RAND NATIONAL DEFENSE RESEARCH INSTITUTE

MICHAEL BOHNERT, AJAY K. KOCHHAR, DANIEL JUSTICE, PAUL DELUCA

Winning the Undersea Knife Fight

A Deterrence Framework to Shape Subsea Dilemmas into Competitive Maritime Security Strategies

This research was made possible by National Defense Research Institute exploratory research funding that was provided through the federally funded research and development center contract and approved by the institute's primary sponsor.

Exploratory Analysis

Under the sea's surface, a potential battle is brewing. This battle, centered on sabotage and deception, involves energy and telecommunication infrastructure being held at risk by a mixture of adversarial, opportunistic geopolitical strategies for expansive influence and control of critical resources, trade, and core industries. The ability to observe this conflict is also more constrained. Operating below the ocean's surface is not like operating in other domains: Maneuvering is complex, and the terrain is highly dynamic.

This cross-sector threat has the potential to affect roughly $10 trillion in global value among critical economic sectors.[1] The tools necessary to carry them out are low-cost and relatively low effort to employ. Approximately 97 percent of the world's communication traverses 300 underdefended undersea cables, and new telecom and power cables are activated every year.[2] Globally, fewer than 25 cable repair ships are available. Europe obtains 50 percent of its gaseous-state natural gas from Norway, most of which is transported undersea through a single pipeline and chokepoint.[3] Similarly, global maritime ports are hubs for trading, and their infrastructure is readily targetable and difficult to protect.[4] Although domestic dependence on these interconnected undersea energy and telecom systems is pervasive in civilian life and in economic and military sectors, few of these assets are domestically owned or controlled, and they are largely unprotected against sea-based attacks.

In this report, we describe the core elements of a deterrence framework against such attacks and propose that an operationally formalized approach to competition be implemented for the undersea domain. The obscured, close-range, and often directly physical nature of this competition is cognitively distinct from other domains. Competition in this domain is opportunistic and carried out via a combination of low-tech, highly precise actions. In this context, we explore the primary issues related to this *undersea knife fight*,[5] deterrence challenges from other domains, and a way to structure options for deterrence for operational use and strategic assessments.

The undersea knife fight is defined by a combination of low barriers to entry for sabotage, high-impact potential, long timelines for detection and response, and chronically poor attribution, all of which make the domain fundamentally different from more-observable and rapidly maneuvered arenas. These characteristics create several key issues: Critical undersea infrastructure is both highly valuable and largely unprotected; hostile actions often manifest slowly and ambiguously; and legal authorities and jurisdictional boundaries leave significant gray areas for both surveillance and response. These factors generate deterrence challenges that often mirror, yet also diverge from, those in other domains: Conventional maritime deterrence lacks timely response capacity; space and cyber deterrence offer partial analogs but differ in observability and persistence; and nuclear deterrence shares the high-impact dimension but does not present analogous detection challenges. To navigate this complexity, we provide a decision framework structured around three interdependent variables: the level of attribution, the choice to reveal or conceal capabilities or knowledge, and the selection of actions that range from passive defense to vertical escalation. By linking the quality of attribution to feasible response pathways and the strategic calculus of signaling, this framework helps decisionmakers calibrate deterrent postures and identify capability or policy gaps that must be closed to credibly deter malign activity in the undersea domain.

Competition Beneath the Waves

Below the sea are hundreds of cables and pipes. Since the mid-1800s, they have come to transport the overwhelming majority of transoceanic telecommunication data and have stabilized the supply of significant quantities of offshore electric and hydrocarbon-based power (e.g., oil and gas). They also have been pivotal

for strategic, global economic and defense objectives. However, this infrastructure lies relatively unprotected on the seafloor. Each year, roughly 100–200 telecommunication cables are broken; most, but not all, such incidents arise from either natural disasters or accidents.[6] Maritime and port- and harbor-based infrastructure also represent substantial strategic and economic value and are as difficult to protect. Attacking undersea infrastructure as an asymmetric target can cripple locations with single connections and have further, global implications.

Acts of sabotage targeting pipelines and power cables are arguably the most consequential among all undersea infrastructure. Access to oil, gas, and electricity is critical to modern economies and broader survivability, and underwater pipelines are the only source for many areas. Destruction of undersea pipelines is difficult to observe and forewarn in real time or attribute with a high level of confidence. Observation often occurs only when tangible effects become visible hours, days, or months later, such as a major oil spill or complete power loss to an area. The result is potential long-term damage to economies and ecosystems.

Fundamentally, this lack of observability and attribution makes the protection of undersea infrastructure difficult and underpins *why* the undersea knife fight is different from competition in other domains. Observing an event requires a presence of some type and the ability to recognize what is occurring (perhaps before it fully transpires). Both requirements present challenges in an undersea environment: Ocean distances are large and difficult to traverse quickly, and the ability to sense, navigate, and adapt to surroundings freely dwindles quickly with location and depth. Vital and valuable strategic resources and national infrastructure can be damaged, destroyed, lost, or held at risk as a consequence. Determining what happened, who was involved, and why can take weeks, months, or years and might never be established. This could suggest that establishing the who and why is not that important; determining what happened and where certainly is, but there may be a trade-off between prevention and rapid reaction.

The undersea knife fight extends beyond critical infrastructure to nation-state competition. Naval

Fundamentally, this lack of observability and attribution makes the protection of undersea infrastructure difficult.

mining, damage to ports, sensing, naval special warfare, and other undersea warfare capabilities are all growing components.[7] The distinction from other domains is that this competition occurs deep in the ocean, out of public view. Therefore, the use of maritime activities to attack undersea infrastructure is a burgeoning problem for the U.S. Navy and U.S. allies—one that has both offensive and defensive components that must be prepared for.

The undersea knife fight is one of the last forms of nation-state competition that can remain clandestine in peacetime. Because it is difficult to observe and attribute such actions, the Navy, with its demonstrated excellence in undersea technology, is well positioned to exploit potential offensive and defensive undersea infrastructure options.

How can nations position themselves for advantage in a high-impact, low-attribution, contested undersea environment? In this report, we explore the undersea knife fight: its historical context, deterrence, why the undersea domain is different, strategies for action, and when to reveal or conceal those actions.

Undersea Assets Become Strategic Interests

Undersea telegraph cables began operation in the 1850s. With the ability to transmit in hours communication that used to take weeks, undersea telegraph cable lines quickly expanded to connect many parts of the globe by the early 1900s. These telegraph cables became so vital that, by 1865, the International Telegraph Union (now the International Telecommu-

nication Union) was established, and the Convention for the Protection of Submarine Telegraph Cables in 1884 resulted in a legal framework for the protection of such cables. However, this type of infrastructure composes only one part of the undersea knife fight—the other part is composed of the assets capable of disrupting such infrastructure.

Mines and torpedoes, initially introduced in the early 1800s as a nascent form of port defense and counter to blockades, were by the mid-1860s advancing toward an operational status. Successful employment of mines in the Russo-Japanese War led to the Convention Relative to the Laying of Automatic Submarine Contact Mines at the Hague Convention of 1907. The combination of undersea infrastructure and these new undersea weapons set the environment for the undersea battle in World War I.

One of the first acts by British forces in World War I was to sever Germany's undersea cables.[8] Both sides of the conflict extensively used naval mines for offensive and defensive purposes. In World War II, the British and the United States cut German and Japanese undersea cables, and U.S. aerially deployed mines crippled Japanese shipping. Cable-cutting and mining had significant impacts on both wars. Cable-cutting forced adversaries to use wireless broadcast technologies that had less data throughput and were easier to intercept. Sea mining protected coastlines and crippled shipping. Combining the two also causes a delay in repairing infrastructure because of the need to clear mines.

