ISSUE BRIEF
IB/64/26

CENJOWS

THE SILENT AI REVOLUTION BENEATH THE SEAS: AUTONOMOUS SYSTEMS AND THE FUTURE OF MARITIME SECURITY

DR NISHAKANT OJHA

www.cenjows.in

CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future

Victory through Joint Knowledge

CENJOWS

THE SILENT AI REVOLUTION BENEATH THE SEAS: AUTONOMOUS SYSTEMS AND THE FUTURE OF MARITIME SECURITY

Dr Nishakant Ojha is a strategic expert on AI, quantum, and emerging technologies, analysing their impact on defence, intelligence, warfare, and geopolitics and a Chair of Excellence at CENJOWS

Abstract

Artificial intelligence is transforming the maritime domain as significantly as it is transforming the battlefields of Ukraine and the data centres of Silicon Valley, but it is doing so largely out of public view, beneath the waves and along shipping lanes that most people never think about. Over the past three years, a wave of autonomous underwater vehicles (AUVs), uncrewed surface vessels (USVs), and AI-enabled sensor networks has moved from experimental prototypes to operational deployment across navies, coast guards, and port authorities worldwide. At the same time, the very infrastructure these systems are meant to protect, undersea cables, pipelines, and offshore energy assets, has come under sustained, deniable attack, most visibly in the Baltic Sea, where more than a dozen cables and pipelines have been damaged since 2022.[1] This brief examines the technological drivers of this "silent revolution," the emerging threat landscape it responds to, the regulatory and legal frameworks struggling to keep pace, and the policy choices facing governments, alliances, and industry. It concludes that autonomous

maritime systems offer real security gains, persistent surveillance, reduced risk to human crews, and cost-effective mass but that their proliferation is outrunning the legal, ethical, and attribution frameworks needed to govern them responsibly.

Introduction

The ocean floor has quietly become one of the most contested spaces in international security. More than 95 per cent of global internet traffic and trillions of dollars in financial transactions travel through a network of roughly 600 submarine cables, while undersea pipelines carry natural gas and electricity between nations that increasingly view one another with suspicion.[2] For decades, this infrastructure was effectively unguarded, protected less by military force than by its own obscurity and by mariners' general reluctance to interfere with it. That assumption has collapsed. Since Russia's 2022 invasion of Ukraine, a series of cable and pipeline incidents across the Baltic and North Seas, from the Nord Stream pipeline explosions to a string of anchor-drag cable cuts attributed to vessels in Russia's so-called shadow fleet, has convinced NATO governments that undersea infrastructure is now an active front in a broader campaign of hybrid warfare.[3]

The response has been technological as much as diplomatic. Navies, coast guards, and private operators are racing to field a new generation of autonomous systems, AI-enabled AUVs that patrol pipelines and detect intruders, uncrewed surface vessels that provide persistent maritime domain awareness, and swarming drone networks designed to overwhelm an adversary's ability to target a smaller number of expensive, crewed warships.[4] This brief surveys that technological shift, situates it within the broader threat environment driving it, and assesses the governance gaps, legal, ethical, and operational, that policymakers must close if autonomous maritime security is to deliver on its promise without generating new risks of escalation, accidents, or unaccountable violence at sea.

The Technology: Autonomous Systems Above and Below the Waterline

Autonomous maritime systems fall into three broad categories, each maturing at a different pace. Autonomous underwater vehicles (AUVs) operate untethered below the surface, using inertial navigation, sonar, and increasingly onboard AI to map the seabed, inspect pipelines, hunt naval mines, and conduct covert reconnaissance without needing a surface link. At the UDT 2026 exhibition in London, the show floor was described as "dominated by autonomy and intelligence, surveillance and reconnaissance systems," with platforms such as the Greyshark AUV marketed explicitly for pipeline protection, port security, and covert reconnaissance, and capable of splitting tasks among a swarm of units after collectively scanning an area.[5] The U.S. Navy has moved a similar capability toward the operational fleet: in March 2026, L3Harris received a Defence Innovation Unit contract to deliver a torpedo-tube launch-and-recovery system that lets submarines deploy and retrieve Iver4 900 AUVs for intelligence, mine detection, and seabed warfare missions without surfacing.[6]

