Hybrid Attack Strategies Against Offshore Infrastructures

Jan Stockbruegger
German Aerospace Center

Abstract

Hybrid attacks threaten offshore infrastructures, including wind farms, shipping lanes, subsea cables, and pipelines. In response, states are developing information-sharing platforms, advanced sensors, and unmanned systems to improve monitoring and threat detection. Yet what type of attacks offshore infrastructures need to be protected against remains unclear. This paper presents a comprehensive analysis of physical hybrid attack strategies targeting offshore infrastructures, encompassing both underwater and surface operations. It argues that attackers need to ensure plausible deniability to reduce the risk of conflict escalation. Yet making sure that attackers and their state-sponsors cannot be identified is a challenge due to the proliferation offshore sensors such as satellites, radar, and cameras. I identify three hybrid attack strategies aimed at ensuring plausible deniability, accident-based strategies, remote attack strategies, and escape strategies, each with specific operational focus, parameters and protection requirements. The findings can inform sensor configurations and protection measures to deter, detect, and disrupt hybrid attack operations.

Keywords

Hybrid Warfare, Offshore Infrastructure, Protection Plausible Deniability, Maritime Security, Unmanned and Autonomous Systems

Introduction

Hybrid attacks are a major threat to the maritime domain and offshore and underwater infrastructures such as windfarms, shipping lanes, and subsea cables and pipelines (Bueger & Liebetrau, 2023; 2021; Sari, 2025). Consequently, analysts, policymakers, and engineers increasingly develop solutions to protect infrastructures including information sharing platforms and innovative sensors and unmanned systems to better monitor infrastructures and collect data for maritime threat detection (Felemban et al., 2015; Wielgosz & Malyszko 2025; Voelsen, 2024).

Yet what exactly infrastructures need to be protected against remains largely unclear. So far, NATO countries have mainly been confronted with espionage and low-level sabotage attacks including civilian vessels that cut cables with their anchors (Praks, 2024). Yet hybrid warfare against offshore infrastructures could quickly escalate and become more intense as competition with Russia, China, and other countries with high technological and organizational capacities intensifies (Yazmyradov et al., 2024). Consequently, policymakers need to prepare for more sophisticated hybrid attack scenarios in the maritime domain involving advanced military grade weaponry and technologies including unmanned, autonomous and remotely operated systems.

A growing literature studies maritime cyberattack and legal strategies (Symes et al., 2024; Sari, 2025), as well as specific strategies, practices, and systems for physical attack (Savitz, 2024; Praks, 2024) against vessels, pipelines, cables, windfarms, and other platforms (Gabriel et al., 2022; Burgherr et al., 2023). However, few efforts have been made so far to analyse physical attack strategies systematically, including the strategic and operational parameters that influence specific hybrid attack operations, what maritime systems and technologies attackers could deploy, and how they can evade maritime sensors and other protection measures (Khawaja et al., 2022a; Savolainen et al., 2023). Consequently, we only have a limited understanding of hybrid attack risks against offshore infrastructures, how likely or unlikely certain attack scenarios are, and what can be done to prevent or deter them.
This paper tries to address this gap by offering a systematic analysis of physical hybrid attack strategies in the maritime domain focusing on both underwater und surface operations. I argue that actors engaged in hybrid warfare need to maintain plausible deniability by obscuring their involvement in attack operations. Yet doing so is difficult due to the proliferation of offshore sensor systems such as satellite and coastal radar and optical cameras (Felemban et al., 2015; Okafor-Yarwood et al., 2024). Attackers thus need to adjust their operations in a way that allows them to evade sensors and to make attack attribution difficult.

I analyze three strategies aimed at ensuring plausible deniability in hybrid maritime attacks. Accident attack strategies are operations in which the attacker obscures attacks as accidents and other safety incidents; remote attack strategies are operations in which the attacker increases the distance between itself and the site of the attack to evade surveillance systems; and escape strategies refer to operations whereby the attacker avoids detection by escaping from the site of the attack before they can be detected or detained and arrested. I argue that these strategies should be used to develop more specific attack scenarios and to configure sensor and protection systems to prevent and disrupt them.

I first discuss the notions of "hybrid" and "grey zone" warfare and "plausible deniability". I then introduce the concepts of "operational" and "strategic stealth" in hybrid attacks. After that I describe the challenge of ensuring strategic stealth and plausible deniability in attacks against offshore infrastructure, before analyzing three distinct hybrid attack strategies. I summarize my argument in the conclusion.

