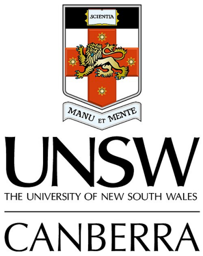

Naval Studies Group Primer No. 1

Maritime Warfare Technological Developments

By Peter Jones and Jennifer Parker*

This primer describes maritime warfare technological developments as they may affect the Australian Defence Force (ADF).

Introduction

Technology has always shaped naval warfare, but the pace and scope of change in the late 20th and early 21st centuries are unprecedented. In 2025 the central debate is whether naval warfare faces a true revolution or merely an evolution. Evidence for a step-change is mounting: Ukraine's uncrewed surface vessels (USVs) have mounted a highly effective Black Sea denial campaign, when coupled with the use of missiles and uncrewed aerial vehicles (UAVs).[1] Houthi forces have used missiles, UAVs and USVs to strike shipping in the Red Sea; and ballistic and hypersonic missiles have entered combat in Europe and the Middle East. Overlaying these advances is the rapid diffusion of artificial intelligence (AI) across sensing, command and weapon systems. Collectively, these trends are reshaping capability acquisition, tactics, operations and, ultimately, maritime strategy.

Since the arrival of the Royal Australian Navy's (RAN) fleet in 1913, there has been a considered approach to acquire ships, aircraft and weapon systems that were the same as, or compatible with, those of Australia's pre-eminent maritime ally, initially the UK and then over a transition period the US. Related to this was an emphasis on high-end systems, in part to compensate for Australia's limited personnel resources, with just under 16,000 permanent RAN members in 2025, which is planned to grow to 20,000 by 2040. In modern times, this approach has largely continued, and this is evidenced

[1] Parker, 'An Evolution or a Revolution in Naval Warfare: USVs in the Black Sea', in *Australian Naval Review*, 2024, <https://www.jennifer-parker.com.au/publications>.

by acquisitions of Aegis destroyers, fitted with Tomahawk land attack missiles, and later, in the next decade, of nuclear attack submarines (SSNs).

During the timeframe discussed in this monograph, the dominant technologies in the maritime and associated environments will largely be those that are in-service today. Some technologies, such as AI enabled systems and uncrewed platforms, are experiencing rapid change and the manner in which they influence the conduct of operations continues to evolve quickly. It is useful to examine these technologies in different domains and then discuss their employment in a system of systems approach.

Moving forward, Australia, like other medium powers, will need to consider how to leverage new technologies that allow navies to achieve greater effects at lower cost and with fewer personnel. Interoperability remains an ongoing challenge in this space, as does connectivity, especially as global positioning system (GPS) and related systems could be the first to be compromised in a kinetic scenario. What constitutes genuine 'autonomy' of autonomous systems, and whether such autonomy is desirable, is a question that applies at multiple levels. Is the system self-powered? Self-directed, i.e., non-reliant on external inputs? What of the command element once autonomous systems are in play? These questions will need to be addressed both theoretically and practically, as such systems are further integrated with current naval capability.

Air Warfare

Since the early days of World War II one of the most challenging aspects of naval operations for the RAN is operating in the absence of air superiority or where it is contested. In its history nearly half of all RAN ship losses to the enemy have been to air attack.[2] This experience was a major driver for the post-war acquisition of aircraft carriers, which provided both air defence for the RAN task group, and also the offensive ability to carry out long range strikes on enemy sea and land forces.[3] The loss of aircraft carriers saw the organic fleet air defence centre on the Standard SM-1, then SM-2 surface-to-air missiles (SAMs) in the destroyers and larger frigates with the Sea Sparrow, then Evolved Sea Sparrow Missile (ESSM) in the Anzac class. Ideally, these ships would operate in higher threat areas with the support of sea or land-based fighters, as was the case in the 2003 Iraq War. A significant development in this domain was the introduction of the suite of indigenous CEA Technologies digital phased array radars, not only into the Anzac class but also into the land forces. These radars, linked to a Swedish Australian 9LV combat system, significantly increased the lethality of existing missiles, but also the survivability of the Anzacs.

The contemporary fleet has evolved from this foundation. The Hobart class destroyers have, or are being retrofitted with, the Aegis Ballistic Missile Defence System (BMDS) and the ~250nm range SM-6 extended range missile. The first of the six Hunter class frigates is expected to enter service in 2032 and will bring to sea a CEA radar, Aegis/9LV, SM-2/ESSM suite of capabilities. Prior to that, in 2029 the first of up to eleven smaller Upgraded Mogami class general purpose frigates should enter service.

The RAN's major surface combatants have active and passive electronic warfare (EW) systems. A notable system is the Australian-US Nulka off-board active decoy that has proved its worth

2 'List of Royal Australian Navy losses', in *Wikipedia*, <https://en.wikipedia.org/wiki/List_of_Royal_Australian_Navy_losses>.