In terms of undersea warfare, 1958 was a pivotal year. The International Cable Protection Committee (ICPC) was established as a forum to promote and protect submarine telecommunication and power transmission cables. The United Nations held the first Conference on the Law of the Sea, which led to the United Nations Convention on the Law of the Sea (UNCLOS) in 1984. UNCLOS includes provisions for cables, pipelines, and underwater vehicles.

More recently, multiple telecommunication and electrical transmission cable incidents occurred in the Baltic Sea from 2022 to 2025, with suspected Russian and Chinese involvement.[9] These incidents highlight the difficulty involved in distinguishing between intentional and unintentional acts, since it is difficult to determine the intent of dragging anchors and fishing equipment. Most of these incidents still lack formal attribution even with identified boats. And even clearly intentional events involving explosives, such as the 2022 sabotage of the Nord Stream pipeline, have not received definitive attribution.

Today, nations across the world are more reliant than ever on ocean infrastructure—especially undersea telecommunication cable networks, power cables, and pipelines. This increasing reliance has far outstripped advances in technology and increases in the capacity to repair, inspect, and militarily act when this infrastructure is damaged. However, the timelines to act and respond in the undersea domain are relatively unchanged, which makes deterrence an attractive strategy.

Leveraging Deterrence for the Undersea Knife Fight

Deterrence is a presentation of a capability, incentive, or disincentive by one party to discourage another from pursuing an action that the first party believes would lead to a less favorable position for itself. For deterrence to be effective, however, the presented capability must be observable, observed, and *interpreted as intended*. Otherwise, an undesired escalation is risked, a wasteful expenditure of resources occurs, or an unintentional disclosure of the extent of one's actual capability and associated potential susceptibilities is irreversibly revealed. Complicating the matter is that different actors have varying capabilities to make observations and may interpret what they see in different ways based on their own objectives.

Deterrence plays an important, regular role in shaping national advantages in modern times and historically served as a lever in a larger, strategic

Deterrence plays an important, regular role in shaping national advantages.

arena of competing interests.[10] Similarly, irregular warfare is routinely employed during engagements to contest advantages. In irregular warfare, the context of an engagement is less precisely defined with respect to its location, timing, and the resources employed, whether they are produced domestically, repurposed, borrowed, or gifted.[11] There is a persistent, unpredictable threat that is applied to contest or destabilize asymmetries in advantage.

Both deterrence levers and irregular warfare shape an operating environment. They are also interrelated concepts: Deterrence strategically and systematically signals intent, and irregular warfare opportunistically pursues objectives and disrupts adversarial capabilities. However, the capabilities used in either concept can be vastly different in type and scope of impact.

In an undersea environment, where the collective ability to operate is expanding and viable threats to critical and strategically important infrastructure have manifested, the key determinations are (1) how to prepare and implement a strategy for addressing risks and (2) which operational issues and deterrence strategies from other domains (as discussed in the remainder of this section) can be leveraged for an undersea knife fight.

Conventional Maritime Deterrence

Traditional military deterrence theories commonly involve considerations for relative capability (the *military balance*) and the cost-benefit of conflict. Beyond these utilitarian and rational factors lie historical, national, and event-driven factors, which extend deterrence to the understanding of broad cost-benefits, such as value to allies, the risks of inviting external actors, and the risks of short- and long-term economic impacts, to name a few. The undersea domain lacks the volume of both military capacity and capability to accurately assess the military balance. This fundamental gap sets an immediate contrast with traditional conventional deterrence in that a conventional response to an action is always possible and timely even if small in comparison.

However, the asymmetric nature of the undersea knife fight presents an interesting cost-benefit paradigm for deterrence. Undersea infrastructure can be national, bilateral, or multinational in design. The simplest capability—dragging anchors to damage infrastructure—has a low barrier to entry and the potential for outsize impacts, creating a minimum capability floor for a military balance. What makes this domain unique is that an adversary that is only dependent on multinational undersea infrastructure, minimally dependent on the ocean, or critical to third-party nations may have few vulnerabilities suitable for an in-kind response. This creates highly discontinuous cost-benefit calculations in which a militarily weaker nation can have few risks of retaliation short of war to any action it takes, whereas other nations can have catastrophic implications, such as total loss of energy or telecommunications from a single undersea incident.

Maritime deterrence is crudely divided into strategies involving sea control and sea denial. Sea control occurs when command of the sea is sufficiently strong that an opposing nation is unable to directly attack commanding forces, thereby enabling military and commercial freedom of maneuver to the commanding nation. Modern examples of this environment are the British Royal Navy in the 19th century and the U.S. Navy in the latter half of the 20th century. When challenged, both navies could locally enforce sea control to contain and deter while enabling systemwide freedom of maneuver. Sea denial is the opposite. It focuses on ensuring that an opposing nation is unable to operate within a specific region without regard for military or commercial use by the denial-imposing nation. In this context, observability and the ability to respond require air and space assets to augment maritime assets over the vastness of the sea.

Decisionmakers considering either maritime deterrence strategy (sea control and sea denial) must also acknowledge that the inherent nature of irregular warfare and the opacity of the undersea domain allow adversaries to bypass sea control and enable sea denial measures. The undersea knife fight is shaped by maritime deterrence strategies, which serve as a means of achieving desired outcomes. However, this domain's aforementioned opacity and the persistent, landlike characteristics of its infrastructure—unlike the fleeting nature of surface maritime activities—reduce the applicability of traditional maritime deterrence frameworks.

Space Deterrence

The space environment (broadly speaking) affords greater observability of and accessibility for individual systems over larger ranges than in a maritime environment, with similar challenges in terms of how to respond. The barrier to enter the space domain is high; only a select few nations and companies have access. In addition, it is easier to observe an anomaly or failure in space, which slightly eases concerns about attribution and enables a potential platform for posturing. What is difficult is knowing *how to respond*: Vast distances can incur long lead times to plan, coordinate, track, and execute responses to potential aggression while expending limited resources. In many ways, such time and effort trade-offs are similar to the undersea knife fight, in that any event undersea takes significant time to plan and execute.

There are differences and interdependencies to consider, of course. For example, in the space domain, the *Kessler effect* is a theorized situation in which the concentration of debris or other, defunct objects present in orbit is sufficient to cause uncontrolled cascading collisions. The result is that the orbit effectively becomes unusable, fundamentally altering the use of an entire region of the operating environment. Although attacking undersea telecommunication and energy cables can affect many nations, there are no realistic undersea actions that would cause permanent loss of maneuverability in the sea. With respect to maneuverability and mission duration, space missions stand to benefit from energy and power system advances more readily than would undersea systems because the ocean environment has compounding negative effects on other systems as platform endurance and speed increase. The space domain also lacks broadly accepted norms for conduct.

However, space missions frequently support operations in both maritime and cyber domains. From a deterrence perspective, this overlap provides an alternative vector for a response and introduces combined defensive and offensive options. Furthermore, although there are tactical and technological differences between space and maritime domains, it has been argued that pursuing *strategic* interests of nations in a contested space environment aligns with historical *maritime* strategies;[12] perhaps some of these linkages can be retuned for *undersea* maritime strategies.

Cyber Deterrence

In cyber operations, the operational terrain is defined entirely by a human-engineered infrastructure, and the primary asset of interest is information, followed closely by command and control of the infrastructure and the ability to influence its usefulness. Cyber operations are characterized as non-kinetic but can result in potentially severe and unpredictable consequences, either to an individual entity or on a larger scale. One event could affect many aspects of a broader system, resulting in multiple effects with different consequences. Broadly, these operations are domain agnostic (e.g., air, land, sea, space, financial, political) with respect to the fundamental tools, apply to the loss of information or its exploitation by adversarial actors, and may entail the loss of control over, or loss of the use of, critical infrastructure systems.

