CURRENT AND FUTURE CHALLENGES IN AUGMENTING SITUATIONAL AWARENESS FOR REMOTE AUTONOMOUS SYSTEMS

KANAKA SAI JAGARLAMUDI, KEVIN LEE,
ARKADY ZASLAVSKY AND SHAINE CHRISTMAS

AUSTRALIAN ARMY RESEARCH CENTRE

/ Australian Army Occasional Paper No. 40

SERVING THE NATION

ARMY.GOV.AU

CURRENT AND FUTURE CHALLENGES IN AUGMENTING SITUATIONAL AWARENESS FOR REMOTE AUTONOMOUS SYSTEMS

KANAKA SAI JAGARLAMUDI, KEVIN LEE,
ARKADY ZASLAVSKY AND SHAINE CHRISTMAS

/ Australian Army Occasional Paper No. 40

ISSN (Print) 2653-0406

ISSN (Digital) 2653-0414

DOI: 10.61451/2675161

All enquiries regarding this publication should be forwarded to the Director of the Australian Army Research Centre.

To learn about the work of the Australian Army Research Centre visit https://researchcentre.army.gov.au

Cover image: A participant in the 2nd Commando Regiment Innovation and Experimentation Group Maker Week waits to launch their prototype unmanned ground vehicle distraction device for a demonstration during leadership day at the Special Forces Training Facility, Holsworthy Barracks. Source: Defence Image Gallery. Photographer: SGT Sebastian Beurich.

/ CONTENTS

/ 1. INTRODUCTION

The Defence Strategic Review 2023[1] evaluates Australia's defence capabilities, posture and preparedness to face the evolving strategic landscape. It represents the most ambitious review undertaken into Australia's defence strategy since World War II, aiming to ensure that the Australian Defence Force (ADF) can protect Australia's national security interests now and into the future. The strategy is driven by the following factors: geopolitical shifts, reduced warning times, technological advancements, climate change, and strategic partnerships.

Australia's contemporary strategic setting is characterised by an increasingly contested Indo-Pacific region. Specifically, the region is experiencing increased tension between the US and China. Analysts recognise that such tension could escalate into conflict, impacting Australia's national security interests. Increased military movements in the region mean that the threats come with little warning, requiring a prepared defence posture. Further, cyber warfare, autonomous systems (e.g. unmanned aerial vehicles (UAVs)), long-range precision strike weapons, and space deployments are changing the nature of conflict. To maintain a competitive edge within the region, Australia is seeking to integrate emerging technologies such as remote autonomous systems (RAS) into its defence capabilities.

RAS carry out missions in circumstances where deploying human operators is either dangerous or otherwise unsuitable.[2] Such situations may include the conduct of surveillance in enemy territory or collecting samples from extremely high-pressure regions in the ocean. To perform complex tasks autonomously, RAS use artificial intelligence (AI), sensors and robust communication networks. Importantly, RAS operate with a degree of autonomy and can be remotely controlled or supervised by human operators. The level of human intervention involved depends on the level of autonomy integrated into the RAS.[3] Their actions are based on the commands and supervision of human operators.

This paper is premised on the assumption that the Australian government is prepared to overcome economic barriers and to invest sufficiently in the adoption of RAS for military use. Assuming this is the case, it focuses primarily on how to address current challenges to the adoption of RAS within the ADF and how such systems can best be developed and deployed by Australia to achieve a strategic edge. The paper is organised as follows.

- Section 1 introduces the paper.
- Section 2 lists the key resources consulted.
- Section 3 outlines the concept of RAS and identifies the importance—and challenges in the achievement—of scalability in situational awareness.

- Section 4 considers the development of RAS technology at a global level, including examples of research agencies that focus on RAS. It also outlines how RAS are being used in several contemporary global conflicts.
- Section 5 provides substantive analysis of the challenges of scaling situational awareness. It explores technological issues such as data collection, quality of context issues, networking and processing. It identifies critical barriers to be addressed.
- Section 6 concludes the paper by summarising the findings and suggesting future research directions to overcome the challenges identified for deploying RAS in military operations.

/ 2. KEY LITERATURE SOURCES

The findings in this paper are based predominantly on a literature review of relevant publications from 2018 and 2024. For the most part, information is derived from non-military publications. This is because military organisations are often reluctant to disclose details of technological systems' design and implementation, as doing so could expose vulnerabilities in their capabilities. As a result, exploring RAS challenges through journals published by the ADF and counterpart militaries provides limited insights. Accordingly, this paper draws predominantly on academic journals and conference proceedings that have specifically focused on autonomous systems and military technologies. The primary literature sources can be summarised as follows.

Primary Journals Targeted for the Literature

- IEEE Transactions on Aerospace and Electronic Systems
- IEEE Transactions on Cognitive and Developmental Systems
- Defense Science Journal
- Journal of Field Robotics
- Unmanned Systems
- IEEE Transactions on Control Systems Technology
- Robotics and Autonomous Systems
- Journal of Defense Modeling and Simulation

Primary Conference Proceedings Targeted for the Literature

- International Conference on Robotics and Automation (ICRA)
- Association for Unmanned Vehicle Systems International (AUVSI)
- International Symposium on Safety, Security, and Rescue Robotics (SSRR)
- International Conference on Unmanned Aircraft Systems (ICUAS)
- IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)

- International Defence and Security Technologies Fair (IDET)
- Military Communications Conference (MILCOM)
- SPIE Defense + Commercial Sensing
- International Conference on Autonomous Agents and Multiagent Systems (AAMAS)

The authors also reviewed a broad range of papers that did not focus exclusively on RAS. These included studies that discussed inherent challenges, state-of-the-art advancements and various use cases. By critically analysing the methods and technologies used in these studies, along with the challenges identified, the authors gained a deeper understanding of the potential obstacles to developing and implementing RAS in a military context. These challenges were shortlisted to identify and reflect on those that affect the situational awareness of RAS most directly. The authors also considered technical features of RAS developed by major military powers available in open-source Smartsheets.

3. REMOTE AUTONOMOUS SYSTEMS—AN OVERVIEW

As Figure 1 shows, RAS are enabled by various technologies that need to be coordinated to function effectively. The three critical enablers of RAS are networks,[4] processing[5] [6] and data.[7] Networks enable connectivity and communication between systems and between the RAS operator and those systems. The technologies that enable such networks include—but are not limited to—Wi-Fi, 5G, 6G and physical connections. Processing involves the computational capabilities of RAS, which usually depend on AI models, hardware (e.g. a central processing unit (CPU), clock speeds) and operating systems (OS). Data is derived from sources such as sensors, knowledge bases (instructions for handling specific situations) and command inputs from the operators. The data fuels the system's decision-making and AI processes.

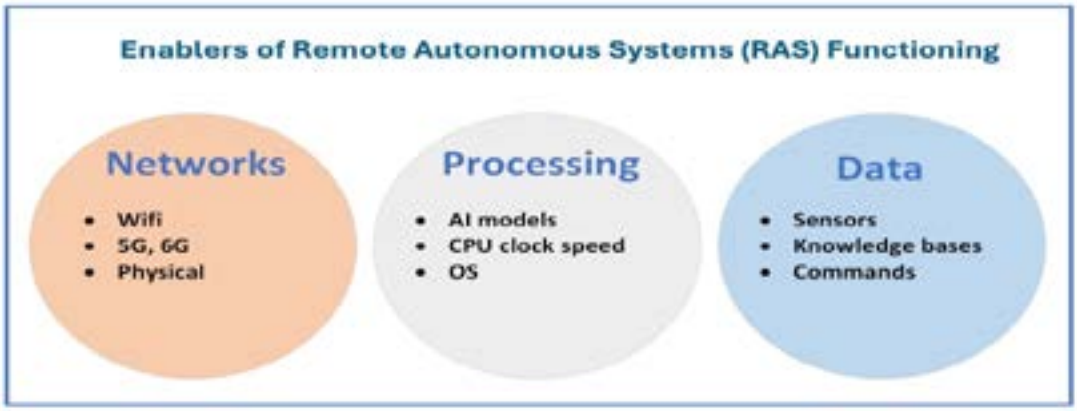

Figure 1: Enablers of RAS—networks, processing elements and data sources —with some examples of these enablers

The following subsections introduce the significance of situational awareness in RAS, along with the process of how it is created and utilised.

Situational Awareness in RAS

To operate effectively, RAS need to achieve situational awareness. Situational awareness[8] is a system's ability to perceive and understand the status of environments in which it operates. In a military context, situational awareness is the characteristic that enables RAS to understand the state of battlefields, to identify potential threats, and to make informed decisions to respond effectively. As Figure 2 shows, data collection, data transmission, data processing and decision-making are the core enablers of situational awareness in RAS.

