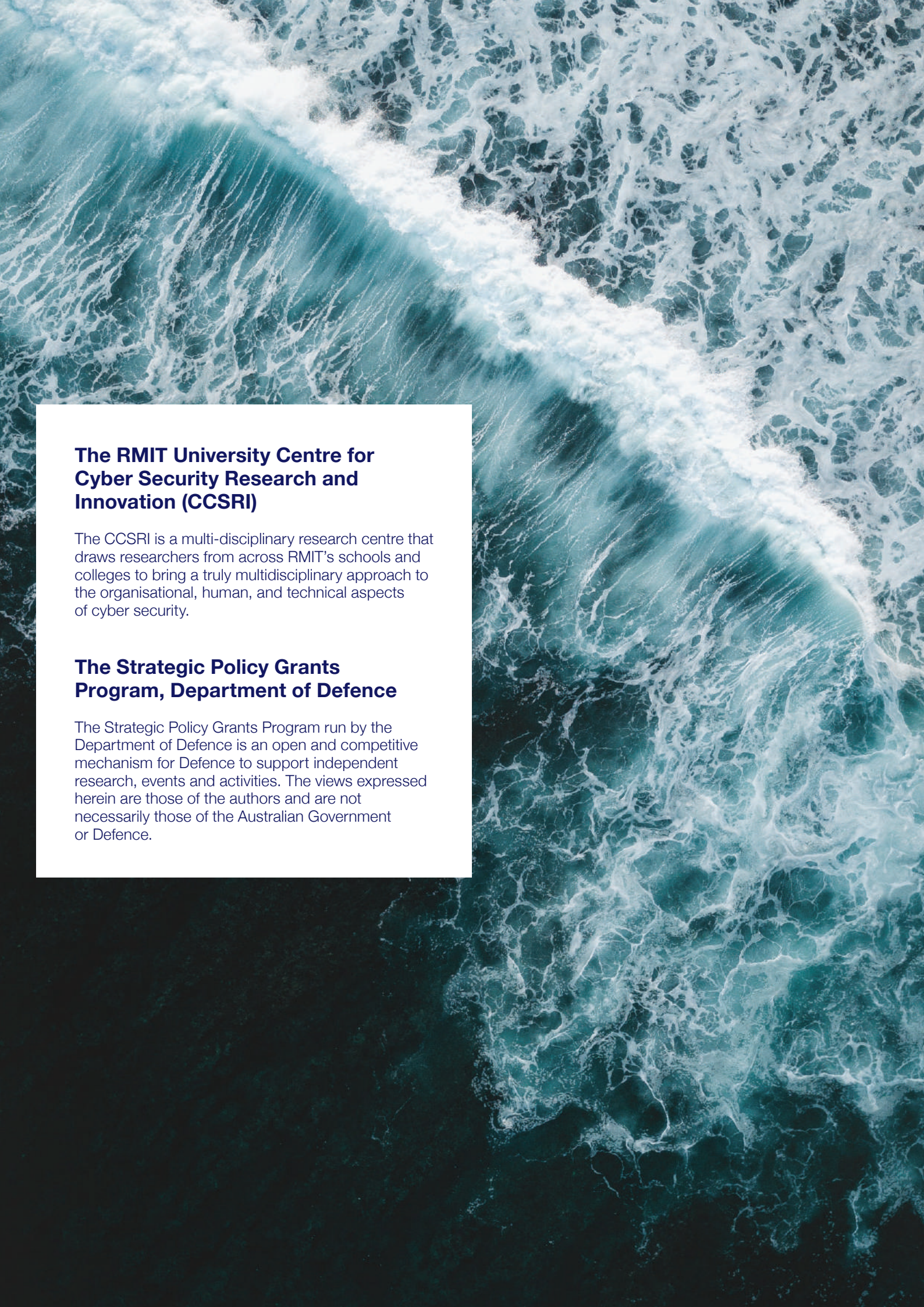
Australia's Trade and the Threat of Autonomous Uncrewed Underwater Vehicles

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.

Contents

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

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.

Executive Summary

Uncrewed, underwater vehicles (UUVs) are projected to play a critical role in future war and peacetime scenarios where maritime trade and sovereign security systems are at risk. With key vulnerabilities in maritime trade and supply chain maritime networks, any malicious use of UUVs is likely to have significant implications for Australian economic and sovereign security.

This report examines the future security threats posed to 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.

Key considerations are featured below:

The time available for the Australian Department of Defence (Defence) to address emerging UUV threats is rapidly shrinking.

Already, key UUV platforms in Artificial Intelligence (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 Communications (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.

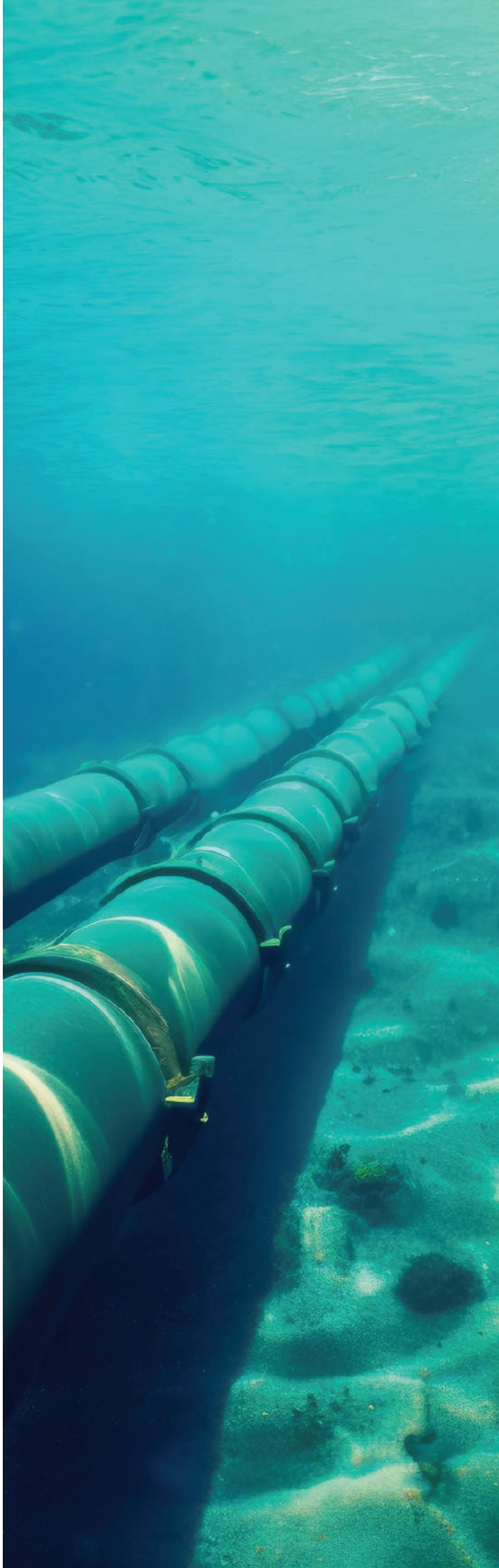
UUV development and capabilities have outpaced regional and international agreements so that in many cases even the language of UUVs is unclear. This has legal implications for concept and technology sharing, and field use. But further considerations must also include regional partnerships for maritime 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 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 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 more so 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.

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.

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

“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).”

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.

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.

Introduction

This report arrives at a critical juncture, when attention to maritime and underwater security has intensified due to recent events, such as the underwater sabotage of the Nord Stream pipeline in the Baltic Sea. Such incidents have underscored the urgency of bolstering Australia's maritime and trade security, particularly given the shifting geopolitical landscape and regional tensions in the Indo-Pacific.

Australia's reliance on maritime trade is significant, accounting for about 99 percent of the country's total trade volume, with two-thirds of exports traversing the South China Sea.[3] Reliance on just-in-time supply chain processes have left the country prone to economic and strategic shocks due to its location as an island nation at the end of global trade routes. An economic culture of obtaining the lowest price for goods in international markets has maximised Australia's spending power, but it has, over time, led to poor strategic resilience and increased vulnerability from these supply chains.[4]

A critical shortfall in these supply chain challenges is fuel supply. Between 2000 and 2022, the national transport fuel import dependency increased from 60 percent to 91 percent, without corresponding plans to protect the country against sudden shocks.[5] The country currently imports 90 percent of liquid fuel and does not have sufficient capacity to meet the 90-day stockholding requirement of the International Energy Agency's recommendation. The implications of these fuel limits are considered grave for the Australian Defence Force (ADF). But also ill-considered in these challenges is the impact on the economy and broader society, should an event occur that delays or denies critical imports of fuel.

The recent tensions and potential conflicts in the Indo-Pacific region exacerbate these challenges to Australia's sea-borne trade. China's expansive claims to ownership of the South China Sea, and recent scenarios involving an invasion of Taiwan, have surfaced repeatedly in defence planning documents to bring focus to regional defence modernisation plans, with new threats located in autonomous uncrewed underwater vehicles.[6]

Robotic weapons are widely believed to be the future of war and autonomous UUVs are part of future warfare. Autonomous UUVs have enormous potential for operating for very long periods without needing to surface to replenish oxygen or fuel supplies, or to return to base to rotate crews. This renders them ideal for roles in which the capacity to loiter undetected is an advantage.[7] They pose a future security threat to Australia's trade routes in the Indo-Pacific region as well as Australia itself. Possible scenarios relate to UUVs attacking shipping in key Australian shipping lanes and ports. But are the future security risks of these new technologies really understood?

Against this backdrop, this report focuses on the potential security threats posed by uncrewed maritime systems and autonomous vehicles. In addressing the technical, ethical, legal, and policy issues related to these technologies, four stages of analysis are adopted. These are:

1. A definitional assessment drawing on the current literature;
2. Scenario development, addressing the impact of emerging technologies in UUV systems;
3. An impact analysis will unpack the threat environment and assess mitigation steps; and
4. A policy analysis will identify future policy considerations.

In addressing the emerging threats of UUVs to Australian security, the project seeks to deliver on three outcomes:

- Raise public awareness about the future risk and threat of autonomous uncrewed underwater vehicles;
- Provide recommendations and inform broader strategic and policy debates on the resilience and security of Australia in relation to autonomous UUVs; and
- Develop future policy recommendations for Defence and the Australia Government to protect Australian maritime trade and infrastructure.

Australian trade and maritime threat landscapes

Seaborne critical infrastructure refers to surface and subsurface equipment and technology anchored to the ocean floor or situated at the nodes of maritime trade and transportation. This infrastructure includes the important seaports, associated structures and storage facilities, undersea sensor capabilities, cables for telecommunication and power transmission, and other stationary equipment for scientific research.

Recent attention to vulnerabilities in undersea commercial and maritime links has revealed what some have stated as an "existential threat" to Australian seaborne critical infrastructure. Undersea fibre optic cables carry 97 percent of the world's communications and over US$10 trillion in daily financial transactions. The locations of these cables remain publicly available, and despite their indispensability as the predominant thoroughfares of the world economy, they receive minimal protection.[8]

Examples of undersea cable vulnerabilities demonstrate the dangers posed by UUVs. In 2007, investigations into Al-Qaeda terrorist activities revealed a plot to take out a key London internet exchange. When Russia annexed Crimea in 2014, it quickly severed the main cable connection Ukraine had with the outside world. More recent activities include attempts by Russia to gain intelligence and sabotage critical infrastructure in the Dutch part of the North Sea,[9] and the severing of an undersea cable connecting satellite assets on Norway's Svalbard Island in the Arctic Ocean in January 2022.[10]

Meanwhile, outside of conflict scenarios, accidental damaging by fishing trawlers, natural disasters, and anchors occurs with surprising frequency, but in some cases can cause significant disruption to communications and commerce, sometimes for months on end.

Grey zone activity scenarios also present a credible threat to underwater critical infrastructure. Grey zone activities are those that fall between the traditional concepts of war and peace.[11] These can include cyber attacks, political subversion, economic coercion, and other tactics that are below the threshold of traditional military conflict but still aim to destabilise or undermine adversaries. Given the vastness of oceans and maritime domains, including the diversity of actors operating in these spaces, the ability for states or non-state actors to hide behind plausible deniability is significant. That such activities are often defined by low levels of moral sensibility, in that outright violence is masked by abstracted outcomes, makes them more attractive for actors looking to participate in asymmetric disruption and violence.[12]

There is ample evidence to suggest UUVs will increasingly be used as tools at the frontline of grey zone warfare. For instance, were Australia's adversaries seeking to preclude a maritime or military response to a direct threat to national interests, the employment of UUVs to disrupt strategic maritime trade channels or ports could delay a critical response and even potentially cripple future military defence operations due to strategic fuel shortages. These scenarios were considered by expert stakeholders as current-day, real-world threats amid existing state-based UUV capabilities.

Recent undersea critical infrastructure events in the Taiwan Strait illustrate the potential for further underwater grey zone activities to develop into existential crises. In February 2023, two undersea cables in the Taiwan Strait linking Matsu Island to the Taiwan mainland were cut. While denied by Chinese authorities, accusations emerged that Chinese vessels sought to deliberately sabotage the cables, whether as practice for some later planned operation or for disruption purposes. The fact that both were cut by Chinese mainland registered ships in separate parts of the ocean (and six days apart) caused many to question the accidental nature of these "accidents." [13]

In such scenarios, the disruption to commerce was minimised, but the threat to a communication break with Taiwan holds significant implications for sovereign defence. In a conflict scenario, damaged communications can prevent a timely counteroffensive. Of course, these scenarios are going to be context-specific. For Taiwan, China's daily fighter plane incursions, its information and cyber campaigns, and state policy to unite Taiwan with the Mainland, underscore the existential nature of these strategic activities. This has led some to refer to such undersea cables threats as Taiwan's "Achilles heel." [14]

In an Australian scenario, deliberate attempts to sabotage undersea cables or disrupt maritime trade hold similar implications for Australian defence and security. An unidentified UUV in a strategically important harbour could hold up traffic for days. Intentional sabotage of cargo vessels in strategically important straits could delay critical supply and even cause costly and permanent rerouting of maritime trade. The threat environment involving UUVs, as these scenarios illustrate, presents an emerging challenge for state security.

A final consideration gaining increasing attention among military authorities is the potential for future seabed warfare. The September 2022 Nord Stream sabotage demonstrated the current vulnerabilities of underwater infrastructure to attacks by state and non-state actors. NATO, in response, established the Critical Undersea Infrastructure Coordination Cell to begin building capabilities to protect seabed infrastructure against kinetic and non-kinetic grey zone attacks.[15] The EU and NATO have also since announced a joint Task Force on Resilience and Critical Infrastructure Protection. Meanwhile, corresponding with similar programs in the UK, Italy, Germany, Sweden, Norway, and the US, France has adopted a Seabed Warfare Strategy with procurement programs aimed at maritime mine countermeasures and future UUV deployment. [16]

These rapid developments reflect the mounting capacity of states to open new domains of war with significant implications for strategic capabilities and national defence. Calls for the development of high-end capabilities to protect maritime domains against "self-propelled underwater weapons" and "clusters of autonomous weapons that lay on the ocean floor until activated" have become much more prevalent. "'Seabed warfare'," writes Salerno-Garthwaite, "is no longer a distant concept: it represents an immediate and legitimate threat to Allies[…]; maritime experts assert that seabed security concerns present an already significant threat that requires immediate defensive action." [17]

Current and future UUV capabilities

In the context of maritime threats, and with a particular focus on UUVs, this report considers whether Australia is adequately prepared for such disruptions.

Uncrewed Maritime Systems (UMSs) have in recent years undergone "aggressive technological progress and operational concept development." UUV capabilities have increased to include a plethora of offensive and defensive technologies, not limited to intelligence, surveillance, and reconnaissance (ISR); mine countermeasures (MCM); antisubmarine warfare; surface warfare; inspection and identification; oceanography; communication and navigation network nodes; payload delivery; information operations; time-critical strike; barrier patrol and operations such as homeland defence, antiterrorism, and force protection; seabase support; electronic warfare; laying undersea sensor grids; sustainment of at-sea operating areas; bottom mapping and survey; and special operations. [18]

In the United States (US), funding allocated to UMSs in recent years has increased by over 300 percent.[19] By 2024, the US expects to deliver prototypes for extra-large UUV (ELUUV) "Orcas" that will, among other things, be capable of covertly deploying hammerhead mines, "a planned mine that would be tethered to the seabed and armed with an antisubmarine torpedo." [20] Initiatives by the Defense Advanced Research Projects Agency (DARPA) further seek to equip forward-deployed surface vessels with autonomous uncrewed vehicles and stations to improve UUV endurance, communication, and data transfer. Further, the US plans to develop rapidly projectable Advanced Undersea Warfare Systems with the ability to break down area access/area denial (A2/AD) networks.[21] In China, the development of the HSU-001 Large Displacement UUV (LDUUV) underscores an expansive program of research and funding for future UUV deployment.

China has achieved several milestones in the development of unmanned submersibles, including the Haidou-1 project, which has set the world record with a dive depth of 10,908 meters. Additionally, China's underwater glider, the Haiyan, has set a new endurance record by sailing 3,619.6 kilometres for 141 days in the South China Sea. Meanwhile, Russia's UUV development seeks to include a "nuclear delivery drone" which operates underwater and can transport a payload up to 6,200 nautical miles.[23] These claims have yet to be verified, but if true, the implications of nuclear-powered and AI-enabled UUVs are significant, with broader concerns for UUV arms race and nuclear material accidents.

Other examples of underwater autonomous vehicle systems include the French ECA Group's "robot drones." These can travel underwater without requiring input from an operator, without a cable, and have their own integrated energy. They can be used for "underwater mine warfare, homeland security, crucial infrastructure protection, harbor and coastal surveillance and protection, rapid environmental assessment," and deep-water survey and inspection. More important to the Australian context, they can be launched and recovered via robots. [24]

UUV development in Australia

There have been renewed calls for the Australian government to invest in networks of UUVs to be "permanently stationed in high traffic areas of Australia's maritime jurisdiction to perform broad search and detect functions." [25] With greater autonomy and low power requirements, UUVs can also allow for extensive and continuous surveillance of Australian maritime areas, meaning threat detection evasion is significantly reduced. Beyond surveillance, research and investment could enable them to contribute to border control processes which have been traditionally hampered by large open maritime spaces and expensive maritime patrol vehicles.

Investment in uncrewed drones is already being explored by the Australian government and military, with several projects in development to increase Australia's surveillance capabilities at sea. Examples include the Triton Uncrewed Aerial System and Anduril's Extra Large Autonomous Undersea Vehicle, Ghost Shark, which will be used for maritime patrol and other surveillance roles. Other capabilities being funded in a maritime context include submarines that form part of the AUKUS agreement between Australia, the United Kingdom, and the United States.

Australian defence readiness has now undergone two recent strategic defence revisions (2020, 2023), with significant implications for maritime defence. In addition to RAN's Robotics, Autonomous Systems, and Artificial Intelligence (RAS-AI) strategy (2021), strong emphasis has been placed on building UUV capabilities to supplement broader conventional capabilities.[26] While there is some discrepancy on the emphasis placed on UMSs in the 2023 Defence Strategic Review (DSR), all strategy documents, including RAN's Plan Mercator (2017) and Plan Perolus (2022), demonstrate the increasing challenge of these emerging technologies and the response required to address the new threats they offer. [27] However, challenges around funding and priorities associated with AUKUS-platform nuclear-powered submarines (SSNs) threaten to marginalise these plans (see appendix A).

Under the DSR 2023, funding has been dedicated to a new Advanced Strategic Capabilities Accelerator that will build upon the Defence Science and Technology Group's planned acquisition for UUVs. This is proposed to be developed alongside "selected technology areas as part of AUKUS Pillar II," prioritising the acquisition of "advanced capabilities[…]in the shorted possible time." [28] Presumably, these acquisitions will occur alongside the RAS-AI strategy and RAS-AI Campaign Plan 2025, which has called for full implementation and offers the clearest articulation of current capabilities in USVs and UUVs being deployed by RAN.[29] Further, it highlights the path forward, and potential capabilities, covering "the rapid development of combat-ready prototypes to accelerate operational deployment of game-changing capabilities." [30]

"UUVs can also allow for extensive and continuous surveillance of Australian maritime areas, meaning threat detection evasion is significantly reduced."

Definitions: Uncrewed Maritime Systems (UMSs)

This report follows NASA's non-gendered approach to autonomous systems nomenclature. "Uncrewed" underwater vehicles in this report is employed as a more inclusive alternative to "unmanned" without significant deviation from meaning.

