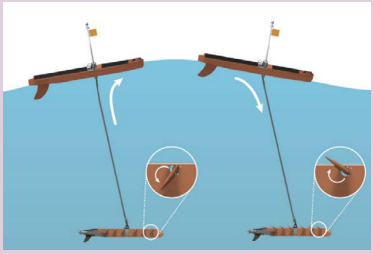
e. **Bio-mimetics.** Platforms that are able to mimic biological creatures may enable platforms to evade detection within the environment.

f. **Additive Manufacturing.** These techniques will enable mass production of highly capable platforms cheaply and quickly.

g. **Sensors and Perception.** Small, smart sensors that can operate across multiple areas of the electromagnetic spectrum are allowing the operation of smaller and more capable sensor platforms.

h. **Common Control Architecture.** New architectures are enabling one human to simultaneously control many systems of different types. Common control architectures also allow RAS to be controlled by different human teams during their operation.

Convergence Example: Wave Glider



The Wave Glider generates power by exploiting the difference between the energy at the water's surface and the decreasing energy at depth. Combined with solar energy storage, sensors and on-board computing, this platform can autonomously monitor an area of ocean for periods of up to 12 months.[12]

12 Image courtesy of Liquid Robotics. https://www.liquid-robotics.com/wave-glider/how-it-works/. Accessed 7 Oct 20

<?>

3.3 The convergence of these technologies into RAS indicates that Defence has the opportunity to develop capabilities that are smaller, cheaper and easier to produce than existing capabilities. However, such systems will only be able to perform one role at a time.

The challenges of employing RAS

3.4 The use of RAS for Defence capabilities creates new challenges relating to trust and the ethics of using machines for Defence missions. Defence currently operates remote control and automated systems and over a number of decades has employed methods for operation and deployment that mitigate the limitations of these types of systems. As Defence adopts autonomic and autonomous systems it must continue to develop and adopt new methods that mitigate these challenges. This will enable Defence to fully exploit the opportunities that these categories of RAS will provide.

3.5 Autonomic and autonomous systems make decisions in a different way to the automatic systems that Defence currently operates. The methods currently used by Defence to verify systems are suited to automatic systems but not autonomic or autonomous systems. Verification activities provide a set of stimuli to the system and confirm that it acts as designed. Autonomic systems that make probabilistic decisions based on a database may provide a different outcome as their database changes. Autonomous systems determine the method that they use to achieve their goals. This is a strength of autonomic and autonomous systems, however new system verification methods are required to determine system performance.

3.6 **Trust.** Trust is the firm belief in the reliability, truth or ability of someone or something. Trust is essential to ensuring that we can responsibly conduct operations using RAS. Therefore, the development of RAS must include the ability to demonstrate that we can trust them. To embrace the opportunity of RAS, Defence must develop a methodology for developing trust in systems that utilise task or goal based reasoning and may change how they perform or operate during an operation or mission.

3.7 **Ethics.** There are ethical concerns associated with the use of RAS. Many of these concerns are practical ones regarding the technical capability of RAS to make decisions that align with the ethical

expectations of those employing them. There are also purely moral objections to the use of RAS, especially where systems make a decision that may result in the taking of human lives. However, societies must also consider the ethics of placing people in high risk situations when a RAS may be able to perform the same task without risking their own personnel.

3.8 The strengths of RAS may create a future legal and ethical obligation to deploy RAS in preference to other means and methods of warfare. It is arguably foreseeable that the abilities of RAS to comply with International Humanitarian Law (IHL) in planning and executing attacks will at some point exceed those of human operators, and as a result, States would be legally obliged to prefer the former over the latter.[13]

3.9 Science fiction has generated wide ranging debate regarding the negative consequences of the adoption of RAS. Defence must ensure that the public are informed, through an open and transparent dialogue, on the interaction between RAS and humans in order to build greater understanding and trust in the benefits and the lawful employment of RAS.

3.10 **Legal.** Existing international law covers the development, acquisition and deployment of any new and emerging capability, including future autonomous weapons systems. Australia undertakes Article 36 legal reviews to ensure that all new and existing capability will be compliant with Australia's domestic and international law obligations.[14] Australia engages in international discussions on possible legal and regulatory frameworks on Lethal Autonomous Weapons Systems (LAWS). Australia and other nations (including the United States and the United Kingdom) have publically declared any bans on LAWS to be premature.[15]

13 Balme J, *The interpretation and application of LOAC in relation to autonomous weapons systems*. 2020

14 A review of a new weapons system to determine whether its employment would, in some or all circumstances, be prohibited by Additional Protocol 1 of 1977 to the Geneva Conventions of 1949, or by any other rule of international law. This includes an assessment of whether the weapon is contrary to the public interest, the principles of humanity and the dictates of public conscience.

15 Department of Defence, *Senate Estimates Brief SB20-000160 – Autonomous Weapons Systems*

3.11 **Algorithms and Data.** The way that algorithms and data interact to achieve a system's output varies depending on the category of a RAS. In an autonomic system the algorithm can be defined and verified, however the data that it interacts with may alter the outcome of the system. In an autonomous system, the goal of the system can be confirmed, however the method that the RAS uses to achieve this goal may not be able to be understood, or may change as the system interacts with data.

3.12 To achieve the output desired of an autonomic or autonomous system it is necessary to provide it with data appropriate to its function. This data must be in a format that is able to be utilised by the system and be representative of the environment for which it is to operate. If a RAS is not provided with appropriate data, it will not produce relevant results. For example, a system to automate the sentencing of offenders produced a biased outcome because the data it utilised from previously applied sentences was found to apply harsher sentences to members of certain ethnic groups.[16]

3.13 **Security.** The algorithms and data utilised by RAS are critical to their operation and unauthorised disclosure can provide adversaries with insight into the vulnerabilities of our systems. RAS algorithms and data must be appropriately secured and this must include consideration of the consequences of an adversary capturing a RAS as the platform will contain an implementation of the algorithm and data set that can be exploited by adversaries.[17]

16 New Scientist, *Discriminating algorithms: 5 times AI showed prejudice*. Viewed 21 Aug 20 https://www.newscientist.com/article/2166207-discriminating-algorithms-5-times-ai-showed-prejudice/

17 DSTG-CR-2020-0151 RAS Concept Red Teaming Report para 3.4.1

The challenges of countering RAS

3.14 The convergence of technologies described in this section will allow adversaries to develop RAS that will be impervious to many of our current counter-measures. RAS will be employed across all domains to suit the strategies of each particular adversary. As such, a concept for countering such a broad range of possibilities must consider the capabilities that RAS will provide adversaries. From these capabilities and characteristics, vulnerabilities to RAS can be assessed, thereby providing guidance for the generation of counters.

3.15 **Decision Superiority.** While Defence will use RAS to enhance our decision-making processes, adversaries will also use RAS to improve their situational understanding and may achieve decision superiority by achieving better and faster decision cycles than our own.

3.16 **Stealth.** By decreasing the requirement for human operators within a platform, designers will be able to optimise future systems for their function rather than cater for life support and protection of humans. This will provide greater opportunity to create RAS with lower signatures or use novel designs to mimic other entities in the operating environment (e.g. underwater vehicles that mimic marine animals).

3.17 **Mass.** Adversaries may be able to generate mass effects at low cost by utilising large numbers of RAS. This will allow actors of limited means the ability to conduct saturation attacks. If an adversary is able to utilise RAS as expendable platforms, they will gain an additional advantage over larger, more expensive Defence capabilities by having a force that is more resilient to attrition.

3.18 **Swarm Behaviours**. The incorporation of RAS that exhibit swarming behaviours will create a mass of resilient systems that cannot be disabled by attacking a central control node. RAS that can sense other systems in proximity and act in conjunction with them creates a well organised mass of systems that cannot be easily disrupted and will overwhelm traditional defensive measures.

3.19 **Intelligence Mission Data (IMD)**. Development of counters will require a detailed understanding of the technical capabilities of adversary RAS. Defence will need to provide counter-RAS capabilities with IMD necessary to develop and employ techniques specific to the systems encountered by Defence.

3.20 Autonomy will introduce new vulnerabilities that may be exploited. The challenges of Trust, Ethics, Algorithms and Data will also apply to adversary's use of RAS. However, these challenges will relate to different adversaries in different ways. Authoritarian regimes will approach trust in different ways to democratic societies. Terrorist organisations with a lower ethical threshold may be willing to accept greater collateral damage than state actors. The implementation of RAS by each adversary will need to be studied so that opportunities to counter their method of employment can be identified.