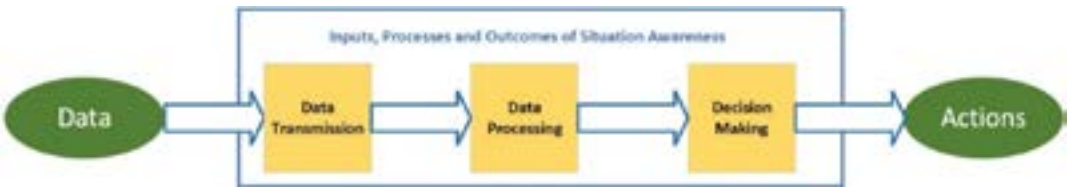

Figure 2: Inputs, processes and outcomes of situational awareness in RAS

- **Data collection.** RAS' onboard sensors or external data sources (such as peer RAS and application programming interfaces (APIs)) provide the data related to target environments. In addition to such data, RAS obtain their mission objectives from human operators.
- **Data transmission.** Data is transmitted through robust and high-speed networks to processing units that are either on board the RAS or in the cloud.
- **Data processing.** Advanced processes and AI models analyse the data in real time, interpreting it and integrating it with existing knowledge bases. The efficiency and effectiveness of these processes rely on the performance of hardware and software, e.g. CPUs, graphics processing units (GPUs), AI and machine learning (ML) algorithms.
- **Decision-making.** By analysing mission objectives, environmental data, and configured and historical actions in the system's knowledge bases, RAS infer current situations and project possible future states.

Based on the inputs, processes and outcomes of situational awareness, RAS execute respective actions. These actions may include adjusting the system's functionality and movements to navigate the environment, avoiding threats or taking other necessary actions to achieve mission objectives.

Example: Situational Awareness in a Military-Grade RAS (MQ-9 Reaper)

A useful military example of RAS with advanced situational awareness is the US Air Force's MQ-9 Reaper[9] (a UAV). The Reaper is equipped with a range of sensors that enable it to collect comprehensive data about its environment. Leveraging data from these sensors and onboard AI processing systems, it can autonomously detect and track potential threats or objects of interest.[10] It also possesses advanced satellite communication channels to transmit surveillance information to ground stations and receive mission commands, including potential engagement instructions.[11]
The capabilities of the Reaper show how data, processing and network modules can operate collaboratively to enable situational awareness in military systems.

Scenario: RAS Situational Awareness in ISR Missions

To understand the significance of situational awareness and its relevance to RAS, it is worthwhile to consider a scenario related to intelligence, surveillance and reconnaissance (ISR) operations. The requirement to conduct such operations currently motivates the Australian Army to incorporate RAS into its ISR capabilities.[12]

Generally, UAVs used in ISR missions are equipped with image vision technology and other sensors (an example is the US Air Force's RQ-4 Global Hawk[13]). In the scenario shown in Figure 3, a UAV with such capabilities is flying over a strategic area and providing continuous surveillance.

Figure 3: Creation of situational awareness in a military drone; it is retrieving the context attributes, processing them and inferring the situation (AI images enhanced by authors)

In this scenario, the drone's image vision cameras and sensors capture raw data such as the number of enemy troops, their GPS locations, and types of artillery. The raw data is then converted as high-level contextual information that represents the situational attributes related to the entity.[14]

The information flow diagram in Figure 4 shows how this occurs[15] and the processes/systems required in each phase. As can be seen, the raw data, once received, is processed by context managers (or context interference engines that exist in context management platforms (CMPs) such as context-as-a-service (CoaaS)[16] and FIWARE.[17]

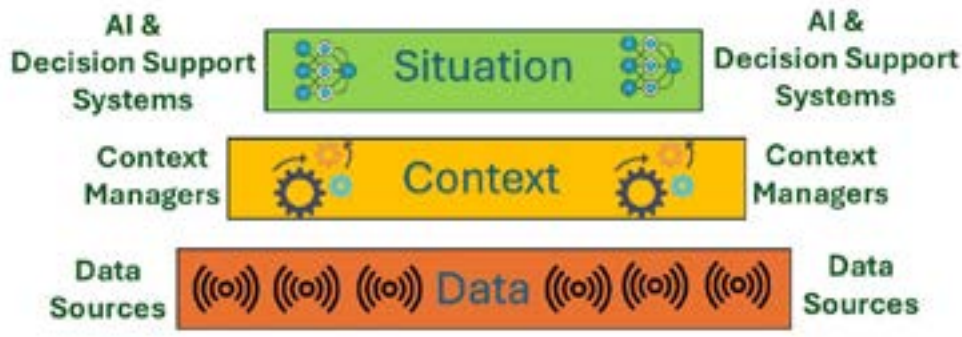

Figure 4: Phases and systems in transforming raw data into situations in RAS

To process the data, CMPs use technologies such as neural networks or ontology-based reasoning[18] to perform context inference. In this way, raw data is transformed into context attributes such as the density of enemy forces, movement patterns, and operational status of their artillery. These context attributes are then analysed by AI and decision-making systems to infer situations, such as identifying potential threats and determining enemy attack plans and movements.

RAS often rely on predefined context sources for situational awareness. Therefore, technologies like CMPs[19] can serve as a bridge between RAS and diverse context sources, dynamically identifying and aggregating relevant information. For example, in real-world deployments, RAS may use fixed environmental sensors or vision systems to gather temperature, vegetation type, and crowd density data. While these sources help assess conditions, such as bushfire risk, enhanced situational awareness often requires dynamic contextual information beyond what predefined sources can provide. For example, in a forest fire scenario, knowing the precise location and available resources of nearby firefighters could enable rapid response. Predefined context sources cannot provide this level of dynamic context, which requires a middleware solution.

RAS and Operational Decision-Making

Incorporating mature RAS into military capabilities can support the achievement of significantly better operational decisions. According to a study on C2 operations in modern warfare[20] published in the Australian Army Journal, commanders no longer have direct visibility over the battlefield; instead, they issue commands from remote headquarters. A typical command-and-control (C2) system involves three key states: the actual state—information about the battlefield relayed to commanders from various sources; the intent—the decisions and actions taken by commanders to achieve a desired outcome; and the outcome—the reflection of mission success.

Incorporating RAS into the C2 information paradigm can significantly enhance the effectiveness of C2. Since the quality of a commander's decisions relies heavily on the quality of the available information, data sources must accurately reflect the true state of the battlefield. Furthermore, the commander's intent must be reliably communicated back to operational entities (e.g. troops or systems), which depends on C2 components such as transmitters and carriers. Figure 5 illustrates how RAS can improve various information states in C2, using a battlefield context as an example.

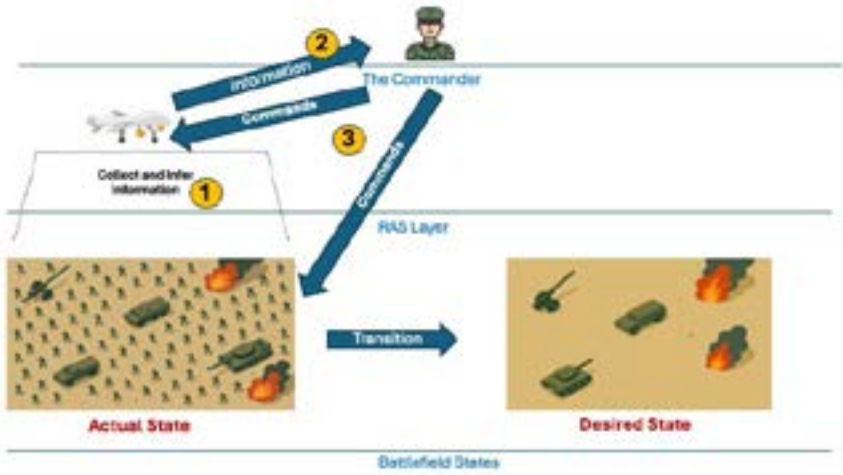

Figure 5: Process of enhancing information states in a command and control (C2) scenario using RAS

Step 1: The UAV collects data from its built-in sensors (e.g. cameras) and peer RAS. The data is then processed to create a situational overview.

Step 2: This overview is then transmitted to the remote commander station. Based on the high-level situational awareness provided by the RAS, the commander concludes that continuing the military engagement could lead to further losses and decides that a fallback is the more appropriate option.

Step 3: The commander issues a command to the field units to retreat to safer positions, using one of the fallback routes suggested by the RAS, moving towards the *desired state*. In parallel, the commander also sends further commands to the RAS, tasking it with monitoring enemy movements or assisting in coordinating the retreat.

In the figure, 'Actual State' shows allied forces under heavy attack, with tanks and soldiers engaged and several areas affected by explosions. In response, RAS units of the allied forces actively collect and analyse battlefield information—determining strategic positioning and viable fallback routes. In this scenario, RAS assists the commander to reach well-informed decisions, even in the 'the fog of war'.

While RAS can access information, make inferences, and even recommend actions, the ultimate authority and accountability remain with the human commander. Accordingly, this process of receiving input from autonomous systems and issuing commands or feedback is called the human-in-the-loop.[21] It ensures ethical oversight and trust in autonomous agents.

/ 4. GLOBAL DEVELOPMENTS IN RAS

According to a work published in the Australian Army Journal,[22] in addition to Australia, many countries with advanced military capabilities, such as the US, China, South Korea, Israel, the UK and Singapore are also focused on the adoption of RAS for military purposes. Analysts consider that these countries are well positioned to overcome technological, resource, ethical and legal, operational, and acceptance barriers to the use of RAS by their armed forces. There is variation among these nations, however, as to their key motivations for adopting the technology. For example, the US and China aim to lead technological innovation to maintain their relative military strategic advantage. Israel and South Korea focus on leveraging RAS to enhance military operational efficiency and reduce risks to military personnel. Meanwhile, Australia aims to keep pace with global superpowers by integrating advanced military technologies into its national security strategies.

