

OCTOBER 2026

Capturing National Security Benefits from Offshore Wind

AUTHORS

Allegra Dawes

Emily Harding

Julia Dickson

Aosheng Pusztaszeri

Joseph Majkut

A Report of the CSIS Energy Security and Climate Change Program and Intelligence, National Security, and Technology Program

CSIS | CENTER FOR STRATEGIC &
INTERNATIONAL STUDIES

OCTOBER 2026

Capturing National Security Benefits from Offshore Wind

AUTHORS

Allegra Dawes

Emily Harding

Julia Dickson

Aosheng Pusztaszeri

Joseph Majkut

A Report of the CSIS Energy Security and Climate Change Program and Intelligence, National Security, and Technology Program

© 2026 by the Center for Strategic and International Studies.

All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means without permission in writing from the Center for Strategic and International Studies (CSIS). CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

Center for Strategic & International Studies
1616 Rhode Island Avenue, NW
Washington, DC 20036
202-887-0200 | www.csis.org

Cover: Ian Dyball/Adobe Stock

Contents

Acknowledgments	V
Acronyms and Abbreviations	VI
Introduction	1
<i>Offshore Wind in the United States</i>	1
The Evolving Threat Landscape in the Maritime Domain	4
<i>Maritime and Subsea Infrastructure Is Increasingly Vulnerable</i>	4
<i>Advances in Autonomous Systems Are Expanding Threats</i>	5
<i>Maritime Threats Are Not Limited to State Actors</i>	5
<i>The Maritime Domain Is Growing Harder to Monitor with Traditional Surveillance</i>	6
Current U.S. Approach to Early Warning and Detection of Maritime Threats	7
<i>Department of Homeland Security</i>	7
<i>The U.S. Navy</i>	8
Offshore Energy Infrastructure as a Potential Force Multiplier for Surveillance	10
<i>The Strategic Positioning of Offshore Wind Infrastructure</i>	11
<i>Expanding Offshore Monitoring with Distributed Acoustic Sensing</i>	12
<i>Moving to an Integrated Sensing Network</i>	12
<i>Longer-Term Models: Offshore Wind Security Hubs</i>	13
Security Risks and Their Mitigation	14
Europe as a Test Case	16
<i>Multilateral Efforts</i>	16
<i>Country Models</i>	17
<i>Poland: Mandatory Military Integration</i>	17
<i>Belgium: Civilian Data Sharing Without Militarization</i>	18
<i>The Netherlands: Institutional Coordination and Non-Price Criteria</i>	18
<i>Norway: Testing to Validate Surveillance Methods for Maritime Infrastructure Protection</i>	18
<i>United Kingdom: Addressing Radar Interference While Advancing Security</i>	19

Recommendations	21
<i>Establish Clear Lines of Ownership and Obligation for Dual-Use Offshore Wind Infrastructure</i>	21
<i>Incorporate National Security Enhancement into the Existing Offshore Wind Review Process</i>	22
<i>Strengthen Co-funding Mechanisms for Dual-Use Technologies</i>	23
<i>Build Regional Collaboration on Shared Infrastructure and Sensing Zones</i>	24
Conclusion	25
Appendix: Ocean Zones and Maritime Infrastructure	26
About the Authors	28
About CSIS	30
Endnotes	31

Acknowledgments

The authors would like to extend their gratitude to the roundtable participants and interviewees for their generous contributions. The authors would also like to thank Kharle Wu and Julia Huh for their design expertise.

This report is made possible by the support from The Pew Charitable Trusts.

Acronyms and Abbreviations

AIS	Automatic identification system
AMO	Air and Marine Operations
AMOC	Air and Marine Operations Center
BOEM	Bureau of Ocean Energy Management
CBP	Customs and Border Protection
Clearinghouse	Department of Defense Military Aviation and Installation Assurance Siting Clearinghouse
DAS	Distributed acoustic sensing
DASA	UK Defence and Security Accelerator
DESNZ	UK Department for Energy Security and Net Zero
DHS	Department of Homeland Security
DOD	Department of Defense
DOI	Department of the Interior
DSTL	UK Defence Science and Technology Laboratory
GW	Gigawatts
MOD	Poland Ministry of National Defence
NM	Nautical miles
PACSD	Power and Communication, Sensor, Defense
PBNI	Programme for the Protection of North Sea Infrastructure
TARS	Tethered Aerostat Radar Systems
TMSS	Tactical Maritime Surveillance System
UAS	Unmanned aerial system

UNCLOS	United Nations Convention on the Law of the Sea
USV	Unmanned surface vessels
UUV	Unmanned underwater vehicles

Introduction

Offshore energy infrastructure—from deep-water oil and gas platforms sited over 100 miles from shore to wind farms that sit 15 miles out—has made the ocean a theater of competing claims among energy developers, national security agencies, shipping interests, fisheries, and coastal communities.¹ For offshore wind infrastructure, this shared use often raises national security concerns. But shared use does not have to mean competing use.

The maritime threat environment is changing in ways that make collaboration essential. Advances in autonomous vehicles, drones, and related technologies mean maritime infrastructure is easier to reach and harder to defend. Civilian infrastructure is now an inseparable component of national security. These dynamics create a need for better, persistent, and distributed tools to enhance maritime domain awareness. Once thought a hindrance, the turbines, platforms, and subsea cables built for one purpose can now be a force multiplier for another; they have moved from obstacle to opportunity in extending the reach of surveillance.

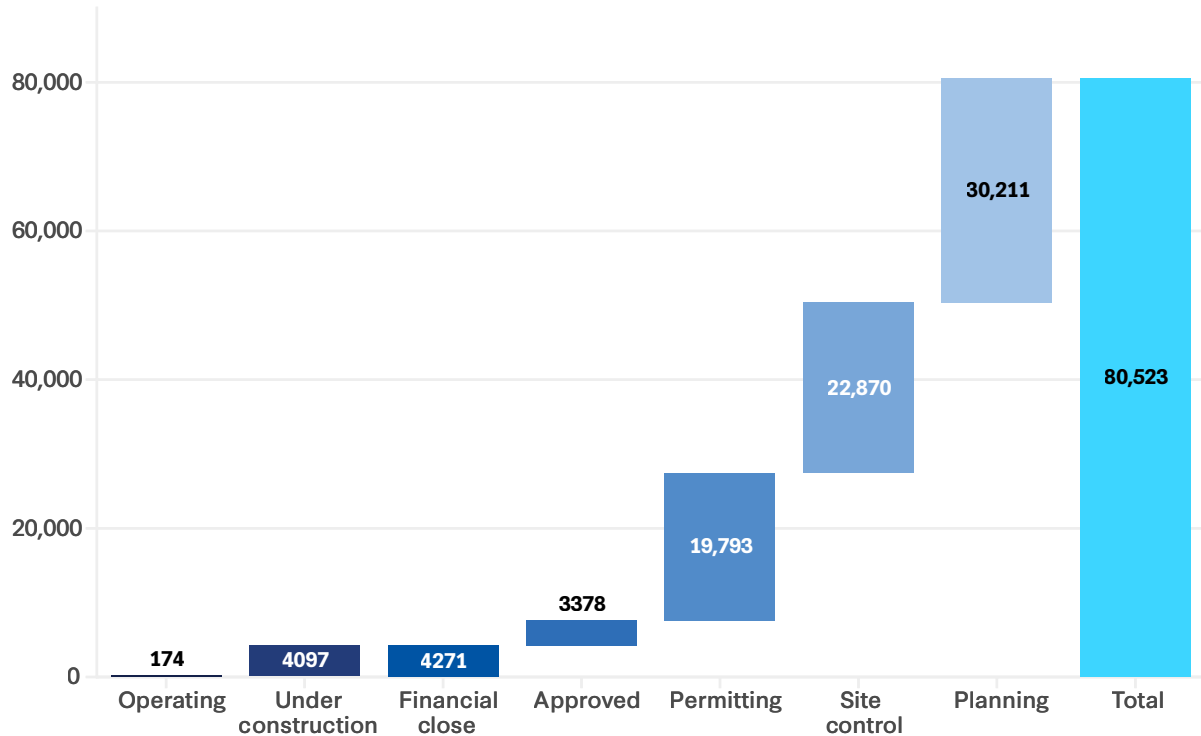
The United States has a compelling interest in managing its ocean resources in ways that balance energy needs, protection of natural resources, and national security. Where those interests reinforce rather than compete with one another, the same infrastructure can serve all of these goals.

Offshore Wind in the United States

U.S. wind generation is at a crossroads. The first utility-scale offshore wind farm in the country, the 132-megawatt South Fork Wind project, began delivering power to Long Island, New York, in late 2023 and was fully commissioned in March 2024. Other projects currently planned or under

construction could increase offshore wind’s contribution to the grid from around 171 megawatts to over 80 gigawatts (GW)—enough to power around 68 million homes.² However, even as the first projects are coming online, offshore wind energy remains entangled in shifting federal policy, disputes over ocean use, and concern over national security.

Figure 1: U.S. Offshore Wind Energy Pipeline



Note: This chart shows offshore wind energy capacity in the United States and where in the development pipeline they are as of May 31, 2024, in megawatts.

Source: Angel McCoy et al., *Offshore Wind Market Report: 2024 Edition* (Golden, CO: National Renewable Energy Laboratory, 2024), <https://www.energy.gov/cmei/systems/offshore-wind-market-report-2024-edition>.

On January 20, 2025, President Donald Trump issued a memorandum temporarily withdrawing all wind energy leasing areas on the outer continental shelf, pausing wind energy permitting, and ordering a review of federal leasing and permitting practices.³ The memorandum cited, among other reasons, navigational safety, commercial interests, marine mammal protection, and national security. The U.S. District Court for the District of Massachusetts struck down the memorandum on December 8, 2025, due to the freeze continuing past the stated 60 days.⁴ Two weeks later, however, the administration paused leases for five large-scale offshore wind projects off Connecticut, New York, Massachusetts, Rhode Island, and Virginia, citing risks identified in classified Department of Defense (DOD) reports. According to the Department of the Interior (DOI), unclassified findings pointed to radar “clutter”—interference from moving blades and reflective towers, which can obscure real targets and generate false ones—as a key concern.⁵ The administration said the pause

would give DOI, DOD, and other agencies time to work with leaseholders and state partners on mitigation approaches.

By early February 2026, federal courts rescinded all five stop-work orders, finding the stated concerns insufficient to justify the halt. Several judges noted the severe economic losses the orders had caused and suggested the affected developers had substantive legal claims.⁶ These developers argued that without access to specifics about the alleged threats, they had no way to address the government's concerns.⁷

National security review is already a standard part of the offshore-wind permitting process, and developers routinely work with federal agencies to identify and avert potential conflicts. But there is additional opportunity for the U.S. government to not only mitigate those risks but also use this infrastructure as a force multiplier for national security.

There is additional opportunity for the U.S. government to not only mitigate [the] risks but also use this infrastructure as a force multiplier for national security.

