Defence Studies

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/fdef20

Sea blindness in grey zone preparations

Oscar Leonard Larsson

To cite this article: Oscar Leonard Larsson (30 May 2024): Sea blindness in grey zone preparations, Defence Studies, DOI: 10.1080/14702436.2024.2359913

To link to this article: https://doi.org/10.1080/14702436.2024.2359913

Published online: 30 May 2024.

DEFENCE STUDIES
https://doi.org/10.1080/14702436.2024.2359913

Routledge
Taylor & Francis Group

ARTICLE

OPEN ACCESS Check for updates

Sea blindness in grey zone preparations

Oscar Leonard Larsson

Department of Political Science, The Swedish Defense University, Stockholm, Sweden

ABSTRACT

Although grey zone and hybrid threats, such as cyberattacks, information campaigns, and sabotage against critical infrastructure, are becoming increasingly common in the contemporary world, relatively little attention has been directed to similar threats in the maritime environment. The recent global pandemic, Russian aggression against Ukraine, the Nord Stream sabotage in 2022, the sabotage of the Finnish-Baltic pipeline in 2023 in the Baltic Sea, as well as drone attacks on shipping in the Persian Gulf are but a few examples that illustrate the fragility of international maritime communications. The present article explores the topic of grey zone and hybrid threats within the maritime environment. Based on an analysis of recent security events, particularly hybrid threats in the maritime environment, the article proposes that it is essential to seek a broader role for naval forces in supporting national sovereignty and international law and order regarding the Open Seas. The article aims to conceptualize and explore the foundations of maritime grey zone threats and the new roles of naval forces operating within this new context, asking whether the UN, through the International Maritime Organization, NATO, and the European Union, suffer from "sea blindness" concerning how they are preparing for the new world order.

ARTICLE HISTORY
Received 16 May 2023
Accepted 22 May 2024

KEYWORDS
Grey zone; maritime security; sea blindness; maritime forces

Whosoever can hold the sea has command of everything
Themistocles (524-460 BC)[1]

Introduction

Until recently, the debate concerning grey zone hostilities and hybrid threats has focused almost exclusively on their implications for individual sovereign states. This has primarily involved exploring new vulnerabilities in the cyber-dimension that affect the democratic political system (info-war), but it has also addressed to a certain extent the essential infrastructure that underlies critical systems (Hoffman 2007; Larsson 2024; Leed 2015; Thornton 2015; Wirtz 2017). In this respect, nation-states have thus been viewed as the main target of *hybrid threats* in the unfolding grey zone security environment.

CONTACT Oscar Leonard Larsson oscar.larsson@fhs.se Department of Political Science, The Swedish Defense University, Drottning Kristinas vag 37, Stockholm 11593, Sweden

The notion of a *grey zone* resides principally upon the idea that *hostilities* between states have begun (re)-emerging today in a manner that disrupts international institutions and blurs the boundary between war and peace. As a result, all measures short of war have been returned to the toolbox of international affairs and diplomatic relations. While this situation is similar to the Cold War, the world is far more technologically advanced and vulnerable to disruptions than before the 1990s. Even though hybrid threats are understood as hostile actions that do not include open threats or the use of military force (Sari 2020; Wirtz 2017), the possibility of escalation from *hybrid* threats to *hybrid* warfare adds substantial gravity to the situation, generating fear and a fundamental sense of insecurity.

Hybrid threats are purposeful, tactical, and covert insofar as attackers seldom reveal their identity. Such threats include efforts to pressure or blackmail political leaders, create and spread fake news and disinformation, gather intelligence, and conduct both cyber-attacks and physical sabotage against critical infrastructure. This may involve the provision of support to political extremists, terrorists, and subversive social and political movements, including the assassination of key political or public figures. In addition, goods, services, and activities that, in normal circumstances, are taken for granted, such as flows of information, energy, food staples, or even medical and genetic technology, may be weaponized (Subhayn et al. 2024). Even movements of people have been purposefully and cynically exploited to destabilize and threaten nation-states, which are often the primary targets of hybrid threats. However, a broad group of international organizations and collaborations support joint efforts to combat such threats. Intense work is underway to heighten resilience and robustness to face current vulnerabilities in hypermodern and technologically dependent nation-states (see Collier and Lakoff 2021; Hybrid CoE 2023; NATO 2023a, 2023b, 2023c; Subhayn et al. 2024).

Not all hybrid threats directly target sovereign states, however. A great deal of damage can be caused indirectly by sabotaging global communications, transport, and the various supply systems for information and crucial goods and products, including shipping, trade routes, and ports. The sea is the facilitator and thoroughfare for global markets, and any interruptions in the marine supply chains for energy, food, medical supplies, and other vital goods can be very costly. Not only is the sea no longer something we may take for granted as a global common, but disputes and disturbances at sea are likely to become far more advanced. For example, the oil pipelines and the submarine cables hidden on the seabed, carrying civil, military, and diplomatic digital traffic worldwide, are also subject to threats and disruptions. Submarine cables carry 95% of global internet traffic, and the world would become silent, and global markets would be brought to a standstill without this critical global infrastructure. The sea and the seabed together thus provide the infrastructure that keeps the world connected and global markets running.

Against this background, certain scholars, professionals, and others engaged with maritime circles maintain that many political and military leaders suffer from "sea blindness" insofar as they do not fully understand the role that the sea, sea coasts, and maritime forces play during both peacetime and war (Bueger and Edmunds 2017; Speller 2019, 8). Moreover, maritime security has recently been focused on the lower level of the threat scale. For instance, while piracy, trafficking, and smuggling are current items on the maritime security agenda, the world appears to be less prepared for more qualified adversaries and the disruptions that more resourceful actors can

cause, such as hostile rogue states with advanced naval forces capable of operations both on and beneath the surface. Full or partial sea blindness also appears evident in the way such organizations as the International Maritime Organization (IMO), the European Union, and NATO attempt to cope with the already deteriorating global security situation, the emerging grey zone, hybrid threats in general, and hybrid threats in the maritime environment. These comprise the issues that the present article seeks to explore.

The research question of this article is as follows: Is sea blindness evident in how the grey zone is portrayed in international organizations' current policy and practice preparations?

Theory: hybrid threats and the maritime environment

There has been an interest in maritime security and naval forces for as long as humans have utilised the sea for resources and communication. The oceans have posed several security problems throughout history, such as piracy, smuggling, trafficking, raiding for loot, and amphibious assaults. The ocean is thus both a blessing and a curse, and no coastal state, large or small, can ignore its sea borders and disregard maritime security.