3 Jones, P., 'Vice Admiral Sir John Augustine Collins KBE, CB, RAN', Cooper, A. & Goldrick, J., *The Navy Chiefs: Australia's Naval Leaders 1911-1997*, Allen & Unwin, Crows Nest, 2024, 199.

operationally with the United States Navy (USN) off the Yemeni coast, during recent Red Sea battles with the Houthis. This system is undergoing further development.

Considerable efforts have been made over recent decades to harmonise operations with the RAAF's growing air defence capabilities. Its mix of 72 F-35A Lightning II, 24 FA-18F Super Hornet and a dozen EA-18G Growler electronic attack aircraft supported by six E-7A Wedgetail Intelligence Surveillance and Reconnaissance (ISR) and seven KC-30A tanker aircraft has few peers in the Indo-Pacific.

Collectively, the sea and land-based systems of the Australian Defence Force (ADF) can intercept aircraft, supersonic missiles and ballistic missiles (near launch and in the terminal phases). They also can destroy the slow-moving UAV or drones. Nevertheless, ballistic missile defence within the ADF is presently quite limited. The ADF presently has no ground-based ballistic missile defence capability, and its broader ground-based missile defence capability is limited to a small number of medium range National Advanced Surface-to-Air Missile System (NASAMS) batteries and shorter-range RBS-70 system, which is in the process of being upgraded.

Air warfare is one of the most challenging of domains, if for no other reason than its short reaction times and the smallest margins of error. The significant challenges in this space are:

- the increased speed and manoeuvrability of anti-ship missiles, including at hypersonic speeds,
- Predicted UAV swarms and current saturation drone attacks observed in Ukraine and elsewhere, and
- the utilisation of AI to maximise the effect of attack missions, including with electronic warfare (EW) systems.

One of the over-riding features of the Russo-Ukrainian War has been the rapid development of UAV capabilities and tactics. The Ukrainians have developed reconnaissance UAVs of up to 28 hours endurance and 2,500 km range[4] and one-way attack (OWA) drones out to about 1,300km range.[5] The 1 June 2025 Ukrainian attack on the Russian strategic bomber force also highlighted the lethality of small drones, if they are covertly forward deployed. There have also been important associated developments in the control and assessment of collected data. For example, the Ukrainians are developing small-data set AI software to enable more autonomous guidance, improved target recognition and post-mission analysis. To paraphrase an old dictum, 'numbers have a quality all of their own'. This is very much the case with UAVs. To give a sense of possible inventories that can be developed, Ukraine acquired from local and overseas sources 1,400 drones in just one three month 'dronation' drive.[6] Even these numbers are being exceeded and the Russian attacks on cities with around a 1,000 drones a day illustrate this point.[7] The takeaway is that large numbers of drones could be in any raid against naval forces and land targets, particularly in littoral waters.

4 *Skeyton*, <https://skyeton.com/>.

5 H Sutton, 'Guide To Ukraine's Long Range Attack Drones', in *HI Sutton*, 2025, <http://www.hisutton.com/Ukraine-OWA-UAVs.html>.

6 'United 24', in *Ukranian Government*, <https://u24.gov.ua/dronation>.

7 T Zadorozhnyy, 'Zelensky sets 1,000-daily interceptor drones goal amid surging Russian attacks', in *The Kyiv Independent*, 25 July 2025, <https://kyivindependent.com/zelensky-sets-goal-of-1-000-interceptors-per-day-amid-surging-russian-drone-attacks/>.

The USN and the Royal Navy (RN) have recognised the need for cost-effective and technology appropriate counter-UAV systems, for operations against Houthi rebels off the Yemeni coast.[8] Such systems are expected to become standard armament in all warships and even merchant ships. The potential to deploy UAVs in larger numbers has been appreciated by several navies.[9] Examples are:

- **Brazil.** It is trialling UAVs onboard the helicopter carrier NAM *Atlântico* (ex HMS *Ocean*) The navy has previously operated the Insitu Scan Eagle RQ-1 system launched from a portable catapult in *Atlântico*.[10]
- **China.** The People's Liberation Army-Navy (PLA-N's) Type 76 amphibious ship will be UAV capable, while separately the 200 metre experimental aviation ship *Zhong Chuan Zi Hao* is trialling drone operations.[11]
- **Indonesia.** The Tentara Nasional Indonesia Angkatan Laut (TNI-AL), is exploring acquiring and converting the decommissioned aircraft carrier *Giuseppe Garibaldi* into an UAV carrier.[12]
- **Iran.** Its navy has commissioned the 41,000 tonne IRIS *Shahid Bagheri* with a capacity to embark both helicopters and Jas-313 multi-role drones.[13]
- **Türkiye.** In 2024 the Landing Helicopter Dock (LHD) TCG *Anadolu* (of the same class as the Adelaide class LHDs) conducted a trial with Baykar Bayraktar TB3 UAV, with the aircraft launching via the ski-jump.[14]
- **Portugal.** In 2022 Portugal ordered a 7,000 tonne multi-functional naval platform to be named NRP *D. João II*. The amphibious ship is designed to embark UAVs as well as helicopters and should commission in 2026.[15]

While questions remain about the utility of drone carriers and the performance of short-range drones in harsh maritime environments, growing international interest signals a clear trend. As maritime UAVs advance, drone carriers could offer a far cheaper way to achieve localised air control—a capability navies like the RAN currently lack.