Beyond strategic imperatives, there are several other factors that affect the way in which nations approach the adoption of RAS. For example:

- The US is able to lead in technological innovation because it allocates substantial economic resources to military research. Nevertheless, it faces challenges in transitioning prototypes to full-scale products due to organisational risk aversion, particularly as it relates to ethical and legal constraints. Further, despite its healthy research budget, the US still struggles with the high costs involved in testing new technologies.
- China's government strongly supports the use of RAS in a military context, but deployment of this technology is constrained by the interoperability challenges involved in coordinating its various military branches. Like other nations, China is also constrained by ethical and legal constraints relating to the use of lethal force.
- South Korea has a high adoption rate for industrial robots and makes significant investments in autonomous systems. However, Korea's deployment of RAS remains constrained by training and organisational issues within the military.
- Despite economic and resource limitations, the Israeli government places a high priority on the rapid deployment of RAS to support ongoing military operations.
- The UK expresses strong interest in RAS, but is hindered by ethical, legal and resource constraints.

- Singapore has a lower resource and technological capacity for deploying RAS in a military context, but offsets this with high cultural acceptance.
- Australia has a strong technological base for the generation of RAS but faces economic limitations in efforts to deploy new technologies.

Research on RAS for Military Use

Worldwide, there are many research institutions involved in efforts to develop RAS for military purposes. Figure 6 shows the organisations (by country) that are known to be working in the field of RAS. This section lists these institutions and highlights a few key RAS research projects.

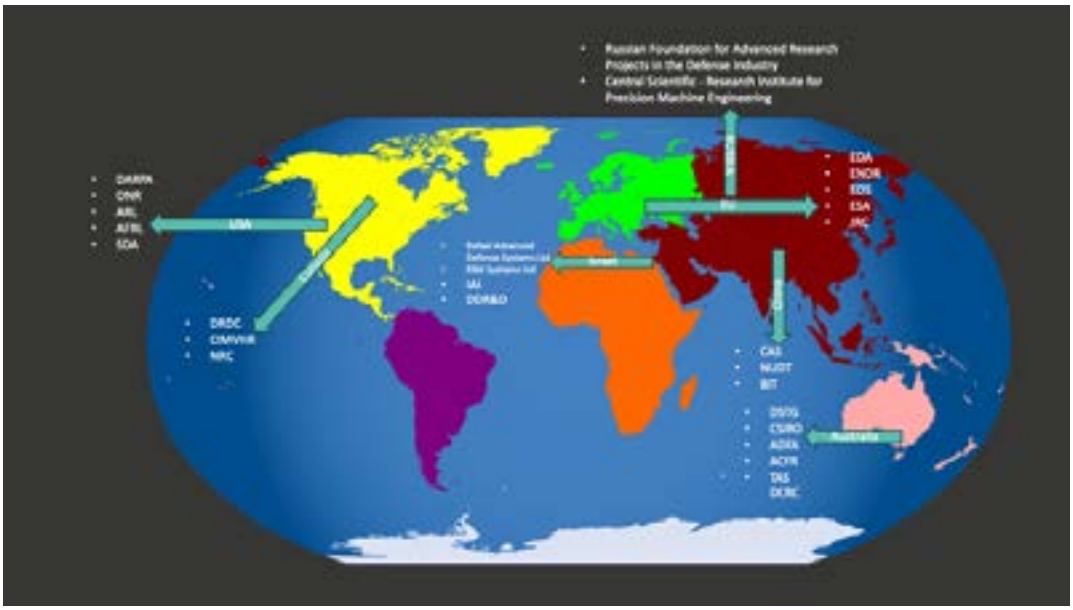

Figure 6: Research institutions that are potentially engaged in RAS research

United States

Research institutions in the US include the Defense Advanced Research Projects Agency (DARPA). It has developed the OFFSET program to gain strategic edge in urban warfare. In an effort to improve military operational flexibility, DARPA focuses on using UAV swarms and the Gremlins program for mid-air deployment and recovery of drones. The Office of Naval Research (ONR) Sea Hunter program has led to the development of autonomous underwater vehicles (AUVs) that can patrol the seas and detect mines.[23] The Air Force Research Laboratory (AFRL) Skyborg program aims to create unmanned aircraft teams for missions in contested environments. The Space Development Agency (SDA) has built a

network of military satellites called the Proliferated Warfighter Space Architecture (PWSA), which can support missile tracking and early warnings.[24]

China

Key academic institutions such as the Chinese Academy of Sciences (CAS), the National University of Defense Technology (NUDT) and the Beijing Institute of Technology (BIT) are involved in China's defence technology development. Several manufacturers, including Hongdu Aviation Industry Group, contribute to the development and production of RAS. For example, Hongdu Aviation Industry Group developed the GJ-11 Sharp Sword UAV, a stealthy autonomous combat drone designed for high-risk reconnaissance and strike missions.[25] NUDT developed AnBot, an autonomous robot designed for surveillance, patrolling and threat detection.[26]

Russia

The Russian Foundation for Advanced Research Projects serves as Russia's counterpart to DARPA. Another key institution, the Central Scientific Research Institute for Precision Machine Engineering, specialises in developing and producing advanced weaponry and military equipment. The Russian Foundation for Advanced Research Projects developed the Marker robotic combat platform,[27] an autonomous ground vehicle capable of navigation, firing, and distinguishing between civilians and enemy troops.

Israel

Key defence research organisations include Rafael Advanced Defense Systems, which has developed precision-guided systems such as the Sea Breaker[28] (a long-range missile—up to 300 kilometres—for maritime and land targets), the Thunder Storm[29] (which integrates UAVs for advanced situational awareness in combat), and Rocks,[30] a high-accuracy air-to-surface missile which is effective even in GPS-denied environments. Also, Elbit Systems Ltd has created several advanced autonomous systems, including Dominion-X (which manages autonomous and semi-autonomous robotic swarms in multi-domain warfare),[31] Torch-X (designed for planning and managing unmanned platforms and missions),[32] and Thor (an unmanned aerial system (UAS) that can carry up to 10 kilogram payloads in diverse weather and terrain conditions).[33]

Israel Aerospace Industries (IAI) manufactures aerospace and aviation systems for military and civilian use and has developed a wide range of UAVs. The Directorate of Defense Research and Development (DDR&D) works to maintain Israel's technological superiority and military edge. DDR&D, in collaboration with Rafael Advanced Defense Systems and Elbit Systems, has developed the Iron Beam laser interceptor system[34] to counter aerial threats.

Canada

Research institutions in Canada include Defence Research and Development Canada (DRDC). DRDC is working on developing AUVs[35] for ISR, mine countermeasures, anti-submarine measures, and inspection.[36] In addition, the Canadian Institute for Military and Veteran Health Research (CIMVHR) supports research on veteran and military health, including technologies that improve soldier performance and resilience. It is also exploring health-monitoring sensors that could be integrated into autonomous systems to provide real-time health data alerts during missions.[37] The National Research Council Canada, Canada's largest research organisation, collaborates with the Canadian Armed Forces to develop autonomous systems for military use. One of its projects focuses on improving ship autonomy in harsh maritime environments.[38] Another focuses on integrating UAVs into Canadian airspace through effective path planning.[39]

European Union

The European Union has several research institutions and initiatives focused on defence research. These include the European Defence Agency (EDA), the European Network of Defence-related Regions (ENDR), the European Organisation for Security (EOS), the European Space Agency (ESA) and the Joint Research Centre (JRC). Among the EU initiatives, notable outcomes in autonomous systems research include OCEAN2020,[40] an EU-funded project under the EDA that has had some initial success in integrating unmanned systems to improve situational awareness in maritime environments.[41] Another example is the European Robotic Orbital Support Services (EROSS) program by ESA, which focuses on autonomous in-orbit satellite servicing[42] such as docking and repairs. This program has led to the development of space-based autonomous systems with successful demonstrations.[43]

Australia

The most notable Australian research initiatives concerning military and autonomous systems involve the Defence Science and Technology Group (DSTG). For example, in collaboration with Boeing Australia, DSTG has developed the Loyal Wingman, an air combat drone that flies alongside piloted aircraft.[44] It uses AI to support manned–unmanned teaming, providing additional ISR and combat capabilities. DSTG has also partnered with Japan's Acquisition, Technology, and Logistics Agency (ATLA) to develop unmanned underwater vehicles (UVVs).[45] This collaboration aims to develop the autonomous systems for underwater ISR missions.

The Australian Army also possesses the M113AS446 armoured personnel carrier (APC). While traditionally requiring a two-person crew to operate, these APCs are being transformed into optional crewed combat vehicles equipped with autonomous capabilities

to operate remotely, reducing soldier exposure to direct combat risks.47 The Army has also acquired the Autonomous Tactical Light Armour System (ATLAS).48 This is an 8x8 armoured vehicle with high levels of autonomy, with obstacle avoidance, route planning and tactical decision-making capabilities. While it can operate independently, a human operator remains in the loop to make critical decisions, ensuring both efficiency and control in complex environments.

Beyond DSTG, commercial entities are achieving technological advances relevant to the ADF. For instance, Boeing Australia has developed the MQ-28 Ghost Bat. This is an uncrewed collaborative combat aircraft designed to act as a force multiplier. It can operate alongside manned fighter jets, providing support in air combat operations.[49] Further, CSIRO's Hovermap drone can navigate autonomously in GPS-denied environments, making it useful for defence, search-and-rescue and environmental monitoring applications.[50] Other institutions involved in RAS research include the Australian Defence Force Academy (ADFA) operating in conjunction with the University of New South Wales; the Australian Centre for Field Robotics (ACFR); and Trusted Autonomous Systems (TAS), which is Australia's first Defence Cooperative Research Centre (DCRC).