Today's global maritime security is a joint task supported by public international law (or the Law of Nations), a codified body of specialized law, and systems for maritime governance. The latter includes the 1982 UN Convention on the Law of the Sea (UNCLOS), which provides a basic framework consisting of 17 chapters and 320 articles. The International Maritime Organization (IMO), established in Geneva in 1948, is a specialized organization within the United Nations (UN). Its aims are presented in Article 1(a) of its original convention as

> to provide machinery for cooperation among Governments in the field of governmental regulation and practices relating to technical matters of all kinds affecting shipping engaged in international trade; to encourage and facilitate the general adoption of the highest practicable standards in matters concerning maritime safety, efficiency of navigation and prevention and control of marine pollution from ships. (IMO 2023)

The IMO is also authorized to deal with administrative and legal matters related to these goals (IMO 2023).

The sea constitutes a medium over which there is little immediate political control. A series of laws, agreements, and accepted practices and customs govern the sea and the activities of a broad set of actors who operate in this environment (Speller 2019, 24). Nevertheless, the sea and its multiple jurisdictions and customs, together with its connectivity, opaque terrain, and the fact that it is regarded as a global common for everyone to use, elicit specific grey zone threats that demand our attention as long as great power competition and hostilities among states continue. Controlling and regulating the oceans have been a daunting and challenging task throughout history. This is sometimes due to divergent interests between states and direct hostile actions. However, it has also been caused by issues associated with internal instability within a given state or the emergence of non-state actors that seek to profit from illegal activities. Maritime security is

a complicated task, not least because of the recent changes regarding international security, grey zone activities, and new means for creating hybrid threats that challenge global maritime security (Rowlands 2019, 15).

Grey zone and hybrid threats

Most attention and conceptualization regarding the grey zone security environment and hybrid threats have focused on territory, the cyber dimension, and the impact such activities can have upon open political systems such as liberal democracies. The grey zone is a concept that describes the re-emergent hostility between states whereby a previously clear boundary between peace and war has become blurred, leading to hostilities below the threshold of war. This includes disruptions within the liberal and judicial world order produced by states that no longer respect public international law, international organizations, or international institutions (Hoffman 2007; Leed 2015; Thornton 2015; Wirtz 2017). Moreover, we are entering a global security situation similar to the Cold War. However, the contemporary world is far more technologically advanced than before, and it relies on critical infrastructure and speedy digital communications in its daily operations. This has, in turn, created increased vulnerability to disruptions in both the physical and cyber realms. Today's hypermodern and advanced societies have thus become more fragile and susceptible to hostile actions as we have grown increasingly dependent on the vital systems that sustain our everyday activities, whether that be in the private, political, or economic spheres (Aradau, Lobo-Guerrero, and Van Munster 2008; Collier and Lakoff 2021).

Adding to the current complexity is that hybrid threats are not always directed against the state and the public administration. For example, they can readily be targeted against civil society and market actors engaged in health care, food production or distribution, or other vital but outsourced functions of society. There is also a psychological dimension to hybrid threats. Cyberattacks, either on their own or combined with disinformation campaigns, can potentially undermine trust in political leadership and public institutions, leading to the population's disillusionment and a breakdown in society's "fighting spirit" (Leed 2015). Particular hybrid threats, including fake news and misinformation, can also be directed against individuals, specific groups, and even entire populations to generate polarization and distrust within society, not least concerning political leaders. In addition, it is presumed and feared that several differing grey zone tactics may be employed simultaneously and strategically to maximize their effect and give rise to chaos, fear, and uncertainty.

The new possibilities that social media have created for reaching the populations of other countries add additional weight to modern info-wars, fake news, and trolling (Treverton 2018). Nevertheless, hybrid threats typically stay below the threshold of open hostility and military action. While they do not constitute decisive blows by themselves, they are capable of paralyzing the state insofar as the latter knows neither how to respond, nor how to defend itself, nor whether there will be an escalation into hybrid war (Hoffman 2007; Wirtz 2017; cf.; Mälksoo 2018, 377).

While this manner of portraying the grey zone and hybrid threats is well established, it is accompanied by the risk of viewing nation-states as "islands" in an ocean. States today are far more interconnected than before and have grown

dependent on international communications and trade. Most countries are, in fact, dependent upon unbroken communications with other countries as well as the export and import of goods such as food, energy supplies, and medical equipment. In addition, the stockpiling of all the vital goods needed to keep a state functioning during war or a large-scale natural disaster is now deemed inefficient and overly costly (see Collier and Lakoff 2021). The recent COVID-19 pandemic illustrates the difficulty of preparing for global crises and interruptions in global logistical and supply chains.

Most industrial production and food distribution now employ the just-in-time model to reduce the costs of stockpiling. Still, this practice forces us to rely on an uninterrupted flow of components and products. Furthermore, digital information and communications are more valuable than raw materials. Notably, the crucial global infrastructure that supports the flow of digital information lies hidden beneath the surface of the oceans. The strategic sabotage of seabed infrastructure could bring the entire world to a standstill (Bueger and Liebetrau 2021).

Oil, gas, and electricity are the cornerstones of both national energy security and the global energy market. Energy security was a crucial element of total defense and the overall military capacity of states during the 20th century, and lubricants and fuels were essential for the ability of any country to conduct war (Yergin 2011). The oil crisis of the early 1970s displayed the world's increased dependency on oil, the extreme vulnerability of supply, and the economic costs of an oil shortage. Although oil prices and energy supplies were relatively stable during the 1980s and 1990s, not only has global demand increased since the 2000s, disruptions of gas supplies in Europe and the pressure to adapt to climate change have again placed energy security high on the global security agenda (Cherp and Jewell 2014). There has been a growing concern since the 2000s that energy security and supply will have a very substantial and direct geopolitical impact.

Concerning the notion of energy rivalry, a Chatham House report presented at the European Security and Defence Forum (ESDF) in 2010 argues that

> The militarization of energy, the recourse to military capabilities to accede, control and manage energy resources, both in upstream and downstream activities, therefore seems to be one of the most alarming prospects facing international systems today. (Sartori 2010)

A 2006 report from the Swedish Defence Research Agency maintains that Russia, for example, has a long history of using its economic power and natural resources to pressure neighbouring countries by cutting natural gas supplies or altering pricing schedules. It also argues that the more a given country pursues "friendly" policies towards Russia, the better the prices and contract terms it offers (Larsson 2006). Within this context, when private businesses manage both critical infrastructure and energy supplies, it is possible to target specific firms, business figures, and public servants in grey zone economic coercion, pressuring, blackmailing, or bribing them into advocating and supporting Russian projects such as pipelines or specific energy options (see Ozava 2021)

This serves to transform energy production and distribution into potential weapons that can be used to further national interests and bring pressure to bear on adversaries. Energy markets and security depend not only on supplies but also on infrastructure and supply channels that can deliver these supplies to the market and, in the end, customers. Oil refineries, ports, and storage facilities – but also pipelines on both land and the

seabed – are all elements of a critical global infrastructure that sustains the international market with energy supplies. These comprise crucial points concerning national interests and constitute potential targets for both state and non-state actors. The September 2022 sabotage of gas pipelines in the Baltic, which removed the possibility of Russia delivering gas to Europe, is a case in point. It remains unclear who sabotaged the pipelines, and Russia, Ukraine and even the United States have been suspected of doing so.