There is considerable variation in the literature when discussing uncrewed vehicles and technologies in a maritime domain. In the broader context, uncrewed systems can be self-governed or remotely controlled and can function underwater or on the surface. They can act as a vessel by themselves or be deployed from air, land, subsurface or surface. These systems can be used in accordance with internationally accepted maritime laws. [31]

There are two main categories or sub-classifications of UMSs: Uncrewed Surface Vehicles (USVs) and UUVs. USVs are considered more versatile and excel more broadly at waterborne communication. For this reason, they are considered more effective in military operations that require C4ISR capabilities and can be engaged in military deception, information operations, electronic warfare, and cyberwarfare. The flaws in communication capabilities of UUVs, compared to USVs, define stronger stealth capabilities and therefore the attractiveness of UUVs for missions requiring attribution deniability and/or surprise. [32]

UUV variability differs with the degree of autonomy allocated to the system. They can be fully autonomous (human out of the loop) with AI onboard capabilities, or semi-autonomously operated (human on the loop) with some form of remote control or umbilical cord function for extended endurance. [33] Earlier definitions adopted by the US Navy illustrate that definitions have varied little over the years. UUVs are "self-propelled submersibles whose operation is either fully autonomous (pre-programmed or real-time adaptive mission control) or under minimal supervisory control and is untethered except, possibly, for data links such as a fibre optic cable." [34]

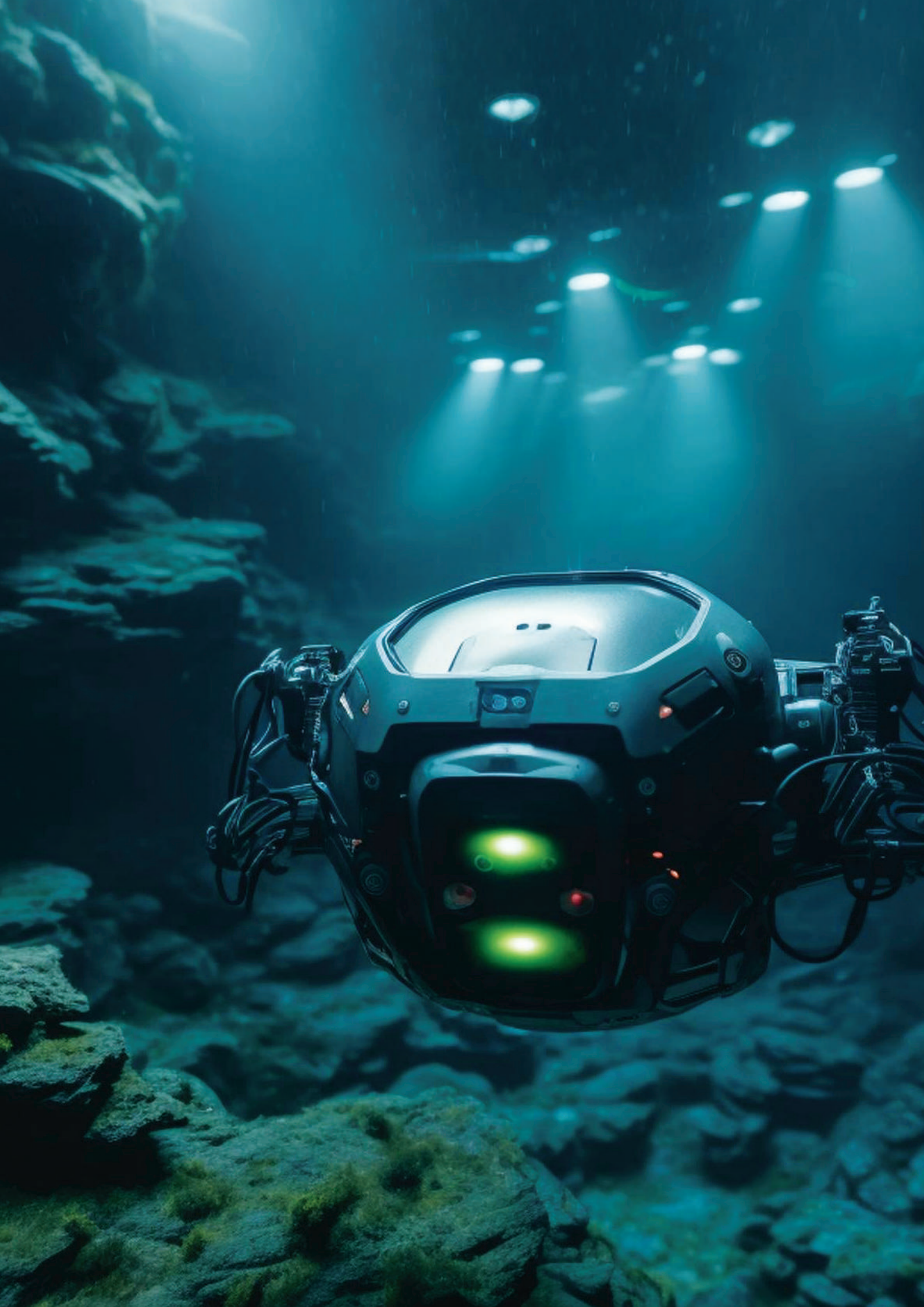
Indicatively, this broad conceptualisation has led to the emergence of duplicated terms with some minor variations in what can be recognised as a "family of devices." These include:

- Amphibious Underwater Vehicles
- Autonomous Submersible Weapon Systems
- Autonomous Underwater Vehicles (AUVs)
- Underwater Naval Vessels (UNVs)
- Unmanned Combat Vehicles
- Unmanned Combat Underwater Vehicles
- Maritime Autonomous Vehicles (MAVs)
- Marine Unmanned Vehicles (MUVs)
- Underwater Maritime Vehicles (UMVs)

An argument for such differentiated terms is that the primary nature of some systems – amphibious underwater vehicles, autonomous submersible weapon systems, and unmanned combat vehicles are designed for military use, either with weapons systems or as a weapon itself in mind. Others suggest that a distinction should be made between those which are "remote-controlled" and "fully autonomous." [35] Still others assert that identifiers like location and whether the vehicle will remain on the surface of the water, or whether it is submersible, should be taken into consideration.

Discernibly, considerable overlap, despite attempts for more nuanced descriptions, can be drawn between the terms above and in their consistency of use across the various publications discussing UUVs. Broadly described, therefore, UUVs are an underwater robot that serves a variety of purposes, including oceanographic research and military operations. It can perform tasks such as conducting underwater surveys, inspecting submerged structures, tracking oceanographic features, mapping the sea floor, laying undersea cable, searching for lost aircraft, and detecting naval mines. [36]

UUVs are effective in gathering data with high resolution in time and space, making them suitable for surveying large areas. They can carry multiple payloads, enabling synoptic coverage and measurements of various parameters, such as water quality, magnetism, and turbulence. AUVs can determine their underwater position through acoustic positioning, dead-reckoning using a Doppler Velocity Log and compass, or by inertial navigation that measures acceleration and rotation.[37]

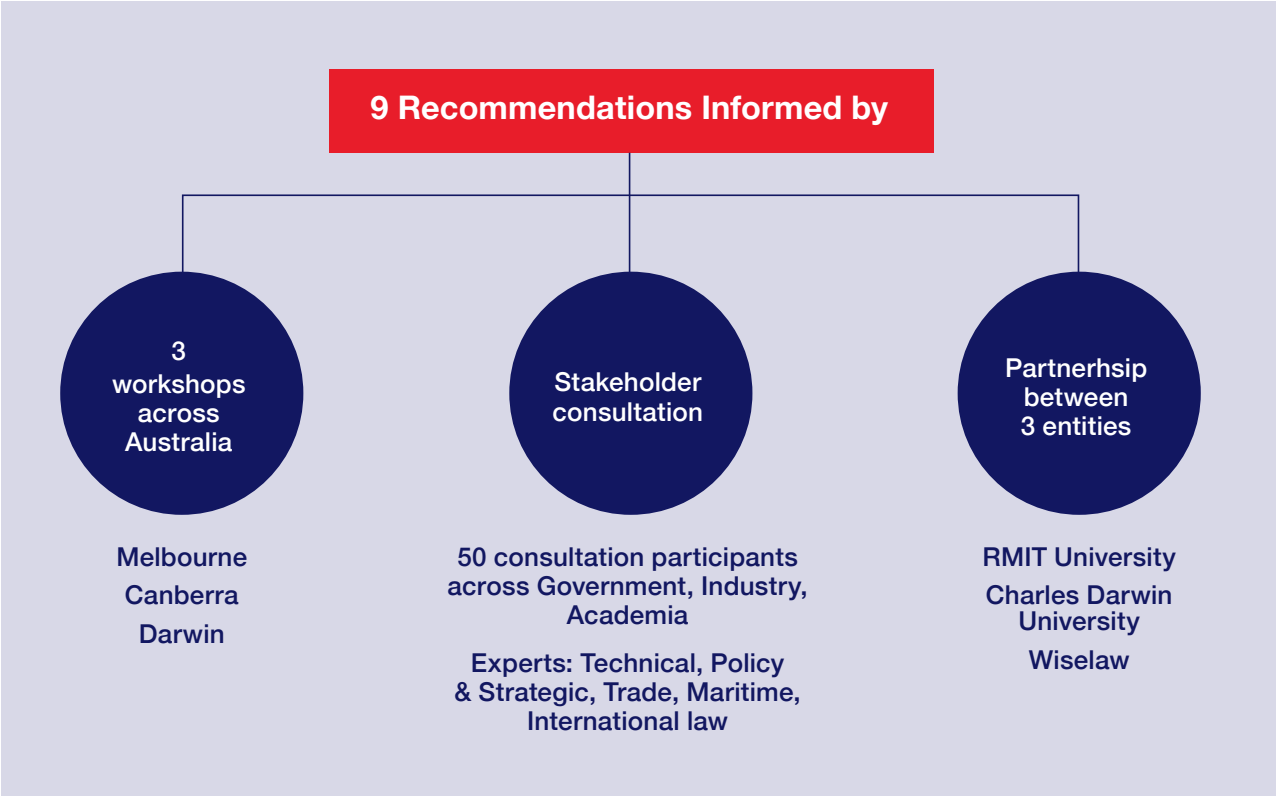


Workshop - Overview and Rationale

The project team invited stakeholders encompassing the Royal Australian Navy (RAN) and the Australian Department of Defence, including engineers and policy personnel, key industry stakeholders in UUV development, leading members of academia, and legal representatives to engage in a series of three workshops located in Melbourne, Canberra, and Darwin during 2023. Expert workshops are an effective platform for engaging with key stakeholders in the research process. As a form of co-creation, where stakeholders jointly generate value, the workshops also allowed for the contribution of "outsider perspectives" in the production chain of knowledge and outcomes.

To further enhance the outcomes of the workshops, the investigators differentiated the scenarios to correspond with the expertise range in each workshop. These ranges cut across policy and strategy, technology, and operational perspectives.

In generating the impact analysis, the workshop considered a series of five scenarios with corresponding questions that would contribute to an expert threat assessment. These scenarios were developed from a desk-based literature review employing published and grey literature, and with key input from industry and legal experts. The insights below are a synthesis of the three workshops.



Scenario 1

How will coordinated attacks by UUVs impact Australian maritime trade and critical underwater infrastructure?

Do UUV coordinated attacks pose a possible security threat to Australia?

Considerable threat:
The consensus from stakeholders among all three workshops was that coordinated UUV attacks posed a considerable threat to Australian security. Coordinated attacks refer to a scenario in which a group of UUVs collaborate to accomplish a particular objective or mission. These risks may originate from state actors, cybercriminals, or pirates. Australia has vulnerable supply chains and Sea Lanes of Communication (SLOCs). The cluttering of these choke points with UUVs could disrupt critical supply to Australia. In such scenarios, low-cost, market-access UUVs can increase the number of potential adversaries or criminal cyber actors who want to experiment. Costs to such actions include disruption to shipping lanes and, notwithstanding delays, increased economic and financial costs, and decreases in the reliability of supply chains; and damage to underwater pipelines, cables, and other critical assets, with implications for economic and national security.

UUV ubiquity:
In this scenario, there is a pronounced difference between current UUV capabilities and future potential uses and capabilities. Most workshop members agreed that current UUV technologies on the open market, with the exception of mining-company-operated drones, are insufficient for major attack scenarios. Nonetheless the growing ubiquity of UUVs is considered to be increasing the space for the employment of simple and cheap (known as “dumb”) UUVs to disrupt, deny, and degrade critical maritime trade infrastructure. One identified scenario by workshop members, for instance, was the deployment of fake or real mines in strategic locations, such as ports. Others could be used to clutter maritime highways and divert trade. Additionally, it was recognised that these mines can be manufactured as UUVs with Improvised Explosive Devices (IEDs) attached.

Currently, more advanced state-based UUV capabilities are closed to open market actors or subject to export control regimes, meaning their employment will likely be limited to offensive actions in wartime scenarios, or for use in grey zone activities, more of which is discussed below in scenario two.

Operational considerations:
Significant technical difficulties characterise current underwater navigation capabilities. Communication for command, control, and data exchange platforms are considerably reduced in underwater environments. Acoustic communication through sonar is the most used platform, but sonar can be easily discovered by other actors with active sensor and sonar capabilities (see Appendix A). Optical communication through light transmission, by contrast, can provide higher bandwidth, but is subject to limited conditions, such as clear water environments. Meanwhile, wire-tether communication is limited in range and mobility.

Radio wave communication:
Radio wave applications are useful for long-range communications where information, critical updates, and data can be transferred by tactical satellite uplinks. This is the most plausible communication technique for long-distance, AI-enabled UUV operations. However, as workshop members highlighted, in scenarios where secrecy and non-detection were key to mission outcomes, any attempt to engage in radio wave communication could be fatal to the UUV and mission if operational requirements require the UUV to surface for communications.

Environmental impact:
An additional operational challenge is underwater navigation and control. UUVs are subject to complex environments where changes in the levels of water salinity, heat, and ocean currents can disrupt navigation. Variances in UUV technological capacity, such as battery life and data and memory storage, will also define the ability to manoeuvre through consistently moving oceans.

For many of the experts, these challenges highlight the improbability that UUVs will be deployed to disrupt or damage undersea cables linking Australia to other parts of the world. While such scenarios are plausible in theory, these actions would be very difficult to undertake. Easier options via the employment of USVs exist where the cables reach land and where they are much easier to locate. Land-based attacks against critical node points would be even easier still.

In envisaging the future of UUV use, it is widely accepted that UUV capabilities will become more diffuse. One potential outcome on this basis is that UUVs will increasingly become the 'scooters of the maritime activity' for criminals and non-state actors. They can boost the efficacy of other attacks and can be used to launch weapons of mass destruction capable of wreaking havoc on Australia's maritime infrastructure.

Discussion of current real-world threats led to several plausible threat scenarios:

Some threat scenarios could include:

- A USS Cole scenario: Instead of a USV attack, UUVs could be used to critically damage shipping while also masking the identity of the attacker. [38] This presents a credible asymmetric advantage, since the loss of one comparatively inexpensive UUV can tie up a US$1 billion warship for many years in a repair yard.
- A nuclear catastrophe involving nuclear payload delivery - UUVs, such as Russia's hyped prototype. In this instance, even if not used as a deliberate weapon, the potential for accidental harm to the unit from fishing vessels or from natural disasters could produce nuclear pollution within Australia's Exclusive Economic Zone (EEZ) or from further off waters that may then require maritime chokepoints to be cut off.
- Biological attack. This scenario envisions UUVs capable of harbouring and letting loose biological agents close to maritime fishing industry crops, like Tasmania's salmon farms, or national tourism ecosystems like the Great Barrier Reef.
- Cyber attack via payload. Small and cheap UUVs may release virus- or malware-infected payloads (USBs) on to a beach, creating havoc for unsuspecting citizens with potentially larger ramifications for cyber security.

What measures need to be taken to safeguard Australia's maritime trade and underwater critical infrastructure against coordinated UUV attacks?

RAS-AI:
Experts agreed that a multifaceted strategy for detecting and mitigating the risks associated with UUVs is considered necessary, given the implications of the future threat landscape discussed above. In this context, RAN's RAS-AI strategy partially contributes to building UMS resiliency and platform capabilities. However, concerns around funding over the long-term, with the commitment to SSN development in the AUKUS arrangement, were persistent (Appendix A).

While some considered SSN submarines game-changers for maritime security, there were concerns about what was not being funded as a result of the high costs of the AUKUS submarine platform. In mitigating potential future UUV threats, suggestions were made for investments in advanced radar technology; networks of sensors along the 12-nautical-mile territorial zone that would act as an advanced coastline communication system; greater familiarity with local oceanography; an advanced understanding of the technical specifications of UUVs; the ability to classify the danger posed by UUVs; and public engagement and education. On this basis, an underlying criticism of current strategy documents and agreements such as AUKUS, RAS-AI, and the DSR underscore that while the government's dedication to enhancing UMS and UUV capabilities is improving, current policy fails to adequately outline how these new capabilities will be developed. RAS-AI, for instance, predated the monumental agreements established in AUKUS and the DSR and is up for review in 2024.

Underwater cables: For undersea critical infrastructure such as internet cables, workshop members agreed that diversifying Australia's financial and economic links to the global economy and building in redundancies was pivotal moving forward. The development of satellite technology has allowed for the rapid diversification of communications. While Australia can request access to US satellite communication and detection capabilities, greater sovereign capacity is required. Currently, consideration of secure communication links with the rest of the world will necessitate moving away from a reliance on one or two underwater cables and building in redundancies in satellite systems and more cables. With further advancements in detection technology, trends in satellite communications are moving toward entire ocean detection capabilities.

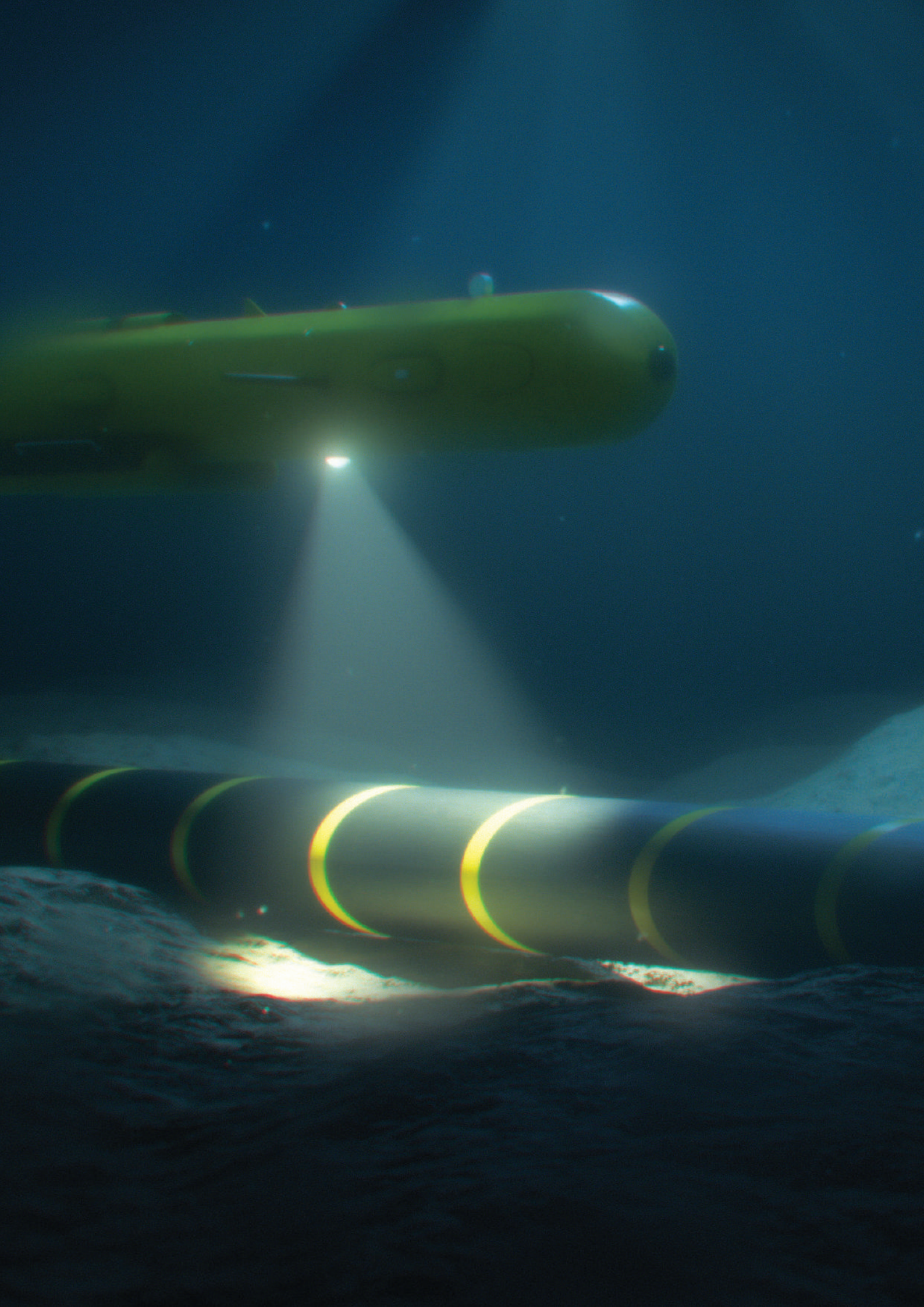
***Telecommunications Act* 1997:** Australia is in a unique position to take advantage of existing policies protecting critical undersea assets. The *Telecommunications Act* 1997 outlines the use of Cable Protection Zones (CBZ) in protecting critical national assets in Australian and associated waters. Any vessels operating within the zones are required to broadcast their positions to the coast guard. Most fishing activities in the zones, including anchoring and bottom trawling, are prohibited to avoid damage to cables.[39] *The Telecommunications Act* 1997 provides Australian authorities with the legal cover to protect these assets, but as UUVs are likely to be employed for undetectable missions, tracking them will require greater and more sophisticated systems for maritime domain awareness. The Triton uncrewed aircraft and other autonomous aircraft systems currently provide surveillance and monitoring capabilities in this domain. Additionally, Australia's fleet of maritime patrol aircraft can send sonar waves into the water and fly low and slowly, listening for detection. However, protecting such a large coastline is challenging. Investments in satellite technologies will help to alleviate the time and resources required to monitor protected maritime zones.