RAS in Current Conflicts

Examples drawn from contemporary conflict indicate that RAS used in contemporary military applications lack fully functional situational awareness. They are not able to perceive, infer, or act based on their surroundings. Instead, they rely heavily on operator commands or pre-programmed parameters. This is a major limitation when operating in network-constrained environments or under constantly changing mission conditions. Nevertheless, RAS are already proving their value as a military capability, predominantly in:

- surveillance and reconnaissance—many drones are equipped with vision technology that enables them to autonomously gather intelligence
- precision strikes—some drones can identify targets using vision or LiDAR technologies and engage them based on pre-programmed parameters
- electronic warfare—some drones can autonomously jam or disrupt enemy communications and radar.

The following are some notable examples where RAS are being deployed in contemporary conflict.

Ukraine–Russia Conflict

In their ongoing conflict, there is extensive use of drones and autonomous systems by both Russia and Ukraine.[51] Ukraine employs a wide range of drones, from small and commercial-off-the-shelf (COTS) models to large military-grade ones. For example, Ukraine uses TB2 Bayraktar, a Turkish-made drone capable of striking heavy ground targets. Ukraine has also repurposed racing and film-making drones for military purposes by retrofitting them with explosives for targeted strikes.

Ukraine's drone strategy has supported cost-effectiveness, flexibility and air superiority over Russia. Ukraine uses TB2 Bayraktar RAS-enabled drones to accurately strike high-value targets by loitering and delivering munitions effectively. In parallel, Ukraine's use of relatively inexpensive COTS drones has enabled it to adapt quickly to changing battlefield conditions, making drones a versatile tool in its arsenal. Readily available and inexpensive smaller drones are deployed for single-use strikes, reducing costs while simultaneously reducing risks to deployed personnel. Ukraine also focuses on adapting drones for electronic warfare by using smaller drones that are harder for Russian forces to detect and shoot down. By deploying large numbers of drones, Ukraine has managed to slow down Russian advances in the air battle. In sum, drones have enabled Ukraine to achieve enhanced ISR on enemy movements and positions and improve its situational awareness on the battlefield, and has ultimately enabled it to compete effectively against a numerically superior Russian army.

In response, Russia has deployed both domestically produced and ally-supplied drones. Russian-made drones include Orion, Eleron-3, Orlan-10 and Lancet. Due to Western sanctions limiting domestic production, Russia has relied heavily on the Shahed-136, an Iranian-made drone capable of carrying up to 100 pounds of explosives over distances up to 1,200 miles. Drones like Orlan-10 are widely used for battlefield reconnaissance, providing intelligence and target acquisition to support artillery and missile strikes. Russia's motivation for adopting these drones is to overcome production challenges caused by sanctions. These drones play a critical role in strengthening Russian forces, delivering vital intelligence and enabling precise targeting. Their use, especially in urban areas, also has a significant psychological impact on Ukrainian forces and civilians, contributing to Russia's overall strategy of attrition.

Israel–Palestine Conflict

Israel is known for its advanced military technology and uses several drones and autonomous systems.[52] Examples include the Hermes 450, designed for surveillance and precision strikes[53] and for flight endurance (up to 17 hours). Larger drones such as the Heron TP and Hermes 900 are also part of Israel's fleet and have been used for missile strikes. These drones form a system for both surveillance and combat. Like Ukraine, Israel

also employs smaller drones for reconnaissance and precision targeting in urban environments.

Israel has adopted drones to achieve operational efficiency, minimise risk to personnel, maintain technological superiority and reduce costs. Most of its drones can operate continuously for long periods, providing surveillance and carrying out operations without interruption. They perform dangerous tasks, reducing the need for soldiers to enter high-risk areas. Using drones also lowers operational costs compared to manned aircraft, allowing for more flexible and frequent deployments.

Sudan

Autonomous systems are known to be used in the ongoing internal conflict between the Sudanese Armed Forces and the Rapid Support Forces. These systems are not as advanced as those used in the conflicts listed above. However, they reflect a growing trend where even less technologically developed countries are able to adopt autonomous solutions for military purposes. The Sudanese Armed Forces are using Iranian-supplied Mohajer-6 drones.[54] These drones, manufactured by Quds Air Industries in Iran, are capable of air-to-surface attacks.[55] There are open-source references to the use of drones by the Rapid Support Forces since mid-2023. There are also reports of the Rapid Support Forces using drones to drop mortar bombs and other explosives, although the origin of these drones remains unclear. The use of drones in the Sudan conflict highlights the evolving nature of modern warfare around the world, even in developing nations.

/ 5. SCALABILITY CHALLENGES

Despite substantial military investments in RAS by many countries, scalability remains a particular challenge. Scalability in this context means the capability of RAS to gather different types of context attributes to generate useful situational insights in dynamically changing environments. Having adequate data sources and network and processing resources is critical for achieving RAS situational awareness and in supporting the C2 of military operations. There are, however, several major challenges to the data collection, transmission and processing capabilities of RAS. For example:

- RAS have difficulty integrating diverse data streams from multiple sources, dynamically allocating and managing network resources, and processing data in real time.
- In remote regions, RAS often face network limitations, such as low bandwidth, which make it hard to stay connected with other RAS units and mission controllers.
- RAS typically lack technology to automatically find relevant data sources.
- RAS often have limited onboard computing power due to energy and space restrictions.

The following subsections explore these and related challenges in detail, focusing on how they impact scalable situational awareness in RAS. The definitions of the challenges and descriptions of their impact on situational awareness can serve as a reference for testing and evaluating the design, development and deployment of RAS by the ADF.

/ 5.1 DATA CHALLENGES

As noted previously, situational awareness in RAS depends on four key processes: data acquisition, transmission, processing, and decision-making. Figure 7 depicts example challenges that may influence each phase of situational awareness in RAS. It shows that current technology is not sufficiently advanced for RAS to dynamically identify relevant information sources and to collect high-quality contextual information.

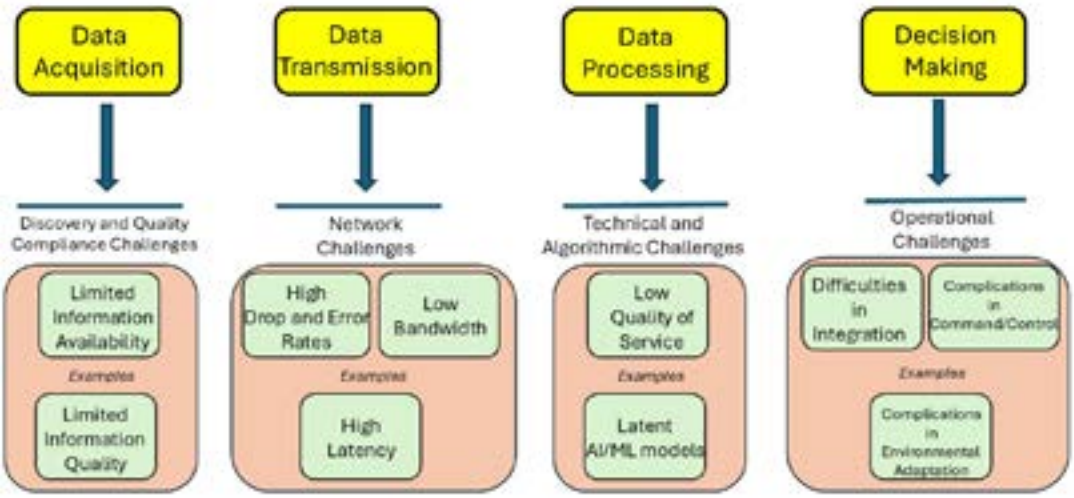

Figure 7: Challenges (with respective examples) affecting the scalability of situational awareness in RAS

Data Acquisition

Real-time data acquisition is essential for situational awareness in RAS. The data collected includes contextual information about the environment in which RAS operate. Contextual information (or context) refers to any information describing the situation of an entity (place, person or object).[56] When considering RAS, context is represented by context attributes, each indicating a piece of mission-related data. These context attributes are aggregated and analysed to infer the overall situation, forming situational awareness and enabling RAS to make informed decisions. For example, combining context attributes like temperature readings, local vegetation type (e.g. dry forest areas) and crowd density allows RAS to assess the risk of bushfires. This situational awareness enables RAS to recommend or initiate preventive measures, improving both safety and responsiveness during deployment.

Data Transmission

Data transmission challenges are mostly network related. They occur in network systems that connect multiple autonomous systems or those that link them to the cloud, control centres or commanders. Common issues include high error rates, low bandwidth and high latency.

For data processing, technical factors such as the quality of service (QoS) of cloud resources (used by the autonomous systems to distribute the processing load) and local processing capabilities within the systems play a critical role. Poor resource availability, reliability or interoperability (which are QoS dimensions related to processing), can disrupt processing and halt decision-making.