This paper examines the operational and regulatory potential of using offshore wind infrastructure to enhance national security. Its central finding is that wind farms could be used as platforms to bolster and extend persistent subsea and surface surveillance. Some U.S. companies and technology developers are already innovating in this space, and several European countries are actively putting such approaches into practice. However, the potential for this infrastructure to support maritime domain awareness still faces some challenges, including (1) cost allocation, (2) ownership and obligations associated with sensors and data, and (3) risks of increased threats directed toward dual-use infrastructure.

This report first lays out the increasing threat to the U.S. homeland from offshore; China, Russia, and nonstate actors such as narcotraffickers are known to take advantage of long coastlines with relatively thin defenses. It then discusses the current U.S. approach to surveilling territorial waters and looks at how new surveillance technology could close gaps, using offshore wind platforms as a home for these advanced capabilities, as well as how offshore wind development may pose risks to traditional national security surveillance. It explores European countries' experience with radar data sharing, sensor integration, and subsea monitoring between offshore wind and national security stakeholders, which could provide a model for the United States. Finally, the paper offers initial recommendations for project developers, state governments, and federal agencies on the technologies, regulatory frameworks, and planning processes that would allow offshore wind infrastructure to contribute to U.S. national security objectives.

The Evolving Threat Landscape in the Maritime Domain

Rapid advances in autonomous, undersea, and other maritime technologies are reshaping the security environment at sea. U.S. adversaries and nonstate actors can operate farther from shore, remain difficult to detect, and exploit civilian offshore infrastructure for military, intelligence, and illicit purposes. At the same time, the growing dependence of modern economies and militaries on subsea cables, pipelines, offshore energy infrastructure, and other maritime systems is creating new vulnerabilities. Together, these trends expand both the range of potential threats and the area that defense authorities should monitor.

Maritime and Subsea Infrastructure Is Increasingly Vulnerable

Subsea cables, which carry roughly 95 percent of the world's internet traffic, are particularly vulnerable to disruption: The roughly 600 cables in operation are concentrated along several corridors.⁸ Damage to even a small subset of these cables could pose serious threats to the global economy. Both China and Russia have demonstrated gray zone tactics that could be used to disrupt critical undersea infrastructure while maintaining plausible deniability. For instance, Russia operates a “shadow fleet” of tankers that evade sanctions and have been linked to cable sabotage operations.⁹ There are also indications of potential Chinese-Russian cooperation in this domain. The *Yi Peng 3*, a Chinese-captained and -crewed cargo vessel (with at least one Russian crew member), departed the Russian port of Ust-Luga before its suspected involvement in damage to undersea infrastructure in the Baltic Sea.¹⁰ Since 2022, at least seven high-profile incidents have involved Chinese- or Russian-flagged vessels, or ones with Chinese or Russian captains or crews, in cases of suspected or confirmed damage to subsea infrastructure.¹¹ While attribution varies across these

cases, the incidents illustrate the growing risks from vessels operating near critical infrastructure with limited transparency and potentially ambiguous intent. Energy infrastructure is also increasingly exposed to sabotage. In September 2022, explosions damaged multiple sections of the Nord Stream 1 and 2 natural gas pipelines on the seabed of the Baltic Sea, disrupting infrastructure that had connected Russia and Europe.¹²

Advances in Autonomous Systems Are Expanding Threats

China is rapidly advancing its autonomous naval capabilities, particularly its unmanned underwater vehicles (UUVs). One of its newest projects, the XXLUV, is a 40-meter (131-foot) unmanned submarine with a range of roughly 11,000 nautical miles and the capability to lay mines, deploy torpedoes, and launch smaller UUVs.¹³ With sufficient range to reach the U.S. mainland, the XXLUV could pose a direct threat to U.S. coastal infrastructure in the event of a conflict with China over Taiwan. It could also sever or disrupt vital subsea communications infrastructure linking Guam, American Samoa, and the Philippines to Hawaii and the continental United States, potentially delaying U.S. support to Taiwan.

Russia is also developing and using advanced autonomous maritime capabilities. The war in Ukraine has accelerated Russia's development and use of advanced high-speed unmanned surface vessels (USVs) such as its Katran and Murena-300S models, which can launch first-person-view reconnaissance and attack drones at sea with ranges of 100–500 kilometers (62–311 miles).¹⁴ Russia has also reportedly used vessels from its shadow fleet to launch small aerial drones to conduct surveillance and map NATO nations' military bases and submarine facilities.¹⁵ These developments demonstrate how relatively inexpensive autonomous systems can extend the reach of maritime surveillance and make it more difficult to identify hostile activity among otherwise routine commercial traffic.

Maritime Threats Are Not Limited to State Actors

Finally, criminal organizations such as drug traffickers have also deployed new technologies and capabilities in the maritime domain. Each year, the U.S. Coast Guard intercepts growing numbers of self-propelled semi-submersibles and UUVs, primarily along Eastern Pacific routes but also in the Caribbean and Atlantic.¹⁶ The narcotics aboard these vessels are often bound for intermediary destinations, such as Mexico, where nonstate actors then traffic them to their end destination in the United States.¹⁷ These vessels are also becoming more sophisticated. A prototype narco-UUV seized by the Colombian military in July 2025—which was equipped with a GPS device, Starlink antennas, and surveillance cameras—suggests that smugglers may be in the final stages of deploying a new class of advanced autonomous self-propelled semi-submersibles. Their compact designs are intended to minimize their acoustic and thermal signatures, making them increasingly difficult to detect through traditional aerial surveillance and radar.¹⁸

The Maritime Domain Is Growing Harder to Monitor with Traditional Surveillance

The development of these technologies and tactics from both state and nonstate actors underscores the new threat environment in the maritime domain. Actors can exploit commercial vessels, operate below the surface, deploy autonomous systems, and conduct activities far from established surveillance networks. At the same time, critical infrastructure is increasingly distributed across large areas of ocean, making it more vulnerable to small, difficult-to-detect actions. This creates a growing requirement for persistent maritime domain awareness, which requires the ability to detect, identify, track, and characterize activity around strategically important infrastructure.

The development of these technologies and tactics from both state and nonstate actors underscores the new threat environment in the maritime domain.

Current U.S. Approach to Early Warning and Detection of Maritime Threats

The United States employs a broad network of military, law enforcement, and commercial capabilities to monitor activity across its maritime domain, including fixed radar installations, aircraft, unmanned systems, undersea acoustic sensors, and other surveillance platforms. Information from these disparate sources is integrated through interagency and international data-sharing networks to provide a common operating picture of activity at sea.

However, the current architecture has several limitations. Many existing capabilities are designed around specific missions such as detecting aircraft, monitoring borders, tracking submarines, and intercepting drug trafficking. While these missions offer substantial threat-detection capabilities, they do not provide persistent distributed surveillance of the maritime domain. Additionally, many of the surveillance systems and approaches are expensive and only available in limited quantities. This can create gaps in coverage, particularly across the vast ocean areas surrounding the United States and around dispersed infrastructure (as discussed below).

The U.S. Department of Homeland Security

Various components within the U.S. Department of Homeland Security (DHS) play a critical role in maritime-threat early warning and detection. For example, Customs and Border Protection's (CBP) Air and Marine Operations (AMO) is responsible for providing air and maritime domain awareness to the department. Operating from 74 locations across the United States, AMO employs a range of capabilities to support maritime-threat early warning and detection, including unmanned aerial

systems (UAS), Tethered Aerostat Radar Systems (TARS), and the Air and Marine Operations Center (AMOC) based in Riverside, California.¹⁹

- AMO's fleet of eight MQ-9 Predator B UAS provides long-range intelligence, surveillance, and reconnaissance of "land borders, inland waters, littoral waters, and high seas" along the mainland United States' Pacific and Atlantic coasts, as well as the Caribbean.²⁰ Although these systems can cover vast distances and provide long-range surveillance, AMO is constrained by the limited number of available drones, resulting in gaps in detection and persistent monitoring.²¹
- AMO's TARS consists of a network of eight tethered aerostats (blimps) that provide persistent radar surveillance to detect and track low-altitude aircraft and surface vessels along the U.S.-Mexico border, the Florida Straits, and Puerto Rico.²² Working as a cost-effective "low-flying satellite," each aerostat is capable of detecting aircraft at ranges of up to 200 miles.²³ In addition, CBP also operates smaller Tactical Maritime Surveillance System (TMSS) aerostats, which are equipped with "wide-area sea surveillance radar and sensors" to monitor and help counter smuggling, illegal immigration, and other illicit cross-border activity along the coasts of California, Texas, and Florida.²⁴
- AMOC operates the Air and Marine Operations Surveillance System, an advanced radar processor.²⁵ The system integrates data from up to 750 individual sensor feeds across North America, enabling it to simultaneously track more than 50,000 aircraft and 150,000 maritime vessels throughout the Americas. Using this system, AMOC coordinates with DOD, the Federal Aviation Administration, the North American Aerospace Defense Command, and international law enforcement partners in Mexico, Canada, and the Bahamas, to "detect, identify, track, and support the interdiction of suspicious aviation and maritime activity in the approaches to U.S. borders."²⁶
- The U.S. Coast Guard, itself a DHS component, possesses its own advanced detection capabilities such as the HC-130J Super Hercules long-range surveillance aircraft.²⁷ However, it still relies on the U.S. Navy for detection capabilities, particularly through collaboration with the Joint Interagency Task Force South.²⁸ Because the Coast Guard possesses law enforcement authority (unlike other branches of the military), it can act on intelligence and surveillance gathered by the Navy from its aerial identification, external intelligence sources, limited-reach ship radars, and Integrated Undersea Surveillance System.²⁹

The U.S. Navy

The U.S. Navy operates its own coastal monitoring stations and the multibillion-dollar Integrated Undersea Surveillance System, a network of UUVs and underwater acoustic surveillance cables equipped with advanced sensors and subsea hydrophones that track and detect enemy submarines and other undersea threats.³⁰ Many details surrounding the system, including the locations, capabilities, and operation of its fixed sensors, remain classified.

The U.S. Navy and Coast Guard also occasionally work with the private sector to develop and deploy new USVs to counter narco-submarines and other drug-smuggling vessels.³¹ For instance, the Navy and Coast Guard have partnered with Saildrone to deploy its autonomous Voyager USV in support of the Navy's Fourth Fleet operations in Latin America and the Caribbean. In an October 2025 operation, intelligence collected by a Voyager USV contributed to the interdiction of an \$81 million cocaine shipment.³²

Offshore Energy Infrastructure as a Potential Force Multiplier for Surveillance

The deployment of systems such as Saildrone illustrates an emerging shift toward distributed, persistent, and increasingly autonomous maritime surveillance. Instead of relying exclusively on a small number of high-end aircraft, ships, and other mobile platforms, agencies can deploy autonomous systems in greater numbers and keep them on station for extended periods, resulting in more cost-effective surveillance.