Uncrewed surface vessels (USVs) operate on the water's surface and have become the most visible face of naval autonomy. The U.S. Navy's Medium Unmanned Surface Vessel (MUSV) program, part of a broader "Golden Fleet" initiative, selected seven companies in May 2026 to build prototypes required to travel 2,500 nautical miles at 25 knots while carrying a 25-ton payload, operate day and night autonomously, and, notably, run in a fully passive mode with no radio-frequency emissions when commanded.[7] The Navy has stated an ambition to field roughly 30 such vessels in the Indo-Pacific by 2030 as part of a much larger unmanned fleet, and INDOPACOM's commander has publicly championed a "hellscape" concept in which swarms of autonomous, low-cost vessels create a defensive barrier against a potential Chinese assault on Taiwan.[8] Complementing these larger platforms, small USVs such as the Global Autonomous Reconnaissance Craft have already been organised into dedicated Navy squadrons, and industry has begun advertising "advanced swarm behaviours" as a standard feature of next-generation designs.[9]

AI-enabled sensor and coordination networks are the connective tissue that make the first two categories more than isolated tools. Modern autonomy stacks fuse sonar, radar, electro-optical, and acoustic data in real time, allowing individual platforms to conduct automatic target recognition and enabling coordinated swarm behaviour in which multiple uncrewed vehicles share situational awareness and divide surveillance or strike tasks among themselves.[10] Port operators have adopted parallel technology for defensive purposes: Ocean Aero's Triton autonomous underwater and surface vehicle, for example, is a solar-powered platform that can operate for up to thirty days and has been adopted by the Port of Gulfport in Mississippi and, through a U.S. donation, by the Philippine Navy to strengthen maritime domain awareness against illegal activity in contested waters.[11] Market analysts now estimate that the broader unmanned underwater vehicle market will grow from roughly $6.9 billion in 2026 to more than $19 billion by 2031, driven overwhelmingly by naval modernisation and critical-infrastructure protection requirements.[12]

The Threat Landscape: Undersea Infrastructure Under Siege

The technological build-out described above did not occur in a vacuum; it is a direct response to a documented and escalating pattern of undersea sabotage. Since late 2023, at least eleven undersea cables and pipelines have been damaged in the Baltic Sea alone, with seven of those incidents occurring in the compressed window between November 2024 and January 2025.[13] The pattern is not confined to accidents. Investigators have repeatedly traced damage to vessels dragging anchors across the seabed, a technique that is inexpensive, deniable, and exceptionally difficult to prosecute, since establishing intent at sea is legally demanding and the vessels involved are frequently reflagged, ageing tankers operating outside normal regulatory scrutiny.[14]

Case Study: The Baltic Sea

The Baltic has become, in the words of one recent analysis, "ground zero" for undersea infrastructure sabotage.[15] The timeline is illustrative: the Nord Stream pipelines were destroyed in September 2022; the Balticonnector gas pipeline and an Estonia-Sweden data cable were damaged in October 2023; the BCS East-West Interlink and C-Lion1 cables were both severed within twenty-four hours of one another in November 2024, with suspicion centered on the Chinese-flagged vessel Yi Peng 3; the Estlink 2 power cable and four telecom lines were cut on Christmas Day 2024, leading Finland to seize the tanker Eagle S; and on the final day of 2025, Finnish authorities intercepted the vessel Fitburg after it allegedly severed a Helsinki-Tallinn data cable, prompting a rapid mobilization of the Finnish Border Guard, Defense Forces, and national leadership.[16] Analysts increasingly describe these incidents not as a series of accidents but as a deliberate campaign connected to Russia's so-called shadow fleet, the network of ageing, opaquely owned tankers originally assembled to evade sanctions on Russian oil exports, which now doubles as a platform for cable sabotage and drone overflight of NATO military and airport facilities.[17]