Employment of RAS

3.21 The central idea proposed to address the military problem is:

> Defence will enhance its combat capability within planned resources by employing RAS in human commanded teams to improve efficiency, increase mass and achieve decision superiority while decreasing risk to personnel. Defence will develop RAS that are optimised to roles which enhance, augment or replace current capabilities.

3.22 The defining feature of the central idea is that Defence will operate RAS in human-machine teams. Depending on the operational scenario and objectives, human commanders will determine the level of human control placed on RAS. Advantage can be obtained by Defence if RAS development focuses on using such systems to increase efficiency, generate mass and decision superiority while decreasing risk to personnel. This central idea maximises the advantage that RAS can provide Defence while mitigating technological and ethical challenges.

3.23 To achieve this central idea, Defence must implement capabilities that future RAS will require to be effective. While RAS will not enhance, augment or replace humans in all roles, Defence must be prepared to utilise this technology where it provides increased combat capability and section 4 of this concept identifies the actions required to implement RAS in Defence.

Human Commanded Teams

3.24 RAS are developing decision making capabilities that utilise probabilistic methods and learning behaviours. While these systems will be more capable than the largely deterministic methods used today, in the near term they will not be able to replicate all elements of human intelligence. Defence must balance the ability of technology to achieve autonomy against the range of operational scenarios that Defence will have to perform. To develop RAS that can be employed across a range of scenarios and tasks, Defence requires the ability to employ RAS in conjunction with humans so that the strengths of RAS are leveraged while mitigating their weaknesses. Defence commanders will determine the level of human control over RAS that is appropriate for its technical capability and the risk of employing it for each operational scenario.

3.25 **Human Responsible.** This concept considers C2 of RAS in accordance with the Future C2 Concept as current doctrine does not provide sufficient consideration of RAS.[18] The Future C2 Concept separates the definitions of Command and Control in its central idea of 'Hierarchal Command, Agile Control'. That is, Command is a human function that determines what forces are to accomplish while Control is a human and/or machine function to determine how these tasks are performed. Within the C2 concept, RAS assists Commanders but RAS can perform Control functions to achieve missions determined by Command.

3.26 The method of controlling each RAS will be specific to the platform, mission and environment. However these methods of human control are categorised into one of the following four levels:

a. **Full Human Control.** A human controls every aspect of the systems function, physically or through remote control.

b. **Human In The Loop.** The system performs some functions independently but requires a human to perform functions that complete the system's task cycle.

18 Department Of Defence, *ADF Concept for Command and Control of the Future Force*. V1.0 13 May 19.

c. **Human On The Loop.** The system performs all functions autonomously but a human may intervene to stop or modify the outcome before the task is complete.

d. **Human Starts The Loop.** A human sets the operational parameters and initiates the systems operation; the machine requires no further human interaction to complete the task.

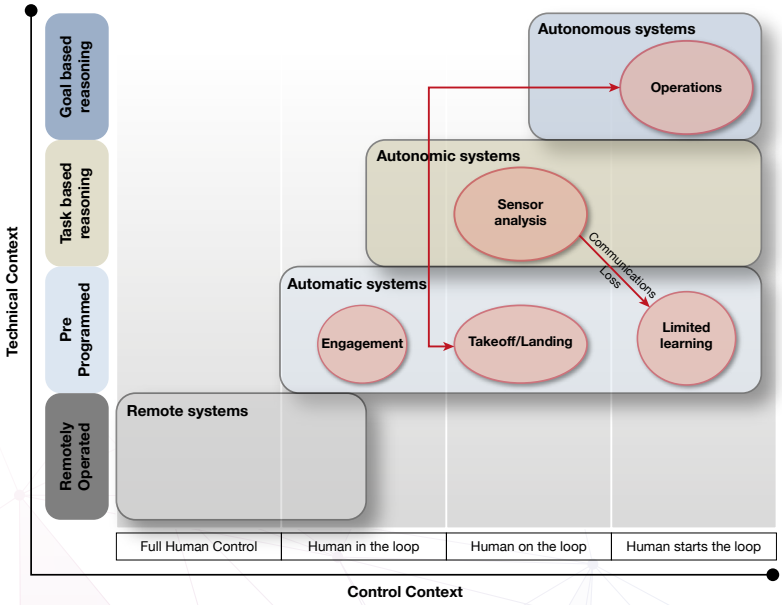


Figure 3 – Categorisation of a platform

3.27 Figure 3 above demonstrates how a Commander could determine the levels of Control for a notional air platform and its sub-systems. This platform has a flight control system that is supervised by a human during take-off and landing but transitions to autonomous operation when performing its mission. The platform is provided with mission goals and then determines where it should place itself in the area of operations to achieve its mission.

3.28 The sensor systems on this platform utilise pre-loaded intelligence databases to categorise targets detected by its sensors. Categorised targets are presented to an operator and allows the operator to adjust the systems output if they determine that the system has identified a target incorrectly. The sensor system has learning functionality, and as more target data is added to the database it is able to improve the quality of its automatic categorisation. However, should a communications loss prevent an operator from confirming target categorisation, the system will limit its learning functions to ensure that incorrect data does not bias the system.

3.29 The sensor systems of this platform are able to provide targeting data to on-board weapons systems for engagement. The platform configures the weapons systems to engage the targets but waits for human confirmation to proceed with the engagement after confirming that the Rules Of Engagement (ROE) have been met. Should a communications loss prevent human approval to engage, the platform will not perform an engagement.

Trust

3.30 Trust in the abilities of a RAS is essential to optimise the employment of these systems. If humans do not trust that the RAS will perform appropriately then it will not be employed, and as a consequence, this will limit the advantages that the RAS can provide. Conversely, trust in RAS may be misplaced due to incorrect expectations about its abilities and limitations. To generate trust in RAS, Defence should conduct activities to confirm the trustworthiness of systems and develop confidence in them. This will develop well-founded trust in RAS.

3.31 **Trusted Systems.** Defence currently determines if a system can be trusted through verification and validation programs that use deductive reasoning to understand what behaviours it should demonstrate. Trust in the system is therefore decided in a binary fashion, either it is trusted or not trusted. It is difficult to use this methodology to develop the same level of trust in autonomic and autonomous systems as they may change their performance during operation. In such systems their performance will change based on the data they access and method they utilise to achieve goals.[19]

19 DSTG-CR-2020-0151 RAS Concept Red Teaming Report para 3.3.1

3.32 **Trustworthiness.** To generate trust in autonomic and autonomous systems Defence must determine if the system is worthy of trust. This can be achieved by demonstrating that a system produces consistently valid results across a range of scenarios. To have confidence in these systems is to deem it to be trustworthy, unlike trust, trustworthiness is a spectrum along which Commanders determine if they can trust RAS to perform in a certain situation.[20]

3.33 **Confidence.** Commanders and operators develop much of their confidence in Defence capabilities through experience. This experience is gained through practical training, exercises and operations. Over the course of many such events, Defence personnel gain familiarity with the strengths and weaknesses of capabilities – from this they develop the operational and tactical methods of employment that overcome weaknesses and capitalise on strengths.[21]

3.34 The implementation of RAS into Defence must be cognisant of the possibility that confidence in systems may vary across the workforce. Certain areas of the workforce may be find it difficult to achieve confidence in RAS if they cannot understand how it functions or gain experience of its strengths and weaknesses. Conversely, some areas of the workforce may be overly confident in the abilities of RAS without understanding or experiencing their weaknesses.

3.35 Developing trust in RAS will be necessary to exploit the advantages that such systems can provide. However, there is no one process that can quickly generate trust in these systems. Defence will need to achieve trust in RAS by developing methods to ensure that RAS capabilities are trustworthy and build the confidence of the people that will employ them. This process must be continuous as RAS will continue to improve during development and use.

3.36 **Algorithms and Data.** As previously described, algorithms are processes or sets of rules to be followed in calculations, data processing or other problem-solving operations. Automated, autonomic and autonomous systems utilise both historical data and data obtained through perceiving the environment to make decisions. The algorithms used by automatic and autonomic systems are largely static and require

20 Ibid

21 Ibid

human intervention to change while an autonomous system may learn from its environment to alter its algorithms. Therefore, both the algorithms and data are vital to the function of a RAS and must be managed to ensure that humans can trust the performance of the system.