The planned offshore wind-power developments in the United States cover much of the Atlantic and mid-Atlantic Coast. Leasing areas and projects under development include ones near the entrances to Narragansett Bay, New York Harbor, and Hampton Roads, the home of Naval Station Norfolk and associated shipyards.³³ While these are all critical centers of commercial and military activity, the areas off of New Jersey and Virginia Beach are also hubs of undersea cable connections on the Eastern Seaboard.

While the use of offshore wind infrastructure for national security and defense remains relatively underexplored compared with efforts to mitigate potential interference with existing military systems, early collaborations between offshore wind developers, technology companies, defense manufacturers, and government authorities suggest these assets could support security missions. In 2021, for example, Swedish defense company Saab and major Danish offshore wind energy company Ørsted tested the installation and operation of Saab's Giraffe 1X 3D active electronically scanned array radar at the Hornsea offshore wind farm in the United Kingdom. The radar system is capable of continuously scanning large amounts of airspace while tracking up to 600 airborne objects. The test aimed to assess the compatibility between the system and the offshore turbine,

as well as the resilience of the radar to harsh environments at sea. The results were deemed “satisfactory,” and the exercise demonstrated areas of coexistence and collaboration between defense and offshore wind stakeholders.³⁴

Offshore wind farms already consist of extensive networks of fixed infrastructure, communications systems, and environmental sensors operating continuously in the maritime domain

The potential value of offshore wind extends beyond the installation of dedicated military sensors. Offshore wind farms already consist of extensive networks of fixed infrastructure, communications systems, and environmental sensors operating continuously in the maritime domain. Projects collect data for permitting, environmental monitoring, operational safety, and predictive maintenance, including information on vessel activity, subsea conditions, weather, and ocean characteristics.³⁵ This existing commercial data infrastructure creates an opportunity to develop dual-use capabilities in which systems designed for energy operations can also contribute to defense authorities’ broader maritime awareness of vessels, subsurface vehicles, and airborne objects, including drones.

The Strategic Positioning of Offshore Wind Infrastructure

The physical characteristics of offshore wind farms make them particularly well suited to augment existing maritime surveillance systems. Wind farms are typically located approximately 10-40 miles offshore, placing them beyond the immediate coastline but within relatively high-traffic portions of the maritime domain.³⁶ Turbine towers can reach approximately 500 feet in height and are supported by substantial fixed foundations. Each turbine is connected by subsea array cables to an offshore substation, which connects to shore through one or more export cables.

This distributed physical footprint creates multiple potential locations for sensing and communications equipment. A radar mounted on the top of an offshore turbine, for example, can have a substantially greater radar horizon than a comparable system positioned at sea level. Subsea fiber-optic cables can provide continuous sensing along cable routes, while offshore substations and other fixed structures could serve as platforms for additional sensors or autonomous systems. Rather than creating a separate surveillance network, these capabilities could complement existing government-operated radar, aircraft, satellite, sonar, and vessel-tracking systems.

The geographic distribution of offshore wind infrastructure could become particularly valuable as the U.S. industry expands. Individual projects may cover hundreds of square miles, and a network of projects could eventually place fixed infrastructure near important harbors and digital infrastructure nodes. Properly integrated, these assets could provide additional observation points in areas where continuous monitoring by crewed military or law-enforcement platforms would be costly or impractical.

Expanding Offshore Monitoring with Distributed Acoustic Sensing

One of the most immediate opportunities for dual-use sensing lies beneath the surface. Traditional approaches to monitoring and protecting subsea infrastructure include hydrophones, sonar, and satellite-based systems, which each struggle to provide persistent real-time coverage across large areas. Distributed acoustic sensing (DAS), which uses optical fibers embedded within subsea cables as sensors, offers a potential pathway to turn existing subsea fiber-optic infrastructure into a continuous sensing network. By detecting the small strains that vibrations and other disturbances induce in the fiber, DAS can register activity along the entire cable route. Potential applications of this sensing include monitoring vessel activity, subsea construction and maintenance, and other events that could threaten cables or offshore infrastructure.³⁷ When combined with conventional radar, sonar, satellite, and vessel-tracking data, DAS could provide an additional layer of information about activity both above and below the surface. Additionally, integrating DAS into U.S. offshore wind infrastructure near known smuggling routes in the Gulf of Mexico could enhance the ability of the U.S. Coast Guard and DHS to identify and interdict semi-submersible drug-smuggling vessels and UUVs operating in the Caribbean.³⁸ Because DAS is sensitive enough to detect the acoustic signatures generated by even small watercraft, such as jet skis, it could provide a promising additional tool for identifying and tracking difficult-to-detect unmanned vessels.

The potential advantage of making offshore wind installations dual use is that much of the necessary physical infrastructure already exists. Export and array cables increasingly incorporate fiber-optic communications lines, meaning DAS capabilities can be added without installing an entirely new network of subsea sensors. France, for example, has begun equipping offshore wind farms in Normandy and Brittany with DAS systems to monitor underwater power cables.³⁹ Companies such as the United Kingdom's Indeximate attach interrogator and analysis units onshore to monitor the health of existing cables.⁴⁰ The data is useful both to assess cable condition and maintenance needs and to expand maritime domain awareness.

Moving to an Integrated Sensing Network

The greatest national security value of offshore wind may ultimately come not from any individual sensor, but from combining multiple sensing capabilities across a distributed network of offshore infrastructure to provide a complete subsea-to-air picture. Radar could monitor surface vessels and low-altitude aircraft, DAS could provide information about activity along subsea cable routes, meteorological and oceanographic sensors could provide environmental context, and autonomous surface or underwater systems could extend sensing beyond the immediate footprint of the wind farm.

Governments can integrate commercial data with other sources, including satellite imagery, automatic identification system (AIS) data, and military and law-enforcement radar, sonar, and aerial surveillance. Advanced analytics could help identify discrepancies between expected and

observed activity—for example, vessels operating without AIS transmissions, unusual activity near critical infrastructure, or acoustic signatures that warrant further investigation.

Longer-Term Models: Offshore Wind Security Hubs

The physical permanence of offshore wind infrastructure also creates opportunities beyond sensing. Offshore substations and other fixed installations could serve as platforms or support locations for autonomous systems, including unmanned surface or underwater vehicles. Such systems could conduct periodic patrols beyond the immediate wind farm, return to offshore infrastructure for charging or data transfer, and operate alongside fixed radar and subsea sensing systems.

Emerging private sector technologies demonstrate the potential for increasingly integrated maritime sensing architectures. Mighty Waves Energy, for instance, is developing the Power and Communication, Sensor, Defense (PACSD) network, a forward-deployed defense system that would turn offshore platforms into unmanned and autonomous maritime situational awareness nodes.⁴¹ According to a July 2026 company briefing to CSIS, PACSD would use sensors capable of continuously monitoring threats across the air, surface, and underwater domains. Once a threat is detected, counter-drone systems such as unmanned aerial vehicles and USVs would be deployed from nearby coastal bases or directly from offshore installations to track, disrupt, or even neutralize the threat.⁴² Although CSIS has not independently assessed the system's performance, the concept illustrates how future offshore installations could be made to detect, track, and characterize multiple types of threats while automatically cueing other systems to respond.

In the longer term, this concept could theoretically be scaled across offshore wind farms throughout the United States. With their fixed structures, electrical power, communications connectivity, fiber-optic cables, and geographic distribution, offshore wind farms could support a range of sensors and autonomous systems. While beyond the scope of this paper, shifting toward such a “detect and neutralize” model would raise a different set of legal and political questions.

Security Risks and Their Mitigation

The potential for offshore wind infrastructure to enhance national security should be considered in relation to two challenges: (1) the risks this infrastructure can pose to national security and traditional land-based maritime domain awareness equipment; and (2) the threats that could be directed at offshore wind infrastructure if it is used for military purposes.

The primary national security concern associated with offshore wind structures is radar interference. In April 2025, the U.S. Government Accountability Office released an unclassified report, which (citing an earlier Department of Energy finding) noted that “wind turbines can reduce the performance of radar systems used for defense and maritime navigation and safety in several ways.” Such radar interference, commonly referred to as clutter, can degrade national security by “reducing detection sensitivity, obscuring potential targets, and generating false targets.”⁴³

Several factors determine the severity of interference: turbine height, spacing between turbines, and the proximity of a wind farm to existing radars.⁴⁴ Importantly, a potential interference risk does not necessarily make a proposed project incompatible with national security requirements. A range of mitigation measures are available, including changes to project siting and turbine configuration, improvements to radar systems, and the deployment of additional radars within or around wind farms (often referred to as infill radars).⁴⁵ This last option is particularly relevant here: Radars positioned within or near a wind farm can compensate for areas in which turbine interference degrades existing coverage. In a dual-use configuration, the same radars that cause interference could also restore degraded maritime domain awareness and extend the ability to detect threats.⁴⁶

Furthermore, the regulatory review process for constructing new offshore wind farms is already well established in the United States. Proposed projects must undergo a national security review by DOI's Bureau of Ocean Energy Management (BOEM), including an assessment of potential radar interference and measures to mitigate it. Only after this review, which involves project developers, federal agencies, and technical experts, can an offshore wind project proceed through permitting and construction.⁴⁷

Similarly, DOD's Military Aviation and Installation Assurance Siting Clearinghouse ("Clearinghouse") evaluates whether proposed wind, solar, transmission, and other energy projects might impede military activities.⁴⁸ Before projects are approved or construction can begin, developers must submit their plans to the Clearinghouse and address potential conflicts with security priorities.

Industry-defense partnerships provide a foundation for the United States to move beyond risk mitigation toward a framework that captures national security benefits.

This process and the technical measures used to mitigate interference reflect robust collaboration among commercial developers, DOD, and other regulators. Despite ongoing political challenges, these industry-defense partnerships provide a foundation for the United States to move beyond risk mitigation toward a framework that captures national security benefits, as the recommendations at the end of this paper describe.

However, wind infrastructure has proven susceptible to cyberattacks, with at least three high-profile attacks against land-based wind farm operators in 2022. Although there do not appear to be publicly reported cyberattacks against offshore wind infrastructure, offshore systems share many of the same vulnerabilities as their onshore counterparts, including internet-connected operational technology.⁴⁹ Moreover, their remote locations introduce additional risks by limiting direct human oversight and routine monitoring, as well as making recovery operations slower and more costly.⁵⁰

Using offshore wind infrastructure for national security data collection could make it an even more attractive target for cybercriminals and state-sponsored actors. These risks, however, could be mitigated through stronger cybersecurity measures such as removing extraneous operational technology network access points, improving cyber hygiene among operators, and implementing robust data-sharing and data-protection frameworks between government authorities and energy companies.⁵¹ There is already precedent for such cooperation. The National Oceanic and Atmospheric Administration, for example, has scientific data-sharing agreements with major oil and gas companies, including Shell and ConocoPhillips, and signed a similar agreement with Ørsted in 2021.⁵² In 2026, Poland moved to formally designate offshore wind farms as "critical infrastructure," subjecting them to stricter cybersecurity requirements, while the France Energies Marines institute is working to standardize and implement stricter cybersecurity measures across the sector.⁵³

Europe as a Test Case

Embedding Security in Offshore Wind Infrastructure

Several European countries have integrated offshore wind infrastructure into defense frameworks for maritime surveillance. These nations' efforts have been driven by acute threat perception and a recognition that offshore wind is a critical element of energy security. In particular, sustained Russian activity against undersea infrastructure has increased the need to integrate security enhancement measures with new and existing offshore infrastructure. In this context, certain European countries view the continent's existing offshore wind sector as both a potential asset and risk, requiring innovative approaches to ensure energy and maritime security.