NATO's response has itself relied heavily on autonomy and persistent surveillance. In January 2025, alliance members launched Baltic Sentry, adding patrol vessels, aircraft, and naval drones to an existing multinational task force, Combined Task Force Baltic, whose mission includes continuous monitoring of undersea installations and shipping lanes.[18] Yet officials involved in the effort are candid about its limits. A Danish naval officer coordinating the task force noted that "the Baltic Sea is bigger than it seems" and that response to any given incident remains the legal responsibility of the coastal state rather than NATO itself, a jurisdictional gap that autonomous sensing can help close but cannot, by itself, resolve.[19] Analysts also caution that the maritime picture is incomplete without attention to cable landing stations, the fixed, shore-based facilities where undersea cables connect to terrestrial networks, which have historically been treated as ordinary telecom infrastructure rather than as strategic assets requiring the same protection as the cables themselves.[20] The problem is not confined to Europe. Analysts tracking undersea cable security note comparable concerns in the Taiwan Strait and the Red Sea, where a single 2025 anchor-drag incident degraded cloud connectivity across South Asia and produced an estimated $3.5 billion in economic disruption.[21] Taiwan, the Philippines, Australia, and other Indo-Pacific states have each begun diversifying cable routes and investing in undersea monitoring in response to similar sabotage concerns linked to Chinese state and irregular maritime actors.[22]

State and Institutional Responses

The United States: From Replicator to the "Golden Fleet"

The Pentagon's Replicator initiative, launched in 2023, set out to field thousands of "attritable" autonomous systems across domains within roughly two years, explicitly framed as a way to offset China's numerical advantage in the Indo-Pacific by imposing a costly targeting problem on any adversary rather than concentrating risk in a small number of expensive, crewed platforms.[23] That logic has since matured into the Navy's Golden Fleet initiative, which folds together the medium and large uncrewed surface vessel programs and has secured close to $5 billion in the 2026 Reconciliation Act, including $2.1 billion earmarked specifically for medium uncrewed surface vessels.[24] The Navy has also demonstrated the unglamorous but essential logistics needed to sustain a genuinely autonomous fleet: in April 2026, the oiler USNS Guadalupe completed the first autonomous astern refuelling of an MUSV at sea, building on DARPA's earlier NOMARS demonstration of the uncrewed vessel Defiant.[25] Officials emphasise that the Indo-Pacific's vast distances make the concentrated drone warfare seen in the Black Sea and Red Sea a poor direct analogy, requiring more creative, distributed employment of autonomous platforms across a wider theatre.[26]

NATO and the European Union

Beyond Baltic Sentry, the European Commission has advanced a Joint Communication on submarine cable security, focusing on prevention, detection, response, recovery, and deterrence, alongside funding for Regional Cable Hubs to monitor threats and coordinate resilience investments between 2025 and 2026.[27] European sovereign-cloud spending is projected to more than triple over the same period, reflecting growing unease about dependence on a small number of hyperscale providers and undersea chokepoints for both connectivity and cloud computing capacity.[28]

Allied and Partner Navies

Autonomous maritime security is not solely a great-power project. The Philippine Navy has begun integrating U.S.-donated Triton autonomous underwater and surface vehicles into its newly acquired offshore patrol vessels, citing the need to expand operational reach and detect illegal maritime activity in the contested waters of the South China Sea.[29] Commercial shipbuilders, including Kongsberg, Textron, and Huntington Ingalls, are simultaneously marketing AUV and USV lines explicitly for mine countermeasures, seabed security, and distributed sensing missions to navies worldwide, reflecting a broader shift in which autonomy is becoming a standard line item in naval modernisation budgets rather than an experimental add-on.[30]