Hybrid attacks in the maritime grey zone

My paper contributes to the debate on "hybrid" or "grey zone" warfare strategies in the maritime domain. Both terms are relatively recent conceptual innovations that aim at capturing the transformation of warfare and competition in the modern age. Hybrid warfare refers to the broadening of warfare operations against an adversary beyond conventional military tools. A hybrid campaign uses multiple tools, vectors and activities to achieve its objective. This includes espionage, sabotage and cyberattacks, as well as engaging in election interference, propaganda or disinformation strategies to weaken and destabilize the enemy from within. Hybrid strategies are thus characterized by the blurring of lines between traditional warfare and other forms of conflict, such as irregular warfare, cyber warfare, and information warfare (Johnson, 2018).

The grey zone, on the other hand, refers to actions against an adversary below the threshold of war – that is actions that create a competitive space between peace (white) and war (black). Grey zone strategies leverage ambiguity and kinetic and non-kinetic means to achieve strategic objectives without escalating to traditional warfare. Grey zone strategies are thus characterized by actions that are intended to harm and weaken an adversary without justifying a conventional military response (Layton, 2021).

In the maritime domain, "grey zone" and "hybrid" warfare practices can include activities like naval patrols, cyberattacks on maritime infrastructure, economic coercion of countries with maritime assets, and the use of proxies to harass or interfere with maritime activities.

Grey zone and hybrid strategies can also include sabotage attacks against offshore infrastructures if these attacks are crafted and conducted in a way that they do not lead to a military response and open war (Patalano, 2018; Larsson, 2024). China (Patalano, 2018), Russia (Praks, 2024) and Iran (Eisenstadt, 2021) are commonly regarded as the main perpetrators of hybrid maritime warfare activities.

One of the ways in which attackers reduce the risk of conflict escalation in hybrid operations against offshore infrastructure is by ensuring plausible deniability – that is by making it difficult to pinpoint the source of an attack. Plausible deniability is crucial in hybrid attacks because it allows an actor to damage an opponent's interests without taking direct responsibility, making it difficult to attribute the actions and limiting the ability of the targeted state to respond decisively. The key aim of ambiguity is not necessarily to hide the true actor behind the activity, but ultimately to stymie a legitimate response by creating ambiguity.

To create plausible deniability, an attackers need to ensure that their operations do not produce evidence that could link them to the attack and justify counteractions including military retaliation (Mumford, 2020; Mumford & Carlucci, 2023). This includes legal evidence that could uphold in a court of law. As Mumford (Mumford, 2020, p. 4) argues, “if significant legal or forensic evidence emerges linking a state to a particular attack then the cloak of invisibility soon reveals itself to be the Emperor’s new clothes”, making deniability implausible. Next, I investigate the operational requirements to ensure plausible deniability in more detail.

Operational and strategic stealth

To better understand the operational implications of plausible deniability, it is useful to conceptualize it as a specific form of stealth that is required to conduct a physical attack. Hybrid attackers staging a physical attack against an offshore infrastructure rely on what might be called stealth at the operational and the strategic level. These two types of stealth overlap but capture distinct dimension and challenges in hybrid attack operations. Operational stealth refers to the attacker’s ability to delay attack detection, while strategic stealth refers to its ability to maintain plausible deniability. Both operational and strategic stealth are vital to carry out a successful grey zone operation, but the latter is the key factor that determines and constraints hybrid attack operations. Operational stealth refers to the attacker’s ability to carry out a successful attack against an adversary’s population or social, economic, or political system. Operational stealth does not mean that the attacker remains invisible and undetected. Instead, it implies that detection is too late for the initiation of countermeasures and to prevent or disrupt an attack operation. Operational stealth is therefore vital to overcome defensive measures and to stage a successful hybrid attack and to cause maximum damage to an adversary’s social, economic and political system.

Strategic stealth, on the other hand, refers to the attacker's ability to maintain plausible deniability and to make attack attribution difficult. Plausible deniability means that the perpetrator of an attack is unknown, or that the defender cannot produce sufficient evidence to prove its involvement in the operation. As pointed out before, plausible deniability is the key to reduces the risk of military retaliation in response to an attack on an infrastructure. If a defender can proof that an actor intentionally attacked its infrastructure, it has strong and justifiable reasons to retaliate militarily and to defend its territory and installations. Ensuring strategic stealth and plausible deniability is thus the top priority of actors engaged in hybrid warfare below the threshold war (Poznansky, 2022; Mumford, 2020).