Submarine cables

Oil and gas pipelines are essential, and the global energy market heavily depends on communications on and below the surface. While any disorder in these lines of communication may have a severe effect on nation-states in peacetime, it can have a devastating effect on the military capabilities of a country that has been targeted. However, there are also other lines of communication on the seabed, such as undersea cables that carry internet traffic and virtually all other forms of digital communication. The importance of safeguarding this network of cables cannot be overemphasized – satellites can manage only a fraction of the current volume of digital communications. It is estimated that "at least 95% of voice and Internet traffic travels through about 300 transoceanic fiber-optic cables along the seabed" (Clark 2016). These cables, which constitute the interconnectedness of the modern world, are vital for the world economy, state governments, national security, and governmental and diplomatic communications.

The global submarine cable system is vulnerable to peacetime accidents, deliberate sabotage and attacks during wartime and heightened hostilities in the grey zone. The undersea cyber network relies upon cables lying on the seabed, which are at risk as they typically lack surveillance and security arrangements (Bueger and Liebetrau 2021; Clark 2016). Proposals have been put forward to increase the number of cables to create multiple lines of communications and eliminate choke points; patrol cables with unmanned vessels and sensors; heighten overall surveillance; and, in general, improve the systems that guard these highways of digital data (see James and Pedrozo 2022). This global network, recognized as "one of the most indispensable infrastructures" (James and Pedrozo 2022, 180), consists of 213 independent systems and a total of 750,000 miles of seabed cables. They are operated by multinational consortia, often marked by multiple and overlapping ownership, and there is no official global registry of the actual owners. The strategic and military importance of communications utilizing undersea cables also transforms such cables into legitimate military targets, even though various legal manuals suggest that hostile actions should be directed against them with great care and only if necessary (see also Bueger and Liebetrau 2021).

1898 during the Spanish-American War, American Commodore George Dewey cut the Manila-Hong Kong cable, owned by a British company and laid under a Spanish concession. This was followed by two similar operations later that same year in the San Juan Channel, Puerto Rico, and the harbor of Cienfuegos, Cuba. These operations were brought before an international tribunal after the war, and the subsequent judgment favoring the American actions held that

> the right of the United States to take measures of admittedly legitimate defense against the means of enemy communications was fully justified. (as cited in James and Pedrozo 2022)

However, what does it mean precisely to state that undersea cables are legitimate military targets in an emergent world of grey zone hostilities? Submarine cables are the information highways in today's world, which is dependent upon digital data and cyber capacity for everyday operations. Notably, many countries now have access to submarines, remotely operated vehicles, and deep-diving submersibles capable of disrupting submarine cable communications by monitoring or sabotaging them. The United States, Russia, and China are among the most capable countries in this regard.

The world's eyes turned to the ocean and the seabed after Nord Stream 1 and 2 were sabotaged – it is still unclear by whom and for what purpose (Bueger and Liebetrau 2022). This deliberate attack could only have been carried out by a capable, resourceful, and skilled actor, most likely a nation-state. These two countries are conducting investigations since the explosions occurred in the Swedish and Danish economic zones. Although their outcome is not yet clear, it is safe to say that maritime security and the protection of critical international infrastructure will become an object of more acute concern after this event. *The Maritime Executive* has reported that Italy, Norway, Germany, and the United Kingdom immediately began surveilling their underwater cables and pipelines when notified of the sabotage. The British Secretary of State for Defense, Ben Wallace, announced in this regard that he had committed to obtaining "two specialist ships with the capability to keep cables and pipelines safe," adding that the first multi-role survey ship for seabed warfare would be purchased by the end of 2022, fitted out in Britain, and become fully operational by the end of 2023. The second ship will be built in Britain and equipped to " cover all . . . vulnerabilities."[2]

A more traditional notion of security maintains that states' political, economic, and military sectors drive international relations and security (Buzan, Wæver, and De Wilde 1998). However, it is important to note that economies and security concerns have become more intertwined with expanding trade and creating extensive global lines of communication. New security agendas and concerns for the oceans have thus come to involve cyber and information technology and military, economic, and environmental dimensions. Regardless of its size, the sea is every state's business with a coastline. While the importance of the sea and maritime security now pertains to peacetime and war, the current grey zone era places further pressure on the coastal states of the world.

It may nonetheless be possible that leading actors suffer from sea blindness in the grey zone and the era of hybrid threats. The article will now address the concept of sea blindness before examining the policies of leading international organizations.

Sea blindness

Despite the immense importance of the sea for communications and transport and as a hub for global markets, it is often taken for granted. Freedom of the sea in international waters fosters the idea of maritime security and constitutes the foundation of oceans as a global common. When transport and communications are disrupted, such as during war or because of a large-scale crisis, the adverse effects are often immediate and extreme. Pertinent examples include the German deployment of U-boats against cargo ships during WWII, which cut off the transport of vital goods to England (O'Keefe 2020); the blocking of the Suez Canal for a month by an Evergreen Marine Corporation cargo

vessel that ran aground; and the blockading of Ukrainian ports by Russian forces, which created a global wheat shortage.

China's irregular maritime activities in the straits and islands of Southeast Asia, along with its growing aggression towards Taiwan, are another source of grey zone activities in the maritime environment. The use of "little blue men" and non-military vessels to extend Chinese control over an increasingly significant area of disputed and reclaimed islands and reefs in the South China Sea is visible in this region. These seaborne militias, consisting of hundreds of fisher folk in motorboats, are intermingled with vessels identified as China's paramilitary forces. These vessels have been known to "buzz" US Navy ships and those of neighbouring countries with competing territorial claims, creating a grey zone of uncertainty regarding rules, interests and intents (Singh 2018).