---

8 R Ceder, 'US Navy hits drone with HELIOS laser in successful test', in *Navy Times*, 5 February 2025, <https://www.navytimes.com/news/your-navy/2025/02/04/us-navy-hits-drone-with-helios-laser-in-successful-test/>.

9 'Rise of flat-top drone carriers', in *Australian Naval Institute*, 5 April 2025, <https://navalinstitute.com.au/30790-2/>.

10 'Rise of flat-top drone carriers', in *Australian Naval Institute*, 5 April 2025, <https://navalinstitute.com.au/30790-2/>.

11 P Lyons & S Cheung, 'China's Type 076 Amphibious Carrier: What It Does and Why It Matters', in *The Diplomat*, 8 April 2025, <https://thediplomat.com/2025/04/chinas-type-076-amphibious-carrier-what-it-does-and-why-it-matters/>.

12 'Indonesia explores acquiring Italy's decommissioned aircraft carrier Giuseppe Garibaldi for naval drone operations', in *Army Recognition*, 2025, <https://armyrecognition.com/news/navy-news/2025/indonesia-explores-acquiring-italys-decommissioned-aircraft-carrier-giuseppe-garibaldi-for-naval-drone-operations>.

13 T Ozberk, 'Ukraine attacks Sevastopol Naval Base and Kerch Bridge with drones - Naval News', in *Naval News*, , 2023, <https://www.navalnews.com/naval-news/2023/07/ukraine-attacks-sevastopol-naval-base-and-kerch-bridge-with-drones/> [accessed 26 March 2024].

14 T Ozberk, 'BAYRAKTAR TB3 UCAV Completes Four Successful Autonomous Sorties Aboard TCG Anadolu', in *Naval News*, 25 April 2025, <https://www.navalnews.com/naval-news/2025/04/bayraktar-tb3-ucav-completes-four-successful-autonomous-sorties-aboard-tcg-anadolu/>.

15 J Binnie, 'DIMDEX 2024: Portugal orders Damen's new 'drone carrier'', in *Janes*, 7 March 2024, <https://www.janes.com/osint-insights/defence-news/sea/dimdex-2024-portugal-orders-damens-new-drone-carrier>.

Surface Warfare

Turning to surface warfare, in some respects this is the offensive side of the coin. From the latter half of the Cold War, the mainstay of the ADF's surface warfare capability was the Harpoon missile which could be launched from submarines, major surface combatants and three different RAAF aircraft types.

By the early 21st century, however, the range-limited sub-sonic missile had reduced lethality in the face of modern anti-ship missile defence (ASMD) systems. The RAN is now transitioning to a maritime strike capability with the medium-range Tomahawk, short-range range Naval Strike Missile and the shorter range Hellfire missiles embarked in the MH-60R helicopter. Whilst the Tomahawk and naval strike missile do not represent long-range capabilities, they do provide a step change in the RAN's lethality. In addition, the RAAF can deliver the Joint Strike Missile and other shorter-range ordnance. These significant improvements in capability now give either parity with or superiority over other Indo-Pacific navies.

As in the air domain, drones have also made their presence felt. Once again the Ukrainians, by dint of necessity and enterprise, have rapidly become leaders in the development of USVs in the course of the Russo-Ukraine war. The Ukrainian Navy has multiple types of USVs, that they have rapidly evolved. Two examples include the Sea Baby (48 knots, 1000km range, 850kg explosive) and the Magura class (42 knots, 800 km range, 1,000kg explosive) for a unit cost of about $USD250,000.[16] In the war so far, Sea Babies have damaged the Kerch bridge, a corvette and other smaller ships.[17] Magura V USVs, for their part, have sunk one corvette, one patrol ship and a landing ship. Notably, in a first for USVs, larger SAM fitted Magura VIIs have shot down a helicopter and two SU-30SM fighters.[18] Some navies are trialling medium and larger-sized USVs. They range in capabilities and missions, for example:

- **China.** The 58 metres, 500 tonnes, 40 knot *Orca* has a reported range of more than 4,000 nautical miles. It is designed to undertake anti-surface, anti-air and anti-submarine warfare (ASW) missions. The USV is equipped with phased array radars and a vertical launching system (VLS) missile system. It can carry rockets, anti-ship missiles, air defence missiles and remote-control weapon stations.[19]
- **South Korea.** In 2025, the Republic of Korea Navy (ROKN) contracted Hyundai Heavy Industries to develop a concept design for a next-generation combat USV. The ROKN have suggested that it may establish a dedicated unmanned maritime command by the 2040s.[20]

---

16 'Naval Drones', in *United 24*, <https://u24.gov.ua/navaldrones>.

17 'Sea Baby', in *Wikipedia*, <https://en.wikipedia.org/wiki/Sea_Baby>.