3.37 **Data Collection.** Each RAS will require data that is relevant to its role, and the environment within which it will operate. Defence must provide RAS with training or learning data that is of the highest quality to ensure that it can operate effectively. To achieve operational capability, collection of data needed to support RAS operations will need to be planned for in the early stages of the capability acquisition process. If data collection is left until after system acquisition the system will not have the foundational datasets necessary to achieve operational capability.

3.38 **Storage.** Defence will collect and hold data that is required by many different systems. This data must be stored in such a way that it is accessible to all systems that require it. Similarly, data collected by relevant sensors and systems must be incorporated into the central data base for future use. To achieve this, Defence requires the ability to store data in a manner that allows for rapid access by systems. Rapid contributions to, and access of the Defence data store will ensure that RAS can improve their performance during operations.

3.39 **Security.** Algorithms and data are areas of critical vulnerability for RAS and must be secured from external interference. Defence requires the ability to securely store and disseminate data for use by RAS. Algorithms used by these systems must also be treated as sensitive technologies. Should an adversary gain access to Defence data or algorithms, they could determine weaknesses in systems' operation or adjust their function to reduce capability.

3.40 **Verification.** The algorithms and data used by RAS will directly affect their functioning, therefore Defence needs to understand the pedigree of algorithms and data to be assured that the system performs its function. Data and algorithms will need to be verified before, during and after operation. Defence will need the ability to confirm that algorithms and data are relevant to the purpose of the RAS and its intended operating environment. This must occur through all stages of the systems life cycle. Defence must verify the functioning of RAS as it is brought into service and how its functioning changes as it learns from

new data. Without continual verification, RAS may develop bias to their actions based on the nature of the data and environments to which they are exposed.

3.41 **Training.** Autonomic and Autonomous systems will need to be trained in a manner similar to human operators by exposing them to operationally realistic scenarios so that they can develop knowledge bases from the data they collect during these events. In addition to the requirement to train system operators on RAS, Defence will need the ability to conduct events that achieve training of RAS and collective training of human teams with RAS. These events will also allow humans who work alongside RAS to gain confidence in the ability of individual systems.

Legal

3.42 The law, both domestic and international, civilian and military regarding the use of RAS remains under consideration. The concept of RAS covers technologies and capabilities along the full spectrum of decision making – from complete human programmed decisions on one end, to the complete removal of the human from machine cognitive functions on the other. A determination on the legality of using a specific RAS system is likely to present differently dependant on where it sits along that spectrum.

3.43 The international community continues to examine the legal implications of RAS, particularly Lethal Autonomous Weapons Systems (LAWS), in discussions held under the auspices of the United Nations Group of Government Experts (GGE) on LAWS. The GGE was established in 2016 under the framework of the *Convention on the Prohibitions or Restrictions on the use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to Have Indiscriminate Effects*. Discussions within the GGE have affirmed that existing international humanitarian law applies fully to all weapon systems, including those which may fall within the definition of RAS.

3.44 Australia has submitted two working papers to the LAWS GGE in an attempt to demonstrate how existing international humanitarian law is sufficient to regulate current and envisaged weapon systems; the first (2018) explained the article 36 weapon review process and the second

(2019) outlined the 'System of Control' which regulates the use of force by the ADF. Within the domestic legal system, the RAS (particularly drones) is being considered in the development and review of legislation on privacy, intelligence services and community safety.

Governance

3.45 Defence should be able to trace the decisions of RAS so that it can perform evaluation of performance and take remedial action if necessary. This includes the decisions that are made by humans and machines and the reasons for them. With this information Defence can improve the performance of both human and machine systems. Explainable AI will allow RAS to provide humans with reasons for their decisions either in real-time or post-event.[22] Understanding the reason for a recommendation or an action will allow humans to develop greater trust in RAS, especially in situations where the RAS develops a novel solution.

3.46 **Command Responsibility.** To execute their responsibilities under IHL, commanders that decide to employ RAS for a task must be provided with sufficient information upon which to make a risk-based decision regarding the level of human control to apply each RAS within a certain operating environment in accordance with LOAC.

3.47 To perform this function, Defence must be able to provide commanders with technical advice on the RAS that they intend to use. Commanders will need to understand the methods that the RAS uses to achieve its mission and the risks that this method of operation poses. Technical advice can also assist in determining the type of controls to be used to mitigate these risks while still achieving the mission. Commanders will be responsible for determining the method of operation based upon their understanding of the capability boundaries of RAS and operational necessity.

Improve efficiency

3.48 RAS provide the opportunity to improve the efficiency of almost all areas of the Defence enterprise and may provide Defence with more flexibility in how it employs its limited resources. RAS will improve

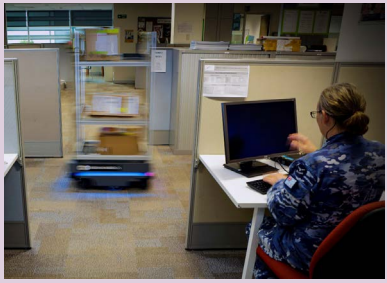
22 Explainable AI is a technology that allows systems to demonstrate their reasoning for an action.

efficiency by performing certain roles faster and more reliably than human operators, thereby increasing capacity. Defence may also use RAS to discover information within its data that can improve the quality of its activities, thereby improving efficiency.

3.49 Defence may employ RAS to conduct certain processes at greater speed, this may include RAS that can perform physical tasks at speeds that humans, or human operated systems cannot achieve. RAS may also perform cognitive tasks faster than humans, machines can ingest information at greater rates than humans and perform analysis of that information at greater rates.

3.50 RAS can perform processes more reliably than human operators. Machines are not subject to the human factors that may impact human decision making or physical performance. For example they do not make poor decisions because they are tired, or make mistakes because they are performing repetitive tasks. The use of RAS in certain processes can increase first-time quality of processes thereby reducing the need to perform a task again.

Example: Autonomous Logistics



An autonomous logistics system could improve the generation of logistic effects by ensuring that critical supplies were available when required. A goal based system could be directed to minimise capability down time by using predictive analytics. The system could optimising movements of critical stores while autonomous distribution robots could find, retrieve and dispatch stores faster than human operators and with a lower error rate.[23]

23 Image: SARAH (Supply Autonomous Robotic - Assistant Hardware) delivers parts from the Logistics Section to Flight Line

3.51 RAS also have the capacity to query larger sets of data than humans are cognitively capable of considering. They are capable of detecting patterns in data that may be missed by humans and provide the potential to increase the efficiency of Defence by understanding the enterprise in greater detail. For example, RAS may be able to query data sets to understand the health of the workforce and introduce preventative healthcare.

3.52 RAS have a number of strengths that can help increase the efficiency of the Defence enterprise, however the challenges of employing RAS must also be considered when determining which processes should be transitioned to RAS. The availability of appropriate data will be key to incorporating such systems and determining how they will be combined with humans to achieve the most effective solution.

Increase Mass

3.53 Increasing the mass of Defence will provide more options to generate an advantageous concentration of combat power, disperse the force or create deception.[24] Traditionally, Defence has had limited ability to generate mass through numbers and has instead focused on generating advantage through technology. RAS provide the opportunity for Defence to increase the mass of the force by developing large numbers of relatively inexpensive platforms and employing the current force more efficiently.[25] In addition to massed physical effects, RAS provide the opportunity to create mass effect in the information environment. For example, autonomous cyber systems can create massed effects without requiring large numbers of operators or physical systems.

3.54 Defence currently employs a small number of large, exquisite and expensive multi-role platforms that generate a large military effect in a limited area for a limited time. The strength of this approach is that it allows Defence to generate a technologically superior force however, reliance on a small number of platforms creates a weakness in Defence as the loss of one platform results in a large loss of capability. By increasing mass through many, small and cheap systems; Defence can

24 Friedman ibid. p 38

25 DSTG-CR-2020-0151 RAS Concept Red Teaming Report para 3.1

achieve greater flexibility, resilience and increase the dilemma for the adversary.