This level of impact also serves to illuminate the varied roles that naval forces may play in maritime security. For instance, in addition to naval forces being one of the essential instruments of the state in wartime, they can be of great use in promoting maritime security in peacetime through the protection of shipping lanes, civilian vessels, and borders in the fight against piracy and trafficking (Booth 2014; Bueger 2015; Rowlands 2019). Given the intrinsic value of the sea for trade, the importance of a broader role for oceangoing forces in heightening security would indeed appear to be beyond question. Naval forces, the sea, and maritime security may nonetheless (still) suffer from the phenomenon of "sea blindness" (Speller 2019; see also Bueger and Edmunds 2017). This issue is worthy of further exploration.

There are few studies on the theoretical level of the naval and maritime aspects of international relations and security. However, recent events, including piracy in Somalia and human trafficking in the Mediterranean, have drawn much-needed scholarly attention. Another recent example displays the importance of the maritime dimensions of fighting insurgent groups. The Tamil Tigers (LTTE) had been able to operate off the coast of Sri Lanka for a substantial period, providing logistical support to their guerilla activities, smuggling arms, conducting maritime terrorism, and employing piracy as a means of acquiring additional resources for their campaign. Justin Smith (2011) maintains that a decisive change occurred, consequent to the Sri Lankan Navy's (SLN) success halting the LTTE's maritime activities. The SLN thereby severely disrupted the Tigers' robust sea-based support network for their swarming suicidal attacks on land, forcing them to confront the government's final land offensives with diminished resources (Smith 2011).

Jacob Børresen argues in a 1994 article that the navy of a small coastal state has two main tasks, namely, deterrence and the maintenance of sovereignty. He states that

> The fewer "creative un-clarities" that exist, the lesser the chances that potentially dangerous conflict situations may arise. (Børresen 1994, 153)

He also observed that the end of the Cold War shifted the focus of small coastal states from deterrence and war towards surveillance, control, and crisis management. Ioannis Chapsos and Elizabeth Ann Norman (2023) argue in much the same vein that

> in the last decade the concept of maritime security has expanded beyond traditional, state-centric security challenges, such as maritime territorial disputes, to encapsulate contemporary threats. (Chapsos and Ann Norman 2023)

The latter include issues that do not immediately threaten the sovereignty of states or involve a violation of territorial waters, such as maritime piracy, illegal fishing and fisheries crimes, trafficking, smuggling-related crimes, and deliberate unlawful damage to the environment, all of which may have complex judicial and international aspects. These concern criminal activities more than outright security threats, and they often place the question of maritime security outside both academic and policy discourses that address security (see Chapsos 2016).

While such prominent naval thinkers as Alfred T. Mahan (1890, 1892) and Julian S. Corbett (2004) have primarily focused on the various ways of employing naval forces in war, strategic thinkers during the Cold War made significant new contributions to the field of naval diplomacy. Cable (1981, 1985), Edward Luttwak (1987), and Ken Booth (2014), not least of all, have framed their assessments of naval diplomacy in terms of a bipolar world system, presenting theories that are realist in outlook, state-centred, and binary in the sense of actors being either active or reactive. In the latter case, the instigator has typically been viewed as a great power, with the more passive actor tending to be a weaker state. In historical terms, this served the purpose of providing a naval balance and deterrence between the United States and the Soviet Union, and it remains clear that warships can be sent to remote places to signal seriousness and the capacity to intervene.

During the Cold War, the main focus was on hard power and less on the many subtle forms of soft power available. However, after the Cold War, a new approach emerged which emphasized a multilateral approach, a broader context of interaction between various actors, and a focus on soft power and cooperation (Rowlands 2019; see also Oscar and Widen 2022). We are likely about to enter a new "Cold War" era but in a world marked by international infrastructure and communications far more advanced than in the 1960s. This can only mean that naval forces must be updated for new tasks, including the surveillance and protection of international infrastructure.

While security studies have advanced following the end of the Cold War from the discipline's traditional focus on states, armed forces, and war towards becoming more "broadened" and "deepened," thereby incorporating a much broader set of security issues, domains, and activities, the associated maritime issues have neither drawn much attention nor generated transformation. Bueger and Edmunds state in this regard that, despite the broadening of the field of security studies in the mid-to late-1990s, maritime security and the naval domain have not been a central focus of analysis within either international relations theory or security studies (Bueger and Edmunds 2017). Emma Björnehed has recently addressed how naval forces throughout history have been thought of and internalized in terms of a supportive role for the army and, later, the air forces. This has not only undermined to a degree the idea of the navy as a fighting power in its own right, but it conceals the much more diversified roles that naval forces play in both war and peacetime, including their contribution to maritime security in general (Björnehed 2022). Although naval forces are widely used in maritime security, this is mainly noted by a narrow group with special interests. At the same time, the public, journalists, and politicians "tend not to understand the use or importance of the sea." Such sea blindness,

understood as the "inability to understand the sea or to recognize its importance to national and international well-being" (Speller 2019, 8), potentially places blinders on states now grappling with the grey zone security environment, where hostilities take place between competent actors rather than between the state and pirates or smugglers.

Method and data

The present study investigates whether grey-zone discourse is marked by sea blindness. It analyzes documents from three central international organizations: the UN via the International Maritime Organization, the European Union, and NATO. These three organizations were selected because they are international in character and consist of many different member states. As such, they should not reflect the interest of any one state but rather a collective of states. Thus, they are more likely to reflect on maritime security issues in relation to International Law and consider oceans and oceanic global infrastructure as global commons.

The approach and design for this study are based on interpretive and qualitative policy analysis (Yanow 2000). This approach suggests that we investigate how central actors with proper influence conceptualize the problems of maritime security that have been discussed. This would inform us about the essential current understandings, policies and practices concerning the specific problem. The qualitative approach focuses on the meanings of policies, values and beliefs, conceptualizations and problematization that key actors express in various sources (Bacchi and Goodwin 2016). Qualitative research is a method of studying things in their natural settings and attempting to interpret or make sense of phenomena based on the meanings that people attribute to them. This approach acknowledges different ways of understanding the world and aims to discover the meanings and perspectives of those critical actors being researched. This helps the scientific community gain knowledge about the beliefs and understandings of different actors and their view of the world instead of relying solely on the researcher's or scientific community's views.

This approach to policies formulated and implemented by various critical actors has also been defined as *problem-finding policy analysis*. It aims to discover the elements of problem definitions in various policies but does not necessarily evaluate the outcomes of those policies or the problem resolutions they propose. This type of analysis instead seeks to determine how actors understand the problems at hand; for instance, who is identified as a stakeholder or key actor in the policy arena, whether the appropriate objectives and priorities have been identified, and the events, both likely and unlikely, that should be included. Briefly stated, the question is whether current policies are oriented towards the "right problems" or the "wrong problems" (Dunn 2015, 14 see also Bacchi and Goodwin 2016). Other approaches might consider mapping the frequency of events and disruptions to reveal if the problem is real and severe. The problem with such an approach is that many incidents and events are demanding to know, and a single incident might not represent the phenomenon or the direct responses it generates. A qualitative approach is preferable if we wish to understand the "inside" view of critical actors.