Data Processing

Limited integration of CMPs and similar technologies forces RAS to rely on predefined context sources, restricting situational awareness. This situation prevents seamless discovery and integration of new or dynamic context sources. For example, in a disaster response scenario where autonomous vehicles assess structural damage using sensor readings,[57] limited access to context attributes means they might use only default sources like proximity sensors and weather data. Without middleware to dynamically access additional context sources (e.g. sensors producing real-time structural vibrations or building layout changes), the vehicles could overlook environment shifts. This may lead to inaccurate assessments of structural stability and delay rescue efforts. Similarly, during a surveillance operation in an urban setting, RAS units equipped only with predefined context sources might misinterpret crowded pedestrian areas as high-risk zones. Without integrating additional contextual information, such as holiday event schedules, the system could overestimate threats, diverting attention and resources from actual security risks.

Decision-Making

Beyond issues related to data acquisition, transition and transmission, there are other factors that affect the situational awareness achievable by RAS that are non-technical in nature. These include issues such as how well RAS integrate into military frameworks, personnel training and environmental conditions. These factors are beyond the scope of this paper but are no less relevant.

/ 5.2 QUALITY OF CONTEXT CHALLENGES

QoC[58] refers to how relevant and usable contextual information is for applications like RAS. The quality properties of a context attribute are represented by distinct QoC metrics, and the combination of these metrics determines the compliance level of each attribute. Common QoC metrics include timeliness, accuracy, completeness, resolution, sensitiveness, representation consistency, and significance.[59]

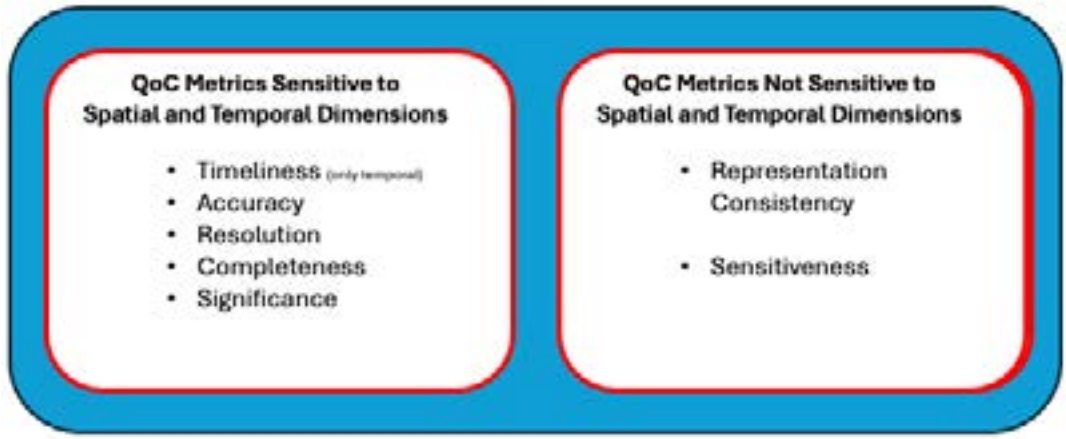

Figure 8: Classification of QoC metrics based on the impact of spatial and temporal dimensions on them

As depicted in Figure 8, several QoC metrics are highly dynamic, being sensitive to both spatial and temporal factors. These metrics impact the real-time performance of RAS by influencing the system's ability to maintain accurate situational awareness. Preserving these metrics requires the selection of adequate context sources. It also depends on robust networks and sufficient processing resources to ensure that RAS remain within their spatial and temporal bounds until the context sources are formed using CMPs. The task of acquiring QoC compliance is challenging because most existing CMP technologies (such as FIWARE[60]) lack standardised methods for achieving it. Additionally, constraints in network bandwidth and processing capabilities further complicate the preservation of these metrics. These challenges and their implications are reviewed in the following subsections.

Before undertaking this review, however, it is worth noting that not all QoC metrics are equally affected. Unlike the other metrics, consistency and sensitiveness are not influenced by spatial and temporal factors. Nevertheless, they indirectly contribute to situational awareness by improving context accessibility and preserving access security. Therefore, they are particularly important in enhancing interoperability between systems.

Timeliness

Timeliness refers to a context attribute's validity with respect to time. It is critical for RAS to obtain timely context, as these systems often operate in dynamically evolving environments where decisions need to be made within strict time constraints. For example, in a surveillance operation, UAVs may rely on real-time GPS data from ground troops to determine their precise location. This data enables the UAVs to identify and engage with the optimal personnel necessary for the mission. However, if there is a delay in receiving this context, and this delay results in outdated GPS data, there may be significant operational implications.

For example, delayed information might cause UAVs to select units that are far from the point of interest or mission-critical zones, leading to prolonged response times and missed opportunities to address mission objectives. In high-stakes scenarios, such as search-and-rescue missions or battlefield engagements, such delays could compromise the success of the operation and increase risks for personnel on the ground.

Accuracy

Accuracy measures how closely the delivered context aligns with the ground truth. Delays in transmitting information, coupled with spatial movements of the target, can cause discrepancies between the sent data and the actual ground truth. For example, in a reconnaissance mission, artillery units may depend on context from UAVs that identify and relay information on civilian vehicles and enemy combat vehicles to determine situations for combat engagement. If the delivered context is inaccurate—such as misclassifying a civilian vehicle as hostile—it could endanger civilian lives and potentially escalate conflict. Similarly, in disaster response scenarios, if a UAV's thermal imaging misidentifies a heat source as a human survivor when it is merely residual heat from equipment or debris, rescue efforts may be wasted on irrelevant areas, delaying aid to actual victims.

Resolution

Resolution represents the granularity of context, which is the level of detail necessary to meet the specific requirements of a task. Resolution can vary over time and across space. Resolution can be classified into temporal and spatial dimensions. Spatial resolution refers to the granularity of accuracy in describing a location. For example, a low spatial resolution

might simply identify a location using the coordinates as a point on a map, while a high spatial resolution would provide details such as whether the point represents a house, a building or a cabin, and even additional details about its structure. By contrast, temporal resolution refers to the granularity of timeliness, detailing the timing of events with greater precision. For example, low temporal resolution might measure updates in seconds or minutes, while high temporal resolution could capture events in milliseconds or microseconds.

Low resolution (whether spatial or temporal) can severely impact the accuracy of contextual information, reducing the situational awareness and operational efficiency of RAS. For example, in a military search-and-rescue mission, low spatial resolution might provide only a broad area (e.g. a 50 metre radius) as the target location, meaning that response teams would need to spend time narrowing down the actual location of the target, delaying assistance. In contrast, high spatial resolution could pinpoint a specific building or even a room within the building, significantly reducing search time and improving the likelihood of a successful mission. In another example, UAVs relaying context with low temporal resolution may only update positional data every few seconds. This delay could cause the system to misidentify a moving target's current location, leading to missed engagements. High temporal resolution would enable near-instant updates, allowing RAS to engage with high effectiveness.

Completeness

Completeness represents the extent to which the delivered contextual information includes all necessary metadata required for its validation. The relevance and importance of this metadata is influenced by both temporal and other special factors. Timeliness is validated based on the timestamps associated with the context, while accuracy (for example) can be inferred based on source reliability. The completeness of the metadata will inevitably vary depending on the operational scenario. For instance, GPS signals might provide less accurate location information in dense urban areas compared to when data is provided by a UAV's image vision system.

Ensuring the completeness of metadata is vital for validating QoC metrics and aligning them with mission requirements. In dynamic battlefield conditions, decision-making based on delayed information can result in unnecessary battle casualties. And in missions conducted in areas where civilians are present, precise geolocation and image recognition details are essential to avoid collateral damage.

Significance

Significance represents the importance of a context attribute to the RAS, which evolves based on its operational priorities. As the RAS moves through different spatial locations or

over time, the relevance of specific context attributes changes, making this metric highly dynamic and influenced by both temporal and spatial dimensions. For RAS operating in network-constrained environments with limited processing power, it is critical to prioritise significant context attributes while filtering out less relevant ones. This ensures that network bandwidth and computational resources are utilised effectively, enabling RAS to maintain optimal situational awareness and operational efficiency.

Representation Consistency

Representation consistency refers to the degree to which the format of contextual information and its metadata align with the requirements of the system processing it. RAS must be able to acquire, interpret and process context data from various sources seamlessly. Achieving this requires that the delivered context and its associated metadata either adhere to conventional formatting standards or are processed using common architectures such as CMPs. Representation consistency thereby promotes interoperability, reduces errors and enhances the overall efficiency and reliability of the system.

For example, in a joint military operation involving RAS units from different agencies—such as a military UAV collaborating with a civilian disaster management system—contextual information, such as real-time location data, might originate from varied sources. If the UAV's system requires GPS data in a specific format (e.g. latitude/longitude in decimal degrees) but receives it in a different format (e.g. as a geotagged image), it may fail to process the information correctly.

Sensitiveness

Sensitiveness represents the extent to which a context attribute should be available to and usable by a system. This can include constraints imposed by controllers, such as specific timeframes or location boundaries, or the level of data and metadata shared. Sensitiveness ensures that context information is shared appropriately while adhering to mission-specific requirements and maintaining necessary security protocols. For example, in a coordinated disaster response scenario involving multiple agencies such as fire and rescue services and police, their RAS may source contextual information from military systems. However, to safeguard sensitive information, accessibility controls must be in place. The military controllers may choose, however, to approve only specific, non-sensitive data to be shared with these external agencies (e.g. to exclude details about troop movements or extant military operations). Ensuring that only relevant and approved information is accessible to external RAS units helps maintain the integrity of sensitive information while enabling effective collaboration across multiple entities. Failing to impose proper accessibility controls may expose classified data, potentially compromising security or operational effectiveness.