Example: Drone Swarms

Employing large numbers of small, easy to manufacture drones that are capable of swarming behaviours will increase the mass that Defence can generate. Autonomic drones could be projected into an area on a mother ship before being released to conduct a task. A large number of drones with different capabilities could coordinate their actions to create a resilient system that achieves its tasks by overwhelming enemy defences and adapting to enemy activity.[26]

3.55 Requiring RAS to perform multiple roles from a single platform will increase the size and cost of the platform, reducing their advantage over human operated systems. Therefore, Defence will need to employ role specific RAS in larger numbers to achieve the same capability as current platforms. This approach will require common platforms with interchangeable payloads to achieve cost effective systems.

3.56 **Swarming.** The term swarming refers to both the military tactic of swarming and swarm intelligence. To achieve an increase in physical mass through RAS with current manning levels Defence requires the ability to employ RAS with swarm intelligence to achieve a swarming tactic that confuse and overwhelm an enemy's defences. To achieve this ability, Defence requires RAS that can perceive their environment,

26 Image: Defendtex Drone 40. (Defence Image)

perceive the actions of other entities within the swarm and self-organise based off group behaviours. Employing this technology will move Defence from a paradigm where one operator controls one system to one where an operator controls a swarm of multiple systems and finally to a paradigm where the operator guides a swarm that controls its own actions. Swarm intelligence will allow Defence to employ swarm tactics without requiring constant communications back to a central control node, or communications between all elements within the swarm.

3.57 **Attrition.** Employing a large number of cheap systems may allow Defence to accept higher levels of attrition without detriment to the force. The operational concept for some RAS could be premised on the destruction of the platform. When paired with the manufacturing capacity necessary to replace platforms as they are expended, attritable systems would allow Defence to impose costs on adversaries as they would need to counter large numbers of low cost systems.

3.58 Defence must still consider its approach to the trade-off of quantity versus quality. While RAS provides the opportunity to accept higher levels of attrition the use of this approach must be balanced with the acquisition of smaller numbers of high-quality systems. The future force will likely benefit from a design that balances both approaches.

3.59 **Manufacturing.** Evolving from a force comprising a small number of exquisite platforms into a force of many, small and cheap systems will require a support base with sufficient manufacturing throughput to sustain the supply of systems. Australia has a modest manufacturing capability compared to other nations in our region, to generate physical mass with RAS, Defence requires the ability to access an indigenous manufacturing base with the capacity to create such systems and then surge to replace them when they are expended through use.

3.60 Reliance on sovereign manufacturing to continually generate large numbers of systems will create an additional vulnerability that adversaries may target. Sustaining operations will require a manufacturing base that can keep pace with operations and if an adversary can interdict our manufacturing they will reduce our ability to sustain operations. As Defence becomes reliant on RAS the resilience of the sovereign manufacturing capability necessary to support RAS must be considered.

Decision Superiority

3.61 Decision superiority assists the force to make and implement better and more accurate decisions while using tempo and leverage to best effect. Decision superiority relies on situational understanding, which is the accurate interpretation of a situation and the likely actions of groups and individuals within it. Defence will utilise RAS to improve the situational understanding of human or machine decision makers by improving their awareness, analysis and comprehension. This will enable timely and accurate decision making that increases the tempo of operations.[27]

3.62 **Awareness.** The FOE will feature complex operating environments and a future force that will have greater capability to generate data that is utilised for battlespace awareness. The processing of sensor data is currently a human activity that is constrained by the cognitive abilities of humans and the size of the workforce that can be allocated to the task. To generate awareness of the future operating environment Defence requires the ability to utilise RAS to sense, process, exploit and disseminate information.

3.63 **Analysis.** Defence currently relies on human experience to analyse a situation and generate courses of action. While this process is conducted by a team of staff that can bring a broad range of experience to a problem, that team will be limited by the experience that they can collect during their time in service. RAS provides the opportunity to conduct analysis using data that represents the collective experience of the whole of Defence while reducing the size of the staff necessary to analyse complex environments.

3.64 Human decision makers and their staff are also limited in their ability to generate courses of action from their analysis due to the time that it takes to develop options then consider their relative merits. In future operations, action that occurs at hypersonic or machine speeds will not allow sufficient time for human decision makers to generate an awareness of the environment and then analyse options. To overcome this problem, some Defence capabilities will need to be able to make decisions at machine speed.

27 ADDP 3.0 Para 1.35

Example: Decision Support

An autonomous decision support system could analyse the operating environment and recommend courses of action. Commanders would provide the goals of an operation to a system that combines all information regarding the operating environment. This system could determine ways that the commander's goals could be achieved and conduct an assessment of risks. Planning staff would consider these courses of action, adjust if necessary and then authorise the system to issue orders.

3.65 **Comprehension.** Human decision makers must be able to understand the analysis conducted by RAS, the options that it generates, the recommended course of action and why it makes such a recommendation. This will require systems that can present the outcomes of complex analysis in such a way that a human commander can understand all of the intricacies of the situation. Defence will require the ability to present RAS derived analysis in a manner that can be comprehended by human decision makers and achieve decision superiority.

3.66 **Decision.** Human commanders will need to consider how human and RAS decision systems should be employed to achieve decision superiority for a given situation. In certain situations the speed of RAS decision making may be necessary for decision superiority, in other situations a human decision maker may be required to consider aspects that a RAS is not suited to, such as cultural impacts.

3.67 There is evidence to suggest that diverse teams achieve better decisions in complex situations, Defence strives for diverse human teams to take advantage of this. When RAS are utilised for decision making Defence should continue to utilise diversity to improve decisions, this should still incorporate diverse human teams but may also utilise diverse RAS. Diversity in the systems utilised to support decision making could provide Defence with better decisions by working with multiple systems utilising different algorithms and data to consider a broader range of options.[28] Therefore Defence requires the ability to achieve decision superiority by flexibly employing diverse RAS and human cognition.

Decrease Risk To Personnel

3.68 RAS provides the opportunity for Defence to decrease the risks that personnel are exposed to during operations. Utilising RAS in place of humans for the performance of dangerous tasks has practical benefits to the force and should be used to provide Defence the ability to build and employ a resilient force.

3.69 **Non-Combatants.** RAS can provide Defence the ability to decrease the risk to non-combatants (and cultural or protected sites) in an area of operations. RAS that contribute to the utilisation of lethal effects could be designed to help decrease the risk of collateral damage. Unlike humans, RAS do not get tired, are not affected by the stresses of combat, do not seek revenge and can be programmed to not preserve themselves. When used in human commanded teams, RAS can help human decision making. For example, compared to human capabilities, the persistence of RAS and access to deep databases could be more likely to identify that a group of non-combatants have been hiding in a building identified for targeting. Such information may be based on data collected weeks prior and might not have been able to be analysed by the limited processing of human teams.

3.70 **Resilience.** RAS can allow Defence to increase the number of platforms that can apply a particular effect. This will provide Defence with greater resilience by allowing it to accept the loss of a larger number of platforms before experiencing a significant detriment to capability. With a robust supply and manufacturing chain RAS can be regenerated faster

28 TG-CR-2020-0151 RAS Concept Red Teaming Report para 3.3.2

than human systems, if a human crew is lost during operations, it can take years to replace the training and experience of the crew. In contrast, the latest data and algorithms can be uploaded to a new RAS as soon as it is built.

Example: Autonomous Armoured Vehicle

An autonomic armoured vehicle would reduce risk to personnel by allowing the platform to be placed in locations and conduct tasks where humans cannot be risked. The vehicle could determine where it should place itself based on the position of other vehicles and personnel. Direction of the vehicle could occur through remote control or hand signals. If necessary, the vehicle could accept that it will be destroyed in order to save the lives of personnel.

Countering RAS

Central Idea

3.71 The central idea to counter RAS is:

> Defence will counter adversary RAS through perception and control system attacks, information warfare and platform destruction.

3.72 Adversaries are likely to utilise RAS to achieve force characteristics similar to those proposed for our own Defence Force. While each adversary will employ RAS differently, they will utilise RAS to achieve efficiency, decision superiority and mass. Should Defence fail to implement capabilities that can counter adversary RAS any advantage gained by our employment of RAS will be lost and the adversary may gain significant advantage over us.

3.73 Over the next 20 years commercial entities and state actors will drive development in RAS. Actors of limited means will exploit commercial technologies for military purposes. Defence will also need to counter RAS that have been developed specifically for military purposes by state actors. Therefore Defence must be able to counter RAS across a broad range of sophistication.