The Legal and Regulatory Frontier

Governance of autonomous maritime systems is only beginning to catch up with their deployment. The most significant recent milestone came on May 22, 2026, when the International Maritime Organisation's Maritime Safety Committee adopted the first global Code of Safety for Maritime Autonomous Surface Ships, the MASS Code, following nearly a decade of multilateral negotiation.[31] The Code establishes a goal-based framework requiring autonomous and remotely operated commercial vessels to meet safety, security, and environmental standards equivalent to conventional crewed ships, and it defines four levels of autonomy ranging from decision-support automation with crew aboard to fully autonomous decision-making with no crew at all.[32] Crucially, the Code entered into force on July 1, 2026, on a voluntary basis, beginning what the IMO terms an Experience-Building Phase that will run until at least 2028, after which a mandatory version is expected to be adopted by 2030 and enter into force in 2032.[33] The Code currently applies only to large, internationally trading cargo ships regulated under SOLAS, not to naval or security vessels, leaving the fastest-growing segment of maritime autonomy, uncrewed military and security platforms, entirely outside its scope.[34]

That gap matters because the law of the sea, more broadly, was not written with autonomous or deniable actors in mind. Legal scholars note that the UN Convention on the Law of the Sea provides only a basic framework for protecting submarine cables, with jurisdiction limited within exclusive economic zones, serious practical difficulty in investigating sabotage once a suspect vessel departs coastal waters, and reliance in places on an 1884 convention never designed for an era of AI-directed drones and deniable proxy vessels.[35] The result is what one Congressional Research Service report on U.S. Navy unmanned vessel programs frames as an ongoing oversight challenge: lawmakers must decide not only how many autonomous vessels to fund, but how to ensure the reliability of their propulsion and navigation systems for long transoceanic deployments and how mature their autonomous decision-making really is before they are entrusted with weapons or used in contested waters.[36] Absent a binding international framework for uncrewed security and naval vessels comparable to the MASS Code for commercial shipping, individual states and alliances are left to develop rules of engagement, attribution standards, and use-of-force doctrine for autonomous platforms largely on their own, a recipe for inconsistent practice and, potentially, dangerous miscalculation between rival naval powers operating uncrewed systems in the same contested waters.

Strategic and Ethical Challenges

Four interlocking challenges deserve particular attention from policymakers.

- **Attribution remains the central unsolved problem.** Even where autonomous sensor networks can detect an anomaly in real time, proving state responsibility for undersea sabotage remains extraordinarily difficult. Investigations into the Baltic cable incidents have repeatedly stalled or collapsed in court for lack of provable intent, as when a Finnish court dismissed the case against the Eagle S tanker's crew in October 2025 after prosecutors failed to establish that the damage was deliberate rather than negligent. [2] Better sensing generates more evidence, but it does not by itself solve the deeper legal and diplomatic problem of assigning responsibility to a state operating through ostensibly commercial, reflagged proxies.
- **Autonomy and the use of force raise unresolved questions of human control.** As uncrewed platforms move from surveillance toward vessels capable of carrying containerised weapons, a stated design goal for some next-generation USVs, the degree of human oversight required before such a system can employ lethal force becomes a pressing ethical and legal question.[37] Existing debates over autonomous weapons systems in international humanitarian law apply with particular force at sea, where communications latency, jamming, and the deliberate use of passive, emissions-silent modes can complicate real-time human supervision of an armed autonomous vessel.[38]

- **Swarming and mass autonomy could lower the threshold for miscalculation.** Concepts such as the U.S. Indo-Pacific "hellscape" are explicitly designed to complicate an adversary's targeting calculus by presenting large numbers of low-cost, distributed platforms rather than a few high-value ships.[39] That same logic, however, multiplies the number of autonomous systems operating in contested or ambiguous waters, increasing the probability of an unintended encounter, collision, or engagement between rival autonomous platforms that neither side intended to escalate.
- **Dual-use proliferation is accelerating faster than governance.** The same AI-enabled autonomy stacks marketed for port security and pipeline inspection, automatic target recognition, swarm coordination, and long-endurance solar power are directly transferable to covert reconnaissance and, with modest modification, to attack roles.[40] With the underwater vehicle market alone projected to nearly quadruple by the early 2030s, driven by both defence and commercial demand, the range of state and non-state actors with access to sophisticated autonomous maritime capability is set to expand considerably, even as the international rules governing military and security applications of that technology remain nascent.[41]

Policy Recommendations

Based on the trends documented above, this brief offers five recommendations for governments, alliances, and industry stakeholders.