Much of the installed and planned capacity for offshore wind in Europe is located in the North Sea and Baltic Sea. Both regions are experiencing growing adversarial activity and sabotage attempts, increasing the need for surveillance and response systems to protect maritime infrastructure and activities. In response, European nations have implemented a spectrum of approaches that build security into the development and planning processes for offshore infrastructure.

Multilateral Efforts

European countries' domestic approaches sit within a multilateral setting that shapes how each nation integrates security enhancement measures with offshore wind. In recent years, the European Union, NATO, and other multinational coalitions have worked to address maritime security and the security and integration of offshore infrastructure in partnership with each other. The EU Maritime Security Strategy, originally enacted in 2014, is the union's umbrella policy regarding maritime security and cooperation. Its 2023 update reaffirmed the importance of securing critical

maritime infrastructure, particularly offshore wind. The strategy calls for stronger maritime domain awareness, reinforced offshore patrol surveillance, and hybrid or cyber threat response.⁵⁴

Countries with infrastructure and assets in the North Sea have committed to a number of agreements aimed at increasing security of wind-power assets and maritime domain awareness. For instance, at the January 2026 North Sea Summit, leaders of the European Union's North Seas Energy Cooperation signed declarations committing to hardening the offshore energy system against physical, cyber, and hybrid attacks.⁵⁵

Country Models

Several European countries have begun to develop strategies to use offshore wind infrastructure as a national security asset. Their approaches range from the mandatory integration of defense-relevant equipment on offshore energy infrastructure to streamlined frameworks for collaboration between energy project developers and defense officials. This section outlines several models for the dual use of offshore wind infrastructure seen in Poland, Belgium, the Netherlands, Norway, and the United Kingdom.

POLAND: MANDATORY MILITARY INTEGRATION

Poland has taken the most assertive posture in Europe as the first country to mandate the installation of defense-relevant equipment across its offshore wind projects. Warsaw's approach integrates security, energy, and environmental goals through early planning processes. At the beginning of every project, all developers must obtain an offshore location license, which defines the national security requirements the project must meet, including obligations to address potential impacts on military operations and to accommodate radar or other sensing systems that may qualify as dual-use equipment. To date, developers bear full responsibility for radar-interference mitigation.⁵⁶

The integration of security review and dual-use approaches can be seen in Poland's flagship offshore wind project, Baltic Power, which sits around 14 miles off the coast near Łeba and Choczewo, and less than 200 kilometers (124 miles) from Russia's Kaliningrad exclave.⁵⁷ The project is installing military-grade sensors and radar under a checklist issued by Poland's Ministry of National Defence (MOD). Planned technologies include (1) air-surveillance radar for drone detection, (2) surface radar and cameras covering vessel traffic, (3) seabed sensors around substations and export cables, (4) hydroacoustic surveillance, and (5) fiber-optic seabed monitoring.⁵⁸

There are several key takeaways from Poland's approach to securing offshore wind infrastructure against potential Russian aggression. First, Poland's approach is largely focused on addressing any potential interference wind projects may cause with security operations and securing offshore infrastructure from attack. The framing of these interventions is less focused on the use of offshore wind infrastructure to strengthen national security. As more projects deploy the required sensors, assessing the success of these additions and collaborations in strengthening maritime domain awareness could be a valuable learning opportunity. Second, Poland's MOD imposes requirements

on developers but offers few incentives to support the integration of sensors, radars, and other technologies.

BELGIUM: CIVILIAN DATA SHARING WITHOUT MILITARIZATION

Belgium has seen significant advances in the level of cooperation between the offshore wind industry and defense authorities. The New Belgian Maritime Code came into effect in September 2020; the Maritime Security Law added updates to the code that came into force in January 2023.⁵⁹ This legislation strengthens the National Maritime Security Authority and increases the amount of data—on vessel traffic, turbine and substation status, weather and metocean patterns, AIS tracking, and maintenance-vessel movements—shared with the Belgian Coast Guard and other security authorities.⁶⁰

A resolution introduced in the Chamber of Representatives in 2023 highlighted the need for improved maritime domain awareness through increases in acoustic hydrophones, drones, and other sensors.⁶¹ These approaches suggest that permits for offshore wind could require developers to propose plans and bear the cost for integrating these sensors into their projects. In particular, the National Maritime Security Authority could require the Princess Elisabeth Energy Island, a planned offshore hub that will bundle cables from a number of offshore wind farms, to install minimum security measures such as acoustic hydrophones, radars, docking stations, and cameras. While the operators would bear the cost for installing these capabilities, relevant defense authorities would manage monitoring and any required interventions.⁶²

THE NETHERLANDS: INSTITUTIONAL COORDINATION AND NON-PRICE CRITERIA

The Netherlands has focused on improving coordination and communication between energy and defense stakeholders. The approach is built around the Programme for the Protection of North Sea Infrastructure (PBNI). Established in April 2023, PBNI brings together five ministries (Defence, Economic Affairs, Climate Policy and Green Growth, Justice and Security, and Foreign Affairs) with private energy and telecom companies to coordinate the protection of offshore infrastructure. The program is organized around five pillars: governance, risk mitigation, situational awareness, crisis management, and international cooperation.⁶³

While not yet aimed at security, non-price criteria for selecting successful project bids have been used in the Netherlands. The rubric often focuses on environmental and community concerns but does provide regulatory authorities with a way to reward developers for building additional attributes into their projects. Extending such criteria to security features beyond the required radar mitigation could help unlock offshore wind's security potential.

NORWAY: TESTING TO VALIDATE SURVEILLANCE METHODS FOR MARITIME INFRASTRUCTURE PROTECTION

Norway's clearest efforts toward offshore wind-related maritime domain awareness are evident at the Marine Energy Test Centre's North Sea offshore site, used to test floating offshore wind solutions.⁶⁴ In 2022, Kongsberg Norcontrol commissioned "the first site surveillance system for Norwegian offshore wind" there. It draws upon existing sensors from the adjacent Kvitsøy Vessel Traffic System and adds information management tailored to the test site's surveillance needs to

give “comprehensive maritime domain awareness for the test site and export cable corridor, while also serving for demonstration and development purposes.”⁶⁵ Crucially, this effort could contribute to the assessment and development of sensors and surveillance approaches that could lead to floating offshore wind being used to support national security. While the United States does not currently have any operational floating offshore wind farms, such projects could offer improved maritime domain awareness, as they are often built farther from shore in deeper waters.

Additionally, the use of distributed acoustic sensing to monitor and assess vessel movement near critical offshore infrastructure has been studied in small-scale environments along export cables in Trondheimsfjord, Norway, providing another model for how this infrastructure can support national security.⁶⁶

THE UNITED KINGDOM: ADDRESSING RADAR INTERFERENCE WHILE ADVANCING SECURITY

The United Kingdom is a “global leader in offshore wind with over 16 GW of operating capacity.”⁶⁷ The country has accordingly launched pilot projects that test technologies’ ability both to address radar interference and expand maritime domain awareness. In particular, the Department for Energy Security and Net Zero (DESNZ), the Defence Science and Technology Laboratory (DSTL), and the Defence and Security Accelerator (DASA) have engaged in initiatives to mitigate the impacts of offshore wind farms on radar and air traffic control systems.

Rather than treating interference as a hard constraint on siting, DESNZ and DSTL co-funded a 2025 demonstration by LiveLink Aerospace at Vattenfall’s Aberdeen wind farm of a passive, radio signal-silent, multi-sensor package. The package fuses electro-optical, thermal, and acoustic detection in a single nacelle-mounted system, mitigating the clutter that rotating blades create for radar while adding independent maritime surveillance capability.⁶⁸ In March 2026, the Ministry of Defence announced a £95 million (around \$126 million) contract with BAE Systems to deliver next-generation air-defense radars intended to clear regulatory hurdles blocking up to 10 GW of currently constrained offshore wind capacity and roughly £20 billion (around \$26 billion) in private investment, while preserving full air-defense detection capability.⁶⁹ The United Kingdom has also designated offshore wind a “critical national priority,” creating a policy presumption that will lend more weight toward approving new offshore projects despite any potential “residual impacts.”⁷⁰

That said, while these innovation-driven partnerships could support dual-use sensing, there are significant gaps. In April 2026, a Royal United Services Institute workshop on North Sea security concluded that “detection and reporting remain in their infancy, resulting in limited situational awareness.”⁷¹

Table 1: Takeaways for the United States

Country	Core security model	Primary technologies	Governance mechanism
Poland	Mandatory dual-use integration under an MOD checklist for all offshore wind projects	Military radars and cameras; fiber-optic seabed monitoring	MOD sets security requirements through the offshore location license; developers bear costs
Belgium	Civilian data sharing with the Coast Guard, without militarization	Turbine-mounted sensors; drones and vessels; AIS data integration	Maritime Security Law; federal government controls camera feeds
Netherlands	Multi-ministry institutional coordination	Seabed monitoring	Five-ministry PBNI program; non-price tender criteria as a possible tool
Norway	Critical maritime infrastructure protection built on oil and gas subsea expertise	Subsea and maritime-security capabilities	Primarily company-led projects on national security and offshore wind
United Kingdom	Radar infill innovation	Passive nacelle-mounted sensors; BAE air-defense radar	DESNZ, DASA, and DSTL co-funded innovation; “critical national priority” designation

Source: CSIS research.

Despite recent progress in cooperation and communication between offshore wind developers and defense agencies, there remain several challenges to a dual-use model that offer important lessons for the U.S. context. First is the inherent tension of something being dual use, in that integrating military equipment into civilian infrastructure may actually increase the threats directed at it. Additionally, cooperation between developers or operators and defense agencies can be complex; while the collection of data from offshore wind infrastructure has improved, information often moves slowly and imperfectly between civilian and defense agencies, reducing the benefits of collaboration. Finally, offshore wind projects are highly cost-sensitive, meaning that increased requirements to install additional sensors can be viewed as burdensome.

Recommendations

European approaches underscore several key points for the U.S. offshore wind industry and national security authorities. Since evolving technologies and risks in the maritime domain demand new methods to enhance maritime security, offshore wind infrastructure can provide an additional layer of persistent data collection to bolster maritime domain awareness. Achieving this will require moving from a risk-mitigation model to one in which the industry is evaluated holistically both for risks and as a new force multiplier for national security. This report proposes four lines of effort to unlock the potential of offshore wind infrastructure.