The period investigated is one year before the sabotage of Nord Stream 1 and 2 and until April 2024 to detect whether this event has led to any policy changes concerning maritime security and the grey zone.[3]

The article uses qualitative content analysis (Boréus and Bergström 2017, 7) to investigate open-source data, including reports, briefs, news, and newsletters from the three organizations, to extract important passages of theoretical relevance from discussions of the grey zone and relevant maritime dimensions.

Results

The United Nations and specialized maritime agencies

The focus of the International Maritime Organization on maritime security principally concerns shipping and counter-piracy operations, and its approach to grey zone problems is mainly oriented towards cyber threats directed towards private shipping companies and harbours. For instance, the IMO's programmatic explanation of its activities states that

> The IMO secretariat, in particular MSF staff with maritime security related duties, work in close cooperation with Member States, partner United Nations agencies, regional organizations, development partners and the wider maritime industry, to safeguard global maritime security and suppress piracy, armed robbery against ships and other illicit maritime activities. This multilateral and cooperative effort ensures that the response in dealing with major maritime security threats and incidents around the world is adequate and effective, at national, regional and international levels (IMO 2022, Maritime Security).[4]

In 2022, the IMO identified piracy, port security, cyber threats, and unregulated migration to be among its top concerns with respect to maritime security (IMO 2023, Hot Topics, Piracy).[5]

Cyber security today illustrates the advanced level of technology that is currently employed on ships, in cargo operations, in port operations, and communications. The IMO states in this regard that:

> Cyber risk management means the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders (IMO 2023, Cyber Security).[6]

The principal goal is to promote safe and secure shipping to become resilient to cyber risks, which is reflected in the manual it has developed for this purpose, *Guidelines on Maritime Cyber Risk Management*. It is notable that although this manual is intended to

> provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyber threats and vulnerabilities,[7]

it generally serves only as a reminder that cyber threats exist – it neither provides examples nor identifies those actors who may be sufficiently resourceful to exercise such threats.

It may be that the IMO, as a UN agency, does not wish to name specific countries as being more inclined than others to conduct cyberattacks and disruptive grey zone

activities in the maritime environment. For instance, China is a member state of IMO and was elected as a Member of the IMO Council in 2023 (it has previously been a member of the IMO Council for 17 years). Russia on the other hand, was excluded from the IMO Council in 2023 but remains a full member with voting rights in the organization.[8]

IMO is however very outspoken concerning the struggle against fighting piracy and ship-armed robbery and has developed guidelines for how to cope with such threats. It is significant that insofar as such activities are mainly carried out by non-state actors with relatively limited capabilities, such as rebels, insurgencies, and criminal networks, it is less difficult to condemn them and provide policy instruments to counter them. It is evident that the International Maritime Organization (IMO) is more sensitive to naming and shaming countries that engage in grey zone activities.

The ports and sea routes on the Black Sea and the Sea of Azov were closed after the Russian invasion of Ukraine. The world quickly realized that the resulting market loss of the grain and fertilizers usually shipped from the three main Ukrainian ports of Odesa, Chernomorsk, and Yuzhny would soon have negative implications on a global scale, particularly for the developing world. However, the IMO and delegates from Ukraine and Russia succeeded in negotiating a treaty at a meeting hosted by Turkey that would permit grains, food staples, and fertilizers to be shipped from Ukraine through a maritime corridor designated for this purpose (IMO 2023, Ukraine Shipping).[9] In December 2023, at the same time as Russia was expelled from the IMO Council, the organization adopted another resolution, A1183(33), entitled "The impact of the Russian Armed Invasion of Ukraine on International Shipping,"

This resolution underscored the importance of preserving the safety and welfare of seafarers, the need to preserve the security of international shipping and the maritime community, and the importance of export-import through the seaports of Ukraine. Through the resolution, the IMO decided to conduct a needs assessment of this issue along with providing technical assistance to support Ukraine in the implementation of IMO instruments as Ukraine continues to operate the special maritime corridor recently established[10]

This illustrates the active role played by the UN and the IMO in safeguarding shipping and trade amid the Russia-Ukraine war. The UN and the IMO may undertake similar missions in the future, ensuring that sea routes remain open during war or conflict.

The International Seabed Authority (ISA) is another relevant UN agency for discussions of critical global infrastructure and global communications. It is an autonomous international organization established under the 1982 United Nations Convention on the Law of the Sea (UNCLOS).

> The ISA is the organization through which States Parties to UNCLOS organize and control all mineral-resources-related activities in the Area for the benefit of mankind as a whole. In so doing, ISA has the mandate to ensure the effective protection of the marine environment from harmful effects that may arise from deep-seabed-related activities (ISA 2023).[11]

The ISA has been chiefly concerned with fair and safe mineral extraction from the seabed and preserving seabed wildlife. It has yet to direct its attention to global infrastructure.

In summary, although the United Nations and its maritime agencies have addressed various maritime security issues, they have focused more on cyber security and protecting shipping against piracy and armed robbery. The IMO has also played a central role in resolving the crisis concerning shipping grains and food staples from Ukrainian ports after the Russian invasion. It has also acknowledged the importance of such critical global infrastructure as cables and pipelines for maritime security after the sabotage of Nord Stream in 2022. However, the IMO has not yet provided any guidelines or policy briefs on how to proceed with this question.

The European Union

In 2014, the European Union adopted the EU Maritime Security Strategy (EUMSS), which was later accompanied by an action plan. The overall aim of the policy and action plan is

> to prevent, deter and counter the multiple security threats and challenges that affect the oceans and to enhance a rules-based order at sea (EEAS 2021).[12]

The EUMSS provides principles and guidelines for ensuring coherence and complementarity among the EU's diverse and sector-specific policies and strategies to help secure the maritime domain. In 2018, it presented a revised action plan to further guide and facilitate the implementation of the EUMSS.[13]

The EUMSS addresses both the internal and external aspects of the EU's maritime security for the purpose of promoting a cross-sectoral approach to maritime security. It should nevertheless be noted that maritime security comprises a broad category that includes maritime safety, fisheries control, marine environmental protection, customs, border control, law enforcement, and defense, research, and development. The EUMSS contributes to the defense and protection of EU maritime interests with respect to security and peace in the world; the rule of international law and the general freedom of the sea; the freedom of navigation; external border control; and maritime infrastructure, such as ports, underwater pipelines and cables, and windfarms.[1415]

In addition to the EUMSS program, the European Union adopted the EU Global Strategy (EUGS) in 2016, which states that

> The European Union will promote peace and guarantee the security of its citizens and territory. Internal and external security are ever more intertwined: our security at home depends on peace beyond our borders (EUGS 2016:7).[16]

The EU seeks to advance a "comprehensive approach" to security that involves not only traditional defense and military responses to security threats but also multilateralism, humanitarian security, and cooperation, including cooperation with civil societies outside the European Union. In its external actions, the EU is

> committed to a global order based on international law, which ensures human rights, sustainable development and lasting access to the global commons (EUGS 2016:9).[17]

In this respect, the European Union has managed three maritime security operations since 2014—EUNAVFOR, Atalanta, and EUNAVFOR MED, or Operation Sophia, which was later transformed into Operation IRINI (Oscar and Widen 2022).