Cyber operations are necessarily *persistent* in their pursuit of threats and ways to address such threats; because of their clandestine nature, attribution is a complicating challenge. When such operations are pursued at a national level and combined with the exploitation of vulnerabilities, nation-state actors can continuously contest and shape a security environment.[13] Cyber operations (especially adversarial ones) may require long time frames for reconnaissance, planning, prepositioning of tools, and execution. As with undersea operations, the details of the terrain are not well known ahead of time: Extensive planning is required in both cases. Some of the developed tactics might inform coordinated defensive operations in a continuously contested undersea environment. From a deterrence perspective, successive space, cyber, and maritime events also have cumulative effects on the risk calculus applied at a strategic level.

Nuclear Deterrence

Nuclear deterrence provides a natural starting point for discussion of an existential threat, considering

its importance in shaping the post–World War II global state. Nuclear platforms simultaneously assert both the military and technological capabilities of a society, presenting an overwhelming advantage that can result in devastating and enduring consequences if used. However, no nation possesses the ability to detect or defend against the launch of an undersea infrastructure attack (in contrast to a nuclear threat) with a large potential impact in an undersea environment. At best, the growing undersea telecommunication infrastructure may act as a post-event sensor network for localizing the event. Although telecommunication infrastructure is ideally engineered to be robustly networked, the global dependence on this geographically expansive infrastructure for economic and governance activities represents a substantial, exploitable risk. And this risk, though potentially large in scope, has no accompanying system for the detection of imminent threats.

The Undersea Domain Is Different

Maritime history is filled with examples of strategies and tactics that exploit stealth, timing, deception, and other overt means to overwhelm perceived adversaries; all these methods are tuned to maritime environments and have analogs across the space, cyber, air, and land domains. The intrinsic challenge in the maritime domain is the time and effort required to maneuver and then employ, deliver, and verify effects. All these activities occur in an environment in which the terrain is natively dynamic: It is literally and figuratively fluid.

Although these characteristics largely apply to the undersea arena, there are conceptual differences that matter in the context of deterrence and response—in terms of the visibility of the seafloor, barriers to entry, and the timing of impact, for example. High-resolution mapping of the seafloor is difficult and costly: Roughly 26 percent of the ocean floor has been mapped to a high resolution,[14] but it is unclear whether the level of resolution is operationally sufficient for infrastructure defense, especially over large geographic areas and variable depths. Nevertheless, when comprehensive, high-quality seafloor maps become available, public datasets will likely accelerate undersea competition (both militarily and commercially) for strategic resources and territorial claims. These maps address only one aspect of the operational terrain, however. The other aspect involves understanding the details of the ocean currents in the water columns being traversed, including their dynamics.

What separates the undersea knife fight is the low barrier to entry: Even basic anchors can cause significant damage.

Successful operations in all domains require detailed planning to achieve targeted effects. What separates the undersea knife fight (especially undersea infrastructure) is the low barrier to entry: Even basic anchors can cause significant damage. Thus, the most basic form of undersea sabotage (cable-dragging) has a lower barrier than even cyberspace sabotage and only exceeds lone-wolf terrorism because of the need for a boat. At the same time, more complicated undersea military operations can involve submarines with capabilities that are more costly and more complex than the capabilities in most other systems. Where this difference is most striking is how the possibility of precision and concealment directly scale with the cost of the employed knife-fight capability.

Unlike in most other domains, only some undersea actions have a sudden impact. Many offensive, deterrent, and defensive operations have significant time lags that take months, years, or even decades to fully manifest. The ability to determine mission success or failure often arises months or years later. A severed cable or destroyed pipeline is almost immediately known, but a damaged cable may fail many days, weeks, or months later. Similarly, without

extensive and complex sensing and surveillance capabilities, the precise reason for a performance change in a disrupted or tapped cable segment may only be discoverable after a substantial effort is applied and specialized resources are employed. A pipeline sabotage can intentionally be time delayed or designed to only occur after significant use. Even today, sea mines from World War I remain a threat to maritime shipping and port infrastructure. The potential for delayed impact creates a dilemma for deterrence. The timescales involved can render deterrent options functionally useless or counterproductive if tensions in other domains are solved well within the time frame of undersea operations. The lack of communication and high degree of autonomy limits the ability to abort operations.

As with other domains in which irregular warfare, terrorism, and other criminal acts occur, local and regional law enforcement plays a role in the undersea domain. This civilian-military overlap creates friction in enforcement and gaps that can be exploited. For example, UNCLOS limits who can do what and where actions can be taken against a ship, but few formalized restrictions in available regulatory frameworks exist for the underwater domain.

International cooperation on the engineering of resilience in submarine cable systems is also necessary among a broad variety of stakeholders with overlapping and potentially competing interests and maritime authorities (commercial, governmental, and international). To ensure the availability of critical services globally across private and public sectors, the International Telecommunication Union and ICPC formed the International Advisory Body for Submarine Cable Resilience in 2024. The challenge here stems from the fact that undersea cable systems are extremely large in in terms of both the geographical extent and the number of geopolitical boundaries traversed.

Time, Range, and Depth Dominate Undersea Operations

The undersea and topside domains have very different timescales for movement and operations, which results in a significant difference in perceptions related to understanding, attribution, and action. These differences create a significant asymmetry in situational awareness, as represented in Figure 1. Situational understanding above water can be expected in hours or days. Situational understanding underwater can easily take months or, in some cases, years depending on depths and ocean environments.

This difference becomes especially apparent when comparing domains by search time after an event. In the space domain, satellites—which pass over many areas of the earth hourly (or even more frequently) and can view hundreds of square miles during each pass—enable situational understanding within minutes to an hour. High-altitude jet aircraft can travel to a search range and investigate within several hours. Medium-altitude propeller unmanned aircraft systems (UAS) can perform this mission within half a day. Helicopters, small UAS, or manned vehicles can arrive and perform searches over ground events. Although attribution may be slower, identifying what happened is likely within a few days.

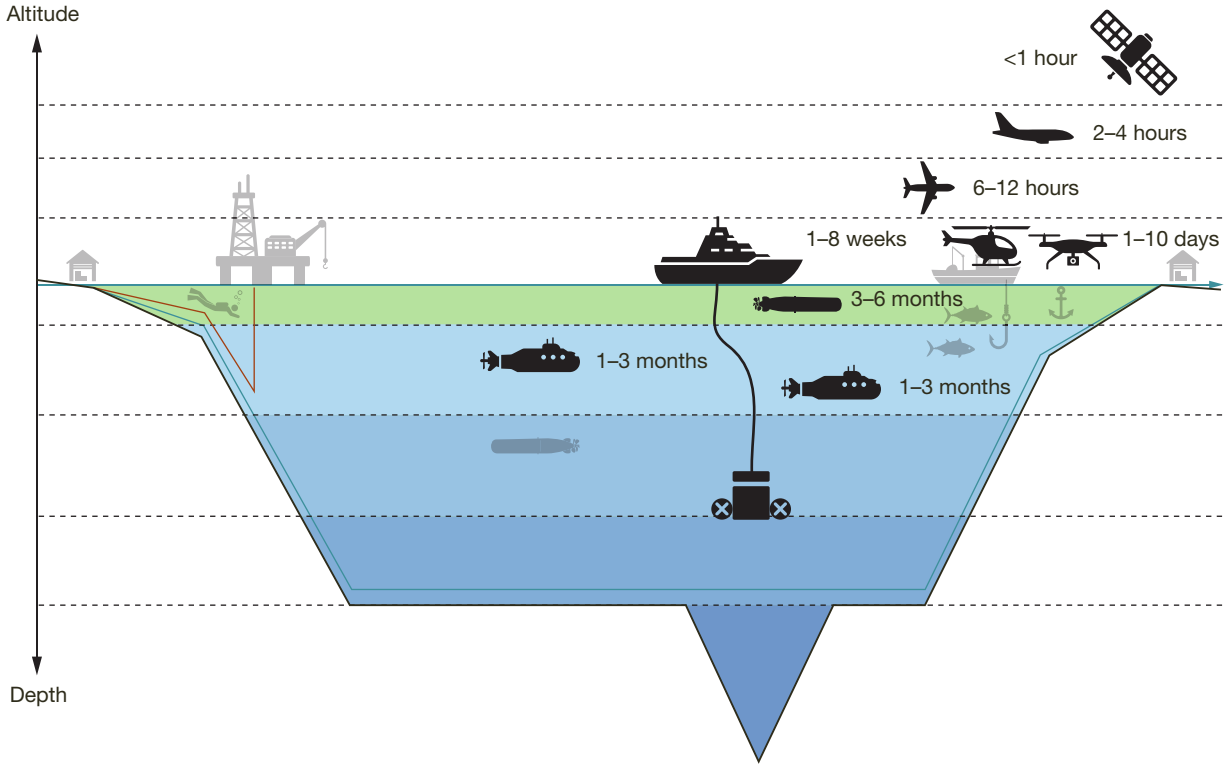
Undersea searches take significantly longer. Sending a surface ship to investigate an undersea event takes days, if not weeks, for the ship to arrive on station, and the search takes even longer. The mission to find the sunken submarines USS *Scorpion* and USS *Thresher*, for example, took two months of dedicated search time in addition to preparation and transit.[15] Sonar searches are slow, and imaging sonar has ranges measured in hundreds of feet. Remotely operated vehicles take hours to get to depth, and then searches can take weeks or even months, as evidenced by ocean aircraft crash searches.

