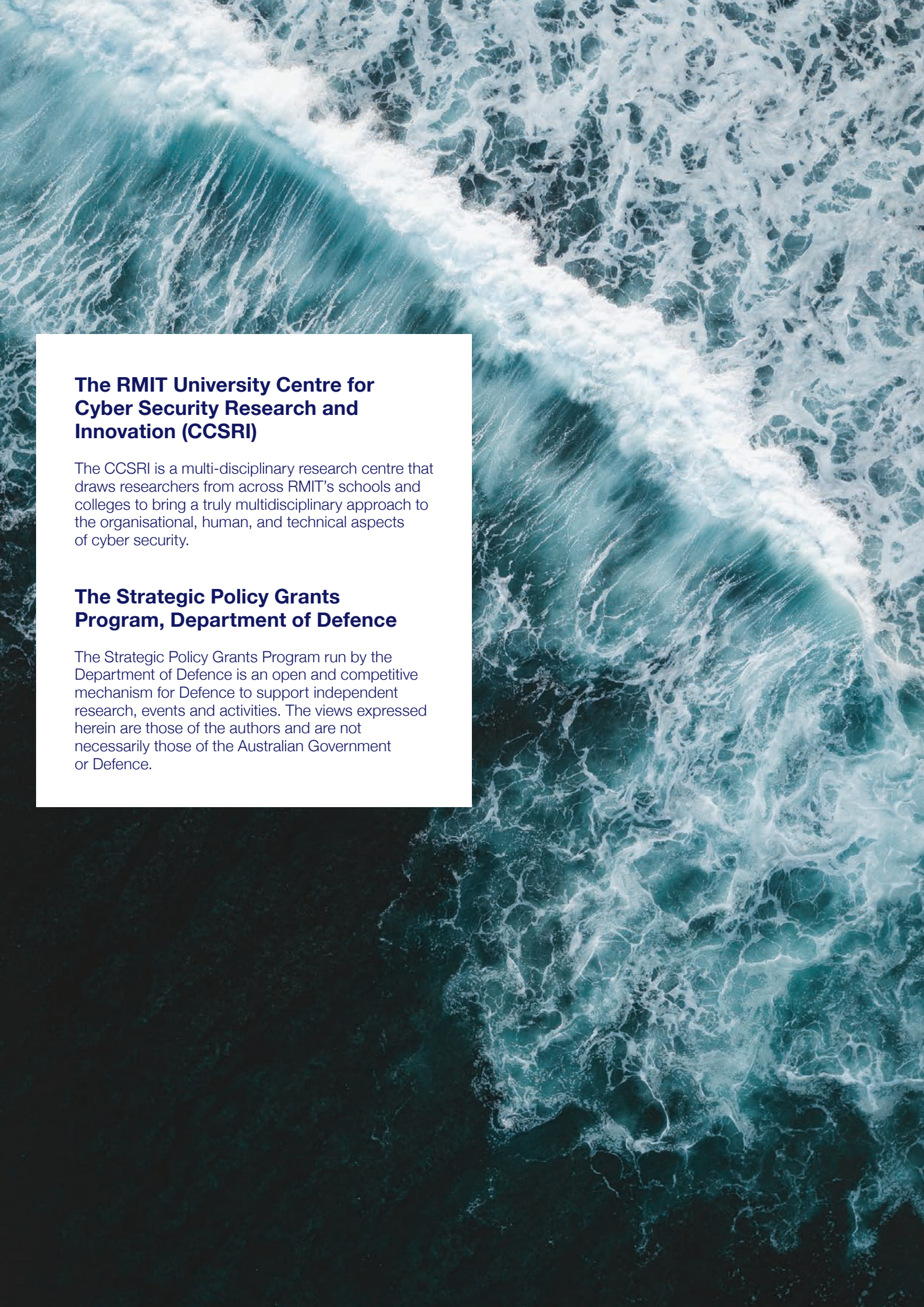
Australia's Trade and the Threat of Autonomous Uncrewed Underwater Vehicles

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation



The RMIT University Centre for Cyber Security Research and Innovation (CCSRI)

The CCSRI is a multi-disciplinary research centre that draws researchers from across RMIT's schools and colleges to bring a truly multidisciplinary approach to the organisational, human, and technical aspects of cyber security.