18 T Zadorozhnyy, 'Ukrainian sea drones down 2 Russian Su-30 jets near Novorossiysk, military intelligence chief says', in *Kyiv Independent*, 4 May 2025, <https://kyivindependent.com/ukraine-sea-drone-downs-2-russian-su-30-jets-near-novorossiysk-budanov-says/>.

19 R Rahmat, 'Airshow China 2024: China debuts 500 tonne unmanned surface vessel', in *Janes*, 12 November 2024, <https://www.janes.com/osint-insights/defence-news/security/airshow-china-2024-china-debuts-500-tonne-unmanned-surface-vessel>.

20 'HD HHI wins landmark contract from Korean Navy for unmanned vessel', in *Korea Joongang Daily*, , 22 April 2025, <https://koreajoongangdaily.joins.com/news/2025-04-22/business/economy/HD-HHI-wins-landmark-contract-from-Korean-Navy-for-unmanned-vessel/2291192>.

- **Singapore.** The Republic of Singapore Navy (RSN) has in operational service a small number of 17 metre 'MARSEC' USVs, each armed with a machine gun for patrolling in Singapore's congested waterways.[21]
- **US.** The USN's programs for USVs are divided between the Large Unmanned Surface Vehicle (LUSV) and Medium Unmanned Surface Vehicle (MUSV). The USN wants to develop and acquire LUSVs and MUSVs as part of an effort to shift the Navy to a more distributed fleet architecture. This involves spreading the USN's capabilities over more hulls and avoids concentrating much of the fleet's overall capability into a relatively small number of high-value ships (i.e., a mix that avoids putting too many eggs into one basket). The larger USVs will have the ability to act as missile arsenal ships with warships able to expend the USV's missiles in an engagement.[22] The focus is still very much in experimentation with USV Squadron 1 a hub for this activity.
- **Australia.** While Australia is exploring small ISR USVs like the OCIUS Bluebottle,[23] it also plans to acquire a large optionally crewed surface vessel (LOSV) as part of its future combatant fleet in the 2030s. Details remain limited, but it is likely to be based on the US. LUSV program, equipped with 32 VLS cells and designed to operate alongside Hobart and Hunter-class ships.[24]

Undersea Warfare

In the Indo-Pacific region there has been a growing number of both conventional and nuclear-powered submarines among an increasing number of navies (see Table 1).

In terms of conventional submarine technologies there have been two notable propulsion developments. Chronologically, the first was the introduction of 'air-independent' propulsion (AIP) systems such as the Stirling engine. This technology is best employed in a patrol area and enables a submarine to remain submerged for extended periods without having to 'snort' to recharge her batteries. In the region some Indian, Japanese, Chinese, Pakistani and Singaporean boats incorporate AIP technology.

The second development is the transition from lead batteries to variants of lithium-ion batteries. The two most significant improvements are weight reduction and power density. A lithium-ion battery is approximately 55% lighter than a lead battery. In terms of power density, a lead battery develops 30-70 watts/hour/kg,[25] whilst a lithium ion battery is ~300 watts/hour/kg.[26] Solid-state lithium ion phosphate batteries will be approximately 400 watts/hour/kg.[27] There had been some hesitancy to

---

21 G Arthur, 'Singapore USVs begin uncrewed patrols in busy waterways', Naval News, 7 February 2025, <https://www.navalnews.com/naval-news/2025/02/singapore-usvs-begin-uncrewed-patrols-in-busy-waterways/>.

22 R O'Rourke, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, Congressional Research Service, 25 March 2025, <https://crsreports.congress.gov/product/pdf/R/R45757>.

23 'Bluebottle Unmanned Surface Vessels (USV), Australia', in *Naval Technology*, , 2023, <https://www.naval-technology.com/projects/bluebottle-unmanned-surface-vessels-usv-australia/>.

24 Department of Defence, *Independent Analysis into Navy's Surface Combatant Fleet*.

25 'Acid Battery', in *Wikipedia*, <https://en.wikipedia.org/wiki/Lead%E2%80%93acid_battery>.

26 'Thunder and Energy', <https://thundersaidenergy.com/downloads/lithium-ion-batteries-energy-density/#:~:text=(in%20mols).-,Today's%20lithium%20ion%20batteries%20have%20an%20energy%20density%20of%20200,per%20kWh%20of%20energy%20storage>.

27 'Solid State Battery', in *Wikipedia*, <https://en.wikipedia.org/wiki/Solid-state_battery>.

adopt lithium ion batteries in submarines because of concerns over their thermal stability, and indeed the now cancelled RAN Attack-class were to have had lead batteries, in part for this reason. In 2020, however, the Japanese submarine JS *Ōryū,* the eleventh boat of Sōryū-class, incorporated lithium-ion batteries which also replaced its AIP system. While the benefits of the newer batteries will be longer submerged endurance and higher speeds, specific performance benefits are not publicly available. Media reports on the forthcoming Korean Hanwha Ocean-class boats indicate their covert endurance will be three times that of a general diesel-operated submarine boat.[28]