What are the roles of maritime law and regulations to protect against possible UUV coordinated attacks?

Legislative reforms: The laws applying to autonomous vessels, including autonomous UUVs, operating in Australian maritime environments are still at an embryonic stage. The Australian Maritime Safety Authority (AMSA), which is the national regulator of vessels operating in Australian maritime environments, has recognised that there will eventually be a need for legislative reform addressing the unique nature of autonomous vessels. However, at this time, the Australian laws regulating autonomous UUVs are those which were written for conventional crewed vessels. This throws up a number of challenges for the operation of UUVs which cannot comply with many existing requirements. These challenges are currently being met by the grant of certain exemptions.

International law:
International law exists to prevent unauthorised land, air, and sea incursions into the territory of other nations. Current maritime law and international norms were broadly recognised by workshop members as playing a fundamental role in Australian responses to maritime threats and defence technology acquisition. However, a consistent and overarching theme was the broader erosion of norms in international waters, as exemplified by China's militarisation of islands in the South China Sea, its use of maritime militia to punish smaller actors, and a broader growing tolerance for disregarding international law.

International law and UUVs:
As it stands, there are legal gaps on the use of uncrewed underwater vehicles, though this does not include UUVs employed specifically as IEDs or moving ordinances. The Vienna Convention on the Law of Treaties underscores that when international law is silent on a particular issue, the authority reverts back to the state or is interpreted in a matter in good faith. One concern here, however, is that as the law of any nation may apply to UUVs, these laws may become customary international law, and may run counter to liberal global norms. China has been very active in building legal public goods for this purpose and, unless it is challenged, could well lead the way in defining legal norms around emerging technologies.



Scenario 2

What cyber capabilities do UUVs possess? What potential effects could these have on Australia's maritime trade and critical infrastructure?

What safeguards are required to protect Australia's maritime infrastructure from cyber attacks posed by UUVs?

Cyber disruptions: Experts agreed that UUV-based cyber attacks could be used for both active and passive attacks. In a maritime scenario, the importance of maintaining systems availability is considered more crucial compared to systems confidentiality (the ability to assure that the system is capable of preventing access to data by any unauthorised entity) and integrity (the capability of a system to prevent unauthorised alterations of data by any entity). Non-availability of communication networks or critical infrastructure could substantially impact essential services (for instance Global positioning systems [GPS]), which could have far-reaching implications for international trade, diplomacy, and security. For instance, the loss of undersea cable connectivity in Australia would necessitate rerouting all international internet traffic to and from Australia via satellite links to neighbouring countries. This scenario would drastically reduce bandwidth and increase latency, impacting the performance of internet-based, high-speed services. Similarly, UUVs could interfere with ship navigation by jamming signals or interfering with communication networks, which could pose a significant threat to maritime security and ship crew safety. A key policy and strategy response for this consideration is to build effective communication and navigation redundancies into maritime systems.

Detection strategies: These can vary based on the malicious activity of UUVs. Strategies could involve developing technology to detect and intercept malicious signals or data transmissions and monitoring for any unusual activity in communication networks or critical infrastructure. If UUVs are designed for passive data collection, preventing them from gathering sensitive information may be more difficult. However, detecting and countering their activities may be easier in the case of an active counter-UUV strategy. The participants also highlighted the interconnected nature of submarine systems, making it difficult to isolate and protect against cyber attacks. Disruption to one system could have cascading effects on other systems, making it essential to take a holistic approach to submarine cyber security.

Can drone approaches/strategies such as swarming be applied to a cyber context, e.g., DDOS attacks and UUVs?

Cyber attacks: Experts covered two themes on this question. The first was the technical capacity for UUVs to carry cyber offensive capabilities. In the present context, UUVs could plausibly be employed as physical access vehicles for proximity-specific operations. Examples like Stuxnet, where it is theorised that a double agent used a USB flash drive to infect computer systems to take out centrifuges in Iran, offer examples of proximity-specific cyber attacks. The question of how a UUV might connect to a ship or other terrestrial systems is important. One expert posited a scenario where a UUV is captured, malware is implanted into it, and the device is returned to the sea (see Appendix C). This was considered a real-world threat, particularly since examples of UUV capture already exist [40] (The capture of the unmanned surveillance drone RQ-170 Sentinel illustrates that the cyber vulnerabilities of unmanned and autonomous systems are not insignificant). The cyber penetration of a US Air Force base housing Reaper and Predator drones in 2011 further highlights the creativity of malicious actors to piggy-back into secure systems on vehicles considered safe by authorities. While the exact source of the implanted malware that followed could not be established, the impact included the theft of passwords and other personal information of US service members, while also logging and monitoring the keystrokes of drone pilots.[41] With more UUV systems in operation, future capture and release scenarios with cyber corruption intentions offer credible threats to defence and commercial networks.

Communication challenges: A broader operational challenge identified with current UUV capabilities in the cyber context is battery capability, particularly on micro (less than 5kg with a range of 100m-1km) small (5kg to 100kg with a range of 10km to 100km) and medium UUVs (100kg to 1000kg with a range of 100km to 1000km). Manoeuvrability will depend on the propulsion systems and power sources. Deeper dives and stronger currents require more power to maintain movement. Further considerations include payloads, such as equipment, instruments, and sensors, connectivity mode, and intended use. Without physical connection, cyber-enabled attacks from UUVs require a surface link with a comparatively slow radio wave connection. If invisibility is critical to mission success, even short periods on the surface could reveal UUV whereabouts. On that basis, experts saw little value to using UUVs for cyber attacks, even with tactical datalink systems.

UUV Swarming: The practicalities of UUV swarming, where multiple vehicles are employed to converge on a target, were also considered of little current value. Swarming can offer AI network collaboration features where short-range positioning and manoeuvrability can be magnified by acoustic communication features for operational enhancement. It may also be useful for providing redundancy in a coordinated attack. However, all experts agreed that there were easier, cheaper, and more sophisticated vehicles (UAVs, USVs) available for cyber offensive purposes rendering their employment at this stage mostly hypothetical.

Other considerations offered were the use of modern electric warfare capabilities via UUV antennas to jam signals and communications or even intercept short range communications. In major shipping lanes, even a few minutes of disrupted communications could prove damaging. In this context, the scenario of further *Ever Given* disasters in the Suez Canal or other key shipping lanes were discussed as plausible threat scenarios.

Do UUV cyber attacks pose a threat?

UUV vulnerabilities: Experts agreed that current UUV cyber capabilities don't pose a serious threat to Australian maritime and territorial defence at the moment. The principle reason for this justification is the limited capabilities for network exploitation among smaller UUVs due to battery power. Because of their size, much of the internal power will be dedicated to drone operation and tactical data link systems. As these systems develop in the future, the capabilities for employing UUVs for cyber attacks will increase. For now, UUVs will need to operate with other systems, such as USVs or UAVs, to be effective in a cyber context, but not in isolation.

Scenario 3

Do UUVs pose a threat to Australian shipping routes and ports?

What safeguards are required to protect Australia's maritime infrastructure from cyber attacks posed by UUVs?

Shipping lanes: Workshop members agreed that UUVs could cause blockages and disruptions to shipping lanes and ports not only close to Australia but also in other regions, such as the Suez Canal and the Malacca Straits. This recalls the example of the grounded *Ever Given*, mentioned above. The cost to global trade over the two weeks was close to US$60 billion.[42] Other scenarios envisage blockages in northern trade chokepoints near Lombok, Indonesia, or east of the Philippines, and illustrate the potential flow-on effects from UUVs being employed by unsophisticated, non state actors. For instance, maritime crises emanating from UUV attacks will create insurance challenges for commercial shipping. The forcing of maritime trade actors to reroute their cargo via less dangerous, but ultimately longer, trade routes or to abandon them altogether to avoid paying exorbitant insurance fees will require Australian authorities to rethink current strategic resource capabilities and other potential costs to delayed critical supply chains.[43]

Trading partners: Another consideration here is the threat of shipping to Australian trade partners. As illustrated in Appendix B on North Australian perspectives, key trade partners who rely on strategic resources from Australia are equally vulnerable to UUV attacks. One estimate is that 15 percent of Japan's total energy imports are sourced from Darwin's Impex Ichthys Facility, which must pass through the narrow mouth of Darwin Harbour. Additionally, as future energy projects such as Sun Cable propose to send power generated by solar via submarine cable from Darwin to Jakarta and Singapore, UUV interference could be financially damaging.[44] Because these threats need to be accounted for in project development, the capacity for Australian maritime forces to secure and protect Australian oceans will also be evaluated.

Extra Large UUVs: The threats posed by UUVs are likely to grow as they become more sophisticated. Extra Large UUVs (ELUUVS) are likely to increasingly take on the roles of modern submarines and maritime surface vessels. This includes payload delivery, which can include nuclear fissile materials or even weapons in black-market operations. Thus, it is considered that their employment for other black market and illegal exchange will become increasingly prevalent as capabilities become more ubiquitous.

Underwater mines: The most significant potential and contemporary challenge for Australian shipping is underwater mines. Self-propelled mining systems can loiter or be preprogramed to target shipping, port terminal gateways, and even avoid mine clearing vessels. These mines can also be deployed via UUVs, making them extremely difficult to locate. While it is considered that Australia's distance is an advantage, as it is most likely any UUV mine deployment device would require a mother ship, large UUV gliders will diminish this advantage over time. Current mine clearing capabilities are time consuming and are desperately limited in Australia.

Psychological threat: A second implication of this discussion is the political fallout from such a recognised threat. A mine does not have to be detonated to create a significant blockage in a major port, such as Fremantle. Additionally, the presence of one mine in one port may prompt a security review of all major ports, leading to more disruptions, panic, and a tightening of resources. A foreign-identified UUV in a major port will likely create a similar threat response, requiring significant delays until a security sweep is conducted. In December 2018, a UAV breach of the runway space at Gatwick Airport in the UK caused the airport to close, rerouting all incoming traffic. An unidentified UUV in a busy maritime port has the same potential.[45]

What measures/steps are essential for maintaining the safety and security of Australia's maritime routes and ports from the threat posed by UUVs?

Responses to mines: Australian forces already conduct littoral force protection operations, littoral interdiction (counter smuggling), and littoral underwater area denial operations, all involving improved uses of UAVs, UUVs, and USVs. Additionally, exercise Autonomous Warrior 2022 (AW2022), a Five Eyes multinational joint advanced military and AI systems training exercise, has encouraged diverse training platforms and helped to build technological solutions into littoral force protection operations. AW2022 included 40 autonomous systems and technologies with input from 40 organisations from across the world.[46] Hosting more exercises integrating such systems would build upon littoral underwater area denial.

To counteract the threat of underwater mining systems, RAN in 2019 initiated the SEA 1905 Maritime Mine Countermeasures (MCM) Program. This proposes to replace the four existing Huon-class Mine Hunter Coastal ships, with Arafura-class offshore patrol vessels capable of deploying modular UUVs with mine hunting and military survey capabilities. But more mine hunters will be required to appropriately monitor and respond to threats in Australia's maritime space. For instance, Australian ocean-borne trade is distributed across six key ports, with other minor ports taking in the rest. While mine hunter vessels can be deployed or transferred to critical choke points in the event of a crisis, crossing the vast distances between the ports will take time. Meanwhile, it is estimated that UUV mine technological advances will create increasing demand for mine clearing capabilities as they become more ubiquitous and are able to travel greater distances. These future technological capabilities will put a premium on seabed detection systems and grid sensor networks, which have not received adequate attention in Australian maritime strategy. For many of the experts engaged in the workshops, the ability to develop counter UUV capabilities was considered fundamental to enhancing Australian maritime defence.

Vulnerabilities: The critical policy response identified by experts was to reduce strategic resource vulnerabilities and increase resiliency in global supply chains and undersea infrastructure. Developing strategic fuel resource capabilities on land was considered the most important measure for Australian authorities. This view was particularly relevant for members of the Darwin-based workshop, where shipping is most visible and relevant. Other suggestions for current low-cost alternatives were submarine nets, counter-UUV operations, and multi-robot UAV and uncrewed maritime systems of detection. These considerations were underscored by the fact that increasingly, uncrewed systems are needed to provide "forward-deployed, wide area, persistent presence, and […] a 'toolbox' of agile, flexible systems." [47]

Scenario 4

How will the attributes of UUVs evolve?

How will new technologies impact the development and capabilities of UUVs, e.g., autonomous UUVs, application of AI and machine learning?

Autonomous navigation: Experts anticipate that emerging AI technologies will play a significant role in both enhancing UUV capabilities and detecting UUVs. For instance, autonomous navigation will increasingly enable uncrewed maritime systems to carry out complex tasks without constant human oversight or communication with command-and-control systems. Corresponding with greater development of more efficient power systems, such as advanced batteries or fuel cells, UUVs will be able to operate for longer periods of time without needing to surface or refuel. The current limitations in this area make UUVs less reliable or useful as vehicles for payload delivery without careful planning and integration with other surface vessels. Some activities, like ISR, are more suitable to current UUV systems, but their employment as vehicles of undersea critical infrastructure sabotage is less credible.

Environmental factors: More data is needed to ensure the development of more trustworthy UUVs. Environmental challenges like ocean density, salinity, currents, and obstacles, among others, pose difficulties for UUVs. For some, these challenges were enough to make open ocean navigation for UUVs close to impossible, even in a distant future timeframe. Further platform challenges like entropy, bounded time autonomy, yawing, trim angles, and energy margins added greater complexity to UUV operating environments. Meanwhile, mission factors such as leakage threats, enemy mines, submarines, and distances to enemy underwater acoustic stations were also considered.

Platform teaming: Overcoming these challenges will require greater sophistication in autonomous capabilities, a point most experts accepted will take place in the near future. Examples of defining features include stronger sensors, such as high-resolution cameras and multibeam sonar. Additionally, as UUVs become more integrated with other systems, such as USVs, their ability to form networks of cooperative underwater robots capable of executing more complex missions will become more pronounced. Many observers are currently watching this space in the US, where platform teaming operations among different maritime systems are being tested. Meanwhile, quantum communication and high-bandwidth laser-optical communication capabilities are likely to improve communication links.

Do you feel whether there are ethical issues around the evolution of UUV using leading edge technologies?

Ethical development: Like their airborne counterparts, UUVs hold important ethical implications for both development and deployment scenarios. These can begin at the design stage and in algorithm development, focused on basic questions such as what decision an autonomous vehicle will make in the event of an imminent accident; for instance, does it avoid other vehicles, swimmers, or even marine life? The participants note that these are complex moral issues that vary by region (see Appendix C).

Black box problems: Other considerations include whether UUV development is made with explicit military value in mind or whether they are off-the-shelf variants. This has implications for the roles of AI and machine learning (ML) in the design and development stages. For instance, as private actors increasingly use AI and ML to aid developmental processes, the threat of black box problems in algorithmic explanation (where ML-generated algorithms cannot be explained by human operators) are likely to become increasingly prevalent. No international legal institution currently addresses this phenomenon, and states involved in AI and other advanced technology competition for strategic purposes are unlikely to sign up to such regulatory prohibitions.


U A S C

Autocracies vs democracies: At this point in time, such ethical conundrums are reliant on domestic state policy to incorporate ethical procedures in design and developmental phases. For democracies, ethical parameters for UUV development are more transparent and subject to greater levels of scrutiny. This is not the case for autocratic countries that view secrecy as a strategic and asymmetric advantage. Key autocratic states like China, Russia, and Iran are at the forefront of drone technologies and their development.

Open-market UUVs: The lack of international regulatory mechanisms has specific connotations for AI-enabled UUVs and similar technologies where the range of human interaction is circumscribed by mission type (referred to human on-the-loop, in-the-loop, and out-of-the-loop). Recent examples include the hypothetical scenario of a drone turning on the human decision-maker in an attempt to complete the mission.[48] For private actors looking to break into the market, black box-integrated algorithms can offer fast-track processes for UUV development and distribution. While these open-market UUVs can be sold as hobby, AI-enabled devices, their potential for misuse by malicious actors presents a range of ethical dilemmas, not just for militaries, but for developers and commercial makers of UUVs.

No integrated standards: These considerations also range across the domains of military and defence industry cooperation. Different rules of engagement exist between militaries and coast guards; experts made the point that this was most evident between Australia and the United States. Decision-making is also impacted by conceptual and linguistic challenges in operational platforms across separate military entities. This has implications for joint missions and disaster relief, but specifically also for issues like target identification. Advanced technological systems like UUVs require significant data, which in some cases may be difficult to come by and will need considerable testing regimes to address inconsistencies and errors in identification. Because there is no integrated standard on testing and training data, the employment of AI-enabled systems across national boundaries is likely to result in operational biases that may impact the safety and the security of the user.

Environmental impact: These discussions broadened further into the environmental impact of UUVs. UUVs can generate noise, potentially disrupting marine life and their habitats. One scenario considered was the employment of noisy UUVs to drive away marine wildlife from key tourist hotspots through the use of sonar booms. Other sensitive UUV deployments could include critical domains such as the Great Barrier Reef and other significant coral deposits and the introduction of damaging biological and biohazard agents. Other concerns include privacy violations that may come about due to the use of UUVs for surveillance. In all, the conclusive round-up of this topic was that humans were only beginning to touch upon some of the more important ethical considerations of UUV development, and this was being done with marginal attention paid to outcomes in real-world scenarios.

Scenario 5

What would be the repercussions if a country (such as a foreign adversary) with a base in the Solomon Islands deployed UUVs from that base?

Do you believe that this scenario is feasible and poses a risk?

Measured threat: Workshop members agreed that the scenario is feasible and poses a risk. UUVs could disrupt, deny, or degrade access to maritime shipping lanes, which could also impact Australia's maritime security indirectly or directly. For instance, the memorandum between China and Papua New Guinea in PNG's western province calls for building a $200 million "comprehensive multi-functional fishery industrial park" on Daru Island.[49] The proposed fishery is a mere five kilometres from Australia's Saibai Island or a six-hour boat ride from Thursday Island, just off the northernmost tip of Australia. Moreover, as UUVs become more advanced and capable, they could further amplify the risk posed to unsecured underwater infrastructure.

Low-threat: Others indicated that the utility of a base in the Solomon Islands, or islands of a similar distance, would be negligible in any deployment or use of UUVs for offensive purposes. One plausible scenario was that the bases could be used as logistical hubs for UUV capabilities and UMS development. For instance, a dedicated adversary could create underwater sensors for UUV and adversarial operations, but these were likely to be detected by satellite systems. Meanwhile, any base agreement between two sovereign entities will be subject to agreements which are likely to preclude such support options. Other considerations in this scenario were that UUVs could be easily transported and launched from ships closer to Australian shores. If distance is not a factor, and for some this was not considered significant, then bases as far away as 2800 kms from Australian mainland shores are likely to contribute as much strategic purpose as bases 5000 kms away.

The broader consensus on this scenario was that, operationally, UUVs did not pose a significant threat at present. As the technology for maritime systems improve, the practicalities of foreign military bases are reduced, particularly in circumstances for ISR and other operations where secrecy is paramount. Additionally, military bases can pose problems for the occupying nation as intelligence and information become increasingly available to competitor countries.

What defensive capabilities does Australia require to mitigate the potential risks in this scenario?