The Strategic Policy Grants Program, Department of Defence

The Strategic Policy Grants Program run by the Department of Defence is an open and competitive mechanism for Defence to support independent research, events and activities. The views expressed herein are those of the authors and are not necessarily those of the Australian Government or Defence.

Acknowledgements

This research has been produced as a result of the collaboration between the RMIT University Centre for Cyber Security Research and Innovation (CCSRI), Charles Darwin University (CDU) and WiseLaw. This research was supported as part of the Strategic Policy Grants Program, by the Department of Defence. Special thanks to our research partners: EJ Wise, CDU staff involved – Hamish Campbell, Mamoun Alazab and Victor Abramowicz, and the RMIT Staff involved – Nirajan Shiwakoti, Peter Stasinopoulos, Asha Rao, Ibrahim Khalil, Meredith Jones, Shah Khalid Khan, Dr. Adam Bartley, Professor Aiden Warren, Professor Matthew Warren and Laki Kondylas.

To Bill Leitch, whose experience as a submariner and engineer provided the passion and context for this project and we are forever grateful for his knowledge and generosity.

Acknowledgement of Country

RMIT University acknowledges the people of the Woi wurrung and Boon wurrung language groups of the eastern Kulin Nations on whose unceded lands we conduct the business of the University. RMIT University respectfully acknowledge their Ancestors and Elders, past and present.

RMIT also acknowledges the Traditional Custodians and their Ancestors of the lands and waters across Australia where we conduct our business.

Acronyms and Abbreviations

A2/AD	Area Access/Area Denial
ADF	Australian Defence Force
AI	Artificial Intelligence
AIMS	Australian Institute of Marine Science
AMSA	Australian Maritime Safety Authority
ASW	Anti-Submarine Warfare
AUKUS	Australia, United Kingdom, United States
AUV	Autonomous Underwater Vehicles
AW2022	Autonomous Warrior 2022
AWS	Autonomous Weapons Systems
C4ISR	Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance (ISR)
COLREGs	Convention on the International Regulations for Preventing Collisions at Sea
CPS	Cyber Physical Systems
DARPA	Defense Advanced Research Projects Agency
DDOS	Distributive Denial of Service
DOS	Denial of Service
DSTG	Defence Science and Technology Group
DSR	Defence Strategic Review 2023
DSU	Defence Strategic Update 2020
DWP	2016 Defence White Paper
ELAUV	Extra Large Autonomous Undersea Vehicles
ELUUV	Extra Large Uncrewed, Underwater Vehicles
EEZ	Exclusive Economic Zone
LDUUV	Large Displacement Uncrewed, Underwater Vehicles
ICJ	International Court of Justice
IED	Improvised Explosive Device
IMO	International Maritime Organization
ISR	Intelligence, Surveillance, and Reconnaissance
MARPOL	International Convention for the Prevention of Pollution from Ships
MAV	Maritime Autonomous Vehicles
MCM	Mine Countermeasures
ML	Machine Learning
MUV	Marine Unmanned Vehicles
RAAF	Royal Australian Airforce
RAN	Royal Australian Navy
RAS-AI	Robotics, Autonomous Systems and Artificial Intelligence
SCS	South China Sea
SLOCs	Sea Lanes of Communication
SOLAS	International Convention for the Safety of Life at Sea
SSN	Nuclear-Powered Submarines
UMV	Underwater Maritime Vehicles
UNCLOS	The United Nations Convention on the Law of the Sea
UUV	Unmanned, Underwater Vehicles
UMS	Unmanned Maritime Systems
UAV	Unmanned Aerial Vehicles
US	United States
USV	Unmanned Surface Vehicles
UNV	Underwater Naval Vessels