The European Union has stated its awareness of the fact that "security threats in the maritime domain [have] become increasingly multifaceted and complex."[18] The European Council reaffirmed its willingness to act as a global maritime security provider in June 2021. However, it has also expressed hopes for maritime multilateralism and cooperation on all levels. The Council has highlighted the growing impact and importance of addressing climate change and environmental degradation, along with the potential negative impact of the degradation of international stability, general maritime security, and *maritime infrastructures*.[19] In addition, the European Union has expressed its ongoing interest in maritime security, explicitly noting that maritime infrastructure is a major concern. It is also well known that the EU cannot implement such commitments without the direct involvement and resources of the Member States. Nonetheless, although such interest and awareness existed prior to the Nord Stream sabotage in September 2022, the EU and the Member States were unable to prevent such an attack on critical maritime infrastructure in the Baltic Sea. This depends, of course, on prior knowledge of the attack and of who carried it out.

The EU is also a member of *The European Centre for Countering Hybrid Threats* (Hybrid CoE). This knowledge center was founded through a Memorandum of Understanding between eight European members and the United States at the initial meeting of its elected Steering Board. The initiative to establish a center for managing hybrid threats was put forward on 6 April 2016, by the European Commission, including the High Representative to the European Parliament and the Council in Brussels. The membership of the Centre, which had grown to 28 states by late 2020, collaborated extensively with the EU and NATO. Hybrid CoE's cross-governmental and cross-sectoral networks consist of over 1,200 practitioners and specialists – governmental officials, experts, private sector actors, and academics – who work with identifying and countering hybrid threats. The ambition is to "lead the conversation on hybrid threats by publishing a wide variety of publications and engaging with various partners in the field" to provide policy proposals and advice in the effort to overcome hybrid threats.[20]

These publications constitute the most important material for the present analysis. They reflect the constitution of problems and potential solutions and exert a direct influence on the policies and actions taken by the participating member states and organizations. Although Hybrid CoE addresses many topics, the article here focuses on how it considers maritime security, hybrid threats, and global maritime infrastructure in its publications. A handbook regarding maritime threats from 2019 provides a conceptual framework and ten scenarios involving complex legal considerations within the United Nations Convention on the Law of the Sea (UNCLOS) (Lohela and Schatz 2019). However, none of these scenarios addressed the sabotage of cables or pipelines, although one covers accidental pipeline damage. An announcement in April 2022, after the Russian aggression against Ukraine, indicated that the handbook would be updated with at least five new scenarios.[21] In March 2023, a new version of the handbook with additional scenarios of undersea cable cuts was published, but pipeline and infrastructure sabotage on seabed infrastructure still remains to be scarcely addressed in the handbook and other publications from the center.[22]

It appears safe to say that legal frameworks, international courts, and litigation will play a limited, if not insignificant, role in a grey zone environment. In the spring of 2023,

EU noted a need to update its Maritime Security Strategy in a press release. It suggested that:

"Security threats and challenges have multiplied since the adoption of the EU Maritime Security Strategy in 2014, requiring new and enhanced action. Long-standing illicit activities, such as piracy, armed robbery at sea, smuggling of migrants trafficking of human beings, arms and narcotics, as well as terrorism remain critical challenges. But new and evolving threats must also be dealt with increasing geopolitical competition, climate change and degradation of the marine environment and hybrid and cyber-attacks" (European Union 2023).[23]

While the EU recognizes many issues as contemporary security threats, they remain on the lower scale of hybrid threats, and its focus is mainly on non-state actors. The EU may thus need to prepare for a higher level of conflict and hostilities in which the rule of international law is not respected.

In March 2018, Hybrid CoE initiated a network of "experts, advisors, researchers, practitioners, government officials, officers, directors and policy-makers from these sectors and communities" regarding the critical infrastructure to be addressed in maritime security, the main purpose of which was to identify vulnerabilities and enhance resilience in the three areas of "Ports, Shipping and Underwater Cables" (Hybrid CoE 2018).[24] To date, however, no specific publication or policy recommendation has been produced which shows that underwater cables have been properly addressed besides a new scenario in the handbook mentioned above. In a manner somewhat analogous to that of the IMO, the issue with respect to maritime security and hybrid threats that have drawn the most significant attention to the EU and the Hybrid CoE concerns the various forms of cyberattacks on navigation, communications, and maritime operations that cause substantial disruption in shipping and on-sea communications.

The North Atlantic Treaty Organization

NATO acknowledges that

> Today's security environment is increasingly complex. The times when peace, crisis and conflict were three distinct phases, when conflicts were fought largely with military means, and when adversaries were well known, are over (NATO 2021).[25]

Cyberattacks and social media information campaigns are recognized as two of the most common hybrid threats. It is indeed the "hybrid" character of such threats, or the "combination of military and non-military instruments," which generates ambiguities that render NATO's situational awareness and, consequently, consensual and timely decision-making far more complex (NATO 2021). Countering hybrid threats has been a top priority for NATO since 2015 when it adopted the *Alliance Strategy on Countering Hybrid Warfare*, and it has subsequently aimed at enlarging the "toolbox" for countering hybrid threats. Critical issues for NATO in this regard are *resilience* and *civil preparedness* (NATO 2021).

NATO finds that with ongoing technological development, as we move from the Internet of Things to the Internet of Everything,

> more and more of the infrastructure that we depend on for the normal functioning of our lives is being automated or controlled from remoter distances or integrated into ever more complex networks. The SCADAs—or automated control systems for electrical grids or energy pipelines—are but one example (NATO 2016).[26]

The increased connectivity between countries, which renders them more dependent on each other, also explains why NATO has been asking its members to increase their resilience further and boost civil preparedness in the era of hybrid threats.