Maritime domain awareness: From a standpoint of policy and strategy, this scenario illustrated the need for stronger preventive measures in government diplomacy. Closer relations with Australia's neighbours would likely have helped to mitigate against emerging situations like a foreign military base being established nearby. Others underscored the need to maintain and enhance maritime domain awareness. This will allow for better detection capacity. Other capabilities include advanced training in the maritime authorities who deal with such threats. For instance, maritime GPS spoofing, masquerading as a trusted platform to alter the direction of a vessel, is an increasing threat on the seas that requires cyber capabilities to mitigate.[50] Personnel requirements will be crucial to Australian maritime security moving forward. These requirements have been recognised in various strategy documents and agreements, including the AUKUS Pact, the DSR, the Defence Strategic Update, and CSRIO's Artificial Intelligence Roadmap 2019.

International partnership: In the meantime, one consideration is for Australian authorities to enable a greater number, and more rotations, of friendly vessels stationed in Australian waters. These vessels can be allowed to conduct their operations with Australian support while also providing monitoring capabilities and training for interoperability across and among AI platforms, including UUVs.

As UUVs become more advanced (extended UUV range, integrated AI), will future risks increase based on this scenario?

More, faster, dumber UUVs: UUVs will continue to improve from their current developmental phase. The number of UUV systems and AI-integrated features will make them more difficult to detect. As current underwater gliders already have significant range, it is generally considered that they will soon be able to get to any part of the world. This scenario generally reduces the importance of near-adversary bases, such as the Solomon Islands to Australia.

The ubiquity of UUVs is also likely to become more apparent as designs and mechanics become more widely available on the open market. This means they will also become "dumber" in some respects, as they are modified by non-state and state actors to achieve limited objectives. Participants expect that ultimately they will become cheaper and faster, and that their proliferation will become more problematic. With basic knowhow, and access to online video tutorial sites like Youtube, potential malicious actors can already access open-source UUV plans for partial and in some cases complete unit creation using 3D printers.

Sensor networks: Accordingly, it is vital to invest in developing and acquiring UUVs, UAVs, and aerial platforms, and focus on building a solid network of sensors and for enhancing seabed warfare capabilities. Furthermore, educating and supporting the local workforce and establishing industries that can support the development and maintenance of these advanced defence technologies in the region will be crucial. This will, in addition, help boost the economy and enhance the country's overall security and defence readiness.

Appendix A

Summary of Literature Review

The literature review is broken down into the following areas:

a. Technology

The technological breadth of Artificial Intelligence (AI) systems in maritime security scenarios is both becoming more sophisticated and expanding. From distributed sensor networks that contribute to situational awareness systems, to Liquid Robotics Wave Gliders, the prospect that whole maritime sectors or even oceans can be digitised to create an "observable ocean" has immense implications for security. Put differently, AI-enabled underwater battlefields are no longer the subjects of fictional stories but are near-future realities.[51] In such scenarios, UUVs are already considered 'game changers' due to their comparatively lower cost outlays and their ability to cover an array of mission briefs.

In the future maritime environment, UUV technologies are likely to play an increasingly sophisticated role in sovereign defence strategies. Nations are spending significantly on advanced AI-enabled platforms to boost forward-deployed defence systems, but also increasingly as a means to fill gaps in existing and expensive systems. One current argument in US defence force acquisition challenges, for instance, is that with US undersea strike capabilities likely to reduce in the mid to long term by more than 60 percent, UUVs will increasingly be employed to replace lost systems.[52] Others highlight the emerging endurance and cost effectiveness for nations in patrolling large waterways and the ability to tie law enforcement and Defence closer in partnership, particular in addressing "low-and-no-profile drug trafficking platforms" like self-propelled semi-submersibles.[53] For countries like Australia with limited maritime security resources, UUV and associated technologies offer additional platforms for swarm-style surveillance, combining land, sea, air, and space networks to fully integrate defence systems and therefore fully "observe" maritime boundaries. [54]

The diffusion of technologies across borders has contributed to the significant rise in UUV employment. As Mathewson states, while currently up to 30 states have indigenous UUV manufacturing capabilities, there are at least up to 55 states that have either owned or currently operate UUVs. For now, UUV proliferation is based on authorised transfers between nations and global corporations, but as systems become more sophisticated, the potential for theft is likely to increase. There have already been notable examples of such incidences, such as Chinese military personnel hijacking US scientific UUVs in the South China Sea.[55] Maritime piracy is likely to further exacerbate UUV technology transfer for misuse and even disaster.

A concomitant challenge with the growing diffusion of UUVs and USVs is the development of anti-drone solutions to deal with UMS threat scenarios. In the UAV domain, counter-drone strategies include Radio Frequency jamming, thermal detection, radar-based detection, camera detection, and multi-drone defensibility systems. While some of these options are open to UUV scenarios, underwater counter-UUV solutions will require greater reliance on a range of sensors, acoustic sonar systems, and undersea energy and communications infrastructure. As one report has noted, "the state of the current technology, the complexity of antisubmarine warfare, and the sheer scale and physics-based challenges of undersea sensing and communications all suggest these systems have a long way to go." [56]

Examples of counter drone and deterrence systems like the US Navy's "Force Protection Advanced Technology" project illustrate that such systems are at the cutting edge of underwater technologies and as such are generally limited to only one or two large global actors.[57] For the United States, these advanced countermeasures are being designed with endurance for force multiplication in anti-access/area denial (A2/AD) environments, such as in the South China Sea, meaning their employment may include partnership with like-minded actors. However, interoperability creates its own set of challenges in communication with undersea systems that already don't communicate well and in the absence of common standards and protocols.

Meanwhile, marine uncrewed cooperative systems that can operate independently with intelligence are still limited by software and hardware challenges. According to Bae and Hong, while countries are pursuing multi-robot and swarm systems, without functionable communications systems, the devices and effects are going to remain unstable.[58] This is one of the key challenges UUV development currently faces.

b. Threat environment

The threat to global stability posed by Russia's invasion of Ukraine, and the subsequent risks of nuclear warfare, has alarmed many capitals around the world. In East Asia and, more broadly, the Indo-Pacific, the largest peacetime build-up of military, and specifically naval, forces in China have forced affected countries in the region to adopt stronger defence postures with a focus on addressing capability shortfalls in conventional systems. Countries like Japan, South Korea, the United States, Australia, Vietnam, and the Philippines have all increased military spending to meet the challenge of an increasingly assertive China with ambitions to invade Taiwan, control the South China Sea (SCS), and dictate norms of international peace and behaviour. [59]

The need for innovative solutions to address significant gaps in forward defence has increased the importance of distributed maritime systems. These systems rely on AI-enabled autonomous vehicles and sensors for integration and threat detection. UUVs, therefore, are likely to become more integral to navies, which are required to cover vast expanses of ocean for detection, deterrence, and ISR. One argument goes so far as to suggest that the high endurance and cost-benefit characteristics of UUVs for deep water missions have changed the paradigm of sea operations.[60] Put differently, as the costs of small and relatively cheaper UUV capabilities and integrated seabed and surface detection networks erode the effectiveness of expensive legacy vessels, like air craft carriers, the traditional operational and tactical concepts of the Navy will become obsolete in their current doctrinal use. Other uses of UUVs in swarm scenarios are projected to offer distributed sensor networks covering vast areas and various depths undersea, with implications for escort support, CMC, and underwater communications.[61] Others examining the changing circumstances of Anti-Submarine Warfare (ASW) are looking to advanced uncrewed maritime systems to pick up capability shortfalls in crewed submarines. [62]

This rethinking of the concepts of seabed warfare and the notions of thresholds in emerging conflict environments has already begun to take place in regional defence strategies. For states like the United States and Russia, these environments are much more integrated into existing naval policies and doctrine, providing an existing basis for advancing seabed warfare capabilities. For instance, the US's acoustic detection network of passive hydrophones, SOSUS (Sound Surveillance System), has existed since the Cold War, but has undergone recent changes to improve detection with multibeam echosounders, with a range of surface and sub-surface systems. SOSUS was renamed as Integrated Undersea Surveillance System (IUSS) to incorporate a range of UUVs with autonomous capabilities, including improved Advanced Undersea Warfare Systems to rapidly project force. With the help of DARPA, these forces include building UUV endurance, communications, and data transfer abilities through fixed submarine stations, referred to as Forward-Deployed Energy and Communications Outposts.

Nations like China are also catching up. Beijing's development of a submarine detection network project, entitled "Underwater Great Wall" in the domains of its maritime claims, is likely to project undersea A2/AD, making it difficult for foreign navies to operate in international waters like the South China Sea.[63] This element of China's maritime domain awareness has been considered a sore point in its maritime defence strategy, particularly given more recent tensions between the US and China vis-à-vis Taiwan, and enhanced minilateral capability building in groups such as AUKUS and the Quadrilateral Security Dialogue.[64] Expectations are that further development of its distributed tactical surveillance capabilities will contribute to real-time location and tracing of maritime vehicles in the SCS.

Meanwhile, the recent activities of Russia's Navy throughout the Atlantic but also the North and Baltic seas have drawn attention to efforts by the Kremlin to actively map allied critical infrastructure on land and the seabed. NATO countries have responded by stepping up patrols in the seas and creating the Critical Undersea Infrastructure Protection Cell to guard against attacks to underwater cables, seabed energy networks, and maritime trade disruption. According to NATO's chief of intelligence, David Cattler, Russia is looking to punish Western nations for supporting Ukraine by targeting undersea cables. As the backbone of the global economic and financial system, cable sabotage could cause financial and economic losses in the trillions, and contribute to delays and denial of services as broad as logistics and transport, business operations, internet security, and communications.[65]

Other attempts to mitigate these emerging threats include NATO's adoption of a Maritime Unmanned Systems Innovation Advisory Board and recent

reports addressing the protection of critical maritime infrastructure by NATO [66] and the EU. [67] These reports highlight the role grey zone activities can play in underwater domains. As Levick states, "the opaqueness of water is perfectly suited to 'hybrid' strategies that use plausible deniability as a modus operandi." [68] Attacks on underwater cables offer an asymmetric advantage for nations willing to exploit such vulnerabilities, making these cables prime targets for sabotage. The recent publication of France's Undersea Warfare Strategy highlights:

"an attack on the underwater part of submarine cables is a potential course of action, with possibilities ranging from a convenient 'accident' in a coastal area, to deliberate military action. In this regard, the intrinsic features of the seabed make it the ideal theatre for non-attributable actions in 'grey zones'." [69]

Because there is "practically no risk" of casualties in this form of warfare, the ability to control the level of escalation in response to such attacks has diminished. The highly roboticized theatre of underwater operations, along with the opacity of the seabed, "carries the risk of unrestrained actions being undertaken by automated systems that are difficult to control due to the nature of the environment." [70]

One weapon that is likely to escalate the conflict of seabed operations quickly is mines. Underwater mines have an outsized influence not only because are they cheap, easy to stockpile, and require no further human labour costs (as set-and-forget weapons), they strongly appeal to under-served militaries looking to create asymmetric impact with A2/AD measures. As Alia Huberman argues, "the cost of a man-out-of-the-loop mine is[…]significantly lower compared with the cost of a manned platform." For interdiction or blockade operations, they are perfect weapons. But as others note, they can also be placed in important sea lanes for disrupting and even paralysing critical trade for some nations. With AI-enabled capabilities for manoeuvrability, smart mines can evade MCM vessels, making them more difficult to control. "Some high-tech capabilities," one report notes, "include clusters of autonomous weapons that lay on the ocean floor until activated, which can then become 'movable mine fields' that are difficult to notice until after damage has occurred." [71]

Despite these dangers, Australian Defence policy-makers have been caught under-prepared as a result of several structural factors, writes Huberman. These include force structure commitments and legacy platforms that outcompete the less 'sexier' mine programs for interest; budgetary decline; and collective amnesia on the impact of mines to surface vessels. The coming resurgence of mine warfare is also likely to exacerbate existing shortfalls in Western MCM capabilities and also because the costs and time commitment for detecting and then countering mines is prohibitive. [72]

A final factor of the emerging threat environment for UUVs and associated technologies is their potential for criminal employment. Criminal uses have included drug smuggling, privacy breaches, blade smuggling, and hacking. Additionally, their potential for terrorist employment in uses such as surveillance, suicidal missions, cyber attacks, and dissemination of propaganda are easily encouraged, given their relative unsophistication and the widespread availability of UUV information on the Internet. As Yaacoub et al. demonstrate further, the global reaction in this area so far has been focused on privacy and general population security concerns, leaving gaps in international regulation as to how to address terrorism and emerging technologies. [73]

Meanwhile, the availability of UUV technology on the open market and the diminishing costs associated with their manufacture have marked their rise as a problematic development for maritime security authorities.[74] The market for UUV systems is currently limited to small submersibles with restricted capacities, though mining sector operators have access to larger and more sophisticated vehicles. Others observe that as detailed UUV plans become more open to market 3D printing, they will increasingly be available, and with greater variability, for adoption in criminal activities. [75]

c. Operational and cyber considerations

There are at least 40 distinct missions that can be performed by UUVs, from Intelligence, Surveillance, and Reconnaissance (ISR), Mine Countermeasures (MCM), Anti-Submarine Warfare (ASW), and payload delivery, to information operations and time critical strikes.[76] However, operational levels currently vary depending on mission criteria. Moving into the more sophisticated uses of UUVs will depend on vehicle sizes, battery capability, levels of autonomy, and sensor capability. At contemporary war fighting needs, and in the near-to-medium terms, however,

key arguments suggest that UUV capabilities are best matched with MCM missions and enhancing maritime domain awareness.[77] For Australia, these platforms are already being advanced on USVs like the Ocius Bluebottle and Defence's Stinger variant, which includes a towed-array sonar submarine detection platform. But UUV capabilities are lacking.

Much of Australia's maritime environment remains "completely unsurveilled, most of the time," according to one account. This means that endurance platforms will need to move beyond current UAV capabilities, like the MQ-4C Triton with a maximum flying time of 24 hours. Emerging maritime domain awareness systems will require a combination of UMVs and UUVs with stronger battery life-cycles and system of systems integration. Future projections of Large Displacement-UUV independent operations are expected to range into months and years and contribute to detection capabilities.[78] For now, Australia's UUV capabilities are troubled by the vast operational environment of its maritime boundaries.[79]

Going forward, UUVs are likely to be more cost-effective solutions for what are now surface vessel and aircraft environments. Scientific mapping and hydrographic reconnaissance by traditional naval vessels have been difficult and time consuming. However, as early as 2003, these operations were being performed across oceans by the US Navy's Remus UUVs with considerable success. Later operations, including the search for the missing aircraft Air France flight AF447, underscored the ability of even semi-"smart" UUVs to advance ISR capabilities.[80] With barely 20 percent of ocean topography accurately measured, and current seabed precision mapping at 2 percent, there is great potential for UUV employment. [81]

In the cyber domains, UMVs networks are susceptible to various cyber attacks in both their software and hardware components. For lower-end units, open source and cross platform communication protocols are exposed to Denial of Service (DoS) and Distributed Denial of Service (DDoS), message forgery, spoofing, and man-in-the-middle attacks. Due to the communication requirement for cyber operations, USVs are more likely to be targets or carriers for cyber attacks in software components than UUVs. Once surfaced, however, UUVs will be subject to similar vulnerabilities, depending on how long they remain on the surface.

Physical cybersecurity issues are also relevant. Devices, if captured, can be tampered with. Concentrated attacks on software infrastructure can consume battery power to critical levels.[82] Acoustic attacks can generate sounds to target frequency settings, affecting position control algorithms. Cyber vulnerabilities are likely to affect commercial variants of UUVs more notably than military-grade devices. However, skilled hackers can still penetrate more secure cyber systems, and such examples have been witnessed among US Sentinel spy UAVs. [83]

While cyber attacks upon Cyber Physical Systems (CPS), such as UUVs and UAVs, may still be complex and difficult operations, defending against them is considered generally more challenging than for conventional cyber systems. One reason for this is that UUVs are made up of multiple independent systems (systems of systems) that are often off-the-shelf components sourced from multiple and diverse vendors.[84] UUVs in some cases require real-time control or command and control transmissions, meanwhile, that are susceptible to corruption, often via wireless links that can take advantage of unsecured networks or low-end encryption via inexpensive data sniffers. Militaries are likely to employ more sophisticated advanced encryption standards with 128- or 256-bit keys or have expertise to address on-time confidentiality challenges. Law enforcement agencies such as Coast Guard and Border Control units are likely to suffer more in these areas.

The literature on the cyber capabilities and vulnerabilities of UUVs demonstrates that critical research in these areas is lacking. Confidentiality and integrity threat analyses have mostly occurred on UAV devices for the reason that these technologies have been around longer and therefore have more data to go on. That being said, confidentiality threats such as UUV capture are likely to be more commonplace in the future, with implications for sensitive information compromise (see also Appendix C).[85] Integrity threats, by contrast, are likely to be more difficult given that communication is much less transmissible, meaning the chances of data corruption are much lower. These can include man-in-the-middle attacks, malfunctioning or jamming of the device leading to crashes, or hijacking by taking over command and control links. As these threats illustrate, the distinct methods of UUVs and cyber warfare are likely to move states on from past modes of traditional warfare to hybrid or grey zone approaches, where casualties are few but costs are high. [86]

d. UUV policy and ethical implications

Policy around UUV development and deployment in, and threats to, Australia is outlined in the 2016 Defence White Paper (DWP), the 2020 Defence Strategic Update (DSU) and the more recent Defence Strategic Review (DSR). The Defence White Paper outlines the first two strategic defence interests as the protection of Australian sovereign territories and the securing of SLOCs in Southeast Asia and the South Pacific. At this time, focus was concentrated on Army, Air Force, and logistical systems with force integration programming. Maritime and ASW capabilities were to receive 25 percent of spending across 10-year investment capabilities streams to 2025-26, but as far as these included UUVs, the white paper remained vague. Its commitment at the time to new patrol boats, submarine acquisition, and other large surface vessels did not include integration platforms for crewed and uncrewed vehicles. [87]

The 2020 Defence Strategic Update dismantled assumptions about new capabilities acquisitions that had been used by previous governments to push back against spending on new platforms. According to the DSU, changes in the geopolitical environment had forced Australian defence planners to consider new force structure priorities, with a focus on "the protection of a geostrategic ecosystem" and deterring revisionist powers in the grey zone domain. More space in the budget was delivered to maritime defence, with a new focus on "smart mines" with the capability to move into adversary harbours, if need be. As James Goldrick argued, there was a recognition of the potential for undersea weapons and systems that has long been overdue.[88] Meanwhile, the future Defence innovation program included continued funding for the Next Generation Technologies Fund and the Defence Innovation Hub, although what technologies these would fund was left unclear. The corresponding strategy report for More, Together: Defence Science and Technology Strategy 2030 outlined spending themes for advanced technologies but did little more to highlight what technologies it was focused on or what was required. [89]

While the Navy strategy Plan Pelorus 2022 did not deviate from the ongoing focus on surface combat systems for the Navy, the Mercator Maritime Domain Strategy 2040 for the first time highlighted the significance of undersea systems, with a focus on UUV integration into naval platforms. This translated into new Navy capacities with lethal capabilities and a program for "evergreening" (continuous capability development) systems to improve supply-chain resilience, increase sovereign industrial capability and capacity, and increase the breadth and depth of partnerships and alliances. [90]

Meanwhile, the development of the AUKUS partnership between Australia, the United Kingdom, and the United States has directed new purpose to underwater defence systems with stronger roles for integrated approaches with crewed and autonomous teaming programs. The AUKUS nuclear-powered submarine pathway will deliver Australia a world-class capability that will see it become one of only seven countries that operate nuclear-powered submarines. The pathway is proposed to strengthen the combined industrial capacity of the three AUKUS partners, with increased cooperation making trilateral supply chains more robust and resilient.[91] AUKUS Pillar II highlights force acquisition and development of technologically advanced systems with "additional undersea capabilities" in collaboration with the submarine focus of Pillar I. This is based on the recognition, writes Davis, that more than nuclear submarines will be necessary to protect maritime zones or win undersea warfare battles.[92] Already, discussions of systems of systems, such as between SSNs, networked sensors, and UUVs, are illustrating the wide-ranging potential for UUVs in undersea applications.