Introduction

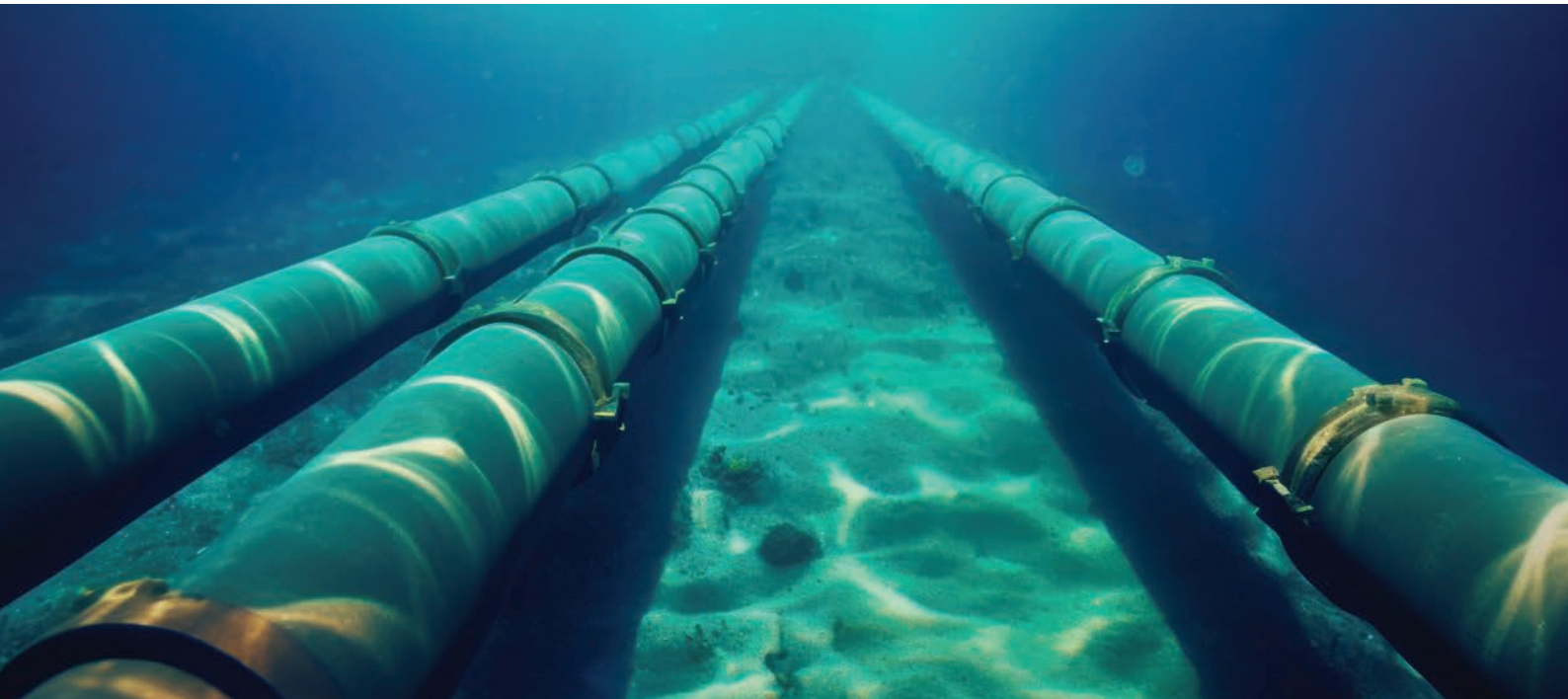
The 2022 underwater sabotage of the Nord Stream pipeline in the Baltic Sea in 2022 has outlined the critical juncture states like Australia now face in the development of seabed warfare capabilities. Research reveals that adversaries are actively building autonomous uncrewed, underwater vehicles (UUVs) and other artificial enabled-platforms to bolster maritime offensive and defensive capabilities. AI-enabled underwater battlefields are no longer the subjects of fictional stories but are near-future realities. Increasingly, UUVs are considered 'game changers' due to their comparatively lower cost outlays and their ability to cover an array of mission briefs.

For Australia, particular vulnerabilities escalate the risk environment these technologies pose. Maritime trade, for instance, accounts for 99 percent of the country's total trade volume, with two-thirds of exports traversing the South China Sea. Just-in-time supply chain processes, coupled with poor strategic resilience, has created maritime bottlenecks that have, until now, been considered acceptable risks. Home port defence capabilities have fallen behind the preponderance of systems, like smart mines, that can lock up critical Navy assets at times crucial to their employment. UUVs, as these challenges illustrate, dramatically change national assumptions about sovereign and maritime security.

This report examines the future security threats posed to Australian maritime trade by autonomous submersible weapons systems. Supported by the Department of Defence's Strategic Policy Grants Program, investigators from the RMIT University Centre for Cyber Security Research and Innovation, Charles Darwin University, and WiseLaw conducted an impact analysis examining the likelihood, impact, and mitigation steps related to autonomous submersible weapon systems scenarios.

Consultations and workshops were undertaken with over 50 stakeholders from members of government public service, the Department of Defence, the Royal Australian Navy (RAN), defence industry, and researchers to generate insights into current UUV development, vulnerabilities in Australian critical maritime infrastructure, and risk management practices.