/ 5.3 NETWORK CHALLENGES

RAS communicate to coordinate among themselves using ad hoc networks. Ad hoc networks are decentralised wireless networks that do not rely on pre-existing infrastructure like routers or access points. The most popular technologies enabling ad hoc networks are Wi-Fi, Bluetooth, Zigbee, Li-Fi, ultra-wideband, and near field communication (NFC). These technologies vary significantly in terms of their service quality and properties. Each node in the ad hoc network participates in routing by forwarding data to other nodes. Which of the nodes forwards that data is determined dynamically based on network connectivity. Communication between RAS and the relevant command centre generally occurs via satellite channels and cellular networks. The heavier processing loads on RAS will be redistributed to these cloud resources, which also act as data storage and analysis units for the commanders.

Figure 9 illustrates a high-level communication infrastructure in a typical instance where multiple RAS are coordinating to complete a mission. In search-and-rescue missions, for example, using multiple UAVs commonly yields better results than can be achieved with a single UAV.[61] Another option is the dual robot model,[62] where the primary robot focuses on rapid exploration and obstacle crossing, while the secondary robot handles object manipulation tasks such as door opening and item carrying in search-and-rescue missions. There are different types of robots available, such as ground robots, aerial robots and amphibious robots.[63]

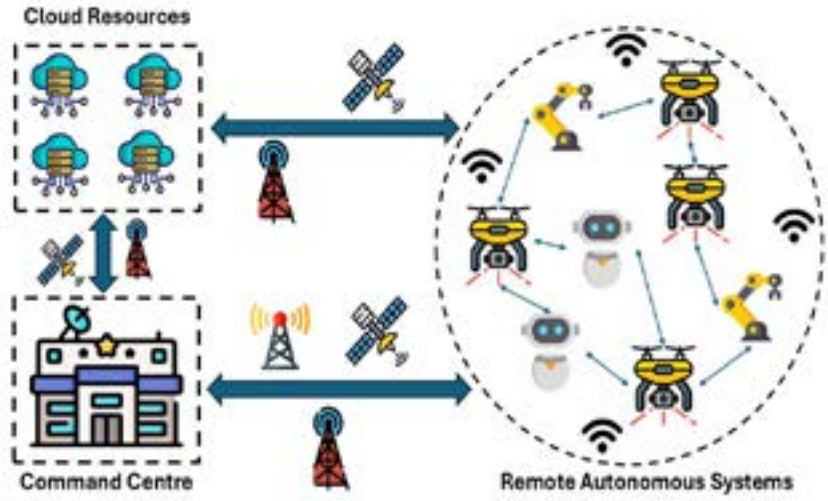

Figure 9: High-level communication architecture in RAS

Network quality of service (QoS) metrics measure the quality of communications in deployed RAS. The metrics related to any network's (peer-to-peer or long-range) QoS include response time, delay, jitter, data rate, bandwidth, and loss and error rates.[64] The significance of these individual metrics differs based on the deployment domain. For example, having an adequate response rate and lower delay is highly significant in mission-critical systems. Low error and loss rates are important in surveillance systems. Using examples from the literature, this section elaborates further on these challenges and how each of these metrics affects the scalability of situational awareness in RAS.

Response Time

Response time is the period (typically measured using the difference between timestamps) between an actor (e.g. a human controller of RAS) sending a request to a system and receiving the response. Higher response times in a network increase the turnaround times between messages from RAS to other relevant systems in the network, such as other RAS, cloud servers and the command centre. If response times are delayed, the real-time inputs required to form situational awareness are delayed. This, in turn, limits the ability of RAS to make decisions without human supervision.

Delay

Delay is the time difference between the data being sent by a system and its receipt at the destination. Long or varying delays in the network affect the data acquisition frequencies in the systems that are involved. Given that RAS rely on fusion of multiple inputs (e.g. from peer RAS, inbuilt sensors and external databases) to obtain situational awareness, delays from one or more of these systems impact their situational awareness. For example, during surveillance and reconnaissance missions, timely data fusion is critical. If a RAS receives delayed information from peer systems or external data sources, it may make outdated or inaccurate situational assessments (such as underestimating the speed or direction of enemy movements) which may compromise the mission.

Jitter

Jitter indicates the variance in the delay exhibited by a system. High jitter causes variation in the time delay of message arrival, leading to disruptions in data streams. High jitter also affects the synchronisation of data streams from multiple sources, making it difficult to integrate and analyse data from numerous sensors of RAS, inputs from the command centre, and cloud resources. For example, in a search-and-rescue operation using multiple drones, each drone will focus on a specific geographic segment and will send video feeds to the cloud centre for analysis. If the network exhibits high jitter, this can lead to inconsistent video feeds from surveillance drones impacting the end user's ability to monitor multiple locations in near real time and thus affecting overall situational awareness.

Data Rate

Data rate is the frequency (e.g. number of bits per second) of data sent out by a system. Low data rates decrease the frequency of data packets transmitted by the network, impacting real-time data analysis by limiting the acquisition of high-resolution data from the RAS (e.g. high-resolution imaging systems). This, in turn, affects situational awareness. For example, consider a mission to map the battlefield using image feeds from multiple drones. In the event of low data rates, the transmission of high-resolution images from these drones would be delayed, hampering the ability to form timely and accurate strategic plans.

Bandwidth

Bandwidth refers to the maximum rate of data carried by the network at an instance of time (e.g. kilobytes per second). Limited bandwidth lowers this rate. In the context of RAS, limited bandwidth restricts the number of RAS that can simultaneously exchange data (among themselves, with the command centre or with the cloud). For example, low bandwidth among surveillance drones would cause congestion in the data transmitted to the cloud and the command centre, affecting real-time monitoring capabilities.

Loss and Error Rate

Loss and error rates represent the lost and misrepresented data bits in the network. High loss and error rates can be evidenced by lost and corrupted messages during data transmission. Reducing these error rates requires robust error correction and retransmission mechanisms. These additional methods increase the overhead on the network, limiting the number of nodes (e.g. RAS and cloud resources) that can be deployed effectively without delayed communication, ultimately affecting scalability. For example, an error or loss in the signal transmitted by a global navigation satellite system (GNSS) signal can lead to incorrect positioning of waypoints, resulting in incomplete coverage of the area of interest, missed critical information and the need for repeated reconnaissance missions. Implementing methods to prevent lost and incorrect signals would delay communications between the GNSS and the UAVs, adversely impacting their situational awareness.

/ 5.4 PROCESSING CHALLENGES

Data collected by RAS is processed using AI and ML methods that in turn generate situational awareness. However, RAS are generally unable to collect and process all data internally. The limited onboard processing capacity of most RAS creates inevitable dependencies on external data collection and processing capabilities. For example, Figure 10 shows that RAS receive data from various sources: peer RAS, command centres, inbuilt sensors, and cloud resources (e.g. databases). Other examples include:

1. In UAV swarms, individual RAS may be reliant on other UAVs that function as intermediate data carriers. Such RAS may also obtain their guidance based on data from lead swarms.[65]
2. RAS may draw on data generated by deployed ground troops who are equipped with sensing devices.
3. RAS may share processing loads with cloud servers or be informed by data that has been processed by systems such as CATE (Collaborative AI at the Tactical Edge). CATE is a system that handles data processing loads using AI and ML algorithms from multiple agents in order to generate situational awareness on the battlefield.[66]

High levels of dependency on external data and processing sources mean that data processing functions are particularly vulnerable to disruption. For example, in remote regions, real-time data exchange with cloud resources may be limited when, for example, communication technologies (such as 5G and 4G) are out of range. In other cases where RAS depend on distributed processing using data-carrying intermediaries, proximity, capacity, time constraints and environmental factors (e.g. terrain) will be relevant.

This section defines the QoS metrics related to processing in RAS and their impact on situational awareness. Figure 10 shows the various types of data processing resources and their QoS metrics in RAS. The QoS metrics availability, reliability and scalability relay the effective completion of time-critical processes in a system.[67] The degree to which each metric needs to be met depends on the application—not all RAS need the highest QoS. For example, while time-critical applications need the highest processing QoS, applications that provide once-a-day updates may not. Given that the RAS may need to interact with, use and discover data obtained from a range of sources (e.g. peer RAS, sensors), other QoS metrics are also relevant. These include interoperability[68] (the ability of the system to effectively function by coordinating with other systems) and service adaptation time[69] (the time the system requires to effectively function upon a service switch).