Strategic stealth is not dependent on operational stealth. An attacker loses operational stealth when the defender detects the attack early enough to initiate countermeasures, even if it fails to attribute the attack to a specific actor. For example, states and private companies are often able to detect and disrupt cyberattacks against their systems, but they are usually unable to identify the individuals and states that carried out these attacks (Canfil, 2022).[16]

Yet even if operational stealth is ensured and a hybrid attack succeeds, the attacker can still lose strategic stealth if the defender is able to produce credible evidence that pinpoints to its involvement in the attack. For example, German authorities and investigators have been able to identify the individuals who carried out the attack against the Nord Stream pipeline in September 2022 and to collect evidence that implicates the Ukrainian state in the attack (Pancevski, 2024)

This perspective suggests that the effectiveness of protection systems that focus on operational rather than strategic stealth is limited. Such systems increase the likelihood that an attack will be detected and disrupted. However, they most likely do little to deter and prevent attacks as long as the attacker can remain anonymous and maintain plausible deniability, thus allowing it to continue attack operations without risking retaliatory countermeasures and conflict escalation (Pischedda & Cheon, 2023).

Cyberattacks, for example, are not only a common hybrid warfare strategy because they can produce significant damage, but also because it is so difficult to identify and prosecute the perpetrators of these attacks and to collect strong forensic evidence that clearly and unmistakenly links them to a state sponsor – even though the state's involvement in the attack is very likely (Simons et al., 2020).

[16] However, according to Canfil plausible deniability in the cyber domain has recently become more complicated in part due to enhanced investigative methods and practices of the U.S. Department of Justice and other authorities (Canfil, 2022).

In short, hybrid attacks require both operational and strategic stealth, but the latter is the key factor when it comes to designing hybrid attack operations and should therefore be at the center of our efforts to develop hybrid attack scenarios and infrastructure protection systems. Next, I apply this framework to investigate the challenges and strategies of hybrid attacks against offshore infrastructures.

Stealth and the "transparent" ocean

The debate on infrastructure protection has so far mainly focused on operational stealth and how to create real-time threat detection and early-warning systems to launch counter-measures and disrupt attack operations. The physical environment at sea makes surveillance over the water relatively easy. The seas are flat and there are little natural or human built physical structures where attackers can hide, such as mountains, hills, rocks, forests, or houses and other buildings.

Indeed, major efforts have been undertaken to monitor infrastructures and to install radar and other sensors on offshore platforms as well as efforts to share and fuse sensor data in a unified operational picture for maritime domain awareness (Balci & Pegg, 2006). This includes ship tracking systems and coastal or satellite radars as well as optical cameras, night-vision sensors and infrared sensors mounted on unmanned aerial vehicles, vessels, buoys and offshore infrastructures. Maritime surveillance is also being enhanced by machine learning algorithms that can help produce real-time situational awareness for anomaly detection and early warning applications (Felemban et al., 2015; Okafor-Yarwood et al., 2024; Wielgosz & Malyszko, 2025; Amani et al., 2022).

Yet creating real-time early warning system remains a major challenge. Poor weather and high waves can reduce visibility and make monitoring maritime activities difficult, especially if vessels have turned off their Automatic Identification Systems (Brandt et al., 2024; Androjna et al., 2024; Bunwaree, 2023). Sensor technologies such as radars and satellites are also costly, and not all offshore infrastructures are equipped with modern radar or other advanced sensor systems (Okafor-Yarwood et al., 2024).

Integrating different sensor data into a unified operational picture and threat detection mechanisms continues to be complicated. Security agencies and infrastructure operators are sometimes reluctant to share sensitive data, especially with other states. Consequently, many countries have not (yet) developed effective surveillance systems to detect threats to offshore infrastructures (Brewster & Bateman, 2024; Bueger, 2015).

Moreover, alert times at sea are often short because attackers can approach infrastructures on busy shipping lanes without raising suspicion. Additionally, offshore infrastructures cannot be fenced off to slow down an attack, and they are often located far off the coast and far away from ports and naval or coastguard assets, leading to long intervention times. Thus, even if security agencies are able to detect an attack, it might be too late for countermeasures to disrupt it and to stop a committed and well-prepared malicious actor from sabotaging a windfarm or an oil platform.