The findings of this report demonstrate a growing predicament for Australia between current mitigation strategies to build resiliency into critical undersea infrastructure and ocean-borne trade and future-based adaptation strategies aimed at developing next-generation technologies for underwater maritime defence.



Research findings

The time available for the Australian Department of Defence (Defence) to address emerging UUV threats is rapidly shrinking. Already, key UUV platforms in AI-enabled mine capabilities have the capacity to paralyse critical resource and supply chain lifelines. Policy and strategy guidelines have highlighted the necessity for stronger mine countermeasures (MCMs). Current strategic pronouncements in the 2023 Defence Strategic Review and among AUKUS partners for advanced capability development and acquisition have sought to address the growing requirement for uncrewed maritime systems (UMS).

Acute challenges continue to exist, particularly with respect to personnel shortfalls and funding priorities, which are likely to burden defence planners as the focus on nuclear-powered attack submarines (SSNs) crowds out other systems in the defence space. This has implications for the Royal Australian Navy (RAN) and their ability to meet strategic goals established in RAS-AI Strategy 2040 – Warfare Innovation Navy (RAS-AI), Plan Mercator, and AUKUS. With capability shortfalls likely to continue in the short-to-medium term, defence authorities will require broader engagement with international partners to participate in burden-sharing and monitoring across strategic Sea Lanes of Communication (SLOCs).

Current UUV development and employment demonstrate that Australia and its defence partners can no longer think of UUV threats as distant or as associated with times of war. Destabilising activities that take place in the grey zone between war and peace are increasingly prevalent. UUVs, which are difficult to detect and can offer states the cloak of deniability, are expected to become more efficient, useful, and strategically relevant to national defence. This requires a rethinking of Navy and maritime defence doctrines and the role of emerging technologies in traditionally “crewed” roles.

A key contribution to Australia’s maritime defence architecture will include a coordinated diplomatic program. UUV development and capabilities have outpaced regional and international agreements so that in many cases even the language of UUVs is unclear. This has legal implications for concept and technology sharing, and field use. But further considerations must also include regional partnerships for maritime surveillance, consistent dialogues on security issues to form shared understandings of maritime UUV threats, and defence collaboration and emerging technology testing. Bolstering diplomatic capabilities will also ensure a scenario like an unfriendly military base close to Australian shores does not eventuate.

The September 2022 Nord Stream sabotage, and October 2023 damage to the Balticconnector pipeline, has caused governments to rethink submarine infrastructure with a new emphasis on mitigating the potential for seabed warfare. Building resilience in maritime domain awareness and creating UUV and sensor capabilities for detection have become mainstream ideas in partners such as the United States, France, the United Kingdom, and more broadly within the EU and NATO. The emergence of seabed warfare commands in Europe and among NATO members illustrates the impact UUVs and seabed warfare scenarios are likely to have in the future, and offers future considerations for Australian Defence planners.

There is broad-based recognition that as UUV development progresses, off-the-shelf UUV variants will proliferate, adding a multiplier effect to existing maritime threats. These fears are currently alive in the domain of uncrewed aerial vehicles (UAVs), and will become sharper in the near future. For instance, improvised underwater torpedos are currently one step removed from existing off-the-shelf UUV capabilities for determined malicious actors, which can include state and non-state-based actors, and criminal actors. With critical shipping lanes contingent upon open, threat-free thoroughfares like the Suez Canal, the Malacca Straits, or Lombok, Indonesia, the potential for UUV interdiction among supply routes is a growing concern.

Recommendations

The insights provided by the experts engaged for this report necessitate a closer look at the policies and strategies adopted by the Australian Government to militate the challenges posed by UUVs. The Australian government and the Department of Defence have some space to consider these challenges in more depth. But the fast-paced development of UUVs is closing this window rapidly. The future of seabed warfare and autonomous systems requires planning now. The following recommendations reflect these challenges.