In the Indo-Pacific region more countries have decided to acquire submarines, whilst those that have submarine arms are looking to modernise or expand them. Examples of the former are the Philippines and Thailand. Within the Indo-Pacific region only China, India, Russia and the US have nuclear propelled submarines, with Australia and possibly South Korea to follow suit. Beyond the Indo-Pacific region, Brazil is also actively pursuing nuclear-powered submarines, expecting to develop its first indigenously built nuclear-powered submarine in the early 2030s.[29] SSNs by virtue of their speed and endurance are well suited for offensive anti-surface and land attack operations. It is often forgotten, however, that one of their main roles during the Cold War was ASW. The former US Chief of Naval Operations, Admiral Arleigh Burke, in a chapter in *Problems of Australian Defence*, pointed out the importance of SSNs in the 'counter-submarine' role and wrote,

> The key element of anti-submarine warfare, then, is the conduct of offensive operations, attacking enemy units as close as possible to their points of origin, continuing to hunt down those which may reach the open sea or which were on station before hostilities began, destroying them as far from the defenders' lines of communication as possible.[30]

This approach arguably will remain valid in the 2030s, as it did sixty years earlier. The operating environment will, however, be much more challenging for SSNs with the advent of improved space-based, air and undersea surveillance systems, conventional submarines with much shorter indiscretion rates, and the growing presence of USVs. As in the other warfare domains there is a range of uncrewed underwater vehicles (UUV) that are either entering service or being trialled. The following gives a flavour of the initiatives:

- **Australia.** In 2022 Australia contracted Anduril Industries to provide three 'Ghost Shark' extra large UUVs by 2025.[31] The concept is for these to be deployed from the support ship ADV *Guidance* as well as being air transportable via C-17 aircraft. The Ghost Shark has a ten-day endurance with an operating floor of 6,000 metres. Its missions will include persistent ISR and strike.[32]

---

28 J Choi, 'Hanwha Ocean Attempts Korea's First Submarine Lithium-ion Battery Installation', in *Business Korea*, , 2024, <https://www.businesskorea.co.kr/news/articleView.html?idxno=208807>.

29 'Brazil's Nuclear-Powered Submarine Project Reaches New Milestone', in *Naval News*, , 10 October 2023, <https://www.navalnews.com/naval-news/2023/10/brazils-nuclear-powered-submarine-project-reaches-new-milestone/>.

30 Burke, A.A., "Anti-Submarine Warfare - A Comment", Gelber, H.G., *Problems of Australian Defence*, Oxford University Press, Melbourne, 1970 ,128-129.

31 'Ghost Shark', <https://en.wikipedia.org/wiki/Ghost_Shark_(submarine)>.

32 'VESSEL REVIEW | Ghost Shark – Royal Australian Navy's newest multi-mission autonomous vehicle', in *Baird Maritime*, 2025, <https://www.bairdmaritime.com/security/naval/unmanned-naval-systems/vessel-review-ghost-shark-royal-australian-navys-newest-multi-mission-autonomous-vehicle>.

- **China.** For employment in the South China Sea, China is developing a suite of anti-submarine systems, which collectively are referred to as the "Underwater Great Wall."[33] The program has five main elements: they are passive seabed arrays, active sonars, UUVs, USVs and space based systems Passive arrays include Superconducting Quantum Interference Devices (SQUIDs) to detect the extremely weak magnetic fields of submarines out to a range of about 20kms.[34] There are also trials with laser-equipped satellites to detect submerged submarines, reportedly to a depth of 160 metres.[35]
- **UK.** The RN has introduced a range of autonomous mine countermeasures (MCM) systems into service. It has also commissioned the 4,600 tonne HMS *Stirling Castle* to act as a 'mother ship' for these systems.[36]
- **US.** The US is developing a suite of UUVs. The largest UUVs, classed as XLUUVs, are those of the Orca program. The first batch of six Orcas has started to enter service. These battery/diesel hybrid powered boats will be able to remain at sea for some months. They displace eight tonnes, have a length of 26 metres and maximum speed of eight knots. Their initial payload would be mines. In contrast, the 16 metre Echo Voyager UUV has a surveillance mission. It also has battery/diesel hybrid propulsion enabling it to remain at sea for six months.[37] The US also has a range of smaller torpedo tube launch and recovery (TTL&R) UUVs. In 2024 USS *Delaware* was the first US submarine to deploy with UUVs. They included the Remus UUV, which is capable of surveillance and MCM missions.

---

[33] Weichert, B, 'China Wants to Rule the Seas—It Claims to Have the Most Advanced Technology to Spy on American Subs'.in Popular Mechanics, 2025, <https://www.popularmechanics.com/military/weapons/a63602193/china-submarine-detection/>.

[34] S Sinha, 'China unveils submarine detection tech with 12-mile underwater range', in *Interesting Engineering*, 20 September 2024, <https://interestingengineering.com/military/china-submarine-underwater-surveillance>.

[35] S Sinha, 'China unveils submarine detection tech with 12-mile underwater range', in *Interesting Engineering*, 20 September 2024, <https://interestingengineering.com/military/china-submarine-underwater-surveillance>.