In short, targeting operational stealth to defend offshore infrastructures against attacks remains very difficult, despite the proliferation of maritime monitoring systems. There are many ways in which offshore infrastructures can be attacked and damaged by vessels, drones or other systems. For example, there is probably not much that security forces can do to prevent a large vessel from rapidly sailing into an offshore windfarm and to crash into a wind turbine, destroy a converter station with explosive devices, and attack sabotage pipelines with remotely operated vehicles.

And yet, the need to maintain strategic stealth and plausible deniability limits hybrid attack options. As a reminder, attackers need to design and conduct attacks in a way that do not produce evidence and that allow them to obscure their involvement in such operations – what I referred to as strategic stealth" in the previous section. Yet ensuring strategic stealth in the maritime domain is considerably more difficult. First, maintaining plausible deniability means that the attacker needs to escape from the site of an attack before security forces can arrive and arrest them. For example, the Finish authorities managed to stop and detain the Lion S., which had destroyed several subsea cables in the Baltic (Kauranen, 2025). Second, the defender can identify the vessels or individuals that carried out the attack and collect evidence that implicate specific actors in the attack.

Indeed, as indicated above, ship identification and monitoring capabilities have improved significantly in recent years. Especially satellite-based monitoring systems including synthetic aperture radar have proved effective to detect illicit activities and to identify ships that turn off their Automatic Identification System (Giompapa et al., 2009; Androjna et al., 2024; Helgesen et al., 2019). Thus, as pointed out before, the German authorities were able to identify the vessels and individuals involved in the Nord Stream pipeline attacks (Pancevski, 2024).

Next, I identify three strategies that attackers can use to avoid or limit strategic stealth risks and to maintain plausible deniability in hybrid attack operations.

Hybrid attack strategies against offshore infrastructure

This section introduces three hybrid attack strategies against offshore infrastructures. Each of these strategies is organized around a distinct approach to ensure strategic stealth and plausible deniability. These approaches are associated with specific operational parameters leading to specific attacking options. The strategies presented here are ideal types. In practice and reality, they often overlap so that specific attacks can include elements from different hybrid attack strategies. Here, however, we focus on these distinct ideal types.

I also show, however, that each of these hybrid attack strategies have problems and disadvantages, and that they sometimes increase the ability of defenders – such as security forces and infrastructure operators – to not only detect and identify attackers but also to prevent and disrupt attack operations.

Accident attack strategies

Accident attack strategies refer to a set of operations whereby an attacker obscures its malicious goals and intention by behaving "normally". The aim here is not to remain "invisible" but "inconspicuous" – that is not to engage in any suspicious practices that are clearly associated with an attack behavior. The key assumption here is that the more "normal" an attacker behaves, the more difficult it will be to prove that a certain activity was, indeed, an attack, creating ambiguity and plausible deniability.

A key example of this approach are operations where attacks that are being obscured as accidents, such as vessels or fishing boats that cut cables with their anchors or fishing gear. Such incidents happen frequently. They are difficult to detected, and it is nearly impossible to prevent them through timely interventions; and if they are detected, it is very hard to find evidence that prove malicious intent and that links the incident to a hostile state actor. For example, in December 2024 Finish authorities were able to detain a vessel suspected of cutting an underwater power cable, yet proving that the vessel's crew intentionally cut the cable has been difficult, despite extensive investigations, and the case is currently being handled by the courts (Kauranen, 2025).

Adversaries could also cause shipping accidents to disrupt shipping traffic and to create environmental catastrophes. For example, Russia has been accused of deploying old and unsafe "shadow tankers" for its oil exports, thus increasing the risk of a major oil spill in the Baltic Sea (Stockbruegger, 2023); and in 2023, a vessel accidentally sailed through a windfarm – without being detected by the windfarm operator or marine traffic authorities – and collided with a wind turbine (Federal Bureau of Maritime Casualty Investigation, 2025).

However, accidental cable cuts and vessel collisions are risky and their effectiveness is limited. For example, cutting cables with anchors is difficult as cables are often buried under the seabed and their precise location is unknown. Moreover, vessels engaged in such operations cannot carry with them sophisticated yet technical equipment to find, locate, and damage vulnerable cable sections, as such equipment could be detected in post-incident investigations. And while crashing a vessel in an offshore windfarm might be a more effective strategy, it would also lead to intense forensic investigations, thus requiring sophisticated planning and preparation to avoid or destroy any incriminating evidence (Kauranen, 2025).