Performing this mission covertly underwater takes even longer. It takes time for submarines to move from a base or station. Imaging sonar means a slow search, and such searches could take months. Operation Ivy Bells to tap Soviet cables in the Sea of Okhotsk took four months of mission time, in addition to planning and engineering modifications made to the USS *Halibut*.[16] The submarine then would need to return to port to provide findings.

A mission conducted by an autonomous, uncrewed underwater vehicle (UUV) would take even longer than submarines. A UUV's battery and diesel power and the craft's resulting speed are fractions of the power and speed of nuclear submarines, constraining the vehicle's ability to maneuver a dynamic and poorly mapped deep ocean environ-

FIGURE 1

Time to Arrive on Station



NOTE: Timelines are based on transit times and guidance on a craft's earliest ability to respond. From top to bottom: Satellite estimates are based on orbit density. Manned fixed-wing aircraft estimates are based on high-subsonic-speed platforms. Large fixed-wing unmanned aircraft estimates are based on mid-to-low-subsonic platforms. Manned and unmanned rotary-wing aircraft estimates account for time to plan and position. Surface craft with tethered remote systems are assumed to transit nominally at 15 knots from distances within a theater. Robotic and autonomous platforms require planning and availability and transit at significantly slower speeds than surface craft. Submarines transit at low speeds, and distance from an event varies throughout the theater.

ment. Every additional day of travel limits time on station to search; multiple trips may be required. The Cold War example of Operation Ivy Bells took months for a very specific operation; this time delay and level of effort for each undersea investigation complicates timely attribution.

Attribution Is a Core Challenge

Attribution is also more challenging in the undersea arena. What course of action is a suitable response when what occurred (and who was responsible) is unknown, given a range of potential outcomes in the short or long term? Without attribution, the consequences resulting from an event might be incorrectly associated with a nation or other actor. Similarly, the intent of the actor may be misconstrued, and the capabilities that were employed may be over- or underestimated. For these reasons, attribution matters.

Attribution assessments must be swift to focus attention on and establish a direct linkage to an incident. Yet, as noted earlier, attribution is constrained by the ability to correctly infer causes, methods, and intent. Unless an actor comes forward and irrefutable evidence is presented, it is largely a game of belief. Understanding what occurred is the first part of the problem; actual attribution can take longer. If the searching vessel takes weeks to arrive, whoever caused the problem is likely gone. Even if ships overhead of an incident can be identified, it is hard to prove responsibility. Incidents can happen in any number of ways and may have been executed in a way that incurs intentional delay. Most of the 2022–2025 Baltic cable and pipeline incidents have yet to be formally attributed.

We developed a rubric that associates a qualitative level of attribution to candidate attacks. These levels act as aids for determining resource prioritization and the applicability of risk mitigation measures or can inform broader discussions regarding strategic or tactical protection measures. In this way, assessing a level of attribution might be viewed as an intelligence activity or a component of a larger mission-planning tool. Candidate attacks would be informed by prior knowledge of potential actors, actor intents, and actor capabilities.

Our proposed levels of attribution, outlined in Table 1, span from no attribution (when nothing can be understood about the event) to self-identified attribution (when the actors present themselves in an obvious, verifiable manner). This rubric is by no means exhaustive of all potential nuance but provides a high-level categorization at the fidelity intended for public discourse.

The level of attribution has a direct effect on which actions can and cannot be taken against the actor responsible. Poor attribution enables few responses that prevent unnecessary escalations, whereas strong attribution enables a full set of military and nonmilitary options. Attribution is also a necessary step to expand potential responses beyond military options, such as undertaking political or legal actions against the perpetrator.

Beyond determining who acted, the means, methods, and motivations must be understood. The questions "How was the action performed?" and "Was the action simple or complex?" directly relate to how one defends and reacts to future incidents. Was it an unintentional operation, an isolated incident, a response to a particular action, or part of vertical or horizontal escalation? The motivations influence the response. Accidents or responses to unintentional escalation can be ignored, whereas intentional actions necessitate a response.

The Legalities and Authorities are Murky

The legal authorities and laws regarding undersea actions are complicated and poorly defined.[17] Actions within 3 nmi of coastlines tend to fall under the jurisdiction of local law enforcement. Actions within the 12-nmi territorial waters tend to fall under national jurisdictions and laws, and there is limited ability to enforce laws between 12 and 24 nmi. Actions within the 200-nmi exclusive economic zones, international waters, and other national waters are even more complicated in scope and are subject to disputes.[18]

Furthermore, it is not entirely clear which actions are legal in peacetime.[19] Surveying infrastructure without permission is legal in most waters. Severing cables, destroying pipelines, surveying infrastructure, and placing sensors clearly constitute acts of war worthy of military response only if the

TABLE 1
Levels of Attribution

Attribution Level	Description
Self-identified	Actors present themselves and produce obvious, verifiable evidence of their contributions to the incident.
Clear	Actors are clearly identified through systematic analysis of evidence, with confirmation verified and established by multiple sources and methods; the presented evidence cannot be repudiated.
Disputable	Candidate actors are clearly identified, but confidence is limited by incomplete intelligence regarding the incident; attacks or involvement are plausibly deniable.
Inferred	Candidate actors are inferred by characterizing the means applied or identified as necessary to execute an attack. The precise roles and extent of the contributions of potential actors remain inferential and based on circumstantial evidence and prior knowledge.
Categorical	The body of evidence (including historical considerations) indicates the potential for adversarial activity, with profiles of required capabilities partially determined.
None	Investigators are unable to determine the cause or fail to clearly discern the methods or perpetrators (whether natural, nonadversarial, or adversarial) of an event with available resources.

action is of catastrophic effect to the nation (e.g., causing severe economic damage or major ecological crisis). In wartime, authorities are significantly broader.[20] Governing laws and authorities include UNCLOS and the 1884 Convention for the Protection of Submarine Telegraph Cables, along with the ICPC, U.S. Cybersecurity and Infrastructure Security Agency, and many others, each with specific authorities. Figure 2 illustrates these authorities in the U.S. context in relation to coastlines and jurisdictions.

The question of who has the authority to act against a vessel causing an underwater incident is even more complex. Under UNCLOS, when a ship commits a crime in international waters, it is the responsibility of the country the ship is flagged under to handle legal matters. This limits a nation's ability to respond to an event, such as sabotage, by boarding, searching, and seizing a vessel. Exceptions are actions to stop an environmental disaster (e.g., oil spill) or an act of terrorism (e.g., acts involving explosives). How these laws apply to stopping uncrewed vehicles is even more opaque.