However, the huge cost outlays of Pillar I are considered so monumental that application for the development of other advanced underwater systems is simply unrealistic. According to Ryan, at AU$11 billion per year, the focus on SSNs will not only reshape Australia's defence planning and architecture, but also crowd out other platforms by absorbing "every spare dollar." [93] At this point in time, the literature shows little engagement with such financial challenges. While some such as Davis believe both pillars can and should be achieved, "and at a relatively fast pace," others are much more ambivalent.[94] This is particularly the case for Ryan, since answers to clear questions about the utility and even survivability of nuclear submarines cannot be guaranteed given the highly uncertain capabilities of new detection technologies and the new generations of autonomous underwater vessels likely to be produced in the coming years. [95]

Such considerations bring in to question the future of current naval strategy documents, such as the 2020 Robotics, Autonomous Systems and Artificial Intelligence (RAS-AI) 2040 strategy. RAS-AI very

clearly outlines that UMS will be developed and employed to enhance and integrate crewed platforms such as submarines and surface vessels. Two further distinctions highlight that RAS-AI anticipates an advanced UMS building capacity to "pursue disruptive RAS-AI technologies that have the potential to be 'game changing'." The second aspect to this is that it does not envisage purchasing military off-the-shelf technologies, but it is unclear in current funding documents what capacity such systems will require in investment. According to Parker et al., "although Defence has raised the share of its procurement sourced domestically from about 45% to 55% over the past five years, it's possible that the pressure to acquire new capabilities quickly will result in more 'off-the-shelf' imports." [96]

Already, there are some troubling aspects, as mentioned by Ryan, that spending themes will reduce the ability to implement RAS-AI over time. Because such AI systems will require significant machine learning capability, and associated computational power, the Navy will require new skills and competencies, and a future workforce that can sustain not only the requirements of AUKUS Pillar I, but also the AI components of UUV and broader UMSs.[97] The mission plan for building these capacities will undergo review in 2024, at which point the outcomes of the March 2023 Defence Strategic Review will become clearer.

To incorporate the AUKUS platforms, but also include new challenges to regional security illustrated in the wake of Russia's invasion of Ukraine, the DSR sets to reprioritise defence spending, force posture, and structure for the foreseeable future. This agenda was configured around six priority areas for immediate action: acquisition of nuclear-powered submarines through AUKUS to improve deterrence capabilities; developing ADF's ability to precisely strike targets at longer-range and manufacture munitions in Australia; improving the ADF's ability to operate from Australia's northern bases; initiatives to improve the growth and retention of a highly skilled Defence workforce; lifting their capacity to rapidly translate disruptive new technologies into ADF capability, in close partnership with Australian industry; and deepening of their diplomatic and defence partnerships with key partners in the Indo-Pacific. [98]

As with the notable challenges to RAS-AI, the DSR's ambitious agenda is likely to face certain trade-offs with implications touching on maritime UUV and defence capabilities. As researchers from the Australian Strategic Policy Institute have found,

significant divergencies between the 2023 military budget, naval strategy, and the DSR exist and are likely to put on hold at least some of the priority areas earmarked for "immediate action." The difficult macroeconomic environment, for instance, has reduced the value of the budget, meaning spending on defence has actually regressed, despite the unprecedented demands of Defence. Meanwhile, long-held plans to boost ADF personnel have been continuously dogged by low recruitment numbers. For year 2022-2023, defence planners sought to raise numbers by 2,201 "but instead faced a contraction in size by 1,389 uniformed personnel." [99]

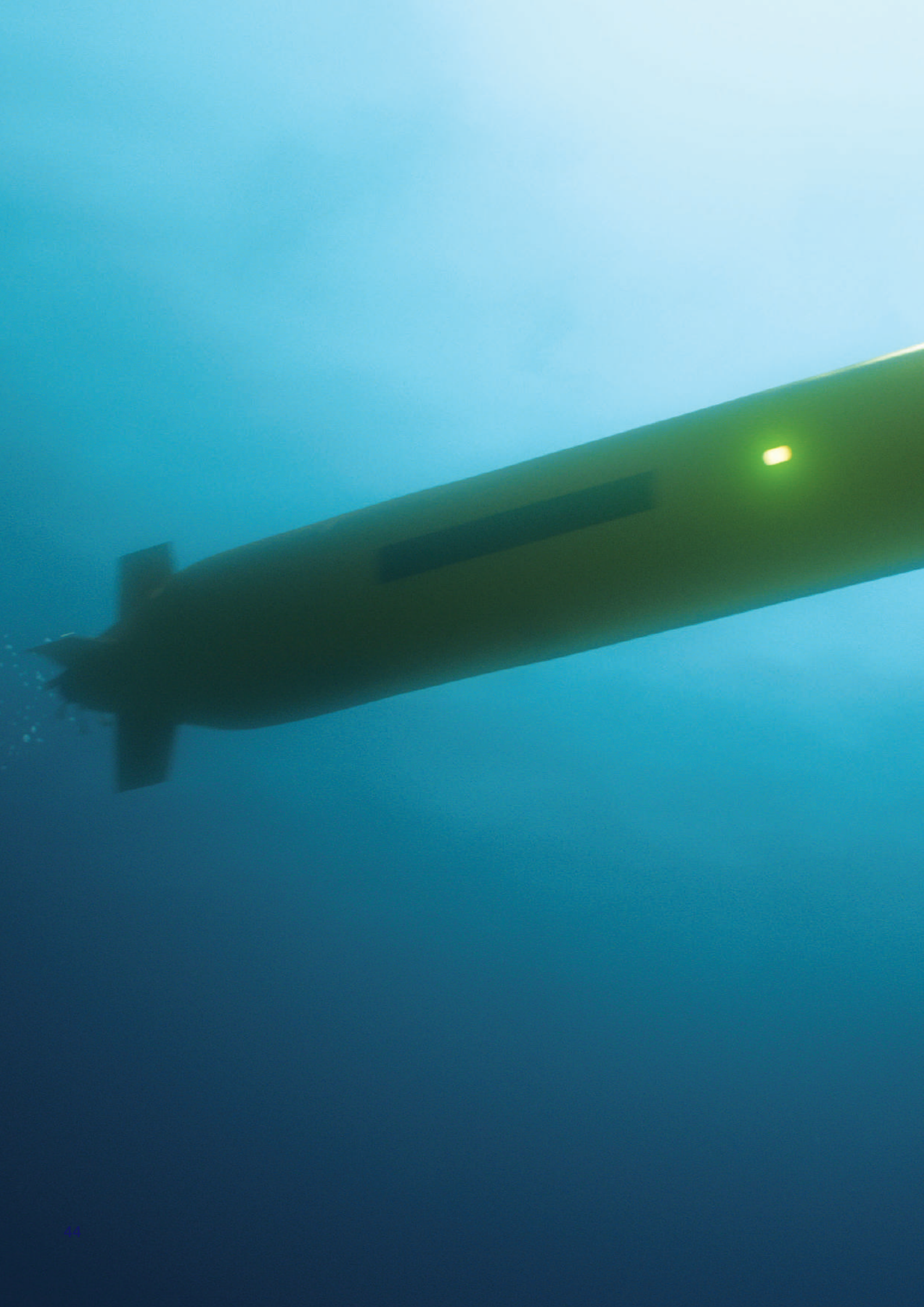
As the funding capabilities become clearer, the trends for underwater defence and maritime domain awareness are set to improve. The DSR includes AU$19 billion worth of investments across the six priority areas. While Pillar I AUKUS submarines provide for the highest cost outlays, the Innovation Accelerator and AUKUS advanced capabilities (Pillar 2) have also received significant focus, with prioritisation, for instance, over the People Retention Initiative. 2024 will likely provide more information as several reviews are due with respect to surface combatant fleet structure, defence infrastructure and estate management, defence industry policy, RAS-AI, and national fuel storage. According to Parker et al., the National Defence Strategy is anticipated to generate more significant movements in the maritime domain, particularly in relation to surface ships and uncrewed and undersea warfare capabilities." [100]

The final concern in the policy space is ethical considerations of UUV development and employment. The literature on AI-enabled systems and robots is well established, covering topics of privacy, manipulation, human-robot interaction, AI moral agency, bias, black box issues in machine learning, and super intelligent systems leading to "singularity" (the point at which robots become uncontrollable).[101] Within these fields, autonomous weapons systems (AWS) have been used to define the category of emerging AI-enable vehicles across UAV, USV, and UUV domains. For the reason that UAV technologies have been employed longer, and with specific experience in combat scenarios, much of the literature has focused on these technologies. However, it is considered that many of the ethical considerations overlap.

Autonomous systems hold important considerations for combat situations where laws of war are relevant (see Appendix C for more discussion on this). UUVs with humans "in" or "on" the loop disrupt the meaningful chains of responsibility. Examples of war crimes perpetrated by UUVs and similar autonomous systems in war zones are likely to become less hypothetical as their use becomes more commonly applied in national defence strategies. In Ukraine, the current war has produced numerous examples of autonomous loitering munitions, such as the US Switchblade and Phoenix Ghost and the Russian Lancet, which can linger in a kill zone until they come in contact with a target.[102] Meanwhile, innovations in GPS and control signal jammers that are used to compromise remote control piloting are creating the space for more AI-enabled features of celestial navigation and simultaneous location and crewing, further removing humans from the loop.

There are several implications for ethics across autonomous systems, including UUVs. The first is the cheapening effect of AWS in warfare conditions. Small but deadly UAVs are orders of magnitude cheaper to produce than traditional combats systems like fighter jets, attack helicopters, and tanks, yet they can produce similar tactical and even strategic advantages. Swarming UAVs, for instance, can overwhelm expensive missile defence systems or be used as psychological weapons against enemy troops or civilians. Because it is much more expensive to intercept loitering munitions or swarmed UAVs, they are likely to erode capabilities much faster. These considerations will play into decisions made to end war earlier through psychological as well as physical devastation of civilian populations, if ending wars earlier is viewed as a means of saving more lives in the long run. Russia's deployment of suicide UAVs on civilian populations illustrates that wartime decision-making continues to employ such rationales.

But autonomous weapons also tend to "absolve humans of any responsibility for life-and-death decisions," encouraging their further employment.[103] The question of accountability in the event that non-combatants are killed cannot be satisfactorily answered. As Regan Ho states, is the programmer who wrote the code the accountable one? The AWS itself? Or the commander who employed its use? Until such legal grey areas are resolved, the answer for Ho is that autonomous systems must be limited in their use.[104] Other discussions examining the positive moral cases for AWS employment see fewer dilemmas. Autonomous systems are likely to reduce the psychological, physical, and moral risk of soldiers. Additionally, the ability to develop advanced technologies is likely to lead to the more non-lethal means of waging war, substantially reducing casualties on both sides.[105]



Appendix B

Australia and the threat of Uncrewed Underwater Vehicles – A North Australia Perspective

Introduction

The geographical location of North Australia and its proximity to other continents, combined with the extent of the coastline (~11,000 km) and a very low and sparse population (less than 350,000 people), make this area significantly vulnerable to foreign interference. The region has a low-skilled workforce and limited transport infrastructure, and due to high seasonal rainfall, much of the coastline is inaccessible for half the year. Therefore, the risks and potential impacts of Uncrewed Underwater Vehicles (UUVs) may differ from the southern and eastern coastlines and must be regarded within a North Australia context.

A major consideration with UUVs that changes the type of risk for North Australia over that of crewed submarines is that they can be deployed en masse and remain dormant and on point for prolonged periods, even years. Then, when required, they have the potential to simultaneously strike multiple targets through either cyber or physical attacks, overwhelming defences, and maximising disruption. The vastness and sparse population of Australia's northern coastline make it particularly vulnerable to this type of interference, where foreign UUVs could operate for long periods with little oversight.

Impacts on North Australian trade, shipping, and critical infrastructure could also arise from UUVs unintentionally. The incorrect usage, malfunction or stranding of UUVs pose collision and obstruction risks. This could cause expensive damage and delays, or even loss of life.

On the positive side, there is a relatively low abundance of Australia's critical infrastructure located in northern Australia, compared to the southern and eastern Australian coastlines. However, major energy projects, submarine cables, commercial shipping routes, and military bases are located across northern Australia, and could be potential targets for foreign entities. Further, both Federal and Jurisdictional governments are undertaking significant investments and have plans to develop the economy, infrastructure, military presence, and human populations across the north. This report considers these future developments in the perspective of foreign interference through the use of UUVs.

How may UUVs impact North Australia Trade?

The north Australian coastline is situated close to Indonesia and a number of ports of national significance are distributed across the north of Australia (Figure 1).

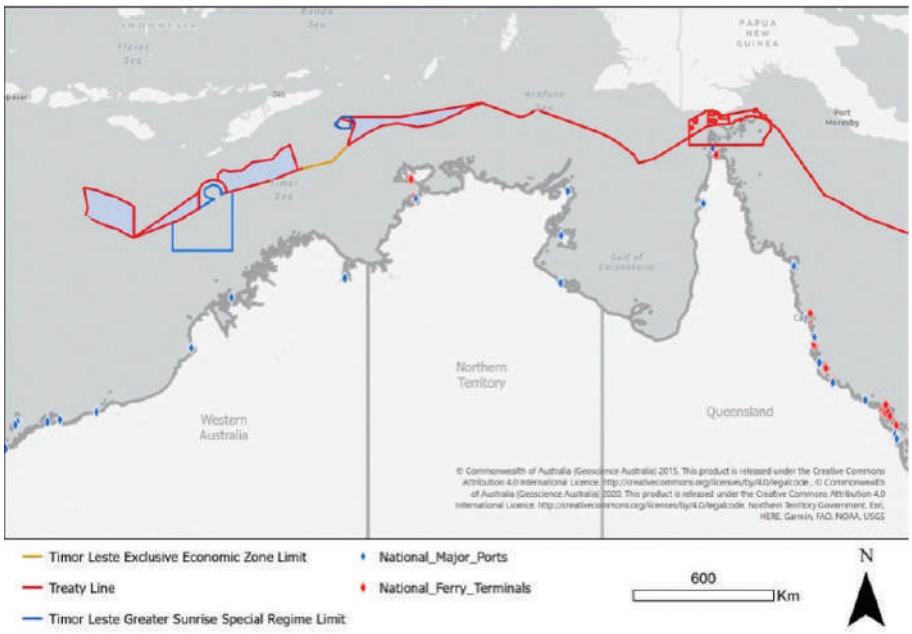


Figure 1. Australia's northern border and locations of national ports and ferry terminals. Data derived from Geoscience Australia (2015).

There are several commercial shipping routes across Northern Australia that serve various industries and markets (Figure 2). These are:

- The Great Northern Shipping Route, which starts from Fremantle in Western Australia and continues along the coast of Western Australia, Northern Territory, and Queensland, serving ports such as Darwin, Broome, Dampier, Port Hedland, Gladstone, Townsville, and Cairns;
- The Pacific Islands Northern Shipping Route, which starts from Townsville and serves the Pacific Islands nations such as Papua New Guinea, Solomon Islands, and Fiji;
- The Kimberley Western Australia Shipping Service, which originates in Broome and serves the remote coastal communities in the Kimberley region of Western Australia, including Dampier Peninsula, Yulmbu, and others;
- The Torres Strait Shipping Service/Island Trader Service, which operates between Thursday Island and Seisia in the Torres Strait, serving around 14 indigenous communities along the way; and,
- The Northern Territory–Timor-Leste-Papua New Guinea Service, which starts from Darwin and connects Timor-Leste and Papua New Guinea to Northern Australia.

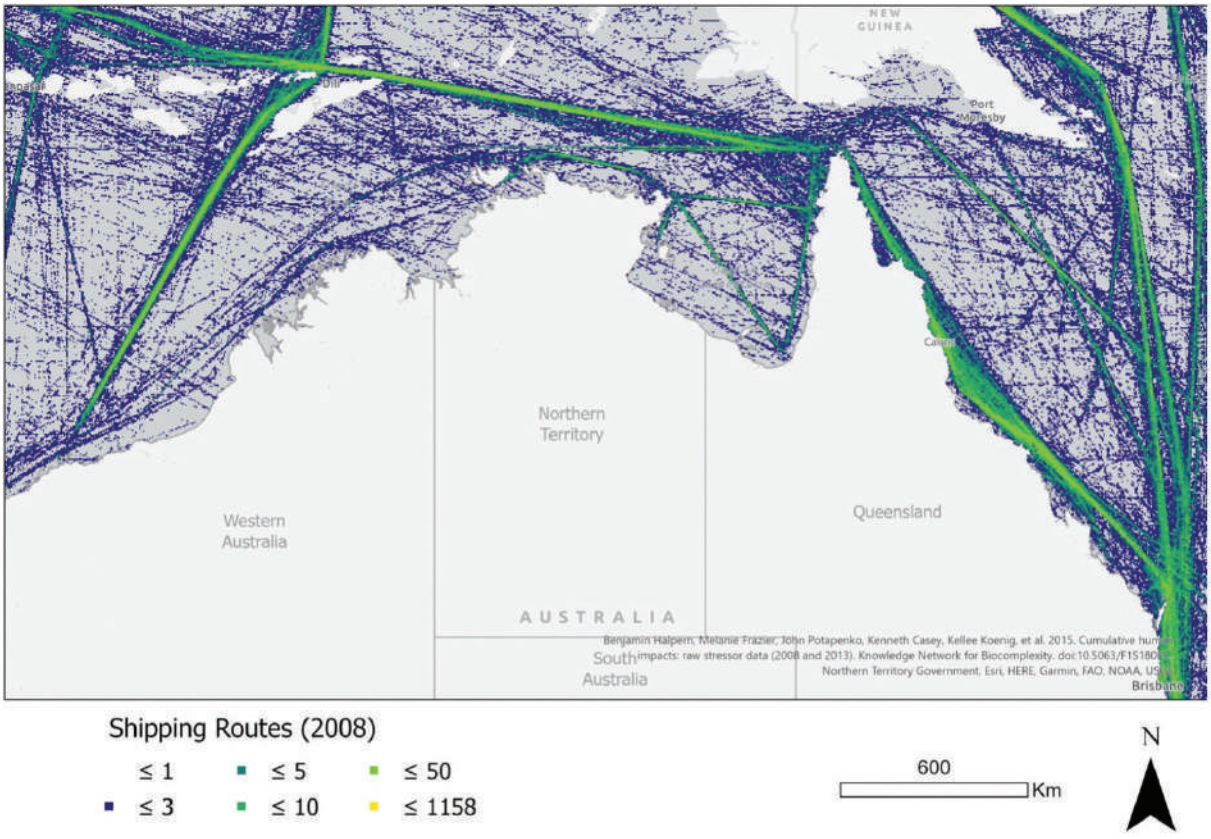


Figure 2. The volume of shipping traffic across north Australia recorded in 2008. Data derived from NCEAS. [106]

These shipping routes cater to different types of cargo, industries, and economic purposes, including mining, oil and gas, agriculture, tourism, and general cargo – all of which could be impacted by intentional or unintended interference by UUVs. This could be through various mechanisms including:

- Collision Risk;
- Obstruction of Shipping Lanes;
- Interference with Underwater Infrastructure; and
- Security and Surveillance Issues.

The Torres Strait is particularly vulnerable to foreign interference due to its proximity to Australia's northern border. On average, 8000 commercial vessels pass through the Strait annually, carrying approximately 40 million gross registered tonnes of cargo, and is the main route between the Pacific and Indian Oceans. The Strait would be an optimal target for both surveillance and interference by UUVs, and is less than 150 kilometres wide at its narrowest point, with commercial-shipping-confined lanes limited to a few deep channels. Even a proposed threat of collision by UUVs could close shipping through the Torres Strait, requiring vessels to make significant detours to reach home ports, and resulting in significant financial cost to Australia.

How may UUVs impact the North Australia Critical infrastructure?

The North Australia Coastline from Port Hedland in the West to Townsville in the East (11,000 km) contains seven urban centres with populations greater than 10,000 people. These are Darwin (154,000), Cairns (153,800), Geraldton (40,000), Karratha (22,000), Port Hedland (14,000), and Broome (15,000).

Darwin is the capital city of the Northern Territory and is where the parliament and administrative oversight are located. Darwin Harbour is a major port for both commercial and naval shipping. The harbour mouth is only 1.6 km wide and presents a bottleneck where UUVs could sit for prolonged periods for intelligence gathering, or present obstruction and collision risk.

Despite the low population, there is considerable critical energy infrastructure across the north of Australia (Figure 3). Major gas and oil fields located across the north include:

- North West Shelf Gas Field: located off the Western Australian coast, the field has estimated total reserves of around 56 trillion cubic feet (Tcf) of gas and over 5 billion barrels of crude oil (bbl);
- Bayu-Undan Gas Field: located in the Timor Sea about 500km northwest of Darwin, it has estimated resources of around 400 billion cubic metres (bcm) of raw gas and 148 million bbl;
- Ichthys Gas Field: located approximately 220km offshore Western Australia, it's estimated to hold recoverable resources of around 12.8Tcf of natural gas and 547 million bbl;
- Greater Enfield Oil Project: located in the Northwest Shelf area and offshore about 60km to the west of Exmouth, Western Australia, it contains around 69 million bbl;
- Darwin Gas Project: located offshore from Darwin, it has estimated reserves of 6.12 Tcf of gas and over 50 million bbl.