1. **Clarify legal parameters for UUV deployment.**

Defence should consider whether the definitions of "defence vessel" and "naval vessel" may inhibit the development of Defence autonomous UUVs by industry and DSTG. Defence should consult with internal stakeholders like the RAN, DSTG as well as the autonomous UUV industry, AMSA, and Trusted Autonomous Systems to ensure that the definitions are not restrictive (especially where interoperability with allied forces is desirable) (see Appendix C in the paragraph titled 'Naval vessels and the development of autonomous UUVs for Defence' regarding the *National Law 2012)*. Key considerations are:

a. That Defence ensures that if UUVs are remotely operated by non-combatant (non-military personnel), this is done either by explicit direction of the government (who will presumably make this decision knowing the ramifications in the international community as regards the commitment of Australia and its personnel in accord with the laws of armed conflict) or with the knowledge that it may expose the operators to being targeted as if they had become part of the fighting forces in an armed conflict scenario.

b. Especially in light of the AUKUS arrangement, Defence needs to be vigilant that the decisions made preparatory to operations (such as creating UUVs, remote piloting arrangements and so forth) are sufficiently compliant with international humanitarian laws ("the laws of armed conflict") so as not to prejudice the arrangement, or the ongoing work with Australia's closest partners.

2. **Undertake rapid implementation of a Whole-of-Government Fuel Council, as recommended in the 2023 DSR.**

Current strategic fuel reserves remain a critical flaw in Australia's trade and national defence. Rapid mitigation of this flaw is required. The anticipated review for the expanded national fuel storage capacity is unspecified in budget timelines. Fast-tracking this review will begin the process for the development of infrastructure and the mitigation of a critical fuel disaster.

3. **Incorporate the role of UUV operations and AI-enabled infrastructure in maritime security strategy.**

Based on emerging risk assessments, such as those on seabed warfare adopted by NATO and the EU,[1] the government should develop a robust maritime security strategy to prevent, deter, and respond to UUV coordinated attacks. This strategy should include measures to secure Australia's supply chains, SLOCs, and other critical maritime infrastructure. Key considerations are:

a. Existing frameworks that provide for force structure and planning currently exist in Rand Corp's *Supporting the Royal Australian Navys Strategy for Robotics and Autonomous Systems: Building an Evidence Base and RAN's RAS-AI Strategy 2040 – Warfare Innovation Navy.* However, these will need to be updated for UUV-specific responses. The anticipated 2024 National Defence Strategy would be a good place to begin this discussion. However, a more specific focus will be required, possibly within the 2024 RAS-AI review. A consideration for inclusion would be a classification system to help prioritise responses to different types of UUV threats, allowing for more efficient use of resources;

b. Defence to consider creating a seabed warfare command with oversight of all current and future UUV and underwater maritime domain awareness assets. This will streamline seabed warfare preparation, appropriately address risk factors, and align with emerging practice in Europe, Britain, and the United States.

“The government should develop a robust maritime security strategy to prevent, deter, and respond to UUV coordinated attacks.”

4. Strengthen regulations and export controls.

The government should consider strengthening regulations and export controls on UUV technologies to prevent their acquisition by non-state actors and criminals. This would involve working closely with international partners and regulating the sale and transfer of UUVs, especially those with advanced capabilities. Key considerations are:

a. Defence should consider whether AUKUS-like opportunities exist for the development of autonomous UUVs with like-minded countries. If pursued, it is noted that such opportunities would require consideration and likely spur reform of Australia’s current autonomous vessel legal regime (see appendix C) as well as potentially other laws, such as the Defence export control regime.

5. Develop redundancies in satellite systems and more submersible cables.

With further advancements in detection technology, trends are moving toward entire ocean detection capabilities. Consideration of secure communication links with the rest of the world will require moving away from a reliance on one or two underwater cables and building multiple redundancies into satellite systems and more cables. Key considerations are:

a. Building resilience into critical infrastructure can be gained by enhancing maritime domain awareness. UUVs are likely to play an increasingly critical role as cost-effective alternatives to traditional awareness systems. A focus on oceanographic and hydrographic exploration and ocean bed sensor grids will provide stronger detection measures for alien UUV interdiction.