Establish Clear Lines of Ownership and Obligation for Dual-Use Offshore Wind Infrastructure

Integrating technologies that can support maritime domain awareness and bolster national security will run into the common challenges of dual-use infrastructure, namely how to manage overlapping obligations and ownership claims between civilian and defense stakeholders. Making this infrastructure more of a target, as discussed above, is one such challenge. Another is the natural tension between project developers and operators on one side and national security authorities on the other over the ownership of sensing equipment and data and the associated obligations to manage and protect it.

Stakeholders will have to settle several questions as they develop dual-use arrangements so that responsibilities are clearly assigned:

- **Ownership:** Who owns and maintains dual-use sensors and technologies?
- **Liability:** Who is liable if a dual-use asset is attacked? Will insurers treat dual-use facilities or infrastructure differently?
- **Cybersecurity:** Who is responsible for ensuring that any collected data is secure and managed appropriately?
- **Reporting Obligations:** When are operators expected to share collected data? What are the appropriate lines of communication between different stakeholders to ensure the timely delivery and analysis of collected information?
- **Maintenance:** What parties are expected to maintain sensors, radars, and other additional equipment? What are the financial obligations associated with this additional maintenance?

Additionally, the Royal United Services Institute found that companies collecting data often do not know what information is relevant, at what level of detail, or to which authorities they should report.⁷² Clarifying these lines of reporting and responsibility is a necessary first step to unlocking dual-use potential. Federal U.S. authorities should provide targeted guidance on what new and existing data to report, in what detail, and to whom. This is particularly relevant in the near term: Even without the addition of new or military-specific sensors and radars, offshore wind farms often collect rich data sets that could add a new layer of persistent maritime awareness. Developing appropriate guidance and channels for sharing this information with relevant federal authorities would be an initial, low-cost step to build collaboration on national security.

Much of this collaboration depends on effective and rapid data sharing and clear guidelines for directing reporting and responses. Data-sharing partnerships between offshore wind operators, supply-chain companies, and defense authorities can build upon existing structures, including the previously mentioned National Oceanic and Atmospheric Administration partnerships.

Incorporate National Security Enhancement into the Existing Offshore Wind Review Process

Poland's model demonstrates that clear requirements for security-enhancing measures can bring sensors and radars onto offshore wind projects quickly. The Netherlands provides another example by incorporating non-price criteria into the assessment and selection of offshore wind bids, typically to advance environmental, economic, and industrial goals. A comparable criterion for national security would encourage developers to identify what capabilities their projects could support, rather than treating security solely as a constraint to be cleared.

The United States should adopt a similar approach to Poland's, in which regulators and defense authorities clearly identify opportunities to enhance national security and incentivize developers to incorporate them into project plans. This should include a review process that weighs a project's potential security benefits alongside its risks, evaluating these factors as early in the review as possible so developers can account accurately for the associated costs.

The United States should build upon its existing national security review to shift from a risk identification and mitigation model to a risk and opportunity model. Initial steps include:

- **Reporting on Maritime Surveillance Gaps:** DOD's Clearinghouse, in partnership with the authorities responsible for maritime security, should publish regular reports on (1) gaps in maritime domain surveillance and (2) specific recommendations for technologies, data-collection approaches, and collaboration with existing and planned offshore wind projects. Reports should follow a set schedule and reflect input from defense and industry stakeholders. Making surveillance gaps known up front would give developers a concrete target and reduce uncertainty about what the government actually wants.
- **Evaluating Proposed Projects on Their Potential Opportunities:** Lessees currently must submit a Construction and Operations Plan in the fourth phase of BOEM's review process to demonstrate that the project does not unreasonably interfere with other uses of the outer continental shelf, including national security applications.⁷³ Moving to an opportunity model would require these plans to include an initial assessment of the sensing capabilities the project already intends to include and any additional sensing it could support. BOEM should also give developers an opportunity to propose national security enhancements earlier, such as at the site assessment stage, so these can be built into design and cost planning.
- **Reviewing Existing and Permitted Projects:** For projects already leased or permitted, the Clearinghouse's gap reports should be used to identify which installations are best positioned to host radars or other sensors. DOD could then offer voluntary retrofit opportunities through agreements that cover installation, power, data sharing, and cost allocation.
- **Implementing a Bidding Process:** There is precedent in the United States to use the bidding process for offshore wind to incentivize investments in areas outside of the scope of the project alone. For instance, BOEM has offered bidding credits to incentivize project developers to invest in workforce development and domestic supply chains.⁷⁴ A "security features" bidding credit could be implemented to encourage developers to include these features in proposed projects.

Strengthen Co-funding Mechanisms for Dual-Use Technologies

Developers remain wary of any additional requirements that could slow projects or add costs in an industry with already challenging economics. In both Poland and Belgium, developers bear the cost of additional sensors and security requirements while defense authorities manage the costs of data and required responses. A similar co-funding model could better support maritime awareness and security and more effectively deliver shared benefits.

Addressing radar interference has historically required project developers to contribute financially to help the military or federal authorities adjust or upgrade radars in the vicinity of offshore wind farms. For example, the five projects addressed in the 2026 pauses all agreed to pay at least \$80,000 each to assist in radar adjustments.⁷⁵ For the most part, funding for the deployment of any additional hardware is determined through case-by-case negotiations between a developer and relevant federal authorities.⁷⁶

Achieving an integrated sensing network that both addresses any potential radar risks and effectively establishes zones of persistent maritime domain awareness will require moving away from ad hoc negotiated agreements and toward a broader incentive structure.

Achieving an integrated sensing network that both addresses any potential radar risks and effectively establishes zones of persistent maritime domain awareness will require moving away from ad hoc negotiated agreements and toward a broader incentive structure. There are a number of approaches that could offer effective cost sharing or incentives for integrating new sensors and data-collection capabilities. For instance, the UK government purchased radar systems that would clear the pathway for substantial offshore capacity. In the United States, DOD or DHS could evaluate areas of particular benefit and offer financial support for new radars that expand maritime domain awareness. Additionally, project operators could earn an operating fee for hosting additional sensing capabilities, offering projects an additional stream of revenue (albeit on a much smaller scale than typical income).

Build Regional Collaboration on Shared Infrastructure and Sensing Zones

Unlocking the full potential of offshore wind infrastructure to enhance national security will eventually require a systems-based approach rather than a project-by-project one. Building a network of sensors, radars, and data sharing could enhance the effectiveness of persistent maritime domain awareness and help mitigate costs borne by any one project or entity. Achieving this will require coordination between the federal government, state governments, and offshore wind developers.

Coordinating and planning a network approach to dual-use sensing and detection could draw on regional approaches to offshore wind transmission. For example, the Northeast States Collaborative on Interregional Transmission consists of representatives of nine East Coast states that work to coordinate transmission and grid-expansion efforts with the U.S. Department of Energy. The organization has worked on a variety of projects with the intention of better integrating shared transmission priorities, coordinating both offshore and onshore infrastructure planning, and establishing common technical standards for offshore transmission facilities.⁷⁷

These lessons carry over to dual-use infrastructure. First, creating avenues for coordination and planning could help integrate an individual project's security capabilities into broader networks. Second, although technologies that expand or add sensing capabilities on wind infrastructure are numerous and growing, significant technical and integration questions remain. Creating industry standards that define opportunities, technological capabilities, and integration of systems on offshore platforms could reduce costs.

Conclusion

The nature of risks to national security in the maritime domain is changing. Rapid advances in autonomous vehicles, drones, and related technologies have left waters harder to surveil effectively and made maritime infrastructure more susceptible to sabotage and attacks from both state and nonstate actors. In Europe, Russian aggression against undersea cables and energy assets shows that civilian infrastructure is now part of the contested space. Offshore wind farms, built in waters where these threats demand better awareness, can help support needed warning capabilities.

In the United States, the link between offshore wind infrastructure and national security has largely been viewed with an eye toward identifying and mitigating potential risks. The regulatory process to review and approve projects includes national security checks to identify conflicts over siting, radar interference, and other issues of overlapping maritime use. To date, there has been little work dedicated to identifying ways offshore wind infrastructure can instead benefit national security.

This is a missed opportunity. Offshore wind infrastructure offers a viable platform and private partner in expanding the persistent collection of maritime data. Lessons from a number of European countries demonstrate that a variety of sensors, radars, and data-collection approaches can build on this infrastructure to bolster maritime domain awareness and support the safety and security of offshore sites. Treating offshore wind solely as a risk to be managed leaves that value untapped. By planning for dual-use capability from the outset, the United States can turn energy infrastructure into a force multiplier for national security, one that strengthens surveillance and warning in an increasingly contested maritime environment.

Appendix

Ocean Zones and Maritime Infrastructure

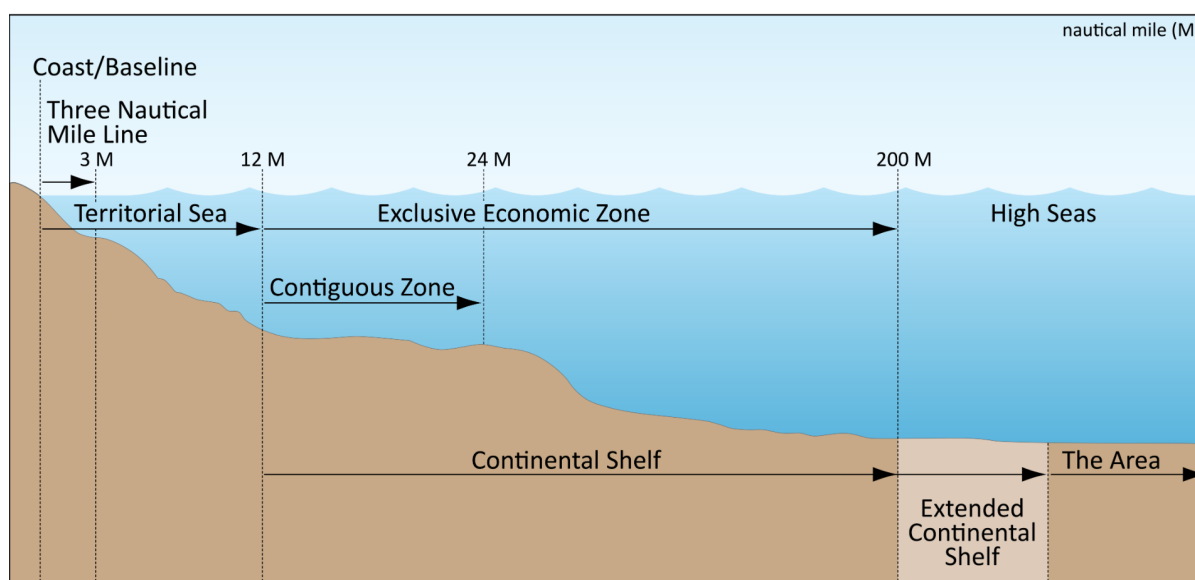
Offshore wind development and offshore energy development more broadly fall under the U.S. Outer Continental Shelf Lands Act, which defines the “outer continental shelf” as submerged lands lying seaward of state waters over which the U.S. has jurisdiction, control, and power of disposition for resource development.⁷⁸ The modern basis for maritime zones is the international law of the sea, which is governed globally by the United Nations Convention on the Law of the Sea (UNCLOS).⁷⁹ To date, the U.S. Senate has not provided advice and consent for U.S. accession to the convention, but it is long-standing U.S. policy to “accept and act in accordance with the balance of interests relating to traditional uses of the oceans [in UNCLOS]—such as navigation and overflight,” and to view such provisions as generally reflective of customary international law that binds all states.⁸⁰ Additionally, in the United States, federal waters generally begin beyond state territorial limits, which typically stretch 3 nautical miles (NM) from the coast.