Escape strategies

Escape strategies refer to a set of operations whereby an attacker aims at ensuring plausible deniability by escaping from the site of an attack before it is being noticed and before security forces can launch counteroperations to stop and arrest the perpetrator. The more time passes between escape and attack detection or the arrival of security forces, the more difficult it is to identify, detain, and investigate the attacker, thus increasing plausible deniability. An example of an escape operation would be if an attacker escapes before security forces arrive to detain and arrest it, thus making investigations to determine culpability more difficult.

The NewNew Polar Bear, for example, managed to escape before it could be detained for destroying subsea cables in the Baltic, thus making it difficult to investigate the vessel and to determine whether or not it had destroyed the cable intentionally (Ringbom & Lott, 2024).

Another example of escape operation is the attacks on the Nord Stream pipeline in September 2022. The attack involved explosives that were detonated several days after the material was planted at the pipelines. This allowed the attackers to escape from the site of the attack before the explosion took place and made it very hard for the authorities to identify and track them down. When the individuals who carried out the attack were eventually identified, they had already fled and could no longer be arrested and prosecuted (Pancevski, 2024). It is not inconceivable that a device explodes not days but weeks or even months after it is being planted at an infrastructure, thus making it nearly impossible for investigators to identify the platforms and persons involved in the operation.

Yet planning and carrying out escape operations is very complicated. Sometimes security forces manage to quickly identify and stop and detain vessels before they can escape. This happened, for example, when Finish authorities detained the Lion S. before it could leave Finish waters (Kauranen, 2025).

Explosive devices or other disruptive systems, moreover, can be found before they cause damage, and properly hiding such devices (e.g. by burying explosive devices at a cable under the sea) might require complex and time-consuming operations near an infrastructure, which increases the risk of detection. The attackers of the Nord Stream pipeline, for example, spent many days in the Baltic searching for the pipeline and placing the explosive devices on the bottom of the sea (Pancevski, 2024).

This does not mean that escape operations are impossible. For example, an attacker could launch autonomous underwater vehicles (AUV) from an unsuspicious vessel to identify vulnerable subsea infrastructures such as unburied cables and then launch remotely operated vehicles (ROV) to plant explosive devices (with timers) from another vessel operating several kilometers away from the infrastructure (Khawaja et al., 2022a; Eleftherakis & Vicen-Bueno, 2020).

Simpler escape operations include the use of sea mines to attack vessels or planting remotely controlled explosive devices at merchant ships or other infrastructures using small speed boats or unmanned systems.

Yet sea mines also endanger the attacker's vessels, and infrastructure sensors and crews might detect explosive devices or the platforms and systems used to plant them on an infrastructure. In other words, escape strategies remain viable, but they are also costly, difficult, and risky.

Remote attack strategies

Remote attack strategies refer to operations that are aimed at increasing the geographic distance between an attacker and the location of the attack. That is, the attacker ensures that the platform from which it launches the attack is far away from the location of the attack so that authorities cannot detect and identify its involvement in the attack. In other words, the key assumption of remote attack strategies is that the larger the distance between the attack platform and the attack location, the more difficult it will be for the authorities to find the attacker and to identify its state sponsor.

There are several ways in which an attacker can increase the distance between itself and the location of an attack. The most likely one is the use of unmanned surface or aerial vehicles that can be launched from a vessel that is located many kilometers away from the targeted infrastructure. Advanced unmanned systems can be operated over very large distances and have batteries that last many hours. Such systems are also commercially available across the world, and that they can be easily built and adjusted for specific operational purposes (Petritoli et al., 2020; Khawaja et al., 2022b; Bukovetskiy et al., 2019).

Hybrid attacks against maritime targets using unmanned systems have already occurred. The Houthi armed group in Yemen, for example, has used unmanned surface vehicles (USV) to attack merchant vessels in the Red Sea (Samaan, 2020; Haugstvedt, 2021), and Ukraine has used USV to damage Russian warships in the Black Sea (Kormych & Malyarenko, 2023; Kollakowski, 2025). Neither Ukraine nor the Houthis, however, tried to obscure their involvement in the attack.