6. **Enhance surveillance and monitoring capabilities.**

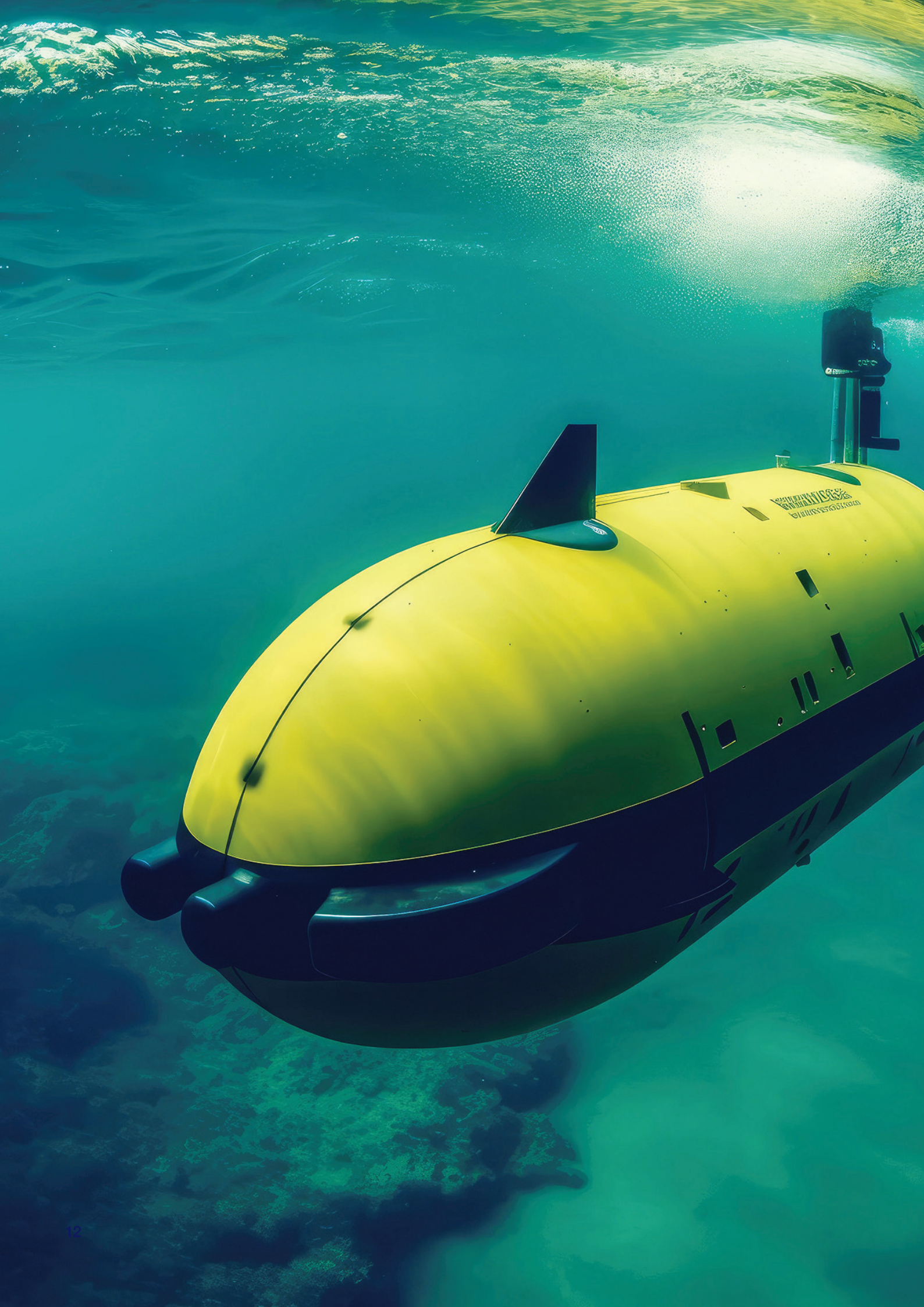
The government should enhance its surveillance and monitoring capabilities to detect and track UUVs in Australian waters. This would involve investing in advanced technologies, such as sensors, radars, and unmanned aerial vehicles (UAVs), to improve maritime domain awareness and early warning capabilities. This is particularly important in a north Australia context where workforce attrition and lack of worker qualification and education creates challenges to coastline and maritime surveillance. Key considerations are:

a. Defence to boost talent acquisition and a more technological workforce: Combating the threat of UUVs in the north is going to require a more technologically skilled workforce. Initiatives need to be developed to build up the opportunities, attract new talent, improve industry reputation, generate efficient-skill recognition, and enhance career guidance.

b. Implement a network of sensors along the 12-nautical-mile territorial zone: Such a network would act as an advanced coastline communication system, helping to detect and track any UUVs that enter Australian waters. In addition to monitoring, sensor capabilities also provide opportunities for data collection that will be necessary for enhancing underwater domain awareness, particularly for autonomous systems.

c. Develop greater familiarity with local oceanography: Understanding local oceanography can help in the detection and tracking of UUVs, as well as provide insights into potential vulnerabilities of Australia's maritime infrastructure. Sufficient, high-quality data will be required to develop and train AI for UUV missions. Additionally, such systems will familiarise authorities with a stronger understanding of Australia's maritime resources.