UNCLOS divides the ocean into six different zones:⁸¹

1. internal waters (i.e., waters landward of the baseline, usually the low-water line of the coast);
2. territorial sea (i.e., an area within 12NM from the baseline, within which a nation exercises complete sovereignty over waters, airspace, and subsea land);
3. contiguous zone (i.e., a zone adjacent to and beyond the territorial sea between 12 and 24NM from the baseline, within which a nation is allowed to “exercise the control necessary to prevent the infringement of its customs, fiscal, immigration, or sanitary laws and regulations”);

4. exclusive economic zone (i.e., a zone overlapping with the contiguous zone between 12 and 200NM from the baseline, within which a nation has sovereignty over natural resources and man-made installations);
5. continental shelf (i.e., “the seabed and subsoil of the submarine areas that extend beyond [a country’s] territorial sea throughout the natural prolongation of its land territory to the outer edge of the continental margin,” or out to 200NM from the baseline, whichever distance is larger, within which a nation has sovereignty over natural resources on or below the ocean floor); and
6. high seas and deep ocean floor (i.e., all parts of the sea that are not included in the exclusive economic zones, territorial seas, or internal waters of a country, as well as the seabed and ocean floor and subsoil thereof, beyond the limits of national jurisdiction).

Figure A1: Maritime Zones Under International Law



Source: “Maritime Zones and Boundaries,” National Oceanic and Atmospheric Administration, updated March 18, 2026, <https://www.noaa.gov/maritime-zones-and-boundaries>.

Such maritime zones are of utmost strategic significance to the United States since they “directly affect maritime operations by determining the degree of control a coastal State may exercise over the conduct of foreign merchant ships, warships, and aircraft operating within these areas.”⁸² For instance, within its territorial sea, a nation exercises full sovereignty over the water, seabed, and airspace. It can regulate foreign vessels but must respect their right of innocent passage through another country’s territorial sea. Within contiguous zones, the coastal nation has limited enforcement powers. It can, however, act to punish violations of customs, fiscal, immigration, and sanitary laws, helping it detect and respond to certain threats before they reach the coast.

About the Authors

Allegra Dawes is a non-resident adjunct fellow with the Energy Security and Climate Change Program at the Center for Strategic and International Studies (CSIS). She previously served as an associate fellow with the Energy Security and Climate Change Program at CSIS, where she authored policy research on offshore wind, carbon markets, and industrial policy for clean technology. She holds an MSc in political economy from the London School of Economics and a BS in mathematics from Union College.

Emily Harding is director of the Intelligence, National Security, and Technology (INT) Program and vice president of the Defense and Security Department at CSIS. As the head of the INT Program, Harding provides thought leadership on the most critical issues facing intelligence professionals and on the future of intelligence work. In her capacity as vice president of CSIS's Defense and Security Department, she is responsible for leading a team of world-renowned scholars providing policy solutions that shape national security. Drawing on her decades of experience in national security, Harding has established herself as an expert on how technology is revolutionizing national security work. She has also served in a series of high-profile national security positions at critical moments. While serving as deputy staff director on the Senate Select Committee on Intelligence, she led the committee's investigation into Russian interference in the 2016 elections, which was lauded for its bipartisanship. At the CIA, she led analysts and analytic programs through moments of crisis, including shepherding the Iraq Group during the attempted Islamic State takeover. During a tour at the National Security Council, she served as director for Iran. After leaving the White House, her team ran the first Office of the Director of National Intelligence-led presidential transition, where she was responsible for briefing the incoming administration. Harding is an adjunct lecturer at the

Johns Hopkins School of Advanced International Studies. Her analysis has appeared in the *Wall Street Journal*, BBC, NPR, Bloomberg, and other outlets. She holds an MA from Harvard University's Kennedy School of Government and a BA from the University of Virginia.

Julia Dickson is a former associate fellow with the INT Program at CSIS. Her research interests included cybersecurity and cybercrime and the role of technology in conflict. Prior to joining CSIS, she was awarded a Fulbright grant and spent a year teaching English in Osh, Kyrgyzstan. She was also previously a research assistant at the Wilson Center, an intern for the Conventional Defense Program at the Stimson Center, and a communications and outreach intern at the International Crisis Group. She holds a BA in international studies with a minor in French from the Johns Hopkins University.

Aosheng Pusztaszeri is a research associate with the INT Program at CSIS, where he focuses on emerging technologies and their implications for national security. Before joining CSIS, he interned in the U.S. Senate and the U.S. House of Representatives and served as an undergraduate research assistant in Cornell University's Department of Government. Aosheng holds a BA in government and history from Cornell University.

Joseph Majkut is director of the Energy Security and Climate Change Program at CSIS. In this role, he leads the program's work understanding the geopolitics of energy and climate change and working to ensure a global energy transition that is responsive to the risks of climate change and the economic and strategic priorities of the United States and the world. Joseph is an expert in climate science, climate policy, and risk and uncertainty analysis for decisionmaking. He is frequently cited in trade and national media on the politics of climate change and has testified before Congress on climate change and science. Before CSIS, Majkut worked as the director of climate policy at the Niskanen Center, where he led that group's efforts to research and promote carbon pricing, low-carbon innovation, regulatory reform, and other market reforms to speed decarbonization. From 2014 to 2015, he worked in the U.S. Senate as a congressional science fellow, supported by the American Association for the Advancement of Science and the American Geosciences Institute. He holds a PhD from Princeton University in atmospheric and oceanic sciences, an MA in applied mathematics from the Delft University of Technology, and a BS in mathematics from Harvey Mudd College.

About CSIS

The Center for Strategic and International Studies (CSIS) is a bipartisan, nonprofit policy research organization dedicated to advancing practical ideas to address the world's greatest challenges.

Founded in 1962, CSIS is led by General Joseph F. Dunford, who was appointed chief executive officer in 2026, succeeding John J. Hamre. The CSIS Board of Trustees is chaired by Thomas J. Pritzker, who has held the position since 2015.

CSIS brings together more than 275 full-time staff and a global network of affiliated scholars working across four core areas of public policy: defense and security, geopolitics and foreign policy, economic security and technology, and global development. Our scholars are regularly called upon by Congress, the executive branch, the media, and others to explain the day's events and offer recommendations to improve U.S. strategy.

CSIS's purpose is to define the future of national security. We are guided by a distinct set of values—non-partisanship, independent thought, innovative thinking, cross-disciplinary scholarship, integrity and professionalism, and talent development. CSIS's values work in concert toward the goal of making real-world impact.

What sets CSIS apart is not only the quality of its research but how that research is conveyed: through original data and open-source analysis; through multimedia and data visualization; and through connecting relevant analysis with key audiences at the moments that matter most. This combination of rigor, independence, and reach has made CSIS a driving force in the policy debates shaping American security and prosperity.

Endnotes

- 1 Offshore wind farms have been sited as close as ~3 miles from the coast. Traditional commercial projects sit around 10-20 miles from shore. Some deep-water and floating wind projects can be sited over 30 miles from shore. “World’s Deepest Oil Rig Platform in the Gulf of Mexico,” *Drilling Maps* (blog), May 20, 2024, <https://blog.drillingmaps.com/2024/05/worlds-deepest-oil-rig-platform-at-8000.html>; and Christopher Martin, “For U.S. Offshore Wind Farms, Sweet Spot Is 15 Miles from Beach,” *Bloomberg Law*, January 3, 2019, <https://news.bloomberglaw.com/environment-and-energy/for-u-s-offshore-wind-farms-sweet-spot-is-15-miles-from-beach>.
- 2 Angel McCoy et al., *Offshore Wind Market Report: 2024 Edition* (Golden, CO: National Renewable Energy Laboratory, 2024), <https://www.energy.gov/cmei/systems/offshore-wind-market-report-2024-edition>; and Blake Ambrester, “How Many Megawatts Does a House Typically Use?” *Solar Bear*, updated March 18, 2026, <https://www.solarbear.com/blog/how-many-megawatts-does-a-house-typically-use>.
- 3 White House, “Temporary Withdrawal of All Areas on the Outer Continental Shelf from Offshore Wind Leasing and Review of the Federal Government’s Leasing and Permitting Practices for Wind Projects,” memorandum, January 20, 2025, <https://www.whitehouse.gov/presidential-actions/2025/01/temporary-withdrawal-of-all-areas-on-the-outer-continental-shelf-from-offshore-wind-leasing-and-review-of-the-federal-governments-leasing-and-permitting-practices-for-wind-projects/>.
- 4 Erika Kranz, “Federal Court Vacates Wind Energy Authorization Pause,” *Environmental & Energy Law Program*, Harvard Law School, December 16, 2025, <https://eelp.law.harvard.edu/federal-court-vacates-wind-energy-authorization-pause/>.
- 5 Eleanor Green, Amanda Lineberry, and Melissa Birchard, “Understanding Recent Federal Actions | Offshore Wind Development,” *Georgetown Climate Center*, updated February 5, 2026, <https://www.georgetownclimate.org/articles/admin-actions-restrict-wind-development.html>.