Yet Unmanned systems have also been used to maintain plausible deniability in hybrid attack operations. In 2021, for example, the Israel-managed oil tanker MT Mercer Street was attacked by Unmanned Aerial Vehicles (UAVs) in the Gulf of Oman. Israeli, United States, and British officials blamed the attack on Iran, but Iran denied its involvement, which took place hundreds of kilometers off its coast (Gunawan et al., 2023). And on 23 December 2023, the tanker Chem Pluto was struck by an anti-ship missile or drone 320 km off India, leading the Indian Navy to board two Iranian vessels near the attack, yet without finding evidence of Iranian involvement in the attack (Phelan Chatterjee, 2023).

Attackers could deploy USVs or UAVs to conduct long-range strikes against offshore infrastructures from unsuspicious fishing or commercial vessels operating dozens of kilometers away from the targeted infrastructure. Especially small and low-flying UAVs cannot be detected easily by radar sensors, and even if they are detected, it will be difficult to identify the vessel from which they were launched. Small USVs can carry a higher payload than most UAVs and are very difficult to detect even with advanced optical and other sensors (The use of AUVs carrying explosive devices for attacks below the sea, however, is more complicated given the difficulty of effective underwater communication and navigation).

Conclusion

This paper has provided a systematic analysis of physical hybrid attack strategies against offshore infrastructures. It has argued that attackers must ensure plausible deniability to reduce the risk of conflict escalation. Yet ensuring that attackers and their state sponsors cannot be identified is challenging due to the proliferation of offshore sensors including satellites, radar, and cameras. I have developed three hybrid attack strategies aimed at ensuring plausible deniability—accident-based strategies, escape strategies, and remote attack strategies —each with generating specific operational parameters and protection requirements.

My paper has implications for how to protect offshore infrastructures against hybrid sabotage attacks aimed at avoiding conflict escalation and staying below the threshold of war. It suggests that the need to maintain plausible deniability makes hybrid attacks much more complicated than previously thought. Having to obscure their involvement in an attack increases the attacker's risks and vulnerabilities and creates opportunities for the defender to prevent and deter such operations.

Simple attack scenarios such as vessels crashing into offshore windfarms or short-range commercial drones attacking wind turbines are thus less likely because they expose the individuals and platforms that carry out these attacks and increase the risk that investigators produce incriminating evidence and that they can attribute the attack to a specific state actor.

References

Amani, M., Farzane M., Layegh, N. F., Nazari, M. E., Fatolazadeh, F., & Salehi, A. (2022). Remote sensing systems for ocean: A Review (Part 2: Active systems). IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing 15, 1421–53. https://doi.org/10.1109/JSTARS.2022.3141980

Androjna, A., Pavić, I., Gucma, L., Vidmar, P., & Perkovič, M. (2024). AIS data manipulation in the illicit global oil trade. Journal of Marine Science and Engineering 12(1). https://doi.org/10.3390/jmse12010006

Balci, M., & Pegg, R. (2006). Towards global maritime domain awareness - Recent developments and challenges. 2006 9th International Conference on Information Fusion, July, 1–5. https://doi.org/10.1109/ICIF.2006.301702

Brandt, P., Munim, Z. H., Chaal, M., & Kang, H-S. (2024.) Maritime accident risk prediction integrating weather data using machine learning. Transportation Research Part D: Transport and Environment 136 (November): 104388. https://doi.org/10.1016/j.trd.2024.104388

Brewster, D., & Bateman, S. (2024). Maritime domain awareness 3.0: The future of information and intelligence-sharing in the Indian Ocean. Australian National University, National Security College.

Bueger, C. (2015). From dusk to dawn? Maritime domain awareness in Southeast Asia. Contemporary Southeast Asia, 37(2), 157–182. https://doi.org/10.1355/cs37-2a

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. Contemporary Security Policy, 42(3), 391–413. https://doi.org/10.1080/13523260.2021.1907129

Bueger, C., & Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? Marine Policy, 155, 105772. https://doi.org/10.1016/j.marpol.2023.105772

Bukovetskiy, A. V., Boyko, V. I., Gavrilov, P. M., Sheveleva, A. A., & Stepanov, B. P. (2019). Modeling of processes of security assurance from threats caused by unmanned air vehicles. Progress in Nuclear Energy, 115, 221–230. https://doi.org/10.1016/j.pnucene.2019.03.036

Bunwaree, P. (2023). The illegality of fishing vessels "going dark" and methods of deterrence. International and Comparative Law Quarterly, 72(1), 179–211. https://doi.org/10.1017/S0020589322000525