- **Extend a MASS-style safety and accountability framework to security and naval autonomous vessels.** The IMO's MASS Code offers a workable template, goal-based standards, phased mandatory adoption, and an experience-building period, but currently excludes the naval and security platforms driving the fastest growth in maritime autonomy.[42] NATO, allied navies, and interested coastal states should begin parallel work now on shared technical and behavioural standards for uncrewed security vessels, rather than waiting for the commercial MASS Code's scope to expand organically.

- **Harden cable landing stations and treat them as critical infrastructure, not commercial telecom facilities.** Because landing stations are fixed, geographically concentrated, and often under-secured relative to the cables they connect to, they represent a higher-value, lower-cost target than the cables themselves; national governments should mandate physical security standards, backup power, and cyber-defence requirements comparable to those applied to energy grids.[43]
- **Invest in persistent, low-cost autonomous sensing as a deterrence and attribution tool, not only a response tool.** Widespread deployment of AUVs and seabed sensor networks along vulnerable cable corridors can shift the burden of proof toward continuous monitoring rather than after-the-fact forensic investigation, improving the odds of real-time attribution even where prosecution remains difficult.[44]
- **Establish clear, publicly stated rules of engagement and human-control requirements for armed autonomous maritime systems.** As uncrewed vessels move toward weapons-carrying roles, allied navies should adopt and publish baseline principles for human oversight of lethal engagement decisions, both to guard against accidents and to provide a normative benchmark that other states can be pressed to match.[45]
- **Strengthen multilateral mechanisms for joint investigation and coordinated response to undersea sabotage.** Structures like Combined Task Force Baltic demonstrate the value of pooled surveillance and rapid multinational response, but officials involved acknowledge persistent gaps in legal authority and geographic coverage; broadening such arrangements and extending analogous cooperation to the Indo-Pacific would reduce the advantage that deniable, single-vessel sabotage currently enjoys over dispersed, jurisdictionally fragmented defenders.[46]

Conclusion

The autonomous systems now spreading across the world's seabeds and sea lanes represent a genuine and largely irreversible shift in how maritime security will be practised for decades to come. They offer real advantages: persistent, low-cost surveillance of vast undersea infrastructure that no crewed fleet could realistically monitor around the clock, reduced risk to human sailors in contested or mined waters, and a credible means of imposing costs and complexity on adversaries who might otherwise enjoy a decisive numerical advantage. But the same qualities that make these systems attractive, their deniability, their proliferation across state and commercial actors alike, and the speed with which AI-enabled autonomy is advancing relative to the law also make them a source of new risk. The Baltic Sea has already demonstrated what happens when technology, geopolitical tension, and legal ambiguity intersect: a sustained campaign of undersea sabotage that has proven strikingly difficult to attribute, prosecute, or deter through existing frameworks. The IMO's adoption of the MASS Code in 2026 shows that international consensus on autonomous maritime governance is achievable, but its exclusion of security and naval vessels leaves the most consequential category of autonomous systems effectively unregulated at the international level. Closing that gap through extended safety codes, hardened infrastructure, transparent rules of engagement, and stronger multilateral investigative cooperation will determine whether the silent revolution beneath the seas strengthens maritime security or simply relocates its most dangerous uncertainties to a domain the public rarely sees.

DISCLAIMER

The paper is the author's individual scholastic articulation and does not necessarily reflect the views of CENJOWS, the Defence forces or the Government of India. The author certifies that the article is original in content, unpublished, and it has not been submitted for publication/ web upload elsewhere and that the facts and figures quoted are duly referenced, as needed and are believed to be correct.