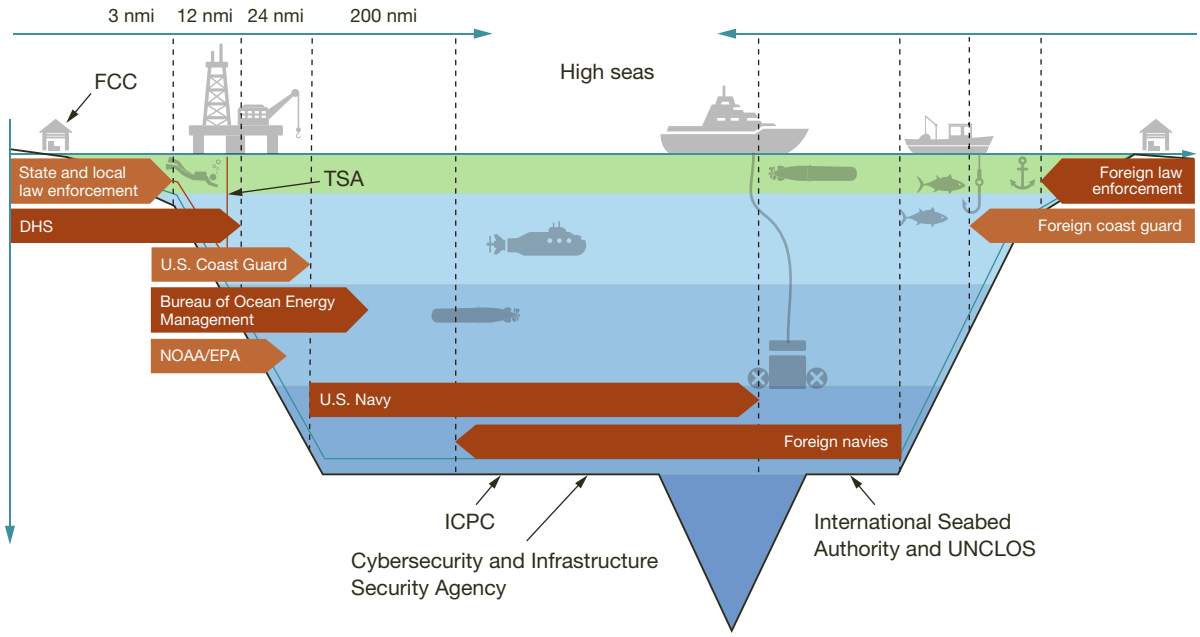
Competing in the Knife Fight

The differences in the undersea domain relative to other domains fundamentally affect how the United States competes and engages with adversaries.[21] The potential timelines, ranges, and depths for undersea operations necessitate deliberate decisions for their execution. These decisions require not just the capability but also an understanding of attribution and the larger consequences of any actions.

This dynamic results in several difficult choices. The lack of timely accessibility results in costly and lengthy responses with potentially enduring consequences. Who can act and whom they can act against are dictated by long-term investments. What is more prominent in the undersea domain is an understanding of the implications of revealing and concealing knowledge and capabilities prior to other decisions. The mere act of revealing or concealing can render entire capabilities useless and limit future capabilities for years.

FIGURE 2

Operational Authorities



SOURCES: Features information from UNCLOS; Gallagher et al., *Protection of Undersea Telecommunication Cables*; and Murphy, *Redundancy, Resiliency, and Repair*.

NOTE: DHS = U.S. Department of Homeland Security; EPA = Environmental Protection Agency; FCC = Federal Communications Commission; NOAA = National Oceanic and Atmospheric Administration; TSA = Transportation Security Administration.

Revealing or Concealing Undersea Activities Is a Tough Choice

In peacetime, it is a strategic choice to reveal or conceal an action or the observation of an action. Revealing an action provides the opportunity to use public perception and pressure against an adversary to compel them to stop or cause others to act. However, revealing an action also exposes the ability to detect and react. Concealing the knowledge of an adversary's action can keep one's capabilities unknown or de-escalate a situation. Concealing one's own action can result in more subtle escalation or can maintain a level of ambiguity. Table 2 outlines a spectrum of revelation and concealment.

The decision to reveal or conceal is directly linked to the level of attribution and understanding of undersea incidents. Without strong attribution or knowledge of the incident, only defensive measures or acknowledgment of an incident can be revealed. However, very low-intensity reactions that are unnotified and unacknowledged can be used to prompt other actors to respond. These subsequent responses can be observed to help with attribution if the incident is repeated or the actor reveals what they know.

The act of revealing can itself be a deterrent because it demonstrates the minimum ability to detect, investigate, and monitor undersea activity. Acts of revealing offensive or active defensive capabilities on inconsequential or even one's own systems have previously served a similar deterrent role, although these revealing actions can cause unintended escalation. Prior examples of both have occurred in the space domain.

Choosing How to Act Is Tougher

There are many ways to act and react in the undersea domain. A precautionary mindset can lead to a focus of peacetime actions being limited to sensing, surveying, and defense versus taking more-offensive operations. This results in a more reactive posture. Reaction is not always necessary; however, a limited suite of options invites future aggression. Options need not be kinetic or destructive in nature; the use of public pressure is a viable nonkinetic response. Physical options are also not necessarily military in nature: Two examples are legislating increased defensive hardening and contracting repair ships on standby. Furthermore, options need not be in the undersea domain, allowing a nation to focus on its national strengths to respond. Table 3 provides a spectrum of option categories.

However, what, when, and how to act and react must be weighed in consideration of the impact on deterrence, level of attribution, risk posture, chosen posture with respect to revealing, and actor. For example, although continuously surveying an adversary is not itself aggressive, the act could alter perceptions of future aggression if discovered. On the other hand, choosing to do nothing could, depend-

TABLE 2
Degrees of Revealing and Concealing

Degrees of Reveal and Conceal	Description
Publicly announced	The government fully reveals an initial action or a response.
Publicly discoverable	The public can see clear evidence of a response, but no public statement confirms or denies involvement. This could also be intentionally announced by a nongovernment entity.
Privately acknowledged	The government privately notifies the other government.
Unacknowledged but militarily discoverable	A reaction occurs that is attributable by an adversary but is not discoverable by the public.
Unnotified but covert response	A reaction occurs that is not attributable but either demonstrates an ability or creates a tangible effect.
Defensive and planning	Actions are taken to harden locations and plan response, but there is no direct linkage to an incident.
None	The government fully conceals knowledge or attribution of an incident.

TABLE 3
Undersea Option Categories for Acting and Reacting

Option	Description
Vertically escalate	Perform actions that are relatively greater in number, greater in intensity, or both
Horizontally escalate	Perform actions that significantly differ from existing operations, including in different domains
Respond in kind, or active status quo	Either perform a similar act to what was performed, continue with status quo–style operations, or take actions to prepare for future operations, such as surveying or prepositioning assets
Active defensive	Actively patrolling and defending locations
Reveal	Choose one of the reveal methods
Passive defensive	Take such actions as placing sensors or putting protective barriers around sensitive areas

ing on the actor, either lead to de-escalation or invite further escalation. Options can signal which of one's capabilities are important based on the pace and scale of a response. Given the scarcity of capacity and variety of options, revealing and concealing is always a strategic decision.

Active defensive options may be the most versatile because they provide a broad set of options for deterrence, attribution, and revealing or concealing and incorporate a controllable time element. These options also can demonstrate ability and provide some degree of preparation for future offensive actions without encroaching on a potential adversary's territory. As an example, a visible, routine patrol of a cable signals the priority of that cable and serves as an active deterrent. A visible deviation from a patrol could reveal a detection capability but could also be a false alarm, generating ambiguity about capabilities. Active defenses provide a near-immediate signaling and response, whereas most other options take months or years. Detecting an adversary action, doing nothing immediately, then taking a separate action over an ever-shortening time frame to match public and diplomatic attention results in a delayed revelation that demonstrates overall capabilities without necessarily divulging or revealing specifics.