- 6 Yejoo Moon, “Offshore Wind Under Siege: Policy, Litigation, and the Cost of Federal Cancellations,” *Cornell Journal of Law and Public Policy*, *The Issue Spotter* (blog), December 4, 2025, <https://publications.lawschool.cornell.edu/jlpp/2025/12/04/offshore-wind-under-siege-policy-litigation-and-the-cost-of-federal-cancellations/>.
- 7 Michael Copley, “Trump administration claims offshore wind poses a threat. But it won't say how,” NPR, January 21, 2026, <https://www.npr.org/2026/01/21/nx-s1-5678635/trump-offshore-wind-national-security-climate-change>.
- 8 Daniel F. Runde, Erin L. Murphy, and Thomas Bryja, “Safeguarding Subsea Cables: Protecting Cyber Infrastructure amid Great Power Competition,” CSIS, August 16, 2024, <https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition>.
- 9 Henri van Soest, “Countering Russia’s ‘Shadow Fleet,’” *National Interest*, January 16, 2025, <https://nationalinterest.org/feature/countering-russias-shadow-fleet-214417>.
- 10 Bojan Pancevski, “Chinese Ship’s Crew Suspected of Deliberately Dragging Anchor for 100 Miles to Cut Baltic Cables,” *Wall Street Journal*, November 29, 2024, <https://www.wsj.com/world/europe/chinese-ship-suspected-of-deliberately-dragging-anchor-for-100-miles-to-cut-baltic-cables-395f65d1>; and Sophie Himka, “Baltic Sea Undersea Cable Security,” Henry M. Jackson School of International Studies, University of Washington, July 9, 2025, <https://jsis.washington.edu/news/baltic-sea-undersea-cable-security/>.
- 11 James Pomfret and Yimou Lee, “China-Linked Shipowner Denies Taiwan Accusation of Damaging Undersea Cable,” *Reuters*, January 8, 2025, <https://www.reuters.com/world/asia-pacific/china-linked-shipowner-denies-taiwan-accusation-damaging-undersea-cable-2025-01-08/>; Koh Ewe and Iting Chiang, “Taiwan jails China captain for undersea cable sabotage in landmark case,” *BBC News*, January 12, 2025, <https://www.bbc.com/news/articles/cwy3zy9jvd4o>; Mark Tyson, “Crew of Russian ‘Shadow Fleet’ Tanker Charged with Intentionally Sabotaging Undersea Cables,” *Tom’s Hardware*, August 13, 2025, <https://www.tomshardware.com/networking/crew-of-russian-shadow-fleet-tanker-charged-with-intentionally-sabotaging-undersea-cables-finnish-authorities-claim-ship-dragged-its-anchor-56-miles-along-the-sea-floor-causing-usd70-million-in-damage-to-five-cables>; Bojan Pancevski, “Chinese Ship’s Crew Suspected”; Reid Standish, “Hunt for Answers Continues over Chinese Ship’s Suspected Role in Damaging Baltic Pipeline,” *Radio Free Europe/Radio Liberty*, November 2, 2023, <https://www.rferl.org/a/china-baltic-pipeline-damaged-russia-newnew-polar-bear/32667867.html>; Huizhong Wu and Johnson Lai, “Taiwan Suspects Chinese Ships Cut Islands’ Internet Cables,” *Associated Press*, April 18, 2023, <https://apnews.com/article/65f10f5f73a346fa788436366d7a7c70>; and Jordan Robertson and Drake Bennett, “A Subsea Cable Went Missing. Was Russia To Blame?,” *Bloomberg*, July 11, 2024, <https://www.bloomberg.com/features/2024-undersea-cable-sabotage-russia-norway/>.
- 12 Bojan Pancevski, “A Drunken Evening, a Rented Yacht: The Real Story of the Nord Stream Pipeline Sabotage,” *Wall Street Journal*, August 14, 2024, <https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c>.
- 13 Michael C. Horowitz, *China’s Undersea Strategy - Investing in Emerging Capabilities to Undermine American Superiority*, Testimony prepared for the U.S.-China Economic and Security Review Commission, 119th Cong., 2nd sess. (February 27, 2026), https://www.uscc.gov/sites/default/files/2026-03/Mike_Horowitz_Testimony.pdf.
- 14 Katherina Popilnichenko, “Ukraine Uncovers Russia’s Secret Fleet of Unmanned Sea Vessels,” *United24 Media*, August 25, 2026, <https://united24media.com/war-in-ukraine/ukraine-uncovers-russias-secret-fleet-of-unmanned-sea-vessels-21953>.
- 15 Dan Sabbagh, “Russia ‘Mounted Drone Surveillance of European Nuclear Sites over 18 Months,’” *The Guardian*, July 2, 2026, <https://www.theguardian.com/world/2026/jul/02/russia-mounted-drone-surveillance-of-european-nuclear-sites-over-18-months>.

- 16 H. I. Sutton, “U.S. Coast Guard Could Face a Narco Submarine Epidemic in 2020,” *Forbes*, January 7, 2020, <https://www.forbes.com/sites/hisutton/2020/01/07/why-america-could-continue-to-face-a-narco-submarine-epidemic-in-2020/>; Barbara Honegger, “NPS OR Team Optimizes Defense against Narco Semi-Subs,” Naval Postgraduate School, December 4, 2010, <https://nps.edu/-/nps-or-team-optimize-s-defense-against-narco-semi-subs>; Victor González, Lenin Naranjo, and Jennifer Scotland, “Uncrewed and Under the Radar: How AUVs Transform Drug Smuggling,” Royal United Services Institute, November 25, 2025, <https://www.rusi.org/explore-our-research/publications/commentary/uncrewed-and-under-radar-how-auvs-transform-drug-smuggling>; Goldberg Defense, “Authorities Continue to Crack Down on Smugglers Using ‘Narco Subs,’” Goldberg Defense, May 30, 2025, <https://www.goldbergdefense.com/blog/2025/05/authorities-continue-to-crack-down-on-smugglers-using-narco-subs/>; and Sam Woolston and Henry Shuldiner, “Under the Radar: What Hundreds of Narco Sub Seizures Tell Us about Global Cocaine Routes,” Insight Crime, May 16, 2025, <https://insightcrime.org/news/under-radar-what-hundred-s-of-narco-sub-seizures-tell-us-about-global-cocaine-routes/>.
- 17 Goldberg Defense, “Authorities Continue to Crack Down.”
- 18 González, Naranjo, and Scotland, “Uncrewed and Under the Radar.”
- 19 “U.S. Customs and Border Protection, Air and Marine Operations Pilot Careers & Salary: A Comprehensive Guide,” Epic Flight Academy, updated January 20, 2026, <https://epicflightacademy.com/hiring-requirements-u-s-customs-and-border-protection/>; “Air and Marine Operations Assets,” U.S. Customs and Border Protection, updated July 13, 2026, <https://www.cbp.gov/border-security/air-sea/aircraft-and-marine-vessels>; and “Air and Marine Operations Operating Locations,” U.S. Customs and Border Protection, updated July 13, 2026, <https://www.cbp.gov/border-security/air-sea/oam-operating-locations>.
- 20 Howard Altman and Joseph Trevithick, “Department of Homeland Security Predator B Drones Are Orbiting over Los Angeles,” *The War Zone*, June 11, 2025, <https://www.twz.com/air/departments-of-homeland-security-q-9-reaper-drones-are-orbiting-over-los-angeles>; and Jonathan P. Miller, *Securing America’s Maritime Border: Challenges and Solutions for U.S. National Security*, Testimony before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Transportation and Maritime Security, 118th Cong., 1st sess. (March 23, 2023), <https://homeland.house.gov/wp-content/uploads/2023/11/2023-03-23-TMS-Witness-Testimony-ALL.pdf>.
- 21 U.S. Customs and Border Protection, “General Atomics MQ-9 Unmanned Aircraft System,” fact sheet, April 29, 2025, https://www.cbp.gov/sites/default/files/2025-04/250429%20FY24%20AMO_10_General%20Atoms%20MQ-9%20Unmanned%20Aircraft%20System.pdf.
- 22 Miller, *Securing America’s Maritime Border*.
- 23 Dave Long, “CBP’s Eyes in the Sky,” U.S. Customs and Border Protection, updated December 29, 2025, <https://www.cbp.gov/frontline/frontline-november-aerostats>.
- 24 Miller, *Securing America’s Maritime Border*.
- 25 U.S. Department of Homeland Security, “Privacy Impact Assessment for the Air and Marine Operations Surveillance System (AMOSS),” U.S. Department of Homeland Security, July 22, 2013, <https://www.dhs.gov/publication/air-and-marine-operations-surveillance-system>.
- 26 Miller, *Securing America’s Maritime Border*; Long, “CBP’s Eyes in the Sky.”
- 27 “HC-130J Long Range Surveillance Aircraft,” U.S. Coast Guard, <https://www.dcms.uscg.mil/Our-Organization/Assistant-Commandant-for-Acquisitions-CG-9/Programs/Air-Programs/LRS-HC-130J/>.
- 28 DHS official, interview by CSIS, August 12, 2026.

- 29 Elizabeth Hutton, “Maritime Law Enforcement on the High Seas: Authority, Jurisdiction, and the Seizure of *The Skipper*,” *Just Security*, December 22, 2025, <https://www.justsecurity.org/127791/maritime-law-high-seas-seizure-skipper/>; and Marshall Grant, “Unmanned Systems for Coast Guard Maritime Domain Awareness,” U.S. Naval Institute, *Proceedings* 152, no. 4 (April 2026), <https://www.usni.org/magazines/proceedings/2026/april/unmanned-systems-coast-guard-maritime-domain-awareness>.
- 30 Joe Brock, “U.S. Revives Cold War Submarine Spy Program to Counter China,” Reuters, September 21, 2023, <https://www.reuters.com/investigates/special-report/usa-china-tech-surveillance/>.
- 31 Saildrone, “Saildrone Supports Coast Guard Missions in the Great Lakes and Northeast,” press release, May 11, 2026, <https://www.saildrone.com/news/saildrone-supports-us-coast-guard-missions-great-lakes-northeast>.
- 32 Saildrone, “Saildrone Voyager Helps Navy Seize \$81 Million in Cocaine,” press release, August 4, 2026, <https://www.saildrone.com/news/saildrone-voyager-helps-navy-seize-81-million-usd-cocaine>; and Lisa West, “Saildrone USV Credited in \$81m Cocaine Interdiction,” *UK Defence Journal*, August 4, 2026, <https://ukdefencejournal.org.uk/saildrone-usv-credited-in-81m-cocaine-interdiction/>.
- 33 “Planned Wind Farms in the United States,” Cleanview, updated October 2026, <https://www.cleanview.co/power-projects/planned/wind-farms/us>.
- 34 Saab, “Securing the World’s Largest Offshore Windfarm with Giraffe 1X,” press release, November 19, 2021, <https://www.saab.com/markets/norway/press-releases/securing-the-worlds-largest-offshore-windfarm-with-giraffe-1x>.
- 35 Sofie M. Van Parijs et al., “NOAA and BOEM Minimum Recommendations for Use of Passive Acoustic Listening Systems in Offshore Wind Energy Development Monitoring and Mitigation Programs,” *Frontiers in Marine Science* 8 (2021): 760840, <https://tethys.pnnl.gov/publications/noaa-boem-minimum-recommendations-use-passive-acoustic-listening-systems-offshore-wind>.
- 36 Hugo Díaz and Carlos Guedes Soares, “Review of the Current Status, Technology and Future Trends of Offshore Wind Farms,” *Ocean Engineering* 209 (2020): 107381, <https://doi.org/10.1016/j.oceaneng.2020.107381>.
- 37 Bernd Drapp and Matthias Mildner, “Enhancing Coastal Critical Infrastructure Protection with Distributed Acoustic Sensing (DAS)” (paper presented at meeting of Undersea Defence Technology, Oslo, Norway, March 25-27, 2025), https://www.apsensing.com/media/1813/download/2025-03%20Enhancing%20Coastal%20Critical%20Infrastructure%20Protection%20with%20Distributed%20Acoustic%20Sensing%20-%20Drapp%20B._DAS_Critical_Infrastructure_Subsea_Cables.pdf?v=1.
- 38 González, Naranjo, and Scotland, “Uncrewed and Under the Radar.”
- 39 AP Sensing, “Fiber Optic Monitoring for Offshore Wind Export Cables,” press release, May 18, 2026, <https://www.apsensing.com/en/news/case-study-fiber-optic-monitoring-for-offshore-wind-export-cables>.
- 40 “Cable Risk Intelligence at Your Fingertips,” Indeximate, <https://indeximate.com/scattersphere/>.
- 41 U.S. Small Business Administration, “Power and Communications, Sensor, Defense Node (PACSD),” Small Business Innovation Research, 2024, <https://www.sbir.gov/awards/208653>.
- 42 Mighty Waves Energy, PACSD presentation to CSIS researchers in Washington, D.C., July 23, 2026.
- 43 Frank Rusco et al., *Offshore Wind Energy: Actions Needed to Address Gaps in Interior’s Oversight of Development* (Washington, DC: U.S. Government Accountability Office, April 2025), 27, <https://www.gao.gov/products/gao-25-106998>.