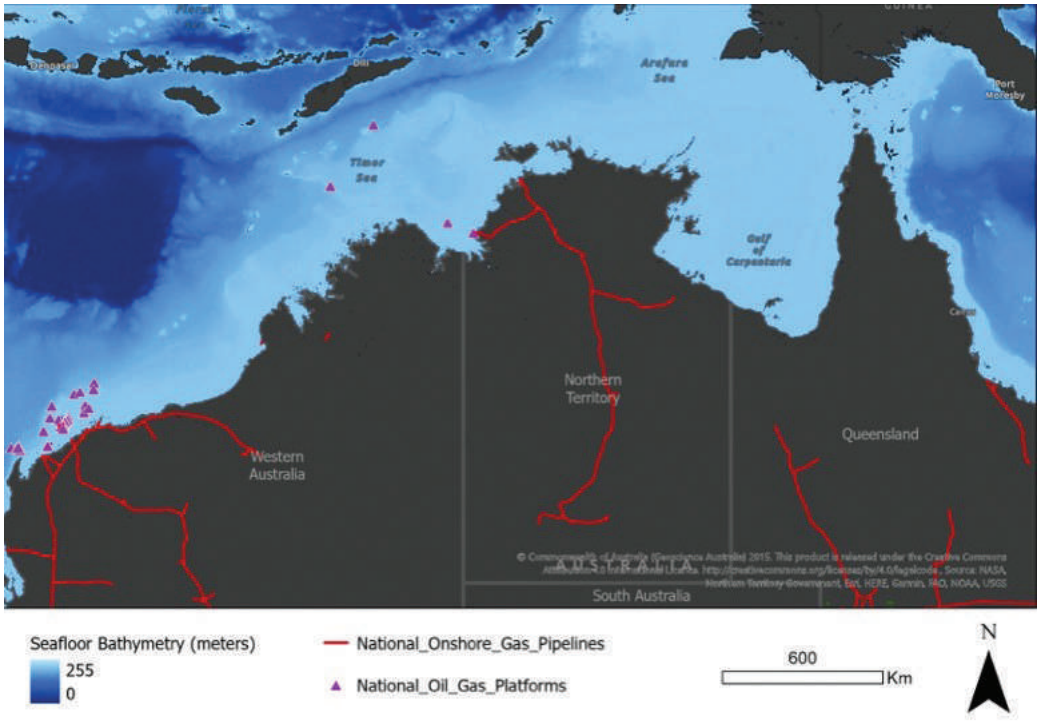


Figure 3. National onshore gas pipelines and off-shore oil and gas platforms across north Australia. Oil and Gas infrastructure data derived from GeoScience Australia and Bathymetry from Marine Constitution Institute.[107]

All these facilities and associated infrastructure could be at risk from UUVs by the means (cyber and physical) listed in this document, resulting in significant economic loss, and even loss of human life. The shallow bathymetry of this area, all the way to Indonesia and PNG (Figure 3), would make it easier for UUVs to navigate across the ocean floor.

Of particular risk is the Impex Ichthys Facility in Darwin. Although it is challenging to find exact figures, it is estimated that around 15 percent of Japan's total energy imports come from the Darwin Ichthys facility, all of which needs to travel through the narrow mouth of Darwin Harbour.

Future energy projects, such as Sun Cable, which proposes to send power generated by solar via submarine cable from Darwin to Jakarta and Singapore, could also be at risk from UUV interference, and this threat needs to be accounted for in project development.

Submarine communication cables are another area where interference by UUVs could generate significant risk to the north. There are several submarine cables that come ashore in the north of Australia, providing important telecommunication connections to remote communities, and supporting global connectivity. The main submarine cables that come ashore across North Australia include:

1.

APCN-2: The Asia-Pacific Cable Network 2 is a submarine cable network that links Singapore, Indonesia, the Philippines, Vietnam, Hong Kong, Japan, Taiwan, South Korea, Guam, Hawaii, Australia, and the United States. The cable lands in the Northern Territory near the city of Darwin;

2.

SEA-US: The South-East Asia-United States Cable System is a submarine cable that connects Indonesia, the Philippines, Guam, Hawaii, and the United States. It lands in Australia at both Jomunga on the Pilbara coast of Western Australia;

3.

PPC-1: The Pacific Papua New Guinea International Cable links Port Moresby in Papua New Guinea with Sydney, Australia. The landing station in Australia is located on the north-eastern coast of Queensland;

4.

North West Cable System: The recently established North West Cable System links Port Hedland in Western Australia with Darwin through an interconnected landing station at the towns of Onslow and Wickham.

How may UUVs impact North Australia Defence infrastructure?

Northern Australia hosts several defence force bases that support the ADF's operations in the region. These include Robertson Barracks, which houses most of the army's combat units; Tindal RAAF Base, which operates F-35 fighter jets and radar systems; RAAF Base Curtin, which provides surveillance and reconnaissance capabilities; and Lavarack Barracks, which is the army's largest base and training centre. These bases may face risks from UUVs, such as collisions with naval vessels or cybersecurity attacks.

Military bases serve as critical infrastructure and complexes that are essential to national defence operations. It is challenging to understand if UUVs pose a specific risk to these bases over other factors. They may cause obstruction and collision risks with naval ships arriving and departing military basis, and may increase the threat of cybersecurity attacks, by the increased proximity of the hack.

The HMAS Coonawarra, RAN's primary base facility in northern Australia, is located in the city of Darwin and is at most risk of UUV threats. With facilities for accommodating navy personnel and operational support, the HMAS Coonawarra operations included naval patrols, vessel maintenance, and surveillance missions. As of 2021, the base had around 400 defence personnel from Australia, New Zealand, and the United States.

Appendix C

Legal Implications of Autonomous Uncrewed Underwater Vehicles

What are UUVs from a legal standpoint?

The following provides a brief overview of how autonomous UUVs are regulated as vessels under the key maritime laws administered by AMSA, including the availability of exemptions and the recently announced Reefworks Regulatory Sandbox. It will conclude by noting how the definition "defence vessel" creates a challenge for entities other than the Australian Defence Force (ADF) to develop UUVs for the Department of Defence.

Australian law (including maritime) attitudes to UUVs

AMSA and the regulation of the maritime environment

AMSA is the national maritime safety regulator, responsible for regulating commercial vessels operating in Australia's maritime environments. AMSA regulates both Australian and foreign vessels operating in Australian waters[108] in addition to its responsibilities for maritime safety, protection of the marine environment, and search and rescue.

AMSA regulates the maritime environment through two main pieces of legislation:

1. The *Navigation Act 2012* (cth); and
2. The *Marine Safety (Domestic Commercial Vessel) National Law Act 2012* (cth) (the 'National Law 2012').

AMSA also has the power to make *Marine Orders* under the *National Law Act 2012*.

The *Navigation Act 2012*

The *Navigation Act 2012* gives effect to the maritime international treaties and conventions that Australia has signed. It is complemented by delegated legislation, including the Navigation Regulations 2013.[109] The *Navigation Act 2012* framework covers a range of different aspects of maritime operations, including:

- Crewing of vessels (chapter 2 of the Act);
- Vessel safety, including seaworthiness and certification of vessels (chapter 3);
- Marine pollution prevention (chapter 4); and
- Safety of navigation (chapter 6).

The *Navigation Act 2012* applies to vessels unless an exemption is granted, and the definition of "vessel" is found in section 14 of the Act:

Section 14:

"…vessel means any kind of vessel used in navigation by water, however propelled or moved, and includes the following:

(a) a barge, lighter or other floating craft;

(b) an air-cushion vehicle, or other similar craft, used wholly or primarily in navigation by water."

This definition draws no distinction between surface and sub-surface vessels. If a vessel navigates by water, then it makes no difference whether it operates on (and in some cases above) or below the surface. Similarly, there is no distinction made between conventional (non-autonomous) and autonomous vessels. That is, it is currently irrelevant whether a vessel is "autonomous" – once it satisfies the definition of "vessel", the *Act* will apply. Therefore, autonomous UUVs are clearly vessels, and are ordinarily subject to the Act in the absence of an exemption.

In accordance with section 334 of the *Act*, there is a general power for the responsible Minister or AMSA to exempt from the application of the *Act*, or parts of the Act, specified vessels or classes of vessels, and a person or class of person.

The *National Law 2012*

The *National Law 2012* was established to replace the previous patchwork of state and territory regulation and provide a single, national regulatory framework for the certification, construction, equipment, design and operation of "domestic commercial vessels" inside Australia's exclusive economic zone.[110]

The definition of vessel is found in section 8 of the *National Law 2012* and is very similar to that found in the *Navigation Act 2012*:

"…vessel means a craft for use, or that is capable of being used, in navigation by water, however propelled or moved, and includes an air-cushion vehicle, a barge, a lighter, a submersible, a ferry in chains and a wing-in-ground effect craft."

As with the *Navigation Act 2012* definition, once it satisfies the characteristics of a vessel, it is not relevant whether it is a surface or sub-surface craft, or whether it is conventional (non-autonomous) or autonomous.

The National Law 2012 specifically regulates the operation of "domestic commercial vessels" and section 7 provides the following definition:

(1) In this Law:

"…domestic commercial vessel means a vessel that is for use in connection with a commercial, governmental or research activity."

This is a broad definition that will cover most vessels, apart from those engaged in "recreational" activities that continue to be regulated by state and territory maritime safety agencies.[111] Therefore, in most instances, autonomous UUVs will fit within this definition and are subject to the *National Law 2012* in the absence of an exemption.

Exemptions

Similar to the *Navigation Act 2012,* section 143 of the *National Law 2012* provides AMSA with the power to make exempt from the application of the Act, or parts of the Act, specified vessels or classes of vessels, and a person or class of person.

Marine Orders

In accordance with section 163 of the *National Law 2012,* AMSA as the National Regulator may make Marine Orders that cover a range of matters relating to commercial vessels, including:

- Vessel certification;
- Vessel identification; and
- Vessel safety standards.[112]

These Marine Orders are regulations made under Commonwealth legislation and AMSA keeps an index of them on its website.[113]

AMSA and the regulation of autonomous vessels

AMSA has been in a holding pattern in relation to the regulation of autonomous vessels, as it awaits the definition of a whole-of-government policy position.[114] The *AMSA Policy on Regulatory Treatment of Unmanned and/or Autonomous Vessels* (the "Policy") indicates the current AMSA approach to the regulation of autonomous UUVs.[115] In short, while the current regulation regime is in place, autonomous vessels will be treated as vessels except where AMSA agrees to provide exemptions.

To date, AMSA has not put forward an official position as to how "autonomous" should be understood in the context of autonomous vessels (including UUVs). Rather, it refers to them generally as remotely operated and autonomous vessels.[116] This fits with the default position that autonomous vessels are regulated the same as conventional (non-autonomous) vessels under the *Navigation Act 2012* and the *National Law 2012.*

There are two types of exemption that exist under the *National Law 2012:*

1. **General exemptions** that AMSA grants on its own initiative and typically have general application to vessels, persons and operations that meet the relevant criteria and conditions. National Law general exemptions are available on the AMSA website.[117]
2. **Specific exemptions** are granted on application in accordance with the regulations by a person and are contained in Marine Order 501 (National Law – administration) 2013 (Marine Order 501).[118]

When deciding whether to grant an exemption, AMSA must first be satisfied that an exemption will not jeopardise the safety of a vessel or a person on board a vessel.[119] It may then consider a range of other relevant factors to determine whether it is appropriate to grant an exemption.[120]

Current limitations and future directions

In summary, the current AMSA regulation of autonomous UUVs as a subset of autonomous vessels does not account for their autonomous nature. Rather, autonomous vessels are treated as conventional (non-autonomous vessels) unless an exemption exists. As Horne et al. have observed, regulatory approaches that are not fit-for-purpose can stifle innovation, and reliance on bespoke exemptions can jeopardise trust and social licence.[121] AMSA has indicated its awareness of the likely limitations of the current regime as autonomous vessel technology proliferates. AMSA has stated on its website that it is "working on a new regulatory approach that will be sustainable in an environment of rapid technological change" [122] and the policy states that AMSA will develop guidance related to the design, construction, operation, safety management, and safety assurance of unmanned and/or autonomous vessels in Australian waters.[123] While no further detail was available at the time of writing, it can be anticipated that the future direction of the regulation of autonomous vessels will see the creation of specific provisions and AMSA guidance that contemplate the particular characteristics of autonomous vessels.

Australian Institute of Marine Science (AIMS): ReefWorks Regulatory Sandbox

AMSA has recently innovated in the regulatory space via the grant of approval to AIMS for the creation of a "regulatory sandbox" as part of its ReefWorks tropical marine technology test range.[124] Generally speaking, regulatory sandboxes are a regulatory structure that permits piloting or testing of services or products within a defined space under a specified set of rules, when those services or products are unable to operate under existing rules.[125] The creation of the Reefworks Sandbox was advocated for by AIMS, the Defence Cooperative Research Centre Trusted Autonomous Systems, and AMC Search. The approval is for five years, and provides for permit-free testing and evaluation of vessels up to 12m in length, traveling up to 20km within the test range.[126]

Naval vessels and the development of autonomous UUVs for Defence

The *National Law 2012* establishes a number of technical (and other) standards that autonomous UUVs will ordinarily not be able to comply with due to the way they are constructed and operated. For example, autonomous UUVs are not crewed in the same way as conventional (non-autonomous) vessels. This means that autonomous UUVs need to obtain an exemption to be built and operated lawfully.

In the Defence context, section 7(3) of the *National Law 2012* also excludes "defence vessels" from the definition of "domestic commercial vessels" and so effectively does not apply to such vessels. The definition of "defence vessel" is included in section 6:

"…defence vessel means:

(a) a warship or other vessel that:

(i) is operated for naval or military purposes by the Australian Defence Force or the armed forces of a foreign country; and

(ii) is under the command of a member of the Australian Defence Force or of a member of the armed forces of the foreign country; and

(iii) bears external marks of nationality; and

(iv) is manned by seafarers under armed forces discipline; or

(b) a government vessel that is used only on government non-commercial service as a naval auxiliary."

Therefore, autonomous UUVs would be exempt from the *National Law 2012* in circumstances that satisfy the requirements of section 6. This may be important for the standards applicable to the development of autonomous UUVs but also for the testing and operation for prototypes.[127] In practice, most autonomous UUV research and development undertaken for Defence would be undertaken by entities outside the ADF and who are not in a position to satisfy the "defence vessel" requirements set out in section 6(a). For example, the requirements in parts (ii) for command by an ADF member and (iv) for crewing by seafarers under armed forces discipline.

This means autonomous UUV development activities undertaken by the Defence Science and Technology Group (DSTG), Defence industry, and research institutions such as universities would be regulated as "domestic commercial vessels" by the National Law 2012 unless an exemption was available (see discussion above). To illustrate this, in 2022 Defence announced a partnership between Defence contractor Anduril, Navy, and DSTG to develop extra-large autonomous undersea vehicles (XLAUVs).[128] While we do not have any visibility into how development and testing is conducted, it can

be observed that if these XLAUVs are not being commanded by ADF personnel, then they do not constitute "defence vessels" and would be subject to regulation by the *National Law 2012*. This appears to be the case, even if the XLAUVs will ultimately be so commanded and become Defence vessels. Policy makers may need to reflect on whether this is a desirable state of affairs for promoting indigenous development of autonomous UUVs.

What is certain is that the challenges facing the RAN in terms of sheer nautical miles of territory to defend, more uncrewed vessels, surface and other, will be brought into service: "the RAN will acquire five Bluebottle USVs and is working with Austal on the patrol boat autonomy trial. The former HMAS *Maitland* will be renamed Sentinel and refurbished to allow for autonomous and remote operations. The RAN has also acquired and tested a maritime tactical systems catamaran, demonstrating a clear desire to expand its USV capabilities." [129]

International law (including maritime) attitudes to UUVs

There is no impediment at law to the use of uncrewed underwater vehicles (UUVs). Weapons (or those which in other senses may appear to be UUVs but are solely created and dispatched as mission-specific weapons) are excluded from this discussion of UUVs. The overarching law, the Vienna Convention on the Law of Treaties 1969, holds that where specific international treaties are silent on a particular subject, then the relevant treaty is to be interpreted in good faith and in light of its object and purpose. Therefore, many of the concerns about whether an underwater autonomous vehicle is or is not a ship (or vessel), is or is not crewed (physically or remotely), and is or is not military by nature, fall away because the purpose of each of the following existing international laws pertaining to vessels and specifically UUVs may be applied: the fundamental object and purpose are, for example, to ensure safe navigation, less pollution or good stewardship of the oceans. Where international law is completely silent on a topic, then the law of any Nation State ("state") will apply to the extent not challenged internationally (and in effect becomes customary international law).

Vienna Convention on the Law of Treaties 1969

Article 31(1): Treaties must be interpreted in good faith and "in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."

The United Nations Convention on the Law of the Sea (UNCLOS)

UNCLOS makes a distinction between submarines and vessels (or ships) which sail on the water: "UNCLOS recognises the right of innocent passage for the ships of all states within the territorial sea (Article 17). Submarines are expressly included within those entitlements, subject to navigating on the surface and showing their flag (Article 20)," meaning that submerged vessels must act like ordinary vessels in order to avail themselves of the right of innocent passage. This may not be practically possible, depending on the design and technology behind a particular UUV, in which case where there is otherwise no international or domestic law or agreement which expressly describes the relationship of underwater vessels (be they autonomous, semi-autonomous or other), then we may apply the logic of the Vienna Convention and include UUVs as ships either by reference to an expansive view of UNCLOS or via state-by-state designation as such via internal laws:

"If the objective of UNCLOS was, as it is believed, to develop a legal framework for the oceans including the operation of 'ships', nationally defined, by states in areas under the jurisdiction of other states and in areas beyond national jurisdiction, then the inclusion of UMVs in national definitions of ships supports both the object and the purpose of the Convention. Furthermore, there is evidence of an increasingly 'evolutionary approach' to treaty interpretation. For instance, the International Court of Justice (ICJ) has found that where a generic term is used, in the particular case the term, 'commerce', and where the relevant provision aims to settle a matter for an indefinite duration, treaty terms 'must be understood to have the meaning they bear on each occasion on which the Treaty is to be applied, and not necessarily their original meaning.' If, in the context of a treaty agreed in the mid-nineteenth century, the term 'commerce' can be interpreted to include 'tourism', it is certainly arguable that the term 'ship' under UNCLOS can include new types of ships as well as UMVs provided that a state designates them as such. It is therefore reasonable to conclude that whether a UMV is a ship under UNCLOS is intentionally left to the contracting state." [130]

"Article 94 [of UNCLOS] is by no means prescriptive, and if the presence of mariners on board is not a prerequisite for 'ship' status, then it arguably makes no difference whether the vessel is remotely operated or operating autonomously. Further, the International Maritime Organisation has defined a maritime autonomous surface ship as 'a ship which, to a varying degree, can operate independently of human interaction', and the fact they have used the word 'ship' suggests their members do not consider unmanned status an impediment to ship status. Further, by way of analogy, when comparing the aviation industry, every form of flying vehicle may be considered an 'aircraft' for the purposes of regulation."

Where there is silence in international law, a state's definition of "ship" or "uncrewed underwater vehicle" (and so forth) in a state's own domestic law (especially where left unchallenged) may prevail. This is because UNCLOS allows for state norms and practice.

Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs)

COLREGS are rules which apply "to all vessels upon the high seas and all waters connected to the high seas and navigable by seagoing vessels." It does not specifically address submerged vessels, however, at Section III – conduct of vessels in restricted visibility (Rule 19), it states "every vessel should proceed at a safe speed adapted to prevailing circumstances and restricted visibility. A vessel detecting by radar another vessel should determine if there is risk of collision and if so take avoiding action." [Emphasis added] This may be extrapolated to modern underwater usage in that where there is non-visual detection, it may behove the driver of the vessel which detects the underwater vessel (autonomous or otherwise) to adapt to that information, rather than continue into a potential collision or otherwise rely on the submerged vessel's ability to accommodate their passage. There may be many submerged vessels that have no ability to navigate that precisely.

International Convention for the Safety of Life at Sea, 1974 (SOLAS)

While the absence of a definition of "ship" under SOLAS leaves it open in theory to apply to UUVs, the tonnage specified in the annexes to SOLAS mean it is unlikely that it will directly apply to smaller UUVs, being more relevant to large UUVs.

International Convention for the Prevention of Pollution from Ships, 1973 (MARPOL)

MARPOL contains a broad definition of the term "ship", however, as stated above, the requirement to define a UUV as a ship is counter to the intent of the good faith interpretation of UNCLOS, SOLAS or COLREGS. What is pertinent is that the drafters operated within the context of the development and technology of their day; looking to the broader object and purpose will sensibly include UUVs, be they military or other.

Convention of the International Telecommunication Union, 1934

The Convention expands Australia's jurisdiction to regulate the use of certain radio-communications services by foreign vessels beyond the territorial sea via Radio Regulations.