To be clear, the undersea knife fight is fundamentally a continuous series of actions and reactions. It is constantly occurring, whether acknowledged or not.

Who Acts, and on What, Is Set by Long-Term Investments

Who acts on what is what brings all elements together. One key aspect of the undersea knife fight is the spectrum of simple, low-cost options up to some of the most complex and most expensive military equipment in existence. As in a knife fight, these options are often specific, opportunistic, and close proximity and involve simple technology. Most low-cost options are either incredibly targeted (divers) or incredibly blunt (dragging a cable cutter). These options also are often readily resourced. Additional resources buy improved concealment and sophistication. It is difficult to hide a surface ship dragging an anchor but relatively easy to conceal a UUV launched from miles away. Presently, no nation has established an advantage for undersea infrastructure defense; doing so requires long-term investments in corresponding protection and deterrence capabilities.

Determining the rough classes of systems and targets involved in the undersea knife fight, organized by cost and accessibility, may help structure an investment strategy (Table 4). Examples of cheaper, more accessible systems include divers, dragging anchors, fishing equipment, and trawlers. Among the higher-cost, less accessible systems are surface vessels using remotely operated vehicles, UUVs, and submarines. As mentioned earlier, the full variety of maritime infrastructure and natural resources are potentially at risk to targeted attacks, including port infrastructure, power distribution and telecommunication cables, energy infrastructure (especially hydrocarbon based), undersea sensors, naval vessels,

TABLE 4
Example Systems, by Increasing Complexity

System	Description
Anchors and fishing nets	These examples (among other equipment) are dragged behind private, commercial, or government boats. They are capable of breaking cables and damaging pipelines but are relatively indiscriminate.
Divers	These are individual people or animals trained to survey, deploy, repair, or damage undersea infrastructure. They operate in limited depths.
Remotely operated vehicles	These are mobile systems deployed from a surface or undersea vessel and usually are controlled by a person. They are able to survey, deploy, repair, or damage undersea infrastructure at depths below the range of divers.
Cable-laying platforms	These are large surface vessels capable of laying and repairing transoceanic cables.
Deployed devices	These are autonomous or semiautonomous objects left undersea to perform a specific function and could be mines, sensors, or other to-be-determined capabilities.
UUVs	These are autonomous vehicles of varying sizes that can survey, deploy, repair, or damage undersea infrastructure. They are relatively slow and limited in range.
Submarines	These are undersea warships with significant capacity for a variety of undersea missions. They are able to operate undetected for long durations.

and fisheries.[22] Each target naturally links to one or more areas of industrial, economic, national, and strategic value. When viewed in this way, the options can inform a prioritized capability portfolio.

These capabilities are portrayed in Figure 3. Recovery systems are not included in this picture for simplicity. However, a capability to rapidly provision resources and perform repairs may have a deterrent effect, similar to a "fleet in being" as a strategic concept.[23] Such a capability may limit an adversary's view of the potential impact of expending resources for an action. In turn, the component systems of such supply chain capabilities are also targets.

A New Framework for Decisionmakers

Competing in the undersea knife fight requires a framework that incorporates deterrence, attribution, legal frameworks, revelation and concealment, actions and reactions, systems, and targets. Deterring adversaries in the undersea knife fight is the desired end state, but thresholds and risk tolerances vary by actors and nations. The peacetime and wartime legalities of the undersea knife fight are vague and subject to interpretation. The systems available to act and react are dictated by national investments and priorities. The targets are defined by the infrastructure and level of dependence on that infrastructure.

The remaining variables—attribution, the choice to reveal or conceal, and the choice to act or react—serve as common denominators in undersea knife fight situations. The matrix in Table 5 illustrates the interaction of these three factors. The framework highlights which actions and reactions (columns) are available to reveal and conceal (rows) and to act and react as a function of attribution (colors). The greater the level of attribution, the more-rational options one has for revealing and acting, and vice versa. Note that the color indicates the minimum attribution level necessary to take the combined action/reaction and reveal/conceal choice.

The matrix shows an approximation of the minimum level of attribution that reasonably fits with existing, but potentially aggressive, Western norms. As an example, if one discovers intentionally damaged underwater infrastructure was but is only able to make a categorical attribution, then only categorically labeled (light blue in Table 5) options to reveal/conceal and act/react, such as a covert defensive action, are reasonable. Reasonable examples are taking covert active defenses or planning for responding in kind. It is reasonable to reveal something has occurred from a defensive and planning standpoint or to perform unnotified but covert

FIGURE 3

Mixed Options for Defense and Deterrence—Friend and Foe

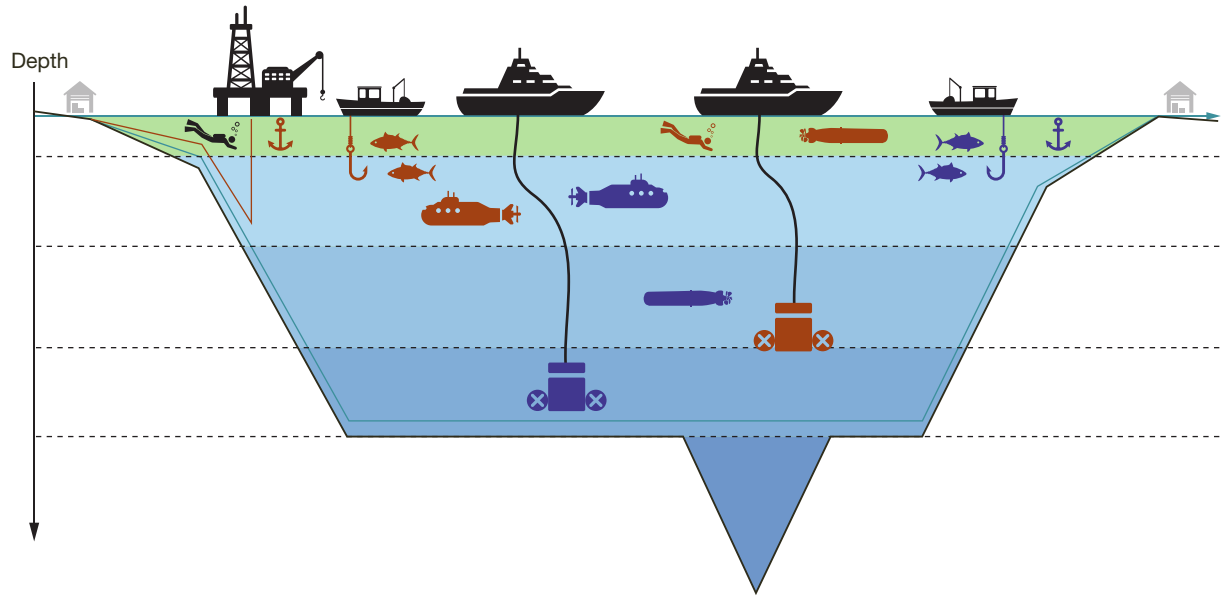


TABLE 5

Decision Support Matrix

	Actions and Reactions						
Reveal and Conceal Choice	**Nothing**	**Reveal**	**Passive Defensive**	**Active Defensive**	**Respond in Kind or Active Status Quo**	**Horizontally Escalate**	**Vertically Escalate**
Nothing	None	N/A	N/A	N/A	N/A	N/A	N/A
Defensive and planning	None	None	None	None	Categorical	Inferred	Disputable
Unnotified but covert	Categorical	Categorical	Categorical	Categorical	Inferred	Disputable	Clear
Unacknowledged but militarily discoverable	Categorical	Inferred	Inferred	Inferred	Disputable	Clear	Self-identified
Privately acknowledged	Categorical	Inferred	Inferred	Disputable	Clear	Clear	Self-identified
Publicly discoverable	Inferred	Disputable	Disputable	Clear	Clear	Self-identified	Self-identified
Publicly announced	Disputable	Clear	Clear	Clear	Clear	Self-identified	Self-identified

limited passive or active defenses. It is not reasonable to overtly (in a publicly discoverable way) vertically escalate by damaging another country's infrastructure without significant improvements in attribution. Decisions regarding actions, revealing or concealing intentions, and the use of attribution are determined by actors and adversaries based on their own criteria.