> Resilience is a society's ability to resist and recover from such shocks and combines both civil preparedness and military capacity. Civil preparedness is a central pillar of Allies' resilience and a critical enabler for the Alliance's collective defence, and NATO supports Allies in assessing and enhancing their civil preparedness (NATO 2022, Resilience).[27]

Since 2018, NATO has evaluated its member states' vulnerabilities and societal resilience in respect to the continuity of government and critical government services; energy supplies; the ability to deal effectively with the uncontrolled movement of people; food and water resources; the ability to deal with mass casualties; communications systems; and transportation systems (NATO 2016).[28]

NATO also states that it has a particular interest in maritime security. In January 2011 NATO adopted the Alliance Maritime Strategy, which identifies NATO's maritime power can "be used to address critical security challenges'" and "play a key role in deterrence and collective defence, crisis management, cooperative security and maritime security."[29] The Alliance reinforced its maritime strength at the 2014 Summit in Wales and placed greater emphasis on developing core maritime competencies and fighting abilities at the 2018 NATO Summit in Brussels. In 2023, NATO stated on its webpage that, even in the current heightened security context,

> the Alliance's naval forces provide essential contributions to maritime situational awareness and presence, maritime security, assistance and deterrence effect (no reference).[30]

The Alliance further adds that it continues

> to implement its maritime strategy through capability development, an enhanced programme of maritime exercises and training, and the enhancement of cooperation with partners, including other international organisations such as the European Union.[31]

It is surprising that although NATO had stated before the 2022 Nord Stream sabotage that it was eager to demonstrate its ambition and capability to provide maritime security, it had been unable to take decisive action. However, in March 2023, NATO launched together with EU the "NATO-EU Task Force on Resilience of Critical Infrastructure." NATO states that "the initiative brings together officials from both organisations to share best practices, share situational awareness, and develop principles to improve resilience."[32] In addition, in August 2023, NATO also created a *Critical Undersea Infrastructure Coordination Cell* to support engagement between NATO Allies, partners, and the private sector.[33] It appears that NATO has incorporated critical undersea infrastructure into its maritime security framework. In addition, it is also the organization that is most outspoken on the maritime activities and disruptions of Russia and

China but even NATO has a difficult time condemning the Chinese activities in East Asia.

Conclusion

In a world characterized by multiple centers of power and a liberal order dedicated to trade and international institutions, promoting maritime security and enforcing the rules of the sea have frequently been understood as relatively straightforward shared tasks. The focus within this type of context falls on pirates, traffickers, smugglers, and rebel groups, none of whom can pose a severe threat to global security or the resources needed to disrupt global infrastructure. Many states and other actors have expressed their interest in contributing to maritime security in this respect, regarding open and safe sea routes as vital means for ensuring global trade.

Significant global actors such as the UN, the EU, and NATO play essential roles in upholding maritime security in a complex and uncertain global security situation. In today's changing structure of international relations, the Russian aggression against Ukraine in February 2022 will likely accelerate the present tensions into a situation similar to that of the Cold War. As a result, global maritime security may be impacted by the new superpower rivalry between Russia, China, the United States, and Europe. New maritime security challenges already emerged in 2022 with the sabotage of pipelines in the Baltic Sea and then again in 2023, port blockades in Ukraine, "little blue men" in the sea of East Asia, and drone attacks against oil shipments in the Middle East, and after Israel-Palestine war in 2024, missile attacks towards shipping in that area. Maritime security is currently facing many challenges.

The policy analysis conducted in the present article reveals that the IMO, the EU, and NATO all acknowledge that the world has entered into a grey zone of heightened hostilities and hybrid threats. While these organizations express concerns regarding hybrid threats in the maritime environment, they have focused primarily on cyberattacks, piracy and disruptions to global trade routes. They also appear more oriented towards countering non-state actors such as pirates, traffickers, and international criminal networks. It is noteworthy that although the EU, NATO, and even the IMO have expressed their concerns regarding pipelines and seabed cables, it is mainly NATO, in cooperation with the EU, that has included critical infrastructure on the seabed and launched task groups. Still, given the severity of the problem and vulnerability, it seems that this is mainly reactive to the event in the Baltic Sea in 2022, but despite this, global actors were still unable to stop the second sabotage in the Baltic Sea in 2023. More needs to be done to secure the global infrastructure on the ocean and on the seabed. We have grown accustomed to just-in-time logistics, with open sea routes comprising the arteries of globalization and international markets. Recent actions and events reveal how readily the flow of communications and vital goods can be impeded.

Global organizations such as the United Nations' International Maritime Organization (IMO), the European Union, and the North Atlantic Treaty Organization (NATO) should increase their efforts to promote maritime security. They should focus on the impact of critical infrastructure damage caused by capable actors, which can lead to severe disruptions in global communication, the economy, and countries' security. These organizations may have already taken steps in this direction, but these actions have

not been discussed in the sources analyzed in this article. The article concludes that these organizations should re-evaluate their strategies and approach to maritime security in the present era of uncertainty.