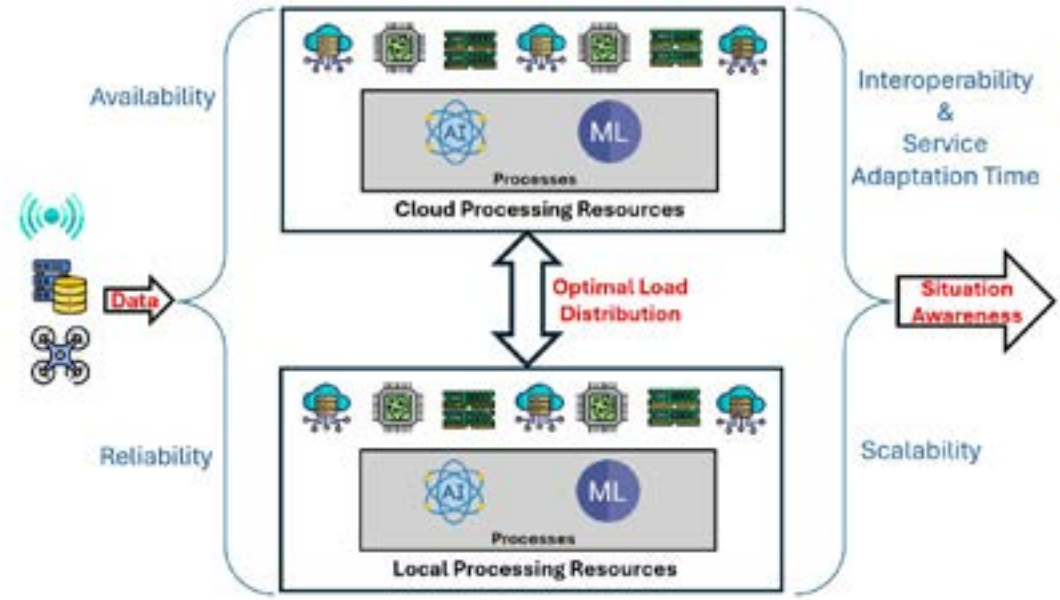

Figure 10: Various types of data processing resources and their QoS metrics in RAS

Availability

Availability refers to the amount of time the system's resources have available to process the data. It is calculated as the difference between the uptime and downtime of a system's resources when it is deployed. The availability metric impacts a RAS's situational awareness, as resource downtime affects its capacity to process data. This can create inaccuracies in any inferences as to situation based on that data. For example, if resources are unavailable to process the images collected by a UAV searching for survivors, the search may overlook geographic areas covered by RAS during resource downtimes.

Reliability

Reliability refers to the ability of a system's processing resources to work without degradation in their performance. For example, if the data processing speed degrades over time—especially when there are multiple streams of incoming data that create the situational awareness in the RAS—a data backlog may occur, causing latency in situational awareness.

Scalability

Scalability refers to the ability of a system's processing resources to work efficiently while accommodating varying processing loads. Low scalability, particularly when the RAS may

need to expand its situational awareness by incorporating other data sources, impacts its situational awareness.

Interoperability

Interoperability refers to the ability of a system's processing resources to connect and operate interdependently with other systems. RAS need to engage with various data sources and switch between various communication technologies. Limited interoperability may constrain the ability of a RAS to switch seamlessly and work with these different systems and technologies, thus limiting its ability to obtain data and expand its situational awareness.

Service Adaptation Time

Service adaptation time refers to the time that a system's resources require to adapt to changes (e.g. the addition of a new data source) and to work as anticipated. Higher service adaptation time delays the RAS in re-engaging with its mission activities upon modifying its resources (e.g. adding new data sources). The added latency may constrain it from forming near-real-time situational awareness.

6. WAY FORWARD—IMPLICATIONS FOR THE AUSTRALIAN DEFENCE FORCE

The Australian government aims to maintain a strategic edge in potential conflicts. In support of this effort, the Australian Army is seeking to obtain autonomous capabilities across land, aerial and maritime domains. At present, the heavy reliance of RAS on human inputs leads to potential inefficiencies and errors during the missions. This may occur due to network disruptions, communication delays and unintentionally incorrect inputs.

This paper has examined the state of RAS technology and the challenges that will face any ADF effort to strengthen its RAS development and deployment strategies. It has focused on the importance of situational awareness in RAS and the need for seamless data acquisition, context acquisition, network connectivity, and processing. It has also identified the relevant QoC and QoS metrics that relate to these factors. Based on this analysis it is evident that any effort by the ADF to augment RAS situational awareness must address the following points:

a. Identify and incorporate solutions to improve QoC compliant context acquisition solutions (mitigating data challenges)

RAS require various context attributes that may not be readily available from fixed sources. These systems need the ability to dynamically discover and acquire context from multiple sources while ensuring the quality of the acquired context meets defined QoC metrics. Potential solutions in this area should focus on developing and integrating tools such as CMPs[70] [71] in the RAS used by the Australian Army to provide these capabilities effectively.

b. Identify and incorporate solutions to improve QoS metrics related to network performance

Table 1 illustrates that networking technologies such as Wi-Fi, cellular (4G/5G), radio and satellite exhibit diverse QoS characteristics, with each technology excelling in specific aspects such as coverage, latency or data throughput. For instance, cellular technologies provide high data rates but are often unavailable or unreliable in remote or hostile environments.

Table 1: Communication technologies and their performance characteristics in various QoS metrics

Metric	Wi-Fi	Other RF (Bluetooth, RFID, LoRa, maritime radio)	Cellular (4G/5G)	Satellite
Distance	**Short range:** ~70 m indoors, up to 250 m outdoors	**Varies widely:** from centimetres (RFID) to many kilometres (maritime / long-range RF)	**Long range**: ~5–8 km in urban areas and up to ~16 km in rural areas (requires base stations)	**Very long range:** global coverage
Data rate	**Very high:** up to ~12 Gbps	**Low to high:** depends on technology and application	**Moderate to very high:** up to ~1 Gbps (4G) and ~20 Gbps (5G)	**Low:** typically up to ~100 Mbps
Loss and error rates	**Moderate:** affected by interference, obstacles and congestion	**Low for short-range** RF (e.g. Bluetooth), **high for long-range** RF (e.g. maritime radio)	**Low to moderate:** 5G generally more reliable than 4G	**High:** affected by distance, weather, and signal degradation
Latency	Low	**Low to high:** long-range RF may experience 10–100 ms delays	**Moderate** (4G ~200 ms) to very low (5G ~1 ms)	**High:** up to ~550 ms

In view of these known performance characteristics, further analysis is needed to achieve seamless interaction between cloud resources, context sources and command entities to support situational awareness in RAS deployments. For instance, RAS should incorporate context-aware network switching mechanisms that dynamically identify and select the most suitable communication technology based on operational conditions, such as mobility, bandwidth demand and environmental constraints.

c. Identify and incorporate solutions to improve QoS metrics related to processing performance

The processing resources that host data fusion and inference methods (e.g. AI and ML) must be scalable to maintain QoS metrics under varying processing loads. When

processing is hosted in the cloud, scalability can be achieved due to vast computational resources. However, this approach is often impractical in remote areas due to unreliable communication links. Conversely, local processing within RAS is constrained by the limited computational capabilities of onboard hardware, which may impede the system's ability to process large volumes of data efficiently and in real time. Therefore, it is essential to investigate and integrate models that enhance the processing capabilities of RAS, ensuring they can handle data effectively while maintaining QoS metrics.

As autonomous systems become more common in modern military operations, Australia must invest in research and development to better integrate these technologies into its military capabilities. A proactive approach to integrating RAS into the military not only safeguards national security but also positions Australia as a strong player in advanced military technologies. The first step towards realising this goal is to fully understand the current limitations of RAS technologies. It is equally important to identify future directions the ADF should pursue to overcome these limitations. In this way Australia can be positioned to develop RAS capabilities that not only meet operational needs but also surpass the current state of similar systems globally.

/ ABOUT THE AUTHORS

Dr Kanaka Sai Jagarlamudi is an Associate Lecturer in Computing at the School of Computer, Data and Mathematical Sciences (CDMS) at Western Sydney University. He worked as a Research Fellow at the Centre for IoT Ecosystem Research and experimentation (CITECORE), School of Information Technology, Deakin University, Melbourne. He received his PhD degree from Deakin University in 2024. His research interests include the internet of things (IoT), autonomous systems, transportation systems and cloud computing.

Dr Kevin Lee is an Associate Processor in Software Engineering and IoT at the School of Information Technology at Deakin University. Previously he held academic positions at Nottingham Trent University, Murdoch University, University of Mannheim and University of Manchester. He received his PhD in Computer Science from Lancaster University, UK, in 2006. He is a recognised researcher in the areas of IoT, distributed systems and adaptive systems. He has over 120 publications and is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a Certified Professional of the Australian Computer Society and a Chartered Member of Engineers Australia.

Dr Arkady Zaslavsky is a Professor of Distributed Systems and Security and Director of CITECORE at Deakin University. Arkady is leading and participating in R&D projects in IoT, mobile analytics and distributed contextual intelligence science areas. He holds Adjunct Professorship appointments with several Australian and international universities. He has published more than 450 research publications throughout his professional career and supervised to completion more than 45 PhD students. He is a Senior Member of ACM and a Senior Member of the IEEE Computer Society and the IEEE Communications Society.

Mr Shaine Christmas is a PhD candidate at the School of Information Technology, Deakin University. He completed his Bachelor of Software Engineering (Honours—first class) in 2022. His research interests include IoT, edge computing, robotics and software architecture.

/ ENDNOTES

1 Australian Government, *National Defence: Defence Strategic Review* (Canberra: Commonwealth of Australia, 2023).

2 Jed Thomas, 'How Remote Autonomous Systems Will Redefine Routine Monitoring', *PIN* (website).

3 Austin Wyatt, Joanne Nicholson, Marigold Black and Andrew Dowse, *Understanding How to Scale and Accelerate the Adoption of RAS*, Australian Army Occasional Paper No. 20 (Australian Army Research Centre, 2024).