This matrix is intended as a tool to help identify and define deterrence questions, future legal reforms, and capability gap analyses and investments. Investments in attribution and response capabilities must be aligned; a lack of alignment could, for example, lead to a significant response capability but no understanding of whom to respond to. Similarly,

The undersea knife fight represents one of the *most consequential* and *least understood* arenas of modern strategic competition.

legal reforms and treaties can be focused on limiting actions not just by impact but also by the ability to attribute and respond.

Considerations and What Comes Next

The matrix presented in Table 5 is intended as a tool to help identify and define deterrence questions, determine future legal reforms, and strategize capability investment decisions. Although similar pathways exist to explore tactical options for deterrence in other arenas, the undersea domain remains underserved. We described several factors that make applying deterrence and defense strategies a challenge in an undersea environment (e.g., an order of magnitude difference in operational timescales) and introduced a rough, initial framework to assess capability investment trade-offs in a broader, strategic context of deterrence and contestation via irregular operations.

However, the undersea knife fight represents one of the *most consequential* and *least understood* arenas of modern strategic competition. As this report has shown, the combination of low barriers to entry, high-impact potential, long timelines for detection and response, and chronically poor attribution creates a uniquely complex environment in which nations must deter, detect, and respond to hostile actions. The ambiguity inherent in undersea incidents—whether involving telecommunication cables, energy infrastructure, sensors, or port facilities—complicates decisionmaking at every step. Legal uncertainty, overlapping jurisdictions, and the challenge of determining intent further constrain response options. These factors, together, underscore the importance of establishing a coherent framework for thinking about deterrence, attribution, and the strategic choice to reveal or conceal actions in the undersea domain.

The framework introduced in this report provides a starting point for evaluating options according to the level of attribution and the strategic posture of the actor. It highlights how choices related to revealing or concealing capabilities, acting or refraining from action, and escalating horizontally or vertically depend not only on evidence but also on risk tolerance, political objectives, and long-term investments in capabilities. It also emphasizes that attribution, revealing, and reacting are deeply interdependent: Investments in improving one without the others can produce substantial gaps in national readiness and deterrence.

Ultimately, advantage in the undersea knife fight will accrue to states that can rapidly understand incidents, credibly demonstrate and control detection and response capabilities, and calibrate actions in ways that shape adversary behavior without precipitating unnecessary escalation.

Moving forward, several areas require deeper analysis and targeted investment:

- **Refine and operationalize the framework.** This framework is a first step in exploring a coherent, multiplatform framework for undersea infrastructure defense and open ocean competition. Decision thresholds and pathways need to be mapped to relevant authorities, and the framework should be tested against real-world scenarios and historical cases. Applying the derived framework to both high-impact events and low-level, ambiguous incidents will help illuminate where policy gaps persist.
- **Assess capability gaps in attribution and response.** A systematic review of existing detection systems, investigative tools, and response assets—across civilian, military, and interagency domains—will help identify

where investments in sensing, rapid deployment, and analytic capacity are most urgent.

- **Clarify legal authorities and policy boundaries.** The patchwork of domestic and international authorities governing undersea actions warrants focused legal research. Options for reform, confidence-building measures, or new agreements should be explored to reduce ambiguity and increase shared understanding among allies.
- **Explore reveal or conceal strategies in-depth.** Future work should examine when revealing capabilities is likely to strengthen deterrence, when concealment provides strategic advantage, and how adversaries might interpret signaling choices. Leveraging historical and conventional strategies from all domains to mature maritime infrastructure defense and response capabilities for a full range of emerging subsea capabilities will be important. Insights from space, cyber, and maritime irregular warfare may prove especially useful in determining a calibrated response.
- **Engage with allies, partners, and third parties.** Because undersea infrastructure is globally interconnected, collaboration is essential. Comparative assessments of allied priorities, capabilities, shared investments in detection and repair capacity, and coordinated policy approaches should be pursued.
- **Develop tools to support both decisionmakers and joint force operations.** Visualization tools, decision matrices, and scenario-based planning aids can help leaders, strategists, and operational commanders apply the framework quickly to assess trade-offs during real incidents, when time, information, and confidence levels are limited.

By advancing these next steps, researchers and policymakers can strengthen the collective understanding of the undersea knife fight and help shape a strategic environment in which hostile actions are riskier, deterrence is more credible, and national infrastructure is better protected against both overt and covert threats.

Notes

[1] International Cable Protection Committee, *Submarine Cables and BBNJ*.

[2] Brown, "Episode 19: Maritime Sabotage"; M and Demony, "UK Says It Deployed Military to Deter Russian Submarines from Attack on Undersea Cables."

[3] Eurostat, "EU Imports of Energy Products."

[4] Rolander, "Irregular Warfare on the Sea Floor and the Case for National Resilience."

[5] We refer to this undersea conflict somewhat colorfully as a *knife fight* because, unlike most naval engagements, the activity occurs in close quarters with poor visibility and often involves physically cutting pipes and cables.

[6] Koshino, "The Changing Submarine Cables Landscape"; Stronge, "Is It Sabotage?"; Iniskt Group, *Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity*.

[7] Port of Seattle, "Port Cyberattack Archive"; Perkins, "Russian Spy Sensors Found Hidden in UK Waters."

[8] McLaughlin, Paige, and Guilfoyle, "Submarine Communication Cables and the Law of Armed Conflict."

[9] Iniskt Group, *Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity*; Jones, "Seabed Zero"; Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*.

[10] Paine, *Deterrence and Denial*.

[11] Dunigan et al., *Characterizing and Exploring the Implications of Maritime Irregular Warfare*; Armstrong, *Small Boats and Daring Men*.

[12] Klein, *Space Warfare*.

[13] Fischerkeller, Goldman, and Harknett, *Cyber Persistence Theory*.

[14] Seabed 2030, "Seabed 2030 Announces Latest Progress on World Hydrography Day."

[15] Ballard, and Archbold, *The Discovery of the Titanic*.

[16] Sontag, Drew, and Drew, *Blind Man's Bluff*.

[17] Office of Economic Security, Supply Chain Resilience Center, and Cybersecurity and Infrastructure Security Agency, *Priorities for DHS Engagement on Subsea Cable Security and Resilience*; Dunley, "A Sea Control Revolution?"

[18] Gallagher et al., *Protection of Undersea Telecommunication Cables*.

[19] International Law Association, *Submarine Cables and Pipelines Under International Law*.

[20] Guilfoyle, Paige, and McLaughlin, "The Final Frontier Of Cyberspace."

[21] Frade, "Leading in the Dark."

[22] van Soest, et al., *Evolving Threats to Critical Undersea Infrastructure*.

[23] Hattendorf, "The Idea of a 'Fleet in Being' in Historical Perspective."

References

Armstrong, Benjamin, *Small Boats and Daring Men: Maritime Raiding, Irregular Warfare, and the Early American Navy*, University of Oklahoma Press, 2019.

Ballard, Robert D., and Rick Archbold, *The Discovery of the Titanic*, updated ed., Grand Central Publishing, 1995.

Brown, Dave, "Episode 19: Maritime Sabotage: The Hidden War Underseas," *The Trident* podcast, September 2025.