Navigation Act (Cth) 2012

Section 6 of this Commonwealth Act rebuts the presumption of Australian laws not being intended to operate extraterritorially (outside Australia and coastal seas). Section 6 provides: "This Act applies both within and outside Australia." AMSA has the authority and responsibility for operational activities of the Navigation Act. The objects of the *Navigation Act* are:

(a) to promote the safety of life at sea;

(b) to promote safe navigation;

(c) to prevent pollution of the marine environment; and

(d) to ensure that AMSA has the necessary power to carry out inspections of vessels and enforce national and international standards.

Interim Guidelines for Maritime Autonomous Surface Ships, 2019

The International Maritime Organization (IMO) has released these interim guidelines with the aim of assisting relevant authorities and stakeholders to ensure safety and security with due regard for the protection of the environment. While these are specific to surface ships, there are many sections (including one on cyber risk management, in section 2.10) that could well apply to the underwater realm, and it is our view the default position is that they apply where possible. The IMO anticipates releasing a non-mandatory goal-based MASS Code to take effect in 2025, which will form the basis for a mandatory goal-based MASS Code, expected to enter into force on 1 January 2028.

Future considerations

Autonomous weapon systems (AWS)

AWS (fully or partially autonomous) development (especially where involving automation, artificial intelligence, machine learning or similar) and deployment must comply with existing treaties and conventions under international humanitarian law, and will need, at a minimum, to include sufficient cyber risk management of the systems and infrastructure used in deployment of such systems. This is extrapolated from the Interim Guidelines for MASS trials (see Interim Guidelines for Maritime Autonomous Surface Ships, 2019 above) and is reflective that modern instruments of international law will be drafted to explicitly require that due consideration is given to "building with security in mind" of technology which may have second, third or further order effects upon populations and the environment.

UUVs

May be operated remotely by military, defence civil service, contractors or civilians. Who operates UUVs has ramifications from a Law of Armed Conflict perspective for the state operating them. Should, for example, a state choose to allow non-uniformed members of its defence (or other branches of their civil service) to operate UUVs where the state is bound by the relevant Geneva Conventions and Protocols etc. of International Humanitarian Law (IHL), then that state must comply with those laws. Meaning that in the case of armed conflict, the engagement of non-combatants into any combatant roles (such as the piloting of UUVs) may waive that state's rights to protection as non-combatants under IHL. How these systems are piloted therefore needs to be a decision made at the highest strategic level of that state.

Under s123 of the Defence Act 1903, the exemption that may apply to military or employees from requirements of state and territory law (e.g., a requirement to register a vehicle or firearm) is not sufficiently broad to exempt those same personnel from the operation of the Commonwealth laws that enable the Geneva Conventions and Additional Protocols (IHL).

Unintended harm

Further consideration as to the size, capacity, dimensions, type of power, containing dangerous goods or large quantities of smaller UUVs must be had: the good faith interpretation required by the Vienna Convention imposes upon Australia a requirement to have regard to public safety, the environment, and numerous related considerations. As an example, consider a fleet of small UUVs the size of a football or smaller, powered by standard batteries. Once expired, the UUV may be an inert item, however, when considered en masse, or as containers of toxic waste, we return once again to designing with safety in mind. Not just cyber or technology safety, but also environmental and human safety.

Being "owned"

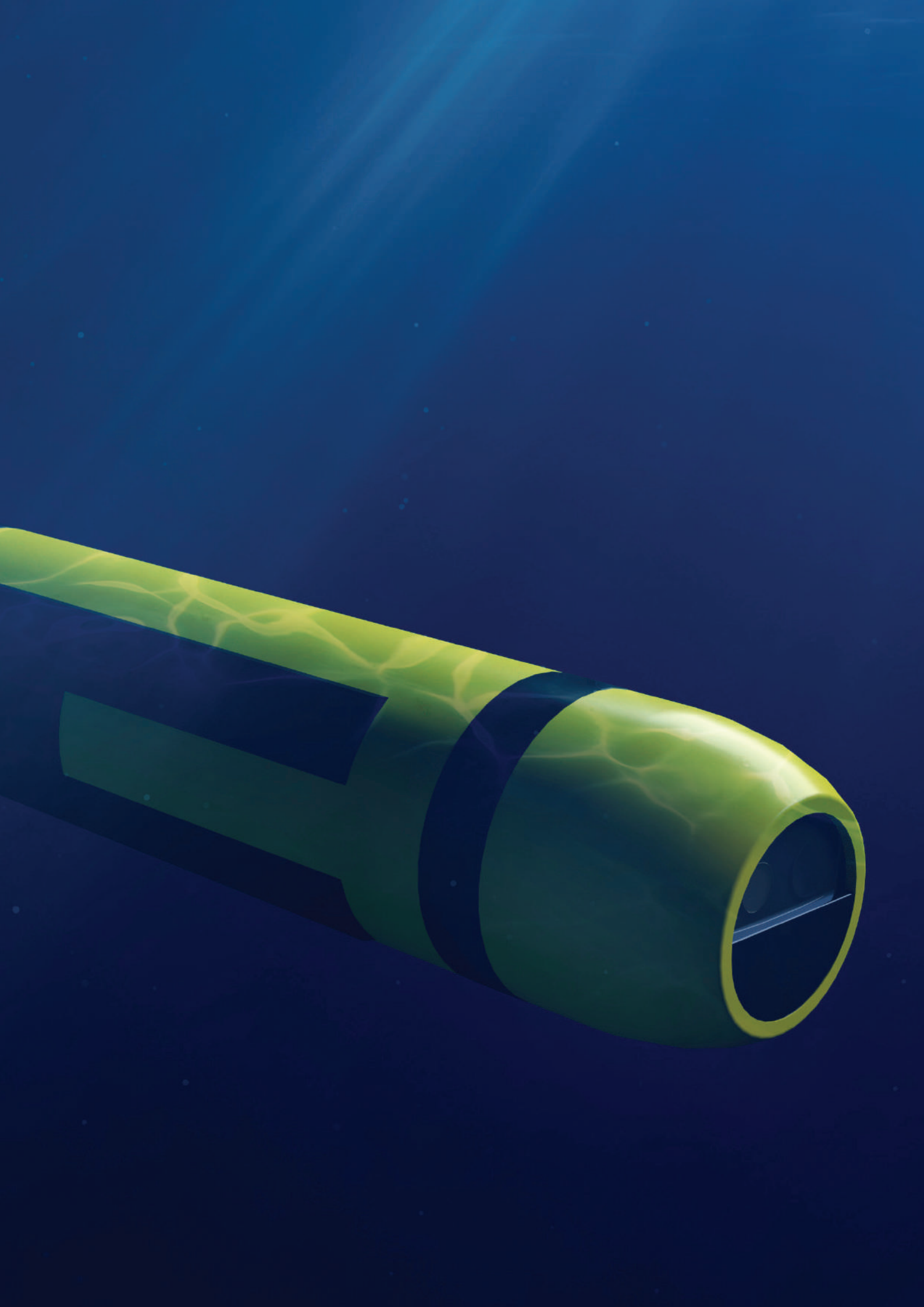
The design of all UUVs is usually focused on its operation. Consideration should be given to its counter-operation: what if this falls into enemy hands? What will they be able to do with those assets if they are turned against Australia? What information will they learn about our capabilities if one of our UUVs falls into their hands? See, for example, the US underwater naval drone/glider seized in the South China Sea by China in 2016. Will Australia have the ability to detect when a UUV has been "turned" and distinguish it from our own or allied forces?

Airspace

Examining how aerial drones have been regulated, as regards national and international airspace, as at least informative if not instructive.

Recreational

It will be helpful to distinguish between recreational UUVs from non-recreational, as has happened in air space. There will naturally be some overlaps (for example, the potential to cause harm in the marine environment), however, the purpose behind the design and construction is relevant.



References

1 Njall Trausti Fridbertson. (2023). “Protecting Critical Maritime Infrastructure – The Role of Technology”, *Preliminary Draft General Report by the General Rapporteur*, NATO Parliamentary Assembly, April 6. Retrieved via https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf; Christian Bueger, Tobias Liebetrau, and Jonas Franken. (2022). “Security Threats to undersea Communications Cables and Infrastructure – Consequences for the EU”, *Director General for External Policies, Policy Department, European Parliament.* Retrieved via https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

2 *RAS-AI Campaign Plan 2025: Warfare innovation Navy*. Royal Australian Navy. Retrieved via https://www.navy.gov.au/sites/default/files/documents/RAS-AI%20Campaign%20Plan%202025.pdf, Royal Australian Navy, (2017) Australian Maritime Operations https://www.navy.gov.au/sites/default/files/documents/Australian_Maritime_Operations_20 17.pdf

3 Engineers Australia (2014) Energy Security for Australia: Crafting a comprehensive energy security policy.

4 Blackburn, J. (2019). “Maritime trade dependencies and risks: A national security issue”, *Australian Naval Review, (2)*, 29-43.

5 *Protecting Australian Maritime Trade.* (2020). Australian Naval Institute and Naval Studies Group, University of New South Wales (Canberra). Retrieved from https://navalinstitute.com.au/wp-content/uploads/Protecting-Australian-Maritime-Trade-Report-March-2020.pdf ; Liam Carter, Audrey Quicke, and Alia Armstead. (2022). “Over a Barrel: Addressing Australia’s Liquid Fuel Security”, *The Australia Institute*, Retrieved via https://australiainstitute.org.au/wp-content/uploads/2022/04/P1036-Over-a-barrel_liquid-fuel-security-WEB.pdf

6 Australian Government – Defence, “Melbourne company to develop maritime unmanned aerial system”, Defence Ministers – Media Release, date published 8 October 2019, https://www.minister.defence.gov.au/media-releases/2019-10-08/melbourne-company-develop-maritime-unmanned-aerial-system; Callus, E. (2022, June 1). Partnership to develop stealthy capability. Defence News. https://news.defence.gov.au/technology/partnership-develop-stealthy-capability

7 R. Sparrow and G. Lucas. (2016). “When Robots Rule the Waves”, *Naval War College Review* 69, No. 4

8 Sunak, Rishi (2017). “Undersea Cables: Indispensable, Insecure”, *Policy Exchange*. Retrieved from https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf; Njall Trausti Fridbertsson. (2023). *Protecting Critical Maritime Infrastructure – The Role of Technology*. Preliminary Draft General Report by the General Rapporteur, NATO Parliamentary Assembly, April 6. Retrieved via https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf

9 “Russia Targets Netherlands’ North Sea Infrastructure, Says Dutch Intelligence Agency”, Reuters 20 February 2023. Retrieved viahttps://www.reuters.com/world/europe/russia-targets-netherlands-north-sea-infrastructure-says-dutch-intelligence-2023-02-20/

10 Thomas Newdick. 2022. Undersea Cable Connecting Norway with Arctic Mysteriously Severed. Real Clear Defense, 11 January. Retrieved via https://www.realcleardefense.com/2022/01/11/undersea_cable_connecting_norway_with_arctic_mysteriously_severed_811460.html

11 Michael J. Mazarr. 2015. *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (US Army War College Press, 2015).

[12] Morris, L. J., Mazarr, M. J., Hornung, J. W., Pezard, S., Binnendijk, A., & Kepe, M. (2019). "Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War", *RAND Corporation;* see also Christian Bueger, Tobias Liebetrau, and Jonas Franken. (2022). "Security Threats to Undersea Communication Cables and Infrastructure – Consequences for the EU", *Policy Department for External Relations Directorate General for External Policies of the Union PE 702.557* - June 2022. Retrieved via https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[13] Wen Li. (2023). "After Chinese Vessels Cut Matsu Internet Cables, Taiwan Seeks to Improve its Communications Resilience", *The Diplomat*, 15 April. Retrieved from https://thediplomat.com/2023/04/after-chinese-vessels-cut-matsu-internet-cables-taiwan-shows-its-communications-resilience/#:~:text=%E2%80%9Cinvisible%20blockade.%E2%80%9D-,When%20Chinese%20vessels%20damaged%20Matsu's%20two%20sea%20cables%20on%20February,until%20the%20end%20of%20March; Huizhong Wu and Lai, Johnson. (2023). "Taiwan Suspects Chinese Ships of Cutting Outlying Islands' Internet Cables", *Los Angeles Times*, 8 March. Retrieved from https://www.latimes.com/world-nation/story/2023-03-08/taiwan-suspects-china-cut-islands-internet-cables

[14] Jacobs, Charity S. and Carley, Kathleen M. (2022). Taiwan: "China's Gray Zone Doctrine in Action", *Small Wars Journal.* Retrieved from https://smallwarsjournal.com/jrnl/art/taiwan-chinas-gray-zone-doctrine-action; Yusuke Saito. (2019). "Reviewing law of armed conflict at sea and warfare in new domains and new measures: submarine cables, merchant missile ships, and unmanned marine systems", T*ulane Maritime Law Journal* 44, No. 1.

[15] "NATO Stands up Undersea Infrastructure Coordination Cell", *North Atlantic Treaty Organization* website, 15 February, 2023. Retrieved via https://www.nato.int/cps/en/natohq/news_211919.htm?selectedLocale=en

[16] Luca Peruzzie. (2023). *Seabed Warfare: NATO and EU Member State response. European Security and Defence*, 11 April. Retrieved via https://euro-sd.com/2023/04/articles/30719/seabed-warfare-nato-and-eu-member-state-responses/

[17] Andrew Salerno-Garthwaite. (2022). "Seabed Warfare Is a 'Real and Present Threat'", *Global Defence Technology*. Retrieved via https://defence.nridigital.com/global_defence_technology_dec22/seabed_warfare_is_a_real_and_present_threat

[18] US Department of the Navy. (2022). *The Commander's Handbook on the Law of Naval Operations*. Retrieved from https://usnwc.libguides.com/ld.php?content_id=66281931

[19] Schmitt MN and Goddard DS (2016) "International law and the military use of unmanned maritime systems", *International Review of the Red Cross,* 98:567-592.

[20] O'Rourke, Ronald. (2023). "Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress", *Congressional Research Service Report R45757.* Retrieved from https://sgp.fas.org/crs/weapons/R45757.pdf

[21] *Seabed Warfare Strategy*. Report by the Working Group, Ministry of Armed Forces, France, February 2023, p. 3. Retrieved via https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf

[22] Panneerselvam, Prakash. (2023). "Unmanned Systems in China's Maritime Grey Zone operations", *The Diplomat,* 23 January. Retrieved from https://thediplomat.com/2023/01/unmanned-systems-in-chinas-maritime-gray-zone-operations/

[23] Mizokami K (2016) "Pentagon Confirms Russia Has a Submarine Nuke Delivery Drone", *Popular Mechanics,* 8 December 2016, available at: www.popularmechanics.com/military/weapons/a24216/pentagon- confirm-russia-submarine-nuke/

[24] Bauk S, (2020) "Performances of Some Autonomous Assets in Maritime Missions"*, International Journal on Marine Navigation and Safety of Sea Transportation,* 14: 875-881.

[25] Mugg J, and Hawkins Z. (2026). "Securing Australia's oceans: the case for unmanned maritime vehicles", Australian Strategic Policy Institute – *The Strategist,* 13 July. Retrieved from https://www.aspistrategist.org.au/securing-australias-oceans-case-unmanned-maritime-vehicles/

[26] Royal Australian Navy. 2020. *RASI-AI Strategy 2040 – Warfare Innovation Navy*, https://www.navy.gov.au/sites/default/files/documents/RAN_WIN_RASAI_Strategy_2040f2_hi.pdf.

[27] Royal Australian Navy. 2018. *Plan Pelorus: Navy Strategy 2022,* Canberra, ACT: Commonwealth of Australia; Royal Australian Navy. 2017. *Plan Mercator: Navy Strategy 2036*, Canberra, ACT: Commonwealth of Australia; Department of Defence. 2020. *2020 Defence Strategic Update*, Canberra, ACT: Commonwealth of Australia; Department of Defence. 2023. *National Defence: Defence Strategic Review 2023*, Canberra, ACT: Commonwealth of Australia.

[28] Department of Defence. 2023. *National Defence: Defence Strategic Review 2023*, Canberra, ACT: Commonwealth of Australia, p. 73.

[29] Dortmans, Peter, Joanne Nicholson, James Black, Marigold Black, Carl Rhodes, Scott Savitz, Linda Slapakova, and Victoria M. Smith. (2021). "Supporting the Royal Australian Navy's Strategy for Robotics and Autonomous Systems: Building an Evidence Base", Santa Monica, *CA: RAND Corporation*. Retrieved from https://www.rand.org/pubs/research_reports/RRA929-1.html; *RAS-AI Campaign Plan 2025: Warfare innovation Navy. Royal Australian Navy.* Retrieved via https://www.navy.gov.au/sites/default/files/documents/RAS-AI%20Campaign%20Plan%202025.pdf

[30] Royal Australian Navy. 2020. *RASI-AI Strategy 2040 – Warfare Innovation Navy,* https://www.navy.gov.au/sites/default/files/documents/RAN_WIN_RASAI_Strategy_2040f2_hi.pdf

[31] US Department of the Navy. (2022). *The Commander's Handbook on the Law of Naval Operations,* Retrieved from https://usnwc.libguides.com/ld.php?content_id=66281931

[32] Schmitt, M. N., & Goddard, D. S. (2016). "International law and the military use of unmanned maritime systems", *International Review of the Red Cross, 98*, 567-592.

[33] Martinic, G. (2014). "Unmanned maritime surveillance and weapons systems", *Journal of the Australian Naval Institute, 151, 86-91*; Khawaja, W., Semkin, V., Ratyal, N. I., Yaqoob, Q., Gul, J., & Guvenc, I. (2022). "Threats from and countermeasures for unmanned aerial and underwater vehicles", *Sensors, 22(10)*.

[34] US Department of the Navy. (2004). *The Navy Unmanned Undersea Vehicle (UUV) Master Plan.*

[35] Klein N, (2019) "Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security", *International Law Studies, 95:* 244-271.

[36] Seto, M.L., Paull, L., & Saeedi, S. (2013). "Introduction to Autonomy for Marine Robots", In M.L. Seto (Ed.), *Marine Robot Autonomy* (pp. 1-46). Springer.

[37] "What is an AUV?", Virginia Institute of Marine Science, date accessed 10 September 2022 https://www.vims.edu/research/units/legacy/cornwallis/auv/index.php

[38] Kil-Joo Ban. (2010). "The Clash of David and Goliath at Sea: The USS Cole Bombing as Sea Insurgency and Lessons for the ROK Navy", *Asian Politics & Policy 2, No. 3*.

[39] Australian Communications and Media Authority, Sydney submarine cable protection zones; Sunak, Rishi (2017). "Undersea Cables: Indispensable, Insecure", *Policy Exchange*. Retrieved from https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf

[40] Terri Moon Cronk. 2016. "Chinese Seize U.S. Navy underwater Drone in South China Sea", *DOD News*, U.S. Department of Defense, 16 December. Retrieved via https://www.defense.gov/News/News-Stories/Article/Article/1032823/chinese-seize-us-navy-underwater-drone-in-south-china-sea/#:~:text=Using%20appropriate%20government%2Dto%2Dgovernment,said%20in%20a%20statement%20today

[41] Shachtman N. “Computer virus hits U.S. drone fleet”, *Wired*,http://www.wired.com/2011/10/virus-hits-drone-fleet/ (7October2011, accessed 31 January 2015).

[42] Alex Christian. (2021). The Untold Story of the Big Boat that Broke the World. Wired, 22 June. Retrieved via https://www.wired.co.uk/article/ever-given-global-supply-chain

[43] *Protecting Australian Maritime Trade.* (2020). Australian Naval Institute and Naval Studies Group, University of New South Wales (Canberra). Retrieved from https://navalinstitute.com.au/wp-content/uploads/Protecting-Australian-Maritime-Trade-Report-March-2020.pdf

[44] Giles Pakinson. (2023). “Giant Sun Cable Solar Project to Start off with Domestic Focus, May Add Wind”, *Renew Economy*, 31 May. Retrieved via https://reneweconomy.com.au/giant-sun-cable-project-to-start-off-with-domestic-focus-may-add-wind/

[45] “Gatwick Airport drone attack: Police have ‘no lines of inquiry’”, *BBC News*, Sep. 27, 2019. Accessed: Dec. 10, 2022. [Online]. Available: https://www.bbc.com/news/uk-england-sussex-49846450

[46] “Exercise Autonomous Warrior Testing New Technologies to Meet Emerging Maritime Security Challenges”, (2022). Australian Government Department of Defence, Media Releases, 16 May. Retrieved from https://www.defence.gov.au/news-events/releases/2022-05-16/exercise-autonomous-warrior-testing-new-technologies-meet-emerging-maritime-security-challenges

[47] Lee Willett. (2021). “RAN Melds Unmanned Systems into New Model Navy”, *Asian Military Review*, 20 April. Retrieved via https://www.asianmilitaryreview.com/2021/04/ran-melds-unmanned-systems-into-new-model-navy/

[48] Tom Vanen Brook and Kim Hjelmgaard. (2023). “US Air Force Says it Did Not Run Simulation in Which AI Drone ‘Killed its Operator’”, *USA Today*, 2 June. Retrieved via https://www.usatoday.com/story/news/politics/2023/06/02/us-air-force-denies-ai-drone-simulation-killed-its-operator/70280780007/

[49] Jeffrey Wall. (2020). “China to Build $200 Million Fishery Project on Australia’s Doorstep”, *The ASPI Strategist*, 8 December. Retrieved via https://www.aspistrategist.org.au/china-to-build-200-million-fishery-project-on-australias-doorstep/

[50] Medina, D.; Lass, C.; Marcos, E.P.; Ziebold, R.; Closas, P.; García, J. (2019). “On GNSS Jamming Threat from the Maritime Navigation Perspective”, *In Proceedings of the 22th International Conference on Information Fusion (FUSION),* Ottawa, ON, Canada, 2–5 July; pp. 1–7

[51] Peter Layton. (2021). “War at Sea in the Age of Artificial Intelligence”, *Australian Naval Review, No. 2*.