ENDNOTES

[1] Jones, Bruce D. "Seabed Zero: Baltic Sabotage and the Global Risks to Undersea Infrastructure." Bulletin of the Atomic Scientists, February 13, 2026. https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/.

[2] Henry M. Jackson School of International Studies. "Baltic Sea Undersea Cable Security." University of Washington, 2025. https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/.

[3] Armed Conflict Location & Event Data Project (ACLED). "Russia's Shadow Fleet Presents a Sustained Hybrid War Threat at Sea." May 22, 2026. https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea.

[4] Hill, John. "UDT 2026: Underwater Systems on Display." Naval Technology, April 15, 2026. https://www.naval-technology.com/news/udt-2026-underwater-systems-on-display/.

[5] Ibid

[6] L3Harris Technologies. "L3Harris to Provide Autonomous Underwater Capability for US Navy Submarines." News release, March 25, 2026. https://www.l3harris.com/newsroom/press-release/2026/03/l3harris-provide-autonomous-underwater-capability-us-navy-submarines.

[7] Barrett, Claire. "US Navy Selects Companies for At-Sea MUSV Prototype Testing." Navy

Times, June 2, 2026. https://www.navytimes.com/news/your-navy/2026/06/02/us-navy selects-companies-for-at-sea-musv-prototype-testing/. See also LaGrone, Sam. "Navy Selects 7 MUSV Designs to Enter Prototype Phase." USNI News, May 22, 2026. https://news.usni.org/2026/05/22/navy-selects-7-musv-designs-to-enter-prototype-phase.

[8] Navy to Deploy Thousands of Unmanned Surface Vessels to the Indo-Pacific by 2030." USNI News, April 21, 2026. https://news.usni.org/2026/04/21/navy-to-deploy-thousands-of-unmanned-surface-vessels-to-the-indo-pacific-by-2030.

[9] Lawrence, Drew F. "Navy Stands Up New Robo-Ship Squadron as Pentagon Pursues Replicator Systems." DefenseScoop, May 20, 2024. https://defensescoop.com/2024/05/20/navy-unmanned-surface-vessel-squadron-three-usvron-established/. See also "U.S. Navy Explores Low-Cost Unmanned Combat Vessels with Textron's MMUSV." Army Recognition, January 14, 2026. https://www.armyrecognition.com/news/navy-news/2026/u-s-navy-explores-low-cost-unmanned-combat-vessels-with-textrons-mmusv.

[10] Hill, John. "UDT 2026: Underwater Systems on Display." Naval Technology, April 15, 2026. https://www.naval-technology.com/news/udt-2026-underwater-systems-on-display/.

[11] Autonomous Vehicles Solve (and Create) Problems for Ports." Marine Technology News, June 22, 2026. https://www.marinetechnologynews.com/news/autonomous-vehicles-solve-create-663595. See also "Unmanned Autonomous Platforms to Beef Up Navy's Security Capabilities." GlobalSecurity.org, June 2026. https://www.globalsecurity.org/military/library/news/2026/06/mil-260625-pna03.htm.

[12] "Unmanned Underwater Vehicles Market to Reach USD 8.72 Billion by 2030, Growing at 8.0% CAGR." MarketsandMarkets, July 9, 2026. https://www.globenewswire.com/news-release/2026/07/09/3324960/0/en/Unmanned-Underwater-Vehicles-Market-to-Reach-USD-8-72-Billion-by-2030-Growing-at-8-0-CAGR-Says-MarketsandMarkets.html.

[13] Henry M. Jackson School of International Studies. "Baltic Sea Undersea Cable Security." University of Washington, 2025. https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/. See also "Cable Danger: Look Beyond the Sea to the Shore." Center for European Policy Analysis, May 18, 2026. https://cepa.org/article/cable-danger-look-beyond-the-sea-to-the-shore/.

[14] "Timeline of Suspected Underwater Sabotage in Baltic Sea." gCaptain, January 4, 2026. https://gcaptain.com/timeline-of-suspected-underwater-sabotage-in-baltic-sea/.