3.74 It is difficult to predict exactly how RAS will be developed into military platforms and it is likely that there will be a range of platform implementations, from improvised threats derived from commercially available systems to bespoke military capabilities. Therefore this concept identifies four approaches to provide Defence with a broad spectrum counter to adversary RAS.

Example: Underwater Sensors

To identify an underwater sensor, Defence must understand its acoustic signature and develop the capability to detect it at operationally relevant ranges. To counter the system, Defence must know how the system operates and how to identify it in the environment so that tailored counters can be applied.

Identifying RAS

3.75 To counter RAS Defence must understand how each system operates. This will require technical and human intelligence to understand the capabilities of adversary systems and how they are employed. This information is also required to detect and identify RAS within a battlespace so that the counter can be applied. During operations, Defence should be able to determine what entities in the operating environment are RAS and what type of systems they are. This will allow Defence to direct the optimum counter against each threat.

3.76 In addition to the physical properties of adversary RAS, the capability of adversary systems will be determined by the algorithms used by those systems and the data that they can access. To understand the capability of a threat RAS and conduct information warfare counters Defence requires the ability to develop technical intelligence on the algorithms and data utilised by adversary RAS.

3.77 As the number of friendly, adversary and neutral RAS in operational environments increases, Defence must be able to prevent collateral damage and fratricide. To achieve this, Defence requires the

ability to determine the location of friendly and neutral RAS. This can be achieved through systems that track friendly RAS or through procedural methods of identification such as patterns of behaviour recognition. This information must be able to be disseminated throughout the force so that elements are aware of all RAS activities.

Perception Attacks

3.78 To operate autonomously, RAS must be able to perceive their environment and orient themselves within it. This can be achieved through external sources, such as GPS or internal sources such as optical sensors. By disrupting the ability of a RAS to perceive its environment, Defence can prevent adversary systems from operating or require them to revert to human controlled methods. Perception system attacks can also be used to alter the behaviour of a RAS by inducing a false perception of the environment.

3.79 **Inhibiting Perception.** Adversary RAS will utilise a variety of perception systems that may include visual, electromagnetic or acoustic sensors and Defence requires the ability to inhibit the perception of RAS. Capabilities to inhibit the perception of RAS may include jammers, laser dazzlers, smoke screens and noise makers.

Example: Smoke Screen

A smoke screen is a simple, yet effective method of inhibiting the perception of a RAS that utilises visual systems to understand its environment. By preventing the RAS from detecting terrain, landmarks or targets the smoke will prevent it from orienting itself and taking action.

3.80 **Altering Perception.** Camouflage is currently used to prevent human adversaries from detecting ADF forces and similar methods can be used to counter RAS. Defence requires the ability to alter signatures to prevent adversary RAS from identifying our forces. The methods of camouflage utilised by Defence will need to be tailored to the types of sensors utilised by RAS. When facing learning systems, Defence will need to change the type of camouflage used to prevent an adversary RAS from learning the signature of the camouflage.

3.81 **Deception.** Perception attacks on adversary RAS can deceive the system as to the true nature of its environment and force it to take action that is not desired by the enemy. Defence requires the ability to deceive the perception of adversary RAS. For example, GPS spoofing could be used to alter a systems understanding of its position and when combined with a control attack force allow Defence to capture it for exploitation.

Control Attacks

3.82 Although RAS are expected to require lower levels of human control, they will still need to receive direction from operators and pass the results of their activity to operators or other systems. By disrupting control systems, Defence can prevent adversary RAS from performing their mission or take over control of the platform. The employment of control system attacks must take care to ensure that they do not place RAS into a mode of operation more difficult to counter.

3.83 **Inhibiting Control.** By preventing an adversary from controlling their RAS, Defence can prevent them from setting tasks or receiving the results of these tasks. While many adversary systems will require very little human control over their function, they will still require a human to start the loop. This represents fewer opportunities to inhibit adversary control of RAS, but does not decrease the effect that can be achieved by this activity. Defence requires the ability to prevent an adversary from controlling their RAS, this may include disrupting communications to platforms or preventing adversary commanders from delegating the use of autonomy.

Example: Inhibiting Control

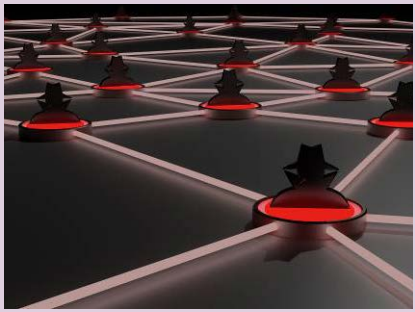
Cyber or Electronic Warfare activities could be utilised to disrupt the systems that an adversary uses to control their RAS. This will prevent an adversary from setting or changing tasks and goals for their RAS. It may also prevent the adversary from receiving critical information from their RAS.

3.84 **Assuming Control.** The ability to assume control of adversary RAS will allow Defence to remove the immediate threat posed by the platform and allow Defence to gain valuable intelligence by capturing adversary platforms for exploitation. Such an activity will require advanced knowledge of adversary control systems so that exploits can be developed. The act of assuming control of an adversary RAS will likely require the combination of a number of counter RAS activities, such as identification (of what platform is to be targeted) and perception attacks (to counter built-in controls that safeguard the RAS from capture).

Information Warfare

3.85 Autonomic and autonomous systems operate by utilising algorithms to query databases of information relevant to their task and then make decisions based on this data. As described in the RAS opportunities section of this concept, the quality of data can alter the outcome of the system. This represents an opportunity to counter RAS. By reducing the quality of the data used by an adversary, Defence can deliberately alter the relationship between what a RAS observes and the database upon which the system makes decisions. This will prevent a RAS from performing an action or force it to perform an action that an adversary does not desire.

Example: Botnet



An autonomous cyber system could be developed to reduce the quality of adversary data. This system could generate data that appears realistic, but is subtly altered before being collected by an adversary. The same system could be utilised to alter data held by an adversary, either before or during conflict. This system may not need to create a 'false reality' but generate uncertainty so that RAS will not act.

3.86 **Collection.** An adversary must collect data relevant to their intended use of RAS and this presents the first opportunity for Defence to influence the quality of the data held by an adversary. Defence requires the ability to generate inaccurate data for deliberate collection by an adversary. This may include purposefully adjusting platform signatures and providing adversaries incorrect data on doctrine and tactics for collection. Defence could utilise deep fakes to present incorrect information that is indistinguishable from reality. Such activities would ensure that in the event of a conflict, adversary RAS will not be able to correlate real signatures or activities to what is expected.

3.87 **Storage.** To build data sets of sufficient size an adversary will need to store collected data for later use. These stores could be manipulated to modify the data collected by an adversary. Defence requires the ability to manipulate data held by adversaries through cyber operations. This can include operations to subtly alter or erase data held by an adversary. Due to the volumes of data that adversaries may collect, Defence will require systems that can autonomously perform this function.

3.88 **Use.** During operations, adversary RAS will be able to learn from their environment and identify the delta between what it observes and its foundational data set. To continue to use information warfare as a counter to RAS, Defence must have the ability to continuously alter the data that is collected and stored by an adversary. This may involve continuously altering platform signatures to continue to confuse learning systems or it may involve autonomous cyber systems that continuously change the way they alter the data in adversary stores.

Platform Destruction

3.89 Defence requires the ability to counter RAS by destroying the platform using kinetic means.[29] Defence can use current capabilities to kinetically kill RAS that are large in size and utilised in small numbers. Future methods to counter RAS must consider that adversary systems will be small in size and cost, this will allow actors mount massed attacks. RAS that utilise swarming behaviours will provide an additional challenge because such systems will not have a centralised controller that presents a critical vulnerability.

3.90 Defence requires the ability to defeat massed attacks of small, swarming RAS by destroying the platform. This will require kinetic kill capabilities with deep magazines to be able to cope with massed attacks. To counter swarming attacks where adversaries make decisions at machine speeds, Defence will require defensive systems that utilise swarming behaviours that adapt to the tempo created by the adversary swarm.

3.91 **Adversary Counter RAS.** Adversaries will also develop counter-RAS capabilities utilising similar approaches to ours. The design of RAS must consider how to harden the system against adversary counter-RAS capabilities. Defence may also need to consider approaches that target the adversaries' ability to perform counter RAS before or during operations. Without such activities, the advantage of RAS may be negated by an adversary.