"The government should enhance its surveillance and monitoring capabilities to detect and track UUVs in Australian waters by investing in advanced technologies, such as sensors, radars, and unmanned aerial vehicles (UAVs)."



7. Build partnerships with industry and research institutions.

The government should build partnerships with industry and research institutions to develop new technologies and capabilities to counter UUV threats. This would involve investing in research and development programs to enhance Australia's ability to detect and respond to UUV coordinated attacks. While such platforms already exist, a stronger focus needs to be placed on emerging technologies, with a focus on force integration and, where possible, interoperability. Improving upon and delivering further military exercises like the Autonomous Warrior will enhance progress in these areas. Meanwhile, actualisation of the RAS-AI Maturity Framework is needed to speed up partnerships with industry and academic institutions.[2]

8. Establish long-range preventive measures to militate against future UUV scenarios.

These include investing in stronger diplomatic initiatives with close neighbours and establishing military bases or collaborating with other countries to screen potential risks before they become a threat. From a cost-benefit ratio, diplomatic initiatives have ordinarily outsized roles in the defence of the nation. The natural maritime geographic area under sovereign control is impossible to manage with limited national resources, making diplomatic agreements and collaborative arrangements significant contributors to maritime security. Key considerations are:

a. Consider collaborating with international partners and organisations to share knowledge, expertise, and best practices in detecting and mitigating the risks associated with UUV attacks. Australia's European partners are well advanced in seabed warfare scenarios. Australia should consider leveraging its connections with democratic allies to build upon knowledge capabilities;

b. Defence must ensure that, while it may not be the leader in the design and manufacture of UUVs, it continues to be regionally and internationally engaged in the discussions (e.g., at relevant UN groups of Governmental Experts or by advising the Department of Foreign Affairs and Trade or other involved departments who are members of those groups) so that when inevitable incursions by the UUVs from other states/non-state actors occur, Defence and the Australian Government are well-placed to respond both internally and internationally.

c. Defence and the Australian Government should explore measures – like incorporating real-time monitoring of shipping lanes using integrated sensors; beefing up vessel regulations and safety practices; and establishing protocols for encounters between uncrewed underwater vehicles and commercial vessels – to prevent and manage all types of possible incidents.

9. Encourage UUV designs with safety in mind, and also counter-operations.

In the design process, consideration needs to be given not just to transparency for operational reasons (did the "killer UUV" act consistently with its programming and was the programming aligned to Australia's obligations in international law?) but also to factors such as:

a. Assigning the most appropriate UUVs to the mission at hand; it is not worth risking new or classified technology for low-level missions where the risk of UUV capture by an opposing state will give way to possibilities such as:

i. The opponent state being able to reverse engineer Australian capabilities and maturity (whether from an operational technology or cyber security perspective);

ii. The opponent state being able to degrade the operation of the UUV;

iii. The opponent state being able to modify the UUV so that it continues to appear as an Australian asset but is now "owned" by the opponent state;

iv. The opponent state being able to use cyber operations to contaminate the data of the UUV, affecting the surveillance/intelligence purpose of the UUV;

b. Can the UUV be remote-wiped in the case of faulty transmission, suspected compromise or similar;

c. Does the responsible entity (Department of Defence, RAN, other) assume a whole-of-life responsibility for the asset in terms of environmental impact; and

d. Ensuring adequate cyber-risk management or assigning the future risks of not doing so.

Contact

Email: ccsri@rmit.edu.au

Website: www.rmit.edu.au/cyber

The RMIT University Centre for Cyber Security Research and Innovation (CCSRI)

The CCSRI is a multi-disciplinary research centre that draws researchers from across RMIT's schools and colleges to bring a truly multidisciplinary approach to the organisational, human, and technical aspects of cyber security.

The Strategic Policy Grants Program, Department of Defence

The Strategic Policy Grants Program run by the Department of Defence is an open and competitive mechanism for Defence to support independent research, events and activities. The views expressed herein are those of the authors and are not necessarily those of the Australian Government or Defence.

Design: majc.com.au

Australia's Trade and the Threat of Autonomous Uncrewed Underwater Vehicles

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation

CRICOS code: 00122A | RTO Code: 3046