Dunigan, Molly, Dick Hoffmann, Peter Chalk, Brian Nichiporuk, and Paul Deluca, *Characterizing and Exploring the Implications of Maritime Irregular Warfare*, RAND Corporation, MG-1127-NAVY, 2012. As of June 11, 2026: https://www.rand.org/pubs/monographs/MG1127.html

Dunley, Richard, "A Sea Control Revolution?" *War on the Rocks*, May 28, 2026.

Eurostat, "EU Imports of Energy Products—Latest Developments," updated March 2026.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett, *Cyber Persistence Theory: Redefining National Security in Cyberspace*, Oxford University Press, 2022.

Frade, Paulo, "Leading in the Dark: How Submarine Commanders Think Under Uncertainty," *War on the Rocks*, May 27, 2026.

Gallagher, Jill C., Nicole T. Carter, Laura B. Comay, Patricia Moloney Figliola, Laura Gatz, Caitlin Keating-Bitonti, Eva Lipiec, Anthony R. Marshak, Pervaze A. Sheikh, and Erin H. Ward, *Protection of Undersea Telecommunication Cables: Issues for Congress*, Congressional Research Service, R47648, August 7, 2023.

Guilfoyle, Douglas, Tamsin Phillipa Paige, and Rob McLaughlin, "The Final Frontier of Cyberspace: The Seabed Beyond National Jurisdiction and the Protection of Submarine Cables," *International and Comparative Law Quarterly*, Vol. 71, No. 3, July 2022.

Hattendorf, John B., "The Idea of a 'Fleet in Being' in Historical Perspective," *Naval War College Review*, Vol. 67, No. 1, Winter 2014.

Iniskt Group, *Submarine Cables Face Increasing Threats Amid Geopolitical Tensions and Limited Repair Capacity*, Recorded Future, July 17, 2025.

International Cable Protection Committee, *Submarine Cables and BBNJ*, August 1, 2016.

International Law Association, *Submarine Cables and Pipelines Under International Law: [Third] Interim Report 2024*, May 2024.

Jones, Bruce D., "Seabed Zero: Baltic Sabotage and the Global Risks to Undersea Infrastructure," *Bulletin of the Atomic Scientists*, February 13, 2026.

Klein, John J., *Space Warfare: Strategy, Principles and Policy*, 2nd ed., Routledge, 2025.

Koshino, Yuka, "The Changing Submarine Cables Landscape: Expanding the EU's Role in the Indo-Pacific," European Union Institute for Security Studies, October 2024.

M, Muvija, and Catarina Demony, "UK Says It Deployed Military to Deter Russian Submarines from Attack on Undersea Cables," Reuters, April 9, 2026.

McLaughlin, Rob, Tamsin Phillipa Paige, and Douglas Guilfoyle, "Submarine Communication Cables and the Law of Armed Conflict: Some Enduring Uncertainties, and Some Proposals, as to Characterization," *Journal of Conflict and Security Law*, Vol. 27, No. 3, Winter 2022.

Murphy, Erin L., *Redundancy, Resiliency, and Repair: Securing Subsea Cable Infrastructure*, Center for Strategic and International Studies, November 2025.

Office of Economic Security, Supply Chain Resilience Center, and Cybersecurity and Infrastructure Security Agency, *Priorities for DHS Engagement on Subsea Cable Security and Resilience*, U.S. Department of Homeland Security, December 18, 2024.

Office of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community*, February 5, 2024.

Paine, S. C. M., ed., *Deterrence and Denial: The Power of Fleets in Being*, Naval Institute Press, 2025.

Perkins, Liz, "Russian Spy Sensors Found Hidden in UK Waters," *The Telegraph*, April 6, 2025.

Port of Seattle, "Port Cyberattack Archive," April 2, 2025.

Rolander, Andrew, "Irregular Warfare on the Sea Floor and the Case for National Resilience," *Small Wars Journal*, May 30, 2025.

Seabed 2030, "Seabed 2030 Announces Latest Progress on World Hydrography Day," press release, June 21, 2024.

Sontag, Sherry, Christopher Drew, and Annette Lawrence Drew, *Blind Man's Bluff: The Untold Story of American Submarine Espionage*, illustrated ed., PublicAffairs, 2016.

Stronge, Tim, "Is It Sabotage? Unraveling the Mystery of Undersea Cable Breaks," TeleGeography, February 3, 2025.

UNCLOS—*See* United Nations Convention on the Law of the Sea

United Nations Convention on the Law of the Sea, December 10, 1982. As of June 11, 2026: https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

van Soest, Henri, James Black, Harper Fine, and Lucia Retter, *Evolving Threats to Critical Undersea Infrastructure: Implications for European Security and Resilience*, RAND Corporation, PE-A3800-1, June 2025. As of February 25, 2026: https://www.rand.org/pubs/perspectives/PEA3800-1.html

About the Authors

Michael Bohnert is an engineer at RAND. His focus areas of research are combat and operations modeling (air, naval, and unmanned systems), cost analysis (naval systems), maritime industrial base management, and analysis of alternatives for systems and force architecture design. He holds a Master of Engineering in systems engineering.

Ajay K. Kochhar is a technical analyst at RAND. Recently, his research has focused on autonomous undersea capabilities, modeling for complex decisions and deterrence problems (air, land, sea, space), modeling for operations in denied environments, joint force readiness, and cyberspace and cyber force challenges. He holds Master of Science degrees in computer science and experimental physics.

Daniel Justice is a U.S. Navy foreign area officer currently serving on the U.S. European Command staff as deputy branch chief for defense industrial base and armaments cooperation. At the time of writing, he was stationed at RAND as a federal executive fellow. Previously, he held roles in policy analysis, international armaments cooperation, and operational assignments.

Paul DeLuca is the acting associate director of the National Defense Research Institute, the director of the Navy and Marine Forces Program, and a senior engineer at RAND. He focuses on technology issues for the U.S. Navy, U.S. Coast Guard, U.S. Special Operations Command, U.S. Air Force, and Australian Department of Defence. He holds a Ph.D. in materials science and engineering.

About This Report

Telecommunication, energy, and transportation infrastructure are increasingly targeted by malign actors. Incidents of sabotage over the past few years highlight the costs incurred and the difficulties in attributing, stopping, and responding to such incidents. Our exploratory effort described in this report delved into the growing contest below the surface of the water. We provide an overview analysis of a burgeoning problem set, options for deterrence, and a framework for investments and competition.

RAND National Security Research Division

This work was conducted within the Navy and Marine Forces Program of the RAND National Security Research Division, which operates the National Defense Research Institute, a federally funded research and development center sponsored by the Office of the Secretary of War, the Joint Staff, the Unified Combatant Commands, the Navy, the Marine Corps, the defense agencies, and the defense intelligence enterprise.

For more information on the RAND Navy and Marine Forces Program, see www.rand.org/nsrd/nmf or contact the director (contact information is provided on the webpage).

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the Department of War.

This publication documents work completed in April 2026, which underwent security review with the sponsor and the Defense Office of Prepublication and Security Review before public release.

Funding

This research was made possible by National Defense Research Institute exploratory research funding that was provided through the federally funded research and development center contract and approved by the institute's primary sponsor.

Acknowledgments

We thank the multiple laboratories, industry partners, research institutions, and government personnel who supported this effort with valuable information and ideas. We thank Bradley Martin and Jake DeWeese for their careful review and quality assurance. We also thank Scott Savitz for the additional insights he provided.

RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/research-integrity.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

Limited Print and Electronic Distribution Rights

This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorized posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/about/publishing/permissions.

For more information on this publication, visit www.rand.org/t/RRA4027-1.

© 2026 RAND Corporation

Cover image: Adobe Firefly, composite image created by Sara Herbst, June 2026.

www.rand.org

RR-A4027-1