[36] 'RN's new autonomous anti-mine system', in *Australian Naval Institute*, 21 March 2025, <https://navalinstitute.com.au/rns-new-autonomous-anti-mine-system/>.

[37] R O'Rourke, *Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress*, US Congrssional Research Service, 19 December 2024, <https://sgp.fas.org/crs/weapons/R45757.pdf>.

Table 1: Indo-Pacific Submarine Forces [38]

Country	2005	2025	2030	2035
Australia	6 SSG	6 SSG	5-6 SSG	2 SSN 4 SSG
Bangladesh	0	2 SS	2 SS	2 SS
Canada	4 SS	4 SS	4 SS	1+12 SSP 2-3 SS
China	1 SSBN,1 SSB, 4 SSN, 8 SSG, 45 SS	6 SSBN, 6 SSN 48 SS	unknown	unknown
India	16 SS	3 SSBN,1 SSN 16 SS	4 SSBN 24 SS	4 SSBN, 1-2 SSN 24 SS
Indonesia	2 SS	4 SS	4	4
Japan[39][40]	16 SS	24 SS[#]	24 SS	24 SS
Korea, North	51 SS 260 Midget	2 SSB, 20 SS 40 SS Coastal 21 Mini SS	unknown	unknown
Korea, South	9 SS 11 Midget	3 SSB 19 SS[¤]	3 SSB 19 SS	3 SSB 19 SS
Malaysia	0	2 SS	2 SS	4 SS
Myanmar	0	2 SS 1 midget	unknown	unknown

[38] Table 1 is based on data from The World Bank: 'Military Expenditure'.

The figure for Russia is from Korsunskaya and Bryanski.

Taiwan figures from 'The World Factbook: Taiwan', in *CIA*, 2025, <https://www.cia.gov/the-world-factbook/countries/taiwan/>.

[39] 'Japan Submarine Capabilities', in *Nuclear Threat Initiative*, 2024, <https://www.nti.org/analysis/articles/japan-submarine-capabilities/>.

[40] JMSF maintains 22 operational subs & 2 training boats. 12 boats are AIP fitted.

Country	2005	2025	2030	2035
Pakistan	8 SS, 3 Midget	8		
Philippines	0	0	1 SS	2 SS
Russia[41]	5 SSBN, 7 SSN 3 SS	5 SSBN, 7 SSN 3 SS	unknown	unknown
Singapore	4 SS	4 SS	6 SS	6 SS
Taiwan	4 SS	4 SS	6 SS	~ 7 SS
Thailand	0	0	Poss. 3 SS	Poss. 3 SS
United States[42]	14 SSBN 54 SSN	14 SSBN 54 SSN	13 SSBN 57 SSN	12 SSBN ~60 SSN
Vietnam	2 Midget	6 SS	6 SS	6 SS

In addition, smaller UUVs are entering service that can be deployed from submarines through either torpedo tubes, or as in the case of the Swedish A-26 Blekinge Class submarines through a larger flexible payload lock. Some of these USVs are controlled via fibre-optic links and some are for surveillance and mining tasks. Importantly they allow the parent submarines to remain covertly at distance from a focal point.

A potentially important UUV role will be both the cutting of, or the protection of, vital undersea cables. These submarine cables account for over 99% of intercontinental data traffic.[43] Actions allegedly by Russia's shadow fleet in the Baltic and Chinese vessels off Taiwan highlight the vulnerability of these systems and the potentially asset-intensive measures needed to protect them. There has been a range of responses in the face of a growing number of submarines and USVs/UUVs in the Indo-Pacific region. Notably in Australia, Blue Ocean Marine Tech Systems are developing an AI enabled autonomous UUV for persistent surveillance of undersea cables.[44]

Impact of the Cyber Domain

Early naval theorists were often criticised for treating the sea in isolation, overlooking how other domains shape maritime warfare. Sir Julian Corbett, who coined the term 'maritime strategy' - was an exception, stressing the relationship between land power and maritime power. In 2025, the

41 Russian Pacific Fleet 12 SS are AIP fitted.

42 USN total sub force.

43 A Mauldin, 'Do Submarine Cables Account For Over 99% of Intercontinental Data Traffic?', 2023, <https://blog.telegeography.com/2023-mythbusting-part-3>.

44 'Blue Ocean Marine Tech Systems Announces Maritime Partnership to Combat Subsurface Threats', in *Blue Ocean Marine Tech Systems*, 2025, <https://www.blueoceanmts.com/news/maritime-partnership>.

interdependence is even starker: land-based missiles and uncrewed aerial vehicles have defined recent campaigns in the Black and Red Seas, while cyber and space capabilities are now integral to maritime command, sensing and targeting. Any effective contemporary maritime strategy must therefore account for the full spectrum of multi-domain effects.

From the early 2000s, however, with the demise of the Soviet threat and the even greater reliance on satellites, not only for communications, but also for geo-location (through GPS) and command and control, there was a doctrinal change to operate overtly as a standard operating practice. This approach, together with a much higher-level reliance on information and communications technology (ICT) at the tactical, operational and strategic level has greatly increased the importance of the cyberspace. They increased the importance of cyber security to allow for the unfettered use of the electronic spectrum and they also offered opportunities to offensively target an enemy's command systems, sensors and weapons that rely on electronic emissions.