29 "Involving the use of forces of dynamic motion/energy to achieve and effect. Includes traditional explosive weapons as well as capabilities that can create radiofrequency effects such as continuous wave jammers, lasers, directed energy and pulsed radiofrequency weapons. ADDP 3.14 Ed 3 Terms and Definitions.

SECTION 4 – IMPLEMENTATION

4.1 RAS have the potential to change the way that every Defence capability generates effects necessary to achieve strategic, operational and tactical objectives. This section identifies the capabilities required to enable the incorporation of RAS into the force structure and to counter the threats that adversary RAS pose. It also identifies capability principles to determine how RAS are to be implemented into the force options development process before providing characteristics of RAS to guide the capability management process.

Ability Statements

4.2 To embrace the opportunity and counter the threat of RAS, Force Design Division must commence enhancement to, and acquisition of capabilities through the DCAP process that will provide the force the following abilities:

a. The ability to securely store and disseminate all data collected by Defence and allow it to be accessed by RAS.

b. The ability to verify that data and algorithms used by Defence are relevant to their purpose and operating environment.

c. The ability to access a hardened manufacturing base that can create and replace RAS at the speed of need.

d. The ability to locate and identify RAS in the operating environment.

e. The ability develop Intelligence Mission Data on the algorithms and data utilised by RAS.

f. The ability to inhibit, alter and deceive the perception systems of RAS.

g. The ability to inhibit and assume control of RAS.

h. The ability to manipulate adversary data through collection, storage and use.

i. The ability to kinetically defeat massed attacks of small, swarming RAS.

4.3 These abilities are the foundational requirements for all RAS that will be employed by Defence. Without immediate investment in these capabilities, the ability of Defence to implement RAS in the manner defined by this concept will be delayed and restricted. This may limit Defence from achieving a timely, asymmetric advantage.

Capability Principles

4.4 Capability managers must consider RAS options for each capability under development. Capability options that utilise RAS are to conform to the following principles:

a. RAS must be employed within Human Commanded Teams.

b. RAS should be optimised to specific roles.

c. RAS should increase efficiency.

d. RAS should increase mass.

e. RAS should enable decision superiority.

f. RAS should decrease risk to Defence personnel and non-combatants.

g. RAS should be countered by a combination of perception and control system attacks, information warfare and platform destruction.

Characteristics

4.5 To achieve the capabilities envisaged by this concept, Defence capabilities should be designed with the following characteristics:

a. RAS must be able to operate with multiple levels of human control.

b. RAS must be able to perform assessments that assist human adherence to IHL.

c. RAS should be able to demonstrate its reasons for actions or recommendations.

d. RAS should utilise swarm intelligence.

e. Defence should utilise RAS to sense, process and disseminate information.

f. Defence should utilise RAS to analyse complex environments.

g. Defence should utilise RAS to generate and analyse courses of action.

h. RAS should assist humans in comprehending complex environments.

i. Defence should utilise RAS and human cognition to make decisions.

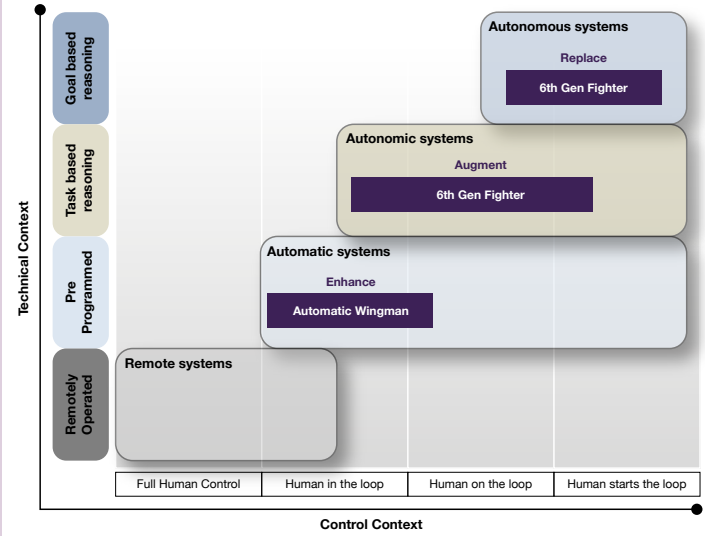
j. Defence should utilise RAS to compliment or supplement high-risk human tasks.

k. Defence should utilise RAS to increase the resilience of the force.

Implementation Options

4.6 There are three options for incorporating RAS into Defence capability. RAS can be utilised to either enhance, augment or replace existing capability. RAS can enhance current ADF capabilities by inserting technology into existing platforms. This will quickly improve

the functionality of existing platforms with a focus on value for money. This approach allows Defence to gain familiarity with RAS; however implementation will be limited by the original platform.



Example: Autonomous Air Combat Systems

RAS may be utilised to improve Defence's air combat capability by enhancing, augmenting, and then replacing current platforms. An automatic wingman could first provide additional mass by contributing additional sensor and effector platforms. This system could evolve into an autonomic system designed to penetrate high risk areas and employ effects where personnel cannot be risked. RAS could then replace 5th generation platforms with autonomous systems that combine human and machine cognition to achieve decision superiority.

4.7 Defence can augment current capabilities by implementing RAS that operate in conjunction with existing platforms. This approach allows Defence to increase the mass and capability of the force incrementally but employment of RAS may still be limited by the inhabited platforms they augment. Defence may replace capabilities with RAS, this will allow Defence to implement platforms that are not constrained by legacy designs or operating concepts.

4.8 Not all Defence capabilities may be suited to progression through enhance, augment, replace stages. As technology and operating concepts for RAS develop, Defence may determine that some capabilities should be augmented by RAS but not replaced, while other capabilities may be immediately replaced by RAS without enhance or augment phases.

4.9 **Integration.** Defence must be able to integrate RAS with major platforms and be interoperable with selected allies. A common control architecture for RAS that is interoperable with allies will allow Australia to share its RAS with partners and also allow us to utilise the RAS of allies.

Priorities

4.10 The process of acquiring data storage and access capabilities for RAS must commence immediately. Such a capability is the foundation for all RAS that will be employed by Defence and without such a system future platforms will be hampered. The process of building human confidence in RAS should also commence so that trust can be built on relatively simple systems in preparation for higher levels of autonomy.

4.11 The decision to prioritise RAS for a particular capability requirements will be dependent on the ability of RAS to perform that role and the capability advantage that is gained. As technology improves, the abilities and advantages of RAS will see them become suitable for more roles and Defence must continually assess the advantage of RAS in any given role.

4.12 Prioritisation of counter RAS capabilities must be cognisant of the rate of development in threat platforms and lead time for development of counters. Intelligence assessments will be required to determine when each type of counter will be required and provide sufficient lead time to develop the counter RAS capability.

Further Development

4.13 This concept identifies a central idea for RAS in Defence, but it cannot detail the implications for every part of the Defence organisation. Further research is required to ensure that the implications of RAS on the following areas is understood and managed.

4.14 **Operating Concepts.** RAS may require a change to the operating concept of Defence to exploit this technology. A new Future Joint Operating Concept (FJOC) is required to determine what changes Defence should make to the way it conducts operations so that it can capitalise on the strengths of RAS while minimising their weaknesses.

4.15 Defence must determine how the central idea of this concept will be developed to generate capability within each domain. The specific challenges and opportunities of each domain need to be identified, then mitigated and exploited. Capability Managers (CMs) must develop domain strategies to determine how they will employ RAS within the capability programs they manage.

4.16 **Policy.** RAS could have significant impacts to how Defence achieves its mission. Defence policy regarding the development and use of RAS must be reviewed as technology matures. As Capability Managers pursue RAS enabled/enhanced capability, consideration of Sensitive Technology Implications is needed.

4.17 **Legal and Policy.** There is a significant degree of debate within the international community, academia and by the media on the legal implications of RAS capable of employing a lethal effect, however it is the Australian position that the existing international humanitarian law framework provides sufficient regulation for such systems. Capability areas must work closely with policy and legal areas of Defence to ensure that the development, deployment and use of RAS continues to align with Defence's strategic objectives and adheres to Australia's domestic and international legal obligations and does not impact on Australia's negotiating position in international negotiations which would impact Defence's future capability and operational parameters.