[52] Heiko Borchert. (2016). “Lethal Undersea Drones: The Ultimate Military Game Changer in the Pacific?” *The National Interest,* 9 May. Retrieved via “Lethal Undersea Drones: The Ultimate Military Game Changer in the Pacific?” | *The National Interest*; Robert Martinage. 2014. “Toward a New Offset Strategy”, Center for Strategic and Budgetary Assessments. Retrieved via “Toward a New Offset Strategy” by Center of Strategic and Budgetary Assessments – Issuu

[53] Coito J (2021) “Maritime Autonomous Surface Ships: New Possibilities – and Challenges – in Ocean Law and Policy”, *International Law Studies*, 95: p. 281.

[54] Zhang, P.; Zhang, C.; Gai, W. “Research on application and development trend of multi-domain cooperative combat for unmanned combat platform”, In *Proceedings of the 2021 2nd International Symposium on Computer Engineering and Intelligent Communications (ISCEIC),* Nanjing, China, 6–8 August 2021; pp. 297–301.

[55] Andro Mathewson. (2021). “The Growing Risk of Militarized Unmanned Submersibles”, *The Maritime Executive*, 30 August. Retrieved via “The Growing Risk of Militarized Unmanned Submersibles” (maritime-executive.com)

[56] Margarita Konaev, Husanjot Chahal, Ryan Fedasiuk, Tina Huang, and Ilya Rahkovsky. (2020). "U.S. Military Investments in Autonomy and AI", *Center for Security and Emerging Technology Policy Brief,* October. Retrieved via U.S. Military Investments in Autonomy and AI_Strategic Assessment (georgetown.edu)

[57] "United States Department of the Navy, Fiscal Year (FY) 2020 Budget Estimates", March 2019, *Navy, Justification Book Volume 1 of 5*, vol 1–259.

[58] Bae, Inyeong, and Jungpyo Hong. 2023. "Survey on the Developments of Unmanned Marine Vehicles: Intelligence and Cooperation", *Sensors 23, no. 10:* 4643. https://doi.org/10.3390/s23104643

[59] Asia-Pacific Defence Reporter. (2022). *Asia-Pacific Countries on Track to Increase Defence Spending*. 18 August. Retrieved via https://asiapacificdefencereporter.com/asia-pacific-countries-on-track-to-increase-defence-spending/; Ken Moriyasu. (2022). "'Geopolitical Powder Keg' Asia Jacks up Global Military Spending", *Nikkei Asia*, 25 April. Retrieved via https://asia.nikkei.com/Politics/International-relations/Indo-Pacific/Geopolitical-powder-keg-Asia-jacks-up-global-military-spending

[60] Yang, Y.; Xiao, Y.; Li, T. "A Survey of Autonomous Underwater Vehicle Formation: Performance, Formation Control, and Communication Capability", *IEEE Communs. Surv. Tutorials* 2021, 23, 815–841.

[61] Khawaja W, Semkin V, Ratyal NI, Yaqoob Q, Gul J, and Guvenc I, (2022) "Threats from and Countermeasures for Unmanned Aerial and Underwater Vehicles", *Sensors 22.*

[62] Walker Mills, Collin Fox, Dylan Phillips-Levine, and Trevor Phillips-Levine. (2021) "Use Emerging Technology for ASW", *U.S. Naval Institute, Proceedings, Vol. 147*, No. 10.

[63] Dolma Tsering. 2016. "China's undersea Great Wall Project: Implications", *National Maritime Foundation*. 9 December. Retrieved via https://maritimeindia.org/chinas-undersea-great-wall-project-implications/

[64] 构建我国海洋水下观测体系的思考 ("Reflection on the Construction of Marine Underwater Observation System in China", available at http://epaper.oceanol.com/shtml/zghyb/20151202/7399.shtml (accessed on 21st November, 2016)

[65] Simon Lindsay. 2021. "Does State Interference with Submarine Cables Constitute an Armed Attack in International Law?*" Australian Naval Review, No. 2;* Zoe Scanlon, "Addressing the pitfalls of exclusive flag state jurisdiction: improving the legal regime for the protection of submarine cables", *Journal of Maritime Law and Commerce, vol. 48(3),* 2017, p. 297; Davenport, 2015, pp. 62–63; Yoram Dinstein & Arne Willy Dahl, *Oslo manual on select topics of the law of armed conflict: rules and commentary*, 2020, SpringerOpen, p. 63; Scanlon, 2017, pp. 296–297.

[66] Njall Trausti Fridbertsson. (2023). "Protecting Critical Maritime Infrastructure – The Role of Technology", *Preliminary Draft General Report by the General Rapporteur,* NATO Parliamentary Assembly, April 6. Retrieved via https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdf

[67] Christian Bueger, Tobias Liebetrau, and Jonas Franken. (2022). "Security Threats to undersea Communications Cables and Infrastructure – Consequences for the EU", *Director General for External Policies, Policy Department*, European Parliament. Retrieved via https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf

[68] Ewen Levick. (2018). "China's 'Underwater Great Wall'", *Maritime-Executive*, 18 June. Retrieved via https://maritime-executive.com/editorials/china-s-underwater-great-wall

[69] *Seabed Warfare Strategy*. Report by the Working Group, Ministry of Armed Forces, France, February 2023, p. 3. Retrieved via https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf

[70] Ibid.

[71] Quoted in Njall Trausti Fridbertsson. (2023). "Protecting Critical Maritime Infrastructure – The Role of Technology", *Preliminary Draft General Report by the General Rapporteur*, NATO Parliamentary Assembly, April 6. Retrieved via https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-04/032%20STC%2023%20E%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT.pdfC4ISRNET (2023). "Europeans Wade Into Fighting Seabed Threats with Drones and Sensors", 9 January. Retrieved via https://www.c4isrnet.com/global/europe/2023/01/09/europeans-wade-into-fighting-seabed-threats-with-drones-and-sensors/?utm_source=sailthru&utm_medium=email&utm_campaign=c4-overmatch

[72] Alia Huberman. "Breaching the Surface – the Future of *Sea Mines in the Indo-Pacific", In Sea Power Centre Australia 2021 Annual: Research Papers and Reports to Create "A Thinking Navy, A Fighting Navy, An Australian Navy," edition one.* September 2021. Retrieved via https://www.navy.gov.au/sites/default/files/documents/SPC-A_2021_Annual_1.pdf

[73] Yaacoub JP, Noura H, Salman O, and Chehab A (2020) "Security analysis of drones systems: Attacks, limitations, and recommendations", *Internet of Things*, 11: 1-39, doi: https://doi.org/10.1016/j.iot.2020.100218.

[74] Chase, Michael S., Kristen Gunness, Lyle J. Morris, Samuel K. Berkowitz, and Benjamin Purser, "Emerging Trends in China's Development of Unmanned Systems", Santa Monica, CA: *RAND Corporation*, 2015. https://www.rand.org/pubs/research_reports/RR990.html.

[75] Poornima, G., Pavithra, R., Praveen, M., Ragusurya, S. and Aashish, C. (2023). "Design and Analysis of 3D Printed Unmanned underwater Vehicles", *AIP Conference Proceedings 2492, Vol. 2492, No. 1.*

[76] U.S. Department of the Navy, *The Navy Unmanned Undersea Vehicle (UUV) Master Plan,* November 2004

[77] Button, Robert W., John Kamp, Thomas B. Curtin, and James Dryden, "A Survey of Missions for Unmanned Undersea Vehicles", Santa Monica, CA: *RAND Corporation*, 2009. https://www.rand.org/pubs/monographs/MG808.html. Also available in print form.

[78] David B. Larter. (2015). "ONR: Large Underwater Drone Set for 2016 West Coast Cruise", *Navy Times*, 17 April. Retrieved via https://www.navytimes.com/news/your-navy/2015/04/16/onr-large-underwater-drone-set-for-2016-west-coast-cruise/

[79] Hawkins Z, and Mugg J, "Maritime drones: the future of Australian border security", Australian Strategic Policy Institute – *The Strategist*, date published 16 November 2015, https://www.aspistrategist.org.au/maritime-drones-the-future-of-australian-border-security/.

[80] Martinic G, (2014) "Unmanned maritime surveillance and weapons systems", *Journal of the Australian Naval Institute, 151:* 86-91.

[81] *Seabed Warfare Strategy.* Report by the Working Group, Ministry of Armed Forces, France, February 2023. Retrieved via https://www.archives.defense.gouv.fr/content/download/636001/10511909/file/20220214_FRENCH%20SEABED%20STRATEGY.pdf

[82] S. Pundir, M. Wazid, D. P. Singh, A. K. Das, J. J. P. C. Rodrigues and Y. Park, "Intrusion Detection Protocols in Wireless Sensor Networks Integrated to Internet of Things Deployment: Survey and Future Challenges", in *IEEE Access, vol. 8,* pp. 3343-3363, 2020; U. C. Cabuk, G. Dalkilic and O. Dagdeviren, "CoMAD: Context-Aware Mutual Authentication Protocol for Drone Networks", in *IEEE Access, vol. 9*, pp. 78400-78414, 2021

[83] M. Mohan, *Cybersecurity in UAVs,'* Ph.D. dissertation, Fac. Utica College, Utica College, Utica, NY, USA, 2016

[84] Madan BB, Banik M, and Bein D, (2019) "Securing unmanned autonomous systems from cyber threats", *Journal of Defence Modeling and Simulation: Application, Methodology, Technology 16:* 119-136.

[85] ibid.

[86] Gill TD, van Haaster J, and Roorda M (2019) “Some legal and operational consideration regarding remote warfare: drones and cyber warfare revisited”, in Ohlin JD (ed) *Research Handbook on Remote Warfare*, Edward Elgar Publishing Limited, 298-334

[87] *2016 Defence White Paper*. Australian Government Department of Defence. Retrieved via https://www.defence.gov.au/sites/default/files/2021-08/2016-Defence-White-Paper.pdf

[88] James Goldrick. (2020). “Defence Strategic Update 2020: A First Assessment”, *The Lowy Interpreter,* 2 July. Retrieved via https://www.lowyinstitute.org/the-interpreter/defence-strategic-update-2020-first-assessment

[89] *More, Together. Defence Science and Technology Strategy 2030*. Australian Government Department of Defence. Retrieved via https://www.dst.defence.gov.au/sites/default/files/basic_pages/documents/Defence%20Science%20and%20Technology%20Strategy%202030.pdf

[90] Royal Australian Navy. 2017. *Plan Mercator: Navy Strategy 2036,* Canberra, ACT: Commonwealth of Australia.

[91] *The AUKUS Nuclear-Powered Submarine Pathway: A Partnership for the Future*. Australian Government Department of Defence. Retrieved via AUKUS Nuclear-Powered Submarine Pathway | About | Defence

[92] Davis M, “AUKUS requires rapid expansion of autonomous undersea warfare systems”, Australian Strategic Policy Institute (ASPI), date published 30 October 2021,https://www.aspi.org.au/opinion/aukus-requires-rapid-expansion-autonomous-undersea-warfare-systems

[93] Mick Ryan. (2023). “Nuclear Submarine Deal will Deeply Impact the Australian Defence Force. Has the Government Got it Right?” *ABC News,* 14 March. Retrieved via https://www.abc.net.au/news/2023-03-14/nuclear-submarine-aukus-how-cost-impact-military-capability/102089496

[94] Davis M, “AUKUS requires rapid expansion of autonomous undersea warfare systems”, Australian Strategic Policy Institute (ASPI), date published 30 October 2021,https://www.aspi.org.au/opinion/aukus-requires-rapid-expansion-autonomous-undersea-warfare-systems

[95] Mick Ryan. (2023). “Nuclear Submarine Deal will Deeply Impact the Australian Defence Force. Has the Government Got it Right?” *ABC News,* 14 March. Retrieved via https://www.abc.net.au/news/2023-03-14/nuclear-submarine-aukus-how-cost-impact-military-capability/102089496

[96] Jennifer Parker, David Uren, Bec Shrimpton, and Rob Bourke. (2023). “The Big Squeeze”, Australian Strategic Policy Institute. 30 May. Retrieved via https://www.aspi.org.au/report/big-squeeze#:~:text=The%20government%20will%20start%20providing,%25%20to%20more%20than%202.3%25

[97] Peter Dortmans, Joanne Nicholson, James Black, Marigold Black, Carl Rhodes, Scott Savitz, Linda Slapakova, and Victoria M. Smith. (2021). *Supporting the Royal Australian Navy’s Strategy for Robotics and Autonomous Systems: Building and Evidence Base.* Rand Australia Research Report. Retrieved via https://www.rand.org/pubs/research_reports/RRA929-1.html

[98] Joint Media Release by Anthony Albanese and Richard Marles. Release of the Defence Strategic Review. Australian Government Department of Defence, 24 April 2023. Retrieved via Release of the Defence Strategic Review | Defence Ministers

[99] Jennifer Parker, David Uren, Bec Shrimpton, and Rob Bourke. (2023). “The Big Squeeze”, Australian Strategic Policy Institute. 30 May. Retrieved via https://www.aspi.org.au/report/big-queeze#:~:text=The%20government%20will%20start%20providing,%25%20to%20more%20than%202.3%25

[100] Jennifer Parker, David Uren, Bec Shrimpton, and Rob Bourke. (2023). “The Big Squeeze”, Australian Strategic Policy Institute. 30 May. Retrieved via https://www.aspi.org.au/report/big-queeze#:~:text=The%20government%20will%20start%20providing,%25%20to%20more%20than%202.3%25

[101] Vincent C. Müller. (2021). "Ethics of Artificial Intelligence and Robotics", *The Stanford Encyclopedia of Philosophy,* Edward N. Zalta (ed.)

[102] Roberto J. Gonzalez. (2023). "Drones of Ukraine: What the War Means for the Future of Remotely Piloted Aircraft in Combat", *The Conversation*, 24 February. Retrieved via https://theconversation.com/drones-over-ukraine-what-the-war-means-for-the-future-of-remotely-piloted-aircraft-in-combat-197612

[103] ibid.

[104] Regan Ho. "The Future is Limited: The Ethics of Lethal Autonomous Weapons Systems", *The Forge.* Retrieved via https://theforge.defence.gov.au/publications/future-limited-ethics-lethal-autonomous-weapons-systems

[105] Erich Riesen. (2022). "The Moral Case for the Development and Use of Autonomous Weapon Systems", *Journal of Military Ethics*, 21:2, 132-150.

[106] Benjamin Halpern, Melanie Frazier, John Potapenko, Kenneth Casey, Kellee Koenig, et al. (2015). "Cumulative human impacts: raw stressor data (2008 and 2013)", *Knowledge Network for Biocomplexity.* doi:10.5063/F1S180FS.

[107] Becker JJ, Sandwell DT, Smith WHF, Braud J, Binder B, et al. (2009) "Global bathymetry and elevation data at 30 arc seconds resolution: SRTM30_PLUS", *Marine Geodesy 32*: 355–371.

[108] State Maritime Safety agencies are responsible for regulating "recreational" vessels.

[109] https://www.amsa.gov.au/about/regulations-and-standards/index-marine-orders

[110] https://www.amsa.gov.au/about/regulations-and-standards/national-law-act-2012#:~:text=The%20Marine%20Safety%20(Domestic%20Commercial,inside%20Australia%27s%20exclusive%20economic%20zone

[111] https://transportsafety.vic.gov.au/maritime-safety/regulation-and-investigation/marine-enforcement-policy

[112] https://www.amsa.gov.au/about/regulations-and-standards/national-law-act-2012#:~:text=The%20Marine%20Safety%20(Domestic%20Commercial,inside%20Australia%27s%20exclusive%20economic%20zone

[113] https://www.amsa.gov.au/about/regulations-and-standards/index-marine-orders

[114] TAS "Current Australian regulatory framework for autonomous vessels" 2022, P.9 available at https://wordpress.rasgateway.com.au//var/files/2022/07/Maritime-Domain-Australian-regulation-SEPT2022.pdf

[115] https://www.amsa.gov.au/sites/default/files/policy-regulatory-treatment-unmanned-autonomous-vessels.pdf

[116] https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/autonomous-vessels-australia

[117] https://www.amsa.gov.au/about/regulations-and-standards/national-law-act-exemptions-marine-orders

[118] Exemptions from the Domestic Commercial Vessel National Law Policy November 2016 available at https://www.amsa.gov.au/sites/default/files/amsa655-exemptions-from-the-domestic-commercial-vessel-national-law.pdf

[119] section 143(6) of the *National Law 2012*.

[120] *See Exemptions from the Domestic Commercial Vessel National Law Policy*, November 2016, p.3.

[121] Horne et al, *Navigating to smoother regulatory waters for Australian commercial vessels capable of remote or autonomous operation: a systematic quantitative literature review*, p.2.

[122] https://www.amsa.gov.au/vessels-operators/domestic-commercial-vessels/autonomous-vessels-australia

[123] https://www.amsa.gov.au/sites/default/files/policy-regulatory-treatment-unmanned-autonomous-vessels.pdf

[124] https://tasdcrc.com.au/an-australian-maritime-regulatory-sandbox/

[125] https://tasdcrc.com.au/wp-content/uploads/2023/05/Report-Excerpt-regarding-Regulatory-Sandboxes-exerpt-17-May-2023.pdf Hilary J Allen, "Regulatory Sandboxes," *George Washington Law Review* 87, no. 3 (2019).

[126] https://tasdcrc.com.au/an-australian-maritime-regulatory-sandbox/

[127] As "Current Australian regulatory framework for autonomous vessels" 2022, p.22, available at https://wordpress.rasgateway.com.au//var/files/2022/07/Maritime-Domain-Australian-regulation-SEPT2022.pdf

[128] https://www.defence.gov.au/news-events/news/2022-06-01/partnership-develop-stealthy-capability

[129] Parker, R., 2023. "To integrate uncrewed surface vehicles into the navy, start with a concept of operations", *The Strategist.* ASPI. 9 June 2023. https://www.aspistrategist.org.au/to-integrate-uncrewed-surface-vehicles-into-the-navy-start-with-a-concept-of-operations/

[130] Veal, R., Tsimplis, R. and Serdy, A., 2019. "The Legal Status and Operation of Unmanned Maritime Vehicles", *Ocean Development & International Law 50* (2019): 23 – 48, pp.16-46.

[131] Lindsay, S., 2020. "Sufficiency of existing legal frameworks for addressing maritime security challenges surrounding autonomous vessels", *Australian Naval Review* (2020): Issue 2, pp.104-116.

[132] Which explains the recent uptick in activity by Australia and allied nations in navigating their freedoms of the sea (and air) around the Strait of Taiwan – see for example https://www.theguardian.com/world/2023/jun/05/taiwan-strait-footage-released-of-near-miss-between-chinese-warship-and-us-destroyer

[133] International Telegraph Conference (Madrid,1932), https://www.itu.int/en/history/Pages/PlenipotentiaryConferences.aspx?conf=4.5

[134] Interim Guidelines for Mass Trials, MSC.1/Circ.1604. Annex pp.1-3, available at https://wwwcdn.imo.org/localresources/en/MediaCentre/HotTopics/Documents/MSC.1-Circ.1604%20-%20Interim%20Guidelines%20For%20Mass%20Trials%20(Secretariat).pdf

[135] Dan Lamothe and Missy Ryan, 2016, *"Pentagon: Chinese naval ship seized an unmanned U.S. underwater vehicle in South China Sea"*, available at https://www.washingtonpost.com/news/checkpoint/wp/2016/12/16/defense-official-chinese-naval-ship-seized-an-unmanned-u-s-ocean-glider/

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