In Australia, these developments are reflected in making the Australian Signals Directorate a statutory Government agency in 2013 and the creation of Cyber Command within the Department of Defence in 2024.[45] In the maritime domain, cyber vulnerabilities of civilian and naval shipping and maritime infrastructure are increasingly exploited. In 2023, Australia launched its 2023-2024 Australian Cyber Security Strategy, which highlights the need to strengthen Australia's maritime cyber security settings, and a focus on a reform agenda tailored to this.

Significantly, in the week before Australia released the 2023 national cyber security strategy, its largest port operator, DP World, was hit by a cyber attack. DP World moves about 40 per cent of Australia's freight. As a result of the cyber attack, which capitalised on a known vulnerability, DP World was forced to shut down operations for about 24 hours, causing 30,000 containers to be stacked up across ports in Sydney, Melbourne, Brisbane and Perth. Although operations resumed after 24 hours, this could have had a dramatic impact on Australia's trade, about 98% of which travels through ports.

Incidents on Ships

The impacts of cyber attacks in the maritime domain are not restricted only to landward facilities, they impact almost all aspects of the maritime industry. The DNV 2023 Maritime Cyber security report stated that according to their research:

> more than six in ten industry professionals expect cyber-attacks to cause ship collisions (60%) and groundings (68%) within the next few years. More than 76 per cent believe a cyber incident is likely to force the closure of a strategic waterway.[46]

Marine cyber risk consultancy CyberOwl's chief executive was quoted in 2021 as saying: 'At the moment we are identifying one new incident a day on average, to give some sense of the scale of this'. Things have likely deteriorated from this point. Reported examples of Cyber attacks include:

- An incident in which bunker surveyors were given access to the computers in an engine control room so they could print documents from a USB stick, which introduced a virus to that system.

---

45 'Joint Capabilities Group', in *Department of Defence*, <https://www.defence.gov.au/about/who-we-are/organisation-structure/joint-capabilities-group>.

46 Christian Parker, 'Maritime professionals warn of insufficient investment in cyber security as risks escalate in the era of connectivity', in *DNV*, 6 June 2023, <https://www.dnv.com/news/2023/maritime-professionals-warn-of-insufficient-investment-in-cyber-security-as-risks-escalate-in-the-era-of-connectivity-244153/>.

- In another incident, a vessel transiting the Strait of Singapore lost two electronic chart display and information systems (ECDIS) navigation networks at the same time on account of a virus and had to fall back on paper charts.

The increasing digitisation of shipping and the rapid expansion of once air gapped networks , being connected to the internet through digitisation of systems and processes is rapidly increasing the risk of cyber attacks from both state and non-state actors.

As ICT and operational technologies (OT) have become critical to safe shipping operations through automation or digital processes, all aspects of the maritime industry have become increasingly vulnerable to cyber attacks.

This threat is further compounded by the tendency of ships and offshore and onshore infrastructure in the maritime industry to operate on legacy software – making them even more vulnerable. A 2022 report by the Australian Strategic Policy Institute found that:

> Various maritime-specific cybersecurity incidents have occurred that have resulted in the malfunctioning of critical control systems, in ships and onshore facilities; the exfiltration of sensitive data that's monetised by criminals, including pirates; the manipulation of systems to allow for trafficking and smuggling activities to occur unnoticed; commercial and military espionage, for instance of ship designs, lading and trading routes; spoofing of navigation systems; and manipulation of identification transmissions.[47]

The maritime sector is thought to lag behind other comparable industries in its level of cyber security maturity. Although this isn't unique to the maritime industry, and is reportedly common practice across many industries, the impacts on the maritime industry are significant, with potential for safety and security threats to manifest.

GPS Interference

The maritime cyber security risk is not just contained to impacting digitised systems onboard ships, or in offshore or onshore facilities. Significant maritime cyber security risks exist through GPS interference, or GPS spoofing. This can take many forms, including interference with GPS in a specific area to interrupt shipping. In 2021 the US issued a maritime advisory about GPS interference stating that,

> Multiple instances of significant GPS interference have been reported worldwide in the maritime domain. This interference is resulting in lost or inaccurate GPS signals affecting bridge navigation, GPS-based timing, and communications equipment. Satellite communications equipment may also be impacted. Over the last six months, areas from which multiple instances have been reported include the eastern and central Mediterranean Sea, the Persian Gulf, and in the vicinity of the Suez Canal.[48]

In addition, there have been cases of onboard manipulation of system by shippers to conceal their illicit activities. It was reported that in 2018 an oil tanker spoofed its GPS data to conceal from authorities a mid-sea transfer of petroleum to a North Korean ship, thereby circumventing UN

---

47 H Le Thu & B Hogeveen, *UK, Australia and ASEAN cooperation for safer seas*, ASPI, 31 March 2022, p. 15, <https://www.aspi.org.au/report/uk-australia-and-asean-cooperation-safer-seas/,>.