[15] Jones, Bruce D. "Seabed Zero: Baltic Sabotage and the Global Risks to Undersea Infrastructure." Bulletin of the Atomic Scientists, February 13, 2026. https://thebulletin.org/2026/02/seabed-zero-baltic-sabotage-and-the-global-risks-to-undersea-infrastructure/.

[16] "Timeline of Suspected Underwater Sabotage in Baltic Sea." gCaptain, January 4, 2026. https://gcaptain.com/timeline-of-suspected-underwater-sabotage-in-baltic-sea/.

[17] Armed Conflict Location & Event Data Project (ACLED). "Russia's Shadow Fleet Presents a Sustained Hybrid War Threat at Sea." May 22, 2026. https://acleddata.com/report/russias-shadow-fleet-presents-sustained-hybrid-war-threat-sea.

[18] "How the Baltic Sea Nations Have Tackled Suspicious Cable Cuts." Atlantic Council Issue Brief, November 26, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/.

[19] "How the Baltic Sea Nations Have Tackled Suspicious Cable Cuts." Atlantic Council Issue Brief, November 26, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/.

[20] "Cable Danger: Look Beyond the Sea to the Shore." Center for European Policy Analysis, May 18, 2026. https://cepa.org/article/cable-danger-look-beyond-the-sea-to-the-shore/.

[21] Lawrence, Drew F. "Navy Stands Up New Robo-Ship Squadron as Pentagon Pursues Replicator Systems." DefenseScoop, May 20, 2024. https://defensescoop.com/2024/05/20/navy-unmanned-surface-vessel-squadron-three-usvron-established/.

[22] Guha Roy, Angana. "Under Sea Cables: Veiled Threats in Hybrid Warfare." Global South Forum, 2026. https://www.globalsouthforum.org/article/under-sea-cables-veiled-threats-in-hybrid-warfare.

[23] Lawrence, Drew F. "Navy Stands Up New Robo-Ship Squadron as Pentagon Pursues Replicator Systems." DefenseScoop, May 20, 2024. https://defensescoop.com/2024/05/20/navy-unmanned-surface-vessel-squadron-three-usvron-established/.

[24] Ceder, Riley. "US Navy Launches New Golden Fleet-Era USV Program, Terminates Old One." Navy Times, March 27, 2026. https://www.navytimes.com/news/your-navy/2026/03/26/us-navy-launches-new-golden-fleet-era-usv-program-terminates-old-one/.

[25] Navy to Deploy Thousands of Unmanned Surface Vessels to the Indo-Pacific by 2030." USNI News, April 21, 2026. https://news.usni.org/2026/04/21/navy-to-deploy-thousands-of-unmanned-surface-vessels-to-the-indo-pacific-by-2030.

[26] Lawrence, Drew F. "Navy Stands Up New Robo-Ship Squadron as Pentagon Pursues Replicator Systems." DefenseScoop, May 20, 2024. https://defensescoop.com/2024/05/20/navy-unmanned-surface-vessel-squadron-three-usvron-established/.

[27] Guha Roy, Angana. "Under Sea Cables: Veiled Threats in Hybrid Warfare." Global South Forum, 2026. https://www.globalsouthforum.org/article/under-sea-cables-veiled-threats-in-hybrid-warfare.

[28] Guha Roy, Angana. "Under Sea Cables: Veiled Threats in Hybrid Warfare." Global South Forum, 2026. https://www.globalsouthforum.org/article/under-sea-cables-veiled-threats-in-hybrid-warfare.

[29] "Unmanned Autonomous Platforms to Beef Up Navy's Security Capabilities." GlobalSecurity.org, June 2026. https://www.globalsecurity.org/military/library/news/2026/06/mil-260625-pna03.htm.

[30] "KONGSBERG Showcases AUV Technology at CANSEC 2026." Marine Technology News, May 26, 2026. https://www.marinetechnologynews.com/news/kongsberg-showcases-technology-cansec-662671.