4 Michael Gargalakos, 'The Role of Unmanned Aerial Vehicles in Military Communications: Application Scenarios, Current Trends, and Beyond', *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 21, no. 3: 313–321.

5 Peter Chin et al., 'TAK-ML: Applying Machine Learning at the Tactical Edge', *MILCOM 2021–2021 IEEE Military Communications Conference (MILCOM)* (San Diego CA, 2021), pp. 108–114.

6 Susan Toth and William Hughes, 'The Journey to Collaborative AI at the Tactical Edge (CATE)', *Proceedings of the SPIE* 11746 (2021).

7 Qi Zhao et al., 'An Intelligent Multi-Sensor Cooperative Perception Framework for Situational Awareness Enhancement', *Sensors and Systems for Space Applications XVI, Proceedings* 12546 (2023).

8 MR Endsley, 'Toward a Theory of Situation Awareness in Dynamic Systems', *Human Factors: The Journal of the Human Factors and Ergonomics Society* 37, no. 1 (1995).

9 'MQ-9 Reaper', *United States Air Force* (website).

10 Joseph Trevithick, 'MQ-9 Reaper Flies with AI Pod That Sifts Through Huge Sums of Data to Pick Out Targets', *The War Zone*, 4 September 2020.

11 Joseph Macey, 'MQ-9 Reaper Drone Tested with Upgraded SATCOM', *Defence Advancement*, 2 June 2023.

12 Australian Army, *Robotic & Autonomous Systems Strategy v2.0* (Commonwealth of Australia, 2022)

13 'RQ-4 Global Hawk', *United States Air Force* (website).

14 Anind K Dey, 'Understanding and Using Context', *Personal and Ubiquitous Computing* 5, no. 1 (2001).

15 Vincenzo Loia et al., 'Enforcing Situation Awareness with Granular Computing: A Systematic Overview and New Perspectives', *Granular Computing* 1 (2016).

16 Alireza Hassani et al., 'Context-as-a-Service Platform: Exchange and Share Context in an IoT Ecosystem', *2018 IEEE International Conference on Pervasive Computing and Communications Workshops* (IEEE, 2018).

17 Martin Bauer, 'FIWARE: Standard-Based Open Source Components for Cross-Domain IoT Platforms', *2022 IEEE 8th World Forum on Internet of Things* (IEEE, 2022).

18 Claudio Bettini et al., 'A Survey of Context Modelling and Reasoning Techniques', *Pervasive and Mobile Computing* 6, no. 2 (2010).

19 Xin Li et al., 'Context Aware Middleware Architectures: Survey and Challenges', *Sensors* 15 (2015).

20 Grant Chambers, Chris Smith and Leanne Rees, *Command and Control in Modern Warfare: The Importance of Talent, Experience and Expertise*, Australian Army Occasional Paper, Command and Leadership Series 001 (Australian Army, 2017).

21 Xingjiao Wu et al., 'A Survey of Human-in-the-Loop for Machine Learning', *Future Generation Computer Systems* 135 (2022).

22 Austin Wyatt, Joanne Nicholson, Marigold Black and Andrew Dowse, *Understanding How to Scale and Accelerate the Adoption of Robotic and Autonomous Systems into Deployable Capability*, Australian Army Occasional Paper No. 20 (Australian Army Research Centre, 2024).

23 Julian Turner, 'Sea Hunter: Inside the US Navy's Autonomous Submarine Tracking Vessel', *Naval Technology*, 3 May 2018.

24 'SDA Layered Network of Military Satellites Now Known as "Proliferated Warfighter Space Architecture"', *SDA* (website), 23 January 2023.

25 Gabriel Honrada, 'China's Sharp Sword Combat Drones Cutting into US Airpower', *Asia Times*, 7 September 2024.

26 Charlie Campbell, 'China Has Launched the Robocops You Have Been Waiting For', *Time*, 26 April 2016.

27 Bishda Das, 'Russia to Upgrade State-of-the-Art Marker Robotic Platform', *The Defense Post*, 12 February 2021.

28 'Sea Breaker: Long-Range Naval & Land Defense System Up to 300 Km', *Rafael* (website).

29 'Thunder Storm: Autonomous Aerial Systems Solution', *Rafael* (website).

30 'Rocks: Autonomous Extended Stand-Off Range Air-to-Surface Missile', *Rafael* (website).

31 'Dominion-X'. *Elbit Systems* (website).

32 'Torch-X Family', *Elbit Systems* (website).

33 'Thor', *Elbit Systems* (website).

34 'Major Milestone in Rafael's High-Power Laser Intercept System Development', *Rafael* (website), 29 October 2024.

35 MM O'Donohue, *Autonomous Underwater Vehicles: A Future Capability for the Royal Canadian Navy*, JCSP Service Paper 42 (Canadian Forces College, 2016).

36 Y Allard and E Shahbazian, *Unmanned Underwater Vehicle (UUV) Information Study* (Defence Research & Development Canada, 2014).

37 Alice B Aiken and Stéphanie AH Bélanger, *Shaping the Future: Military and Veteran Health Research* (Kingston, Ontario: Department of National Defence, 2011).

38 'Project: Greater Autonomy in the Operations of Ships and Offshore Platforms', *Government of Canada* (website).

39 'Integrated Aerial Mobility Program', *Government of Canada* (website).

40 'OCEAN2020: The Second Sea Demonstration of the European Research Project for Maritime Surveillance Successfully Completed', *Leonardo* (website), 10 September 2021.

41 Ibid.

42 'EROSS IOD Becomes EROSS SC', *EROSS-SC* (website).

43 Máximo A Roa et al., 'EROSS: In-Orbit Demonstration of European Robotic Orbital Support Services', *2024 IEEE Aerospace Conference* (IEEE, 2024).

44 'The Answers Are Still Blowing in the Wind', *Defence Science and Technology Group* (website), 5 August 2021.

45 Jr Ng, 'Australia and Japan to Jointly Develop Underwater RAS Technology', *Asian Military Review*, 26 January 2024.

46 'MS113AS4 Armoured Personnel Carrier', *Australian Army* (website).

47 'M113 AS4 Optionally Crewed Combat Vehicle (OCCV)', *BAE Systems* (website).

48 Nigel Pittaway, 'ATLAS Brings Autonomy to the Fight', *The Australian*, 30 October 2024.

49 'MQ-28 Ghost Bat', *Boeing* (website).

50 'Hovermap', *CSIRO* (website), 9 January 2017.

51 Kristen D Thompson, 'How the Drone War in Ukraine Is Transforming Conflict', *Council on Foreign Relations* (website), 16 January 2024.

52 Seth J Frantzman, 'In the War Against Hamas, Israeli Drones Are Key. Here Is Why', *The Jerusalem Post*, 20 October 2023.

53 Agnes Helou, 'How Drone Warfare in Israel Could Dramatically Change If Hezbollah Joins the Fight: Analysts', *Breaking Defense*, 20 October 2023.

54 Khalid Abdelaziz, Parisa Hafezi and Aidan Lewis, 'Sudan Civil War: Are Iranian Drones Helping the Army Gain Ground?', *Reuters*, 11 April 2024.

55 'Iran Drones Become Latest Proxy Tool in Sudan's Civil War', *Al Arabiya English*, 24 January 2024.

56 Dey, 'Understanding and Using Context'.

57 Tasmeen Ornee et al., 'Context-Aware Status Updating: Wireless Scheduling for Maximizing Situational Awareness in Safety-Critical Systems', *2023 IEEE Military Communications Conference (MILCOM)* (IEEE, 2023).

58 Kanaka Sai Jagarlamudi et al., 'Requirements, Limitations and Recommendations for Enabling End-to-End Quality of Context-Awareness in IoT Middleware', *Sensors* 22, no. 4 (2022).

59 Ibid.

60 Bauer, 'FIWARE'.

61 Georgy Skorobogatov, Cristina Barrado and Esther Salamí, 'Multiple UAV Systems: A Survey', *Unmanned Systems* 8, no. 1 (2019).

62 Gongcheng Wang et al., 'Development of a Search and Rescue Robot System for the Underground Building Environment', *Journal of Field Robotics* 40, no. 3 (2023).

63 Jeffrey Delmerico et al., 'The Current State and Future Outlook of Rescue Robotics', *Journal of Field Robotics* 36, no. 7 (2019).

64 Eric Crawley et al., 'A Framework for Integrated Services and RSVP over ATM,' Request for Comments 2382 (RFC 2382), I*nternet Engineering Task Force*, 1998.

65 Skorobogatov, Barrado and Salamí, 'Multiple UAV Systems'.

66 Toth and Hughes, 'The Journey to Collaborative AI at the Tactical Edge (CATE)'.

67 Jagarlamudi et al., 'Requirements, Limitations and Recommendations for Enabling End-to-End Quality of Context-Awareness in IoT Middleware'.

68 Li et al., 'Context Aware Middleware Architectures'.

69 Konan-Marcelin Kouame and Hamid Mcheick, 'Architectural QoS Pattern to Guarantee the Expected Quality of Services at Runtime for Context-Aware Adaptation Application', *SN Applied Sciences* 1:405 (2019).

70 Hassani et al., 'Context-as-a-Service Platform'.

71 KS Jagarlamudi et al., 'Validating Quality of Context in Pervasive Computing Systems: Surf Life Saving Use Case', *2023 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events* (IEEE, 2023).

RESEARCHCENTRE.ARMY.GOV.AU

CG: APR031-26