48 'Maritime Advisory Issued Concerning GPS Interference', in *Seafarers International Union*, , 22 March 2021, <https://www.seafarers.org/maritime-advisory-issued-concerning-gps-interference/>.

sanctions. The same thing reportedly occurred with an Iranian ship in 2013 off the coast of Malaysia. These tactics are being employed to support a large spectrum of blue crimes, including illegal, unreported and unregulated fishing.

Impact of the Space Domain

The space domain now permeates every layer of maritime operations, turning what was once a relatively self-contained naval battlespace into a vertically integrated, multi-domain contest for information advantage. Persistent, near-real-time satellite ISR shrinks oceanic distances, allowing even medium powers to cue long-range fires with precision and to hold warships at risk far beyond the horizon. Positioning, navigation and timing (PNT) services delivered via global navigation satellite systems have become indispensable for precision strike, uncrewed systems, and routine navigation alike; yet their vulnerability to jamming or spoofing exposes a critical Achilles heel. Consequently, modern maritime strategy must treat assured access to space-enabled ISR and PNT as a prerequisite for sea control and sea denial, while simultaneously investing in passive deception, alternative PNT solutions and electronic-warfare resilience to blunt an adversary's space-based sensing and targeting advantage.

The race for advantage in space is reshaping how navies and air forces share tasks. Weapons that can knock out satellites now come in many forms, so fleet commanders can no longer assume they will always have satellite maps, communications and timing data during a fight. Gigantic commercial networks such as Starlink now carry much of the ADF's traffic, which means Defence must work closely with industry and update the rules that protect these shared systems. Building space tools through Australia, UK and US (AUKUS) Pillar II can help Australia make its own decisions and avoid relying on a single fragile link, but only if government also hardens ground stations, finds more launch options and bakes space thinking into every naval plan. In short, from orbit to ocean, control of space is both the backbone of sea power and a battleground.

* Peter Jones is an adjunct professor at NSG and a retired vice admiral who served in the RAN for 40 years. He is author of two naval biographies and has written extensively on strategic and naval affairs.

Jennifer Parker is an adjunct fellow at NSG UNSW Canberra, with affiliations across various think tanks. She spent over 20 years in the RAN as a warfare officer, has published on a wide range of maritime and defence issues and frequently appears as a commentator in national and international media.

Reference List:

Australian Government, Department of Defence, *National Defence Strategy 2024*, Canberra: Commonwealth of Australia, 2024.

Australian Strategic Policy Institute, *Maritime Cybersecurity: Safeguarding Australia's Interests*, Canberra: ASPI, 2022.

Australian Government, Department of Home Affairs, *2023–2030 Australian Cyber Security Strategy*, Canberra: Commonwealth of Australia, 2023.

DNV, *Maritime Cyber Priority: DNV 2023 Maritime Cyber Security Report,* Høvik: DNV, 2023.

CyberOwl, 'Industry Cyber Risk Report', *CyberOwl Reports*, London, 2021.

U.S. Maritime Administration (MARAD), *Global Positioning System (GPS) Interference Advisory*, Washington D.C.: U.S. Department of Transportation, 2021.

United Nations, *United Nations Convention on the Law of the Sea (UNCLOS),* 10 December 1982, entered into force 16 November 1994.

Corbett, Julian S., *Some Principles of Maritime Strategy*, London: Longmans, Green & Co., 1911.

Burke, Arleigh, 'The Role of Submarines in the Defence of Sea Lines of Communication', in T.B. Millar (ed.), *Problems of Australian Defence*, Canberra: Australian National University Press, 1965.

Anduril Industries, *Ghost Shark XL-UUV Program Overview*, Sydney: Anduril Australia, 2024.

Naval News, 'Ukraine's Sea Baby and Magura V USVs: Lessons for Modern Naval Warfare', *Naval News*, 2024.

Royal Australian Navy, *The Navy and the Nation: 1913–2023*, Canberra: Department of Defence, 2023.

United States Navy, *USV Division 1: Unmanned Surface Vessel Program Overview*, Washington D.C.: U.S. Navy, 2025.

Royal Navy, *Autonomous Mine Countermeasures Capability Program Report*, London: UK Ministry of Defence, 2024.

Republic of Korea Navy, *Future Combat Unmanned Surface Vessel Concept Design Program*, Seoul: ROKN, 2025.

People's Liberation Army Navy, *The Underwater Great Wall Project*, Beijing: PRC Ministry of National Defense, 2024.

Baykar Technologies, *Bayraktar TB3 Naval UAV Flight Trials*, Istanbul: Baykar Defence, 2024.

Czajkowski, J. and Hill, R., 'The Integration of Artificial Intelligence in Maritime Operations', *Naval War College Review*, Vol. 78, No. 3 (2024).

Blue Ocean Marine Tech Systems, *AI-Enabled Undersea Cable Surveillance Initiative*, Perth: Blue Ocean Marine Tech Systems, 2024.

Australian Government, Department of Defence, *Naval Shipbuilding and Sustainment Plan 2024*, Canberra: Commonwealth of Australia, 2024