4.18 **Doctrine.** Doctrine for employing and countering RAS must be considered. Defence must determine if current doctrine is sufficient for these systems or if new ideas must be generated.

4.19 **Workforce.** RAS will drive change in the Defence workforce and the development of a workforce strategy will be necessary to understand and prepare for the impact of RAS. From this RAS concept, a workforce strategy can begin to look usefully at both organisation and workforce fundamental inputs to capability, then assess impacts across different timeframes to cover the current, objective and future force.

4.20 While RAS will replace some roles currently performed by humans, they may also require the workforce to hold new skills and in some cases more advanced skills. RAS will require specialist skills to maintain and operate, Defence needs to determine the skills it must develop and maintain within its own workforce and how much reliance it places on industry operation and support.

4.21 Defence must develop a RAS workforce strategy to examine which roles should be developed within the workforce and which roles might be replaced. This strategy must drive capability program requirements to ensure that RAS are developed in a manner suited to the design of the future Defence workforce. A workforce strategy will also identify to industry what skills Defence will hold and why, this will allow industry to offer capability solutions suitable for employment with the planned workforce.

4.22 **Capability Life Cycle** (CLC). The development of RAS technology will occur faster than the rate it can be adopted through the current CLC.30 Adversaries that are able to adopt RAS technologies as they are developed will gain an advantage over Defence if it retains the current CLC. A RAS concept of generating mass through the use of many small and cheap systems provides the opportunity to consider RAS as short life-cycle platforms. Defence must develop an acquisition strategy for large quantities of short life-cycle platforms that are sustained through a process continual replacement. This will allow rolling upgrades to be implemented into the RAS capability rather than phased approaches to incorporating technology.

30 The opinion was voiced by a number of industry and academic participants in development workshops.

4.23 **Verification.** The process by which Defence verifies that capabilities are fit for operational use will need to be reviewed. This process will need to be amended to suit probabilistic systems that will learn during operation. Defence will need to understand how to verify systems that are the subject of continual improvement while balancing this need against the necessity of providing capability certainty that commanders will require to trust that RAS can be operated autonomously.

4.24 **Trust.** This concept has discussed the importance of human trust in RAS and that Defence will not be able to exploit RAS if it does not trust them. Further research is required to understand how Defence can determine if systems are trustworthy by building confidence in their abilities. Culture must also be considered, some of the ways that Defence currently conduct business will need to be altered to take advantage of RAS.

4.25 **Culture.** Should Defence adopt short life cycle, disposable platforms then a substantial cultural shift is required to embrace the potential of this operating paradigm. Capability acquisition and sustainment communities will need to let go of the principles developed to ensure long life cycle sustainment. Operators of disposable platforms will need to truly believe that their platforms are expendable and have a chain of command that supports loss of systems during training or operations.31 Further study is required to understand how to achieve such a change in workforce and industry.

4.26 **Security.** The Defence security principles framework should be reviewed to determine if current security guidance is sufficient for RAS. RAS is dependent on high quality data and therefore this data must be secured during storage, transmission and use. Should adversaries be able to access Defence data stores and captured RAS they could identify weaknesses in RAS or possibly conduct Information Warfare activities to alter the operation of our systems.

31 DSTG-CR-2020-0151 RAS Concept Red Teaming Report para 3.2.1

4.27 **Organisation.** Defence requires a central organisation for RAS to coordinate the collaboration between the services so that a common approach can be achieved. This organisation can further the development of operating concept, terminology and integration.

Partners

4.28 To develop RAS into operational capabilities Defence must consider Allies, Industry and Academia as partners critical to the advantage that we aim to achieve. At all stages of the implementation of this concept, Defence must be open about its requirements for RAS and engage widely to find novel solutions to Defence requirements.

4.29 **Industry.** The domestic defence industry allows Defence to develop capabilities customised to Australian requirements and provide timely delivery of systems at the pace required to sustain short life-cycle capabilities. Defence concepts and strategies must be developed in conjunction with Australian defence industry so that companies can be given guidance as to the products that they should develop and capacity that they should maintain.

4.30 Defence requires access to a manufacturing base that can produce enough systems to generate mass. Defence will require the ability to access manufacturing capacity during the acquisition of systems and then produce replacements. The ability to replace RAS during conflict will be a vulnerability that may be exploited, if an adversary is able to interdict the manufacturing process or supply chain then Defence would not be able to continue to employ disposable systems on mass.32 Further studies must determine how to generate and harden the sovereign manufacturing base required to support this concept.

4.31 A holistic consideration of the sustainment of RAS will allow Defence to determine the level of maintenance and manufacturing that should be organic to Defence or domestic industry. This requirement may surge during conflict, therefore the Defence Industry Capability Priorities must be reviewed to ensure that Defence invests in the industry required for RAS.

32 Ibid. para 3.2.2

4.32 **Academia.** Australian academics are already in the process of developing the ideas and technologies that will be required to fulfil the promise of this concept. However, Australian academic institutions can also assist Defence in creating an interdisciplinary understanding the implications of the employment of RAS for military purposes. Defence should engage with academia, to fully understand the implications of the use of RAS, and how it should address these implications.

4.33 The Trusted Autonomous Systems Defence Cooperative Research Centre (TASDCRC) fosters collaboration between Australia's defence industry and research organisations and aims to increase small and medium enterprise participation in its collaborative research to improve the research capabilities of the Australian defence industry. This organisation should be involved in all activities required to implement RAS in Defence.

SECTION 5 - CONCLUSION

5.1 RAS represent an opportunity for Defence and a new threat to be countered. The convergence of a number of technologies will drive the development of RAS that are small and cheap, allowing them to be employed at scale to generate mass effects at low cost. Embracing the opportunity of RAS will require Defence to think differently about its force structure, including how it shapes its workforce and develops trust in systems. Countering adversary use of RAS will require a multi-faceted approach that provides a number of defensive options.

5.2 To embrace RAS Defence must first understand the technology. The definitions and categories of RAS in this concept provide a simple way for Defence to characterise the abilities of RAS and how they are operated. These definitions allow Defence to have an open and honest dialogue about the capabilities it intends to pursue. The categories of RAS are a gateway to a deeper understanding of the technology that enables specific implementations.

5.3 Defence will not achieve advantage through RAS if it simply replaces current capabilities with RAS. Defence has the opportunity to achieve advantage by using RAS to increase the mass of the force by employing a large number of small, cheap and expendable RAS instead of a small number of large, exquisite and expensive platforms.

5.4 Adversaries will also develop RAS to attempt to gain advantage from this technology and in the future operating environment Defence will need to counter RAS developed by sophisticated state actors and RAS that have been improvised for military use by non-state actors. Defence must be able to identify RAS in the battlespace so that it can employ a suite of countermeasures against the specific threat.

5.5 There are significant challenges to utilising RAS for Defence capabilities. Defence must commence acquisition of the 10 capability requirements in section 4 to set the foundations for the employment of RAS and to counter the threat that these systems pose. RAS must then be considered for all Defence capabilities under development. Capability managers must adhere to principles for employment of RAS to ensure that Defence will gain advantage through RAS. Finally, integrated

program managers must ensure that RAS selected for acquisition have the characteristics necessary to overcome the problems associated with the employment of RAS while embracing the opportunity they represent.

Disrupting the operating environment

5.6 Emerging, disruptive technologies can only generate advantage if they are employed in a way that disrupts the operating environment. Defence can disrupt the future operating environment by employing RAS in human commanded teams to increase efficiency, generate mass and decision superiority while decreasing risk to personnel. To maintain this advantage Defence must also counter adversary RAS through perception and control system attacks, information warfare and platform destruction. Achieving these goals will require cooperation between Defence, Industry and Academia to realise the potential of people and technology.