- 44 “Mitigating Wind Turbine Radar Interference,” U.S. Department of Energy, <https://www.energy.gov/cmei/systems/mitigating-wind-turbine-radar-interference>.
- 45 Jennifer M. Granholm et al., *Update on the Efforts of the Wind Turbine Radar Interference Mitigation Working Group* (Washington, DC: U.S Department of Energy, February 2024), 3, <https://manuals.plus/m/28c7dc05e55a8403dec96990adbb6f5e84b80bc5d4afaaee12d0069d206552b7.pdf>.
- 46 “In-Fill Mitigation for Wind Farm Radar Interference,” Pager Power, updated April 25, 2016, <https://www.pagerpower.com/news/in-fill-mitigation-for-wind-farm-radar-interference/>.
- 47 “Regulatory Framework and Guidelines,” Bureau of Ocean Energy Management, <https://www.boem.gov/renewable-energy/regulatory-framework-and-guidelines>.
- 48 *Military Aviation and Installation Assurance Clearinghouse for Review of Mission Obstructions, U.S. Code 10* (2024), § 183a, <https://law.justia.com/codes/us/title-10/subtitle-a/part-i/chapter-7/sec-183a/>.
- 49 Dragos, Inc., “Assessing Industrial Cyber Risk to the European Wind Industry,” Dragos, April 5, 2023, <https://www.dragos.com/blog/assessing-industrial-cyber-risk-to-the-european-wind-industry>.
- 50 Anna Knack, Yvonne Kam Hwei Syn, and Kimberly Tam, *Enhancing the Cyber Resilience of Offshore Wind* (London: The Alan Turing Institute, *CETaS Research Reports*, June 2024), 18, 37, <https://cetas.turing.ac.uk/publications/enhancing-cyber-resilience-offshore-wind>.
- 51 *Ibid.*, 30-39.
- 52 John Konrad, “NOAA Joins Forces with Big Oil to Share Ocean Data,” gCaptain, August 25, 2011, <https://gcaptain.com/noaa-joins-forces/>; National Oceanic and Atmospheric Administration, “NOAA Signs Data-Share Agreement with Offshore Wind Energy Company,” press release, March 29, 2021, <https://www.noaa.gov/media-release/noaa-signs-data-share-agreement-with-offshore-wind-energy-company>.
- 53 Baltic Wind, “Poland Reframes Offshore Wind as Critical Infrastructure amid Baltic Hybrid Threats,” Baltic Wind, June 12, 2026, <https://balticwind.eu/poland-reframes-offshore-wind-as-critical-infrastructure-amid-baltic-hybrid-threats/>; and France Energies Marines and France Cyber Maritime, “France Energies Marines and France Cyber Maritime Join Forces to Enhance Offshore Wind Cybersecurity,” press release, April 14, 2025, <https://www.france-energies-marines.org/wp-content/uploads/2026/08/251104-cp-FEM-France-Cyber-Maritime-EN.pdf>.
- 54 “Maritime Security Strategy,” European Commission, https://oceans-and-fisheries.ec.europa.eu/maritime-security/maritime-security-strategy_en.
- 55 EU Directorate-General for Energy, “Commission Welcomes Renewed Commitment to Power Clean, Independent and Secure Offshore Energy in the North Seas Region,” press release, January 26, 2026, https://energy.ec.europa.eu/news/commission-welcomes-renewed-commitment-power-clean-independent-and-secure-offshore-energy-north-seas-2026-01-26_en.
- 56 Wlodek Rzycki et al., “When Offshore Wind Meets National Security: Lessons from Selected European Markets,” Couto, Graça & Associados, August 6, 2026, <https://www.cga.co.mz/en/moz/legal-updates/when-offshore-wind-meets-national-security-lessons-from-selected-european-markets>.
- 57 “About the Project,” Baltic Power, <https://balticpower.pl/about-the-project/>.
- 58 “Europe’s Wind Farm Army,” Support4Partnership, <https://support4partnership.org/en/news/europes-wind-farm-army>.
- 59 International Comparative Legal Guides, “Belgium - Shipping Laws and Regulations 2026,” September 21, 2026, <https://iclg.com/practice-areas/shipping-laws-and-regulations/belgium#section08>; and Gaëtan Motmans, “The New Maritime Security Law: Belgian Navy’s Role in the Legal Shield for Protection of

Critical Infrastructure,” *Marineblad* 135, no. 5 (2025): 14-20, https://www.marineblad.nl/images/Marineblad/2025/Nr._5/Motmans%20G.%20The%20New%20Maritime%20Security%20Law%20Marineblad%20nr.%205%20augustus%202025%2014-20.pdf.

60 Ibid.

61 Peter Buysrogge et al., “Proposition de Résolution 3228/001 Concernant l’extension de Notre Espace Maritime aux Fonds Marins en Vue de Protéger Notre Infrastructure Sous-Marine Critique” [Motion for Resolution 3228/001 Concerning the Extension of Our Maritime Area to the Seabed with a View to Protecting Our Critical Undersea Infrastructure], Belgian Chamber of Representatives, March 15, 2023, <https://www.dekamer.be/FLWB/PDF/55/3228/55K3228001.pdf>.

62 Motmans, “New Maritime Security Law.”

63 “North Sea Infrastructure Protection Program,” Dutch Ministry of Infrastructure and Water Management, <https://noordzeeloket.nl/en/functions-use/kabels-leidingen/pbni/>.

64 “About METCentre,” METCentre, <https://metcentre.no/about>.

65 Kongsberg, “Kongsberg Provides First Site Surveillance System for Norwegian Offshore Wind,” press release, April 1, 2022, <https://www.kongsberg.com/news/stories/2022/3/kongsberg-provides-first-site-surveillance-system-for-norwegian-offshore-wind/>.

66 Menno Buisman and Lukas Thiem, “Monitoring Vessel Movement above Critical Offshore Infrastructure Using Distributed Acoustic Sensing,” *Journal of the Acoustical Society of America* 160, no. 1 (July 2026): 245-57, <https://pubmed.ncbi.nlm.nih.gov/42390163/>.

67 “Offshore Wind,” RenewableUK, <https://www.renewableuk.com/our-work/offshore-wind/>.

68 Vattenfall, “Successful Demonstration of Cutting-Edge Air Defence Technology at Aberdeen Offshore Wind Farm,” press release, December 4, 2025, <https://group.vattenfall.com/uk/newsroom/pressreleases/2025/successful-demonstration-of-cutting-edge-air-defence-technology-at-aberdeen-offshore-wind-farm>; Ben Adler, “Vattenfall, ORE Catapult, LiveLink Aerospace Revolutionize Air Defence with Wind Farm Radar Tech,” *Defence Innovation Review*, December 4, 2025, <https://defenceinnovationreview.com/2025/12/04/vattenfall-ore-catapult-livelink-aerospace-revolutionize-air-defence-with-wind-farm-radar-tech/>.

69 UK Department for Energy Security and Net Zero, “Wind Power: Radar, Question for Department for Energy Security and Net Zero,” UK Parliament, UIN 123402, April 1, 2026, <https://questions-statements.parliament.uk/written-questions/detail/2026-03-24/123402>.

70 UK Department for Energy Security and Net Zero, “Consultation | Planning for New Energy Infrastructure: Revised Draft National Policy Statements for Energy Infrastructure,” March 2023, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1159360/revised-draft-nps-for-energy-infrastructure.pdf.

71 Dan Marks, “Offshore Wind and Security in the North Sea: Key Findings from a Workshop,” Royal United Services Institute, May 30, 2026, <https://www.rusi.org/event-summaries/offshore-wind-and-security-north-sea-key-findings-workshop>.

72 Ibid.

73 “The BOEM Process,” National Wildlife Federation, <https://offshorewind.nwf.org/boem-process/>.

74 Walter Musial et al., *Offshore Wind Market Report: 2022 Edition* (Washington, DC: U.S. Department of Energy, August 2022), <https://www.energy.gov/sites/default/files/2022-09/offshore-wind-market-report-2022-v2.pdf>.

- 75 Ian M. Stevenson, “How Offshore Wind Permits Handled DOD Concerns before Interior’s Pause,” E&E News, January 5, 2026, <https://www.eenews.net/articles/how-offshore-wind-permits-handled-dod-concerns-before-interiors-pause/>.
- 76 Ibid.
- 77 “Northeast States Collaborative on Interregional Transmission,” Ralph O’Connor Sustainable Energy Institute, Johns Hopkins University, <https://energyinstitute.jhu.edu/northeast-states-collaborative-on-interregional-transmission/>.
- 78 *Outer Continental Shelf Lands*, U.S. Code 43 (2025), § 1331 et seq., <https://www.law.cornell.edu/uscode/text/43/chapter-29/subchapter-III>.
- 79 “United Nations Convention on the Law of the Sea,” opened for signature December 10, 1982, *United Nations Treaty Series* 1833 (1994): 397-581, https://treaties.un.org/doc/publication/CTC/Ch_XXI_6_english.pdf.
- 80 Ronald Reagan, “Statement on United States Oceans Policy,” speech, March 10, 1983, <https://www.reaganlibrary.gov/archives/speech/statement-united-states-oceans-policy>.
- 81 “Maritime Zones and Boundaries,” National Oceanic and Atmospheric Administration, updated March 18, 2026, <https://www.noaa.gov/maritime-zones-and-boundaries>.
- 82 U.S. Navy, U.S. Marine Corps, and U.S. Coast Guard, *The Commander’s Handbook on the Law of Naval Operations* (Norfolk, VA: Navy Warfare Library, March 2022), 1-2, https://www.marines.mil/Portals/1/Publications/MCTP%2011-10B.pdf?ver=9Qihccgl32_CwiklrnUOoQ%3D%3D.



1616 Rhode Island Avenue NW, Washington, DC 20036
202.887.0200 | www.csis.org

FOLLOW CSIS