Burgherr, P., Siskos, E., Spada, M., Lustenberger, P., & Dupuy, A. C. (2023). Energy security in the context of hybrid threats: The case of the European natural gas network. In B. Hämmerli, U. Helmbrecht, W. Hommel, L. Kunczik, & S. Pickl (Eds.), Critical information infrastructures security (Vol. 13723, pp. — —). Lecture Notes in Computer Science. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-35190-7_15

Canfil, J. K. (2022). The illogic of plausible deniability: Why proxy conflict in cyberspacemay no longer pay. Journal of Cybersecurity, 8(1), tyac007. https://doi.org/10.1093/cybsec/tyac007

Eisenstadt, M. (2021). Iran's gray zone strategy: Cornerstone of its asymmetric way of war. PRISM, 9(2), 77–97.

Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to increase the security of underwater communication cables: A review of underwater monitoring sensors. Sensors, 20(3), 737. https://doi.org/10.3390/s20030737

Federal Bureau of Maritime Casualty Investigation. (2025). Allision with an offshore wind turbine in the Gode Wind 1 wind farm by the PETRA L on 24 April 2023 (Investigation Report 192/23). Hamburg.

Felemban, E., Shaikh, F. K., Qureshi, U. M., Sheikh, A. A., & Qaisar, S. B. (2015). Underwater sensor network applications: A comprehensive survey. International Journal of Distributed Sensor Networks, 11(11), 896832. https://doi.org/10.1155/2015/896832

Gabriel, A., Tecklenburg, B., & Sill Torres, F. (2022). Threat and risk scenarios for offshore wind farms and an approach to their assessment. In Proceedings of the 19th ISCRAM Conference (pp. 162–173).

Giompapa, S., Gini, F., Farina, A., Graziano, A., Croci, R., & Distefano, R. (2009). Maritime border control multisensor system. IEEE Aerospace and Electronic Systems Magazine, 24(8), 9–15. https://doi.org/10.1109/MAES.2009.5256382

Gunawan, Y., Wati, E., & Corral, E. (2023). Iran's responsibility for the MV Mercer Street attack under international law. Brawijaya Law Journal, 10(1), 72–88. https://doi.org/10.21776/ub.blj.2023.010.01.05

Haugstvedt, H. (2021, September). Red Sea drones: How to counter Houthi maritime attacks. War on the Rocks. https://warontherocks.com/2021/09/red-sea-drones-how-to-counter-houthi-maritime-tactics/

Helgesen, Ø. K., Brekke, E. F., Helgesen, H. H., & Engelhardtsen, Ø. (2019, July). Sensor combinations in heterogeneous multi-sensor fusion for maritime target tracking. In 2019 22th International Conference on Information Fusion (FUSION) (pp. 1–9). https://doi.org/10.23919/FUSION43075.2019.9011297

Johnson, R. (2018). Hybrid war and its countermeasures: A critique of the literature. Small Wars & Insurgencies, 29(1), 141–163. https://doi.org/10.1080/09592318.2018.1404770

Kauranen, A. (2025, August 25). Suspects blame technical faults for Baltic Sea cable breaches. Reuters. https://www.reuters.com/business/media-telecom/suspects-blame-technical-faults-baltic-sea-cable-breaches-2025-08-25/

Khawaja, W., Semkin, V., Ratyal, N. I., Yaqoob, Q., Gul, J., & Guvenc, I. (2022a). Threats from and countermeasures for unmanned aerial and underwater vehicles. Sensors, 22(10), 3896. https://doi.org/10.3390/s22103896

Khawaja, W., Semkin, V., Ratyal, N. I., Yaqoob, Q., Gul, J., & Guvenc, I. (2022b). Threats from and countermeasures for unmanned aerial and underwater vehicles. Sensors, 22(10), 3896. https://doi.org/10.3390/s22103896

Kollakowski, T. (2025). War in the Black Sea: The revival of the Jeune École? Journal of Strategic Studies, 1–33. https://doi.org/10.1080/01402390.2025.2471067

Kormych, B., & Malyarenko, T. (2023). From gray zone to conventional warfare: The Russia-Ukraine conflict in the Black Sea. Small Wars & Insurgencies, 34(7), 1235–1270. https://doi.org/10.1080/09592318.2022.2122278

Larsson, O. L. (2024). Sea blindness in grey zone preparations. Defence Studies, 24(3), 399–420. https://doi.org/10.1080/14702436.2024.2359913

Layton, P. (2021, August 11). Responding to China's unending grey-zone prodding. Royal United Services Institute. https://rusi.org/explore-our-research/publications/commentary/responding-chinas-unending-grey-zone-prodding

Mumford, A. (2020). Ambiguity in hybrid warfare. The European Centre of Excellence for Countering Hybrid Threats.