ANNEXES:

A. Consultation Record

B. Definitions

C. Protected Annex (Available from Force Exploration Branch)

ANNEX A – CONSULTATION RECORD

Author

SQNLDR Robert Vine	(FDD)

Consultation

DG Future Land Warfare	(ADFHQ – Army)
DG Warfare Innovation – Navy	(ADFHQ – Navy)
DG Strategy and Plans – Air Force	(ADFHQ – Air Force)
DG ISREW & Cyber	(JCG)
Deputy Commander Joint Logistics	(CJLOG)
DG Capability Integrations Test and Evaluation	(FID)
DG Force Options and Plans	(FDD)
Assistant Secretary Maritime Analysis	(Contestability)
DG Military Strategy	(SP&I Group)
Executive Director Innovation	(CTO Division)
Deputy Chief Joint Operations	(JOC)
DG Special Operations Modernisation	(SOCOMD)
DG Workforce Planning	(DPG)
Director Land Force Design	(ADFHQ – Army)
Director Robotics and Autonomous Systems	(ADFHQ – Navy)
Director Plan Jericho	(ADFHQ – Air Force)
Director Defence Artificial Intelligence Centre	(JCG)
Director Joint Logistics Futures	(JLC)

Director C4ISR Design	(FID)
Director Force Options Development	(FDD)
Director Defence Analysis	(Contestability)
Assistant Secretary Strategic Capability Policy	(SP&I Group)
Director Technical Intelligence Assessment	(DIO)
Director Special Operations Development	(SOCOMD)
Chief Of Staff – Australian Defence College	(ADC)
Director Military Strategic Plans	(MSP)
Chief Of Staff – Head People Capability	(DPG)
Deputy Director Operations and Humanitarian Law	(Defence Legal)

References

This concept was developed with reference to the following sources:

- Balme, JH, '*The interpretation and application of LOAC in relation to autonomous weapons systems'* 2020
- Bell, SJ, *'What does the proliferation of automation throughout the Kill Chain mean for the Air Domain in the next decade?'* 13 Mar 20
- Blueprint Lab Submission
- Bluezone Group Submission *'Maximising ADF Capability in Maritime RAS'* 20 May 20
- Boulanin, Davison, Goussac, Carlsson, Stock *'Limits on Autonomy In Weapon Systems'* Stockholm International Peace Research Institute June 2020
- Britton Maritime Submission
- Brokk Systems Submission
- Defence Strategic Update 2020
- Defence Force Structure Plan 2020
- Defence Science and Technology Group, *'A method for ethical AI in Defence'* 2020
- Defence Science and Technology Group, *'Automated and Autonomous Systems for Combat Service Support: Scoping Study and Technology Prioritisation'* Oct 2016
- Defence Science and Technology Group DST-Group-CR-2020-XXXX, *'Concept for Robotic and Autonomous Systems Survey Analysis'* DRAFT
- Department Of Defence, *'Australian Army Robotic & Autonomous Systems Strategy'* Oct 2018
- Department Of Defence, Senate Estimates Brief *'Autonomous Weapons Systems*' SB20-000160 2020

- Department Of Defence *'Australia's System of Control and applications for Autonomous Weapon Systems'* CCW/GGE.1/2019/WP.2/Rev/1. 2019
- Fusion ECS Submission
- Layton, P 'Algorithmic Warfare' 2018
- Lockheed Martin Submission *'Design Considerations for a Reasoning Architecture'* Nov 18
- Dr Eve Massingham Submission
- McBain, HJ *'A future for the counter explosive hazard spectrum'* 2017
- Milani, P *'Autonomous Weapon Systems For The Land Domain'* 2020
- New York Times Magazine, *'Are Killer Robots the Future of War? Parsing the Facts on Autonomous Weapons'* 15 Nov 18
- Seabrook, R *'The Application of Artificial Intelligence to Military Operational Planning'* 8 Apr 19
- Spearpoint Solutions Submission *'The Integration Digital Soldier Concept' and 'Signature Management in Accelerated Warfare'* 31 May 20
- UK Ministry of Defence, *'Joint Concept Note 1/18 Human-Machine Teaming'* 2018
- US Army, *'Robotic and Autonomous Systems Strategy'* Jan 17
- US Congressional Research Service *'US Ground Forces Robotics and Autonomous Systems and Artificial Intelligence Considerations for Congress'* 20 Nov 18
- US Department Of Defense, *'AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense'*
- US Department Of Defense, *'Joint Concept for Robotic and Autonomous Systems (JCRAS)'* 19 Oct 16

- US Department Of Defense, *'Summary of the 2018 Department of Defense Artificial Intelligence Strategy'* 2018
- US Department Of Defense Directive, *'Autonomy in Weapon Systems'* 8 May 17
- Williams, Scharre, *'Autonomous Systems: Issues for Defence Policymakers'* NATO ACT publication 2017
- Young, SD, *'UAS Mounted Hyperspectral Imagery in IED Detection'* 26 Jun 19

Engagement

Force Exploration Branch conducted a wide range of engagement to develop this concept. Collaboration with Grounded Curiosity and The Central Blue blogs for a series on #ADFRAS2040 has generated an open debate on the role of RAS in the ADF. A summary of posts can be found here. Submissions were also sought from Industry and Academia to gain greater perspective on the subject. The author wishes to thank the individuals and organisations that contributed to the concept through workshops and submissions of papers.

ANNEX B – DEFINITIONS

Robotic and Autonomous System (RAS) RAS is an accepted term used by academia and the science and technology community to highlight the physical (robotic) and/or cognitive (autonomous) aspects of a system (or platform).[33]

Categories of RAS:

Remote Control Systems. A system that is operated by a human via remote methods. Without the remote control element the system has little ability to operate independently.[34]

Automatic System. A system that is pre-programmed to respond to stimuli in a rules based, deterministic manner and may achieve its function without further human input.

Autonomic Systems. A system that achieves human defined tasks by operating with reference to a set of pre-defined guidelines and responds to stimuli in a probabilistic manner. Autonomic systems may require human input to complete its function or may run without further supervision.

Autonomous Systems. A system that determines how to perform the tasks necessary to achieve a defined goal. An autonomous system responds to stimuli in a probabilistic manner and can alter how it performs tasks.

Control Categories:

Full Human Control. A human controls every aspect of the systems function, physically or through remote control.

33 US Joint Chiefs of Staff, *Joint Concept for Robotic and Autonomous Systems*, 19 Oct 2016

34 Andrew Williams. *Defining Autonomy in Systems: Challenges and Solutions.* NATO ACT Publication 2017. Page 30

Human In The Loop. The system performs some functions independently but requires a human to perform functions that complete the system's task cycle.

Human On The Loop. The system performs all functions autonomously but a human may intervene to stop or modify the outcome before the task is complete.

Human Starts The Loop. A human sets the operational parameters and initiates the systems operation; the machine requires no further human interaction to complete the task.

Algorithms are clear processes or sets of rules to be followed in calculations, data processing or other problem-solving operations.

Artificial General Intelligence (AGI) refers to the intelligence of a machine that could successfully perform all intelligent actions that a human can. Whilst AGI is being widely globally researched it does not yet exist.

Artificial Intelligence (AI) is a collection of interrelated technologies used to solve problems and perform tasks that, when humans do them, requires thinking.[35]

Autonomy. The ability of a machine to perform a task without human input. Thus an autonomous system is a machine, whether hardware or software, once activated performs some task or function on its own.[36]

Command. The authority that a military member lawfully exercises through rank or appointment to determine what is to be achieved by subordinate forces" (ADF Concept For Command and Control of the Future Force 2019)

Control. The act of coordinating forces towards outcomes determined

35 Defence Enterprise Artificial Intelligence Strategy 2019

36 Paul D Scharre. *The Opportunity and Challenge of Autonomous Systems*. NATO ACT publication 2017

by Command. Control is undertaken by elements that integrate the actions of forces necessary to achieve Command intent. (ADF Concept For Command and Control of the Future Force 2019)

Counter RAS. Counter RAS includes specified capabilities and techniques in which friendly force RAS is defended, protected and secured, with the potential to employ offensive capabilities targeted against adversarial RAS elements.

Goal Based Reasoning. A system that is programmed to achieve human defined goals and allowed to determine its own method of achieving these goals.

Machine Learning uses statistical techniques to give computer systems the ability to recognise patterns in data without being explicitly programmed. Machine learning can be achieved utilising a number of different methods that may or may not be specific to a task.

Software Agent (Bot). Refers to a system that is not physically autonomous but is authorised to act on behalf of a human to conduct non-physical, or cyber, tasks. To differentiate between physical and non-physical robots, software agents are colloquially known as ‘Bots’.

Swarming. Swarming includes the large mass of autonomous systems interoperating collectively to act and respond in a coordinated effort to provide an overwhelming effect.

Task Based Reasoning. A system that is programmed to conduct human defined tasks by operating with reference to a set of pre-defined information and guidelines.

AUSTRALIAN
DEFENCE FORCE