[31] International Maritime Organization. "IMO Adopts First Global Code for Autonomous Ships." Press briefing, May 22, 2026. https://www.imo.org/en/mediacentre/pressbriefings/pages/imo-adopts-mass-code.aspx.

[32] "IMO Adopts International Safety Code for Autonomous Shipping." Hill Dickinson. Accessed July 2026. https://www.hilldickinson.com/our-view/articles/imo-adopts-international-safety-code-for-autonomous-shipping/.

[33] "IMO Adopts MASS Code: The Autonomous Ship Moves from Drawing Board to Regulated Reality." gCaptain, June 1, 2026. https://gcaptain.com/imo-adopts-mass-code-the-autonomous-ship-moves-from-drawing-board-to-regulated-reality/.

[34] "IMO Adopts International Safety Code for Autonomous Shipping." Hill Dickinson. Accessed July 2026. https://www.hilldickinson.com/our-view/articles/imo-adopts-international-safety-code-for-autonomous-shipping/.

[35] Instituto Español de Estudios Estratégicos. "Critical Infrastructure in the Context of Hybrid Warfare." 2026. https://www.defensa.gob.es/documents/2073105/3154532/ieee2026-Submarine-cables-Baltic-Research03.pdf.

[36] Congressional Research Service. Navy Large Unmanned Surface Vessels (USVs): Background and Issues for Congress. R45757. Washington, DC: Library of Congress, 2026. https://www.congress.gov/crs-product/R45757.

[37] "U.S. Navy Explores Low-Cost Unmanned Combat Vessels with Textron's MMUSV." Army Recognition, January 14, 2026. https://www.armyrecognition.com/news/navy-news/2026/u-s-navy-explores-low-cost-unmanned-combat-vessels-with-textrons-mmusv.

[38] Barrett, Claire. "US Navy Selects Companies for At-Sea MUSV Prototype Testing." Navy Times, June 2, 2026. https://www.navytimes.com/news/your-navy/2026/06/02/us-navy-selects-companies-for-at-sea-musv-prototype-testing/.

[39] "Navy to Deploy Thousands of Unmanned Surface Vessels to the Indo-Pacific by 2030." USNI News, April 21, 2026. https://news.usni.org/2026/04/21/navy-to-deploy-thousands-of-unmanned-surface-vessels-to-the-indo-pacific-by-2030.

[40] Hill, John. "UDT 2026: Underwater Systems on Display." Naval Technology, April 15, 2026. https://www.naval-technology.com/news/udt-2026-underwater-systems-on-display/.

[41] "Autonomous Underwater Vehicles (AUV) Emerging as Fastest-Growing Segment in Naval Defense Tech." Newswire, July 9, 2026. https://www.newswire.ca/news-releases/autonomous-underwater-vehicles-auv-emerging-as-fastest-growing-segment-in-naval-defense-tech-898344155.html.

[42] "IMO Adopts MASS Code: The Autonomous Ship Moves from Drawing Board to Regulated Reality." gCaptain, June 1, 2026. https://gcaptain.com/imo-adopts-mass-code-the-autonomous-ship-moves-from-drawing-board-to-regulated-reality/.

[43] "Cable Danger: Look Beyond the Sea to the Shore." Center for European Policy Analysis, May 18, 2026. https://cepa.org/article/cable-danger-look-beyond-the-sea-to-the-shore/.

[44] Hill, John. "UDT 2026: Underwater Systems on Display." Naval Technology, April 15, 2026. https://www.naval-technology.com/news/udt-2026-underwater-systems-on-display/.

[45] "U.S. Navy Explores Low-Cost Unmanned Combat Vessels with Textron's MMUSV." Army Recognition, January 14, 2026. https://www.armyrecognition.com/news/navy-news/2026/u-s-navy-explores-low-cost-unmanned-combat-vessels-with-textrons-mmusv.

[46] "How the Baltic Sea Nations Have Tackled Suspicious Cable Cuts." Atlantic Council Issue Brief, November 26, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/how-the-baltic-sea-nations-have-tackled-suspicious-cable-cuts/.