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. European Journal of International Security, 8(2), 192–206. https://doi.org/10.1017/eis.2022.19

Okafor-Yarwood, I., Eastwood, O., Chikowore, N., & De Oliveira Paes, L. (2024). Technology and maritime security in Africa: Opportunities and challenges in Gulf of Guinea. Marine Policy, 160, 105976. https://doi.org/10.1016/j.marpol.2023.105976

Pancevski, B. (2024, August 14). A drunken evening, a rented yacht: The real story of the Nord Stream pipeline sabotage. The Wall Street Journal. https://www.wsj.com/world/europe/nord-stream-pipeline-explosion-real-story-da24839c

Patalano, A. (2018). When strategy is 'hybrid' and not 'grey': Reviewing Chinese military and constabulary coercion at sea. The Pacific Review, 31(6), 811–839. https://doi.org/10.1080/09512748.2018.1513546

Petritoli, E., Cagnetti, M., & Leccese, F. (2020). Simulation of autonomous underwater vehicles (AUVs) swarm diffusion. Sensors, 20(17), 4950. https://doi.org/10.3390/s20174950

Chatterjee, P. (2023, December 24). Tanker hit off India coast by drone from Iran, says US. BBC News. https://www.bbc.com/news/world-asia-india-67811929

Pischedda, C., & Cheon, A. (2023). Does plausible deniability work? Assessing the effectiveness of unclaimed coercive acts in the Ukraine war. Contemporary Security Policy, 44(3), 345–371. https://doi.org/10.1080/13523260.2023.2212464

Poznansky, M. (2022). Revisiting plausible deniability. Journal of Strategic Studies, 45(4), 511–533. https://doi.org/10.1080/01402390.2020.1734570

Praks, H. (2024). Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage. The European Centre of Excellence for Countering Hybrid Threats.

Ringbom, H., & Lott, A. (2024). Sabotage of critical offshore infrastructure: A case study of the Balticconnector incident. In A. Lott (Ed.), Maritime security law in hybrid warfare. Brill | Nijhoff. https://doi.org/10.1163/9789004707993_008

Samaan, J. L. C. (2020). Missiles, drones, and the Houthis in Yemen. Parameters, 50(1), 51–63.

Sari, A. (2025). Protecting maritime infrastructure from hybrid threats: Legal options. The European Centre of Excellence for Countering Hybrid Threats.

Savitz, S. (2024). Uncrewed maritime vessels: Shaping naval power in hybrid threat operations. The European Centre of Excellence for Countering Hybrid Threats.

Savolainen, J., Gill, T., Schatz, V., & Giannoulis, G. (2023). Handbook on maritime hybrid threats: 15 scenarios and legal scans (Vol. 16). Hybrid CoE Paper. The European Centre of Excellence for Countering Hybrid Threats.

Simons, G., Danyk, Y., & Maliarchuk, T. (2020). Hybrid war and cyber-attacks: Creating legal and operational dilemmas. Global Change, Peace & Security, 32(3), 337–342. https://doi.org/10.1080/14781158.2020.1732899

Stockbruegger, J. (2023). Reducing Russia's oil revenues: Does the allied price cap work? The RUSI Journal, 268(5), 34–42.

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). Cyberattacks on the maritime sector: A literature review. Journal of Marine Science and Application, 23(4), 689–706. https://doi.org/10.1007/s11804-024-00443-0

Voelsen, D. (Ed.). (2024). Maritime kritische Infrastrukturen: Strategische Bedeutung und geeignete Schutzmaßnahmen (Version 1). Stiftung Wissenschaft und Politik. https://www.swp-berlin.org/10.18449/2024S03/

Wielgosz, M., & Malyszko, M. (2025). A method for early identification of vessels potentially threatening critical maritime infrastructure. Applied Sciences, 15(15), 8716. https://doi.org/10.3390/app15158716

Yazmyradov, S., Lee, H., Lee, Y. S., Kamolov, A. A., & Kang, D.-W. (2024). Innovations and challenges in submarine security systems: A comprehensive analysis of modern threats and countermeasures. International Journal of Advanced Smart Convergence, 13(4), 111–121. https://doi.org/10.7236/IJASC.2024.13.4.111