Notes

1. As cited in Speller (2019):1.
2. The maritime executive 2023. https://www.maritime-executive.com/article/after-nord-stream-attack-europe-scrambles-to-secure-subsea-pipelines. Retrieved 2023-01-17.
3. The initial period when submitting the first version of the article was 6 month after the first incident in the Baltic Sea. During the peer-review process and revisions during the spring of 2024, the sources were revisited, but there was still little change in the official policies and the original findings hold. At this time, I still followed up on the issues and events addressed in the original submission. The issue with seabed sabotage is sensitive and potentially these critical actors do not wish to reveal their work in public channels. If one wishes to continue investigating this issue, interviews with experts in the organizations are advisable but could generate knowledge that is not publishable. The idea here is to instigate a more general discussion, both in academy and among policy actors and organizations in the world.
4. IMO 2022, Our Work, Maritime Security. https://www.imo.org/en/OurWork/Security/Pages/GuideMaritimeSecurityDefault.aspx. Retrieved 2022-12-19.
5. IMO 2023, Hot Topics, Piracy. https://www.imo.org/en/MediaCentre/HotTopics/Pages/piracy-default.aspx. Retrieved 2023-01-17.
6. IMO 2023, Cyber Security. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx. Retrieved 2023-01-17.
7. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx. See also IMO 2022, *Guidelines on Maritime Cyber Risk Management*. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf. Retrieved 2023-01-17.
8. The Maritime Executive 2023, Russia Voted Off of IMO Council, https://maritime-executive.com/article/russia-voted-off-of-imo-council. Retrieved 2024-03-21
9. IMO 2023, Ukraine Shipping. https://www.imo.org/en/MediaCentre/PressBriefings/pages/BlackSeaMaritimeCorridorAgreement.aspx. Retrieved 2023-01-17.
10. IMO 2023 Maritime Security and Safety in the Black Sea and Sea of Azov. https://www.imo.org/en/MediaCentre/HotTopics/Pages/MaritimeSecurityandSafetyintheBlackSeaandSeaofAzov.aspx. Retrieved 2024- 03-21
11. *About ISA*. https://www.isa.org.jm/about-isa. Retrieved 2023-01-16.
12. EEAS 2021, Maritime Security. https://www.eeas.europa.eu/eeas/maritime-security_en. Retrieved 2023-01-18.
13. EUMSS 2018. https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/maritime-security-strategy_en. Retrieved 2023-01-18.
14. EUMSS 2014, https://data.consilium.europa.eu/doc/document/ST 11205 2014 INIT/EN/pdf. Retrieved 2023-01-18. See also https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1483.
15. EEAS 2023, Maritime Security. https://www.eeas.europa.eu/eeas/maritime-security_en. Retrieved 2023-01-18.
16. EUGS 2016. https://www.coe-civ.eu/kh/a-global-strategy-for-the-european-unions-foreign-and-security-policy. Retrieved 2023-01-18.
17. EUGS 2016. https://www.coe-civ.eu/kh/a-global-strategy-for-the-european-unions-foreign-and-security-policy. Retrieved 2023-01-18.
18. EEAS 2023, Maritime Security. https://www.eeas.europa.eu/eeas/maritime-security_en. Retrieved 2023-01-18.
19. EU Council 2021, on maritime security. https://data.consilium.europa.eu/doc/document/ST-9946–2021-INIT/en/pdf. Retrieved 2023-01-19.

20. *What is Hybrid CoE?* https://www.hybridcoe.fi/who-what-and-how/. Retrieved 2023-01-21
21. It should be noted that no such changes was available for examination on January 20, 2023 when the research first was conducted but during the revision of the article it was noted that five new scenarios was included in March 2023 with one case specifically addressing undersea cable cuts.
22. Hybrid CoE 2024. In, on, and under the sea: New maritime hybrid threat scenarios presented in a Hybrid CoE handbook https://www.hybridcoe.fi/news/in-on-and-under-the-sea-new-maritime-hybrid-threat-scenarios-presented-in-a-hybrid-coe-handbook/. Retrieved 2024-03-21
23. European Union 2023, Maritime Security: EU updates Strategy to safeguard maritime domain against new threats https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1483. Retrieved 2024-03-22
24. Hybrid CoE 2018. https://www.hybridcoe.fi/news/network-on-maritime-vulnerabilities-and-resilience-launched/. Retrieved 2023-01-20.
25. NATO 2021. https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html. Retrieved 2023-01-25.
26. NATO 2016, Virtual vulnerabilities. https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html. Retrieved 2023-01-30.
27. NATO 2022, Resilience. https://www.nato.int/cps/en/natohq/topics_132722.htm. Retrieved 2023-01-30.
28. NATO 2016, Civil preparedness. https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html. Retrieved 2023-01-31.
29. NATO 2011, Alliance Maritime Strategy. https://www.nato.int/cps/en/natohq/official_texts_75615.htm. Retrieved 2023-01-31.
30. NATO 2023b, NATO's capabilities, Other initiatives, Maritime security. https://www.nato.int/cps/en/natohq/topics_49137.htm. Retrieved 2023-01-31.
31. NATO 2023b. Retrieved 2023-01-31.
32. NATO 2023c, NATO and European Union launch task force on resilience of critical infrastructure https://www.nato.int/cps/en/natohq/news_212874.htm Retrieved 2024-03-29
33. NATO 2023c, NATO's maritime activities https://www.nato.int/cps/en/natohq/topics_70759.htm#undersea
Retrieved 2024-03-29

Acknowledgments

The author wishes to thank the anonymous reviewers and the responsible editor for insightful comments on the manuscript. I also wish to thank Andrew Blasko for assisting me with proof-reading and language editing.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

No funding or grant has supported this study.

Notes on contributor

Oscar L. Larsson is Associate Professor in Political Science at the Swedish Defence University. His research concerns how war and preparedness shape security politics and practices. Larsson's previous publications have addressed modes of governance in relation to sovereign power/domination in *Critical Policy Studies*, *Regulation & Governance*, and *Policy Sciences*; collaborative crisis management in *Risk, Hazards and Crisis in Public Policy* as well as resilience and difficulties of grey zone preparation in *Security Dialogue*.

ORCID

Oscar Leonard Larsson http://orcid.org/0000-0002-9537-7569

References

Aradau, Claudia, Luis Lobo-Guerrero, and Rens Van Munster. 2008. "Security, Technologies of Risk, and the Political: Guest Editors' Introduction." *Security Dialogue* 39 (2/3): 147. https://doi.org/10.1177/0967010608089159.

Bacchi, Carol, and Susan Goodwin. 2016. *Poststructural Policy Analysis: A Guide to Practice*. New York: Springer.

Björnehed, Emma. 2022. "What Is the Value of Naval Forces? Ideas As a Strategic and Tactical Restriction." *Defence Studies* 22 (1): 1–15. https://doi.org/10.1080/14702436.2021.1931133.

Booth, Ken. 2014. *Navies and Foreign Policies*. Abingdon and New York: Routledge.First published in 1977 by Croom Helm.

Boréus, Kristina, and Göran Bergström. 2017. *Analyzing Text and Discourse: Eight Approaches for the Social Sciences*. London: SAGE.

Børresen, Jacob. 1994. "The Seapower of the Coastal State." *Journal of Strategic Studies* 17 (1): 148–175. https://doi.org/10.1080/01402399408437544.

Bueger, Christian. 2015. "What Is Maritime Security?" *Marine Policy* 53 (C): 159–164. https://doi.org/10.1016/j.marpol.2014.12.005.

Bueger, Christian, and Timothy Edmunds. 2017. "Beyond Seablindness: A New Agenda for Maritime Security Studies." *International Affairs* 93 (6): 1293–1311. https://doi.org/10.1093/ia/iix174.

Bueger, Christian, and Tobias Liebetrau. 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, Christian, and Tobias Liebetrau. 2022. "Nord Stream Sabotage: The Dangers of Ignoring Subsea Politics." https://theloop.ecpr.eu/nord-stream-sabotage-the-dangers-of-ignoring-subsea-politics/. Retrieved 2023-02-15.

Buzan, Barry, Ole Wæver, and Jaap De Wilde. 1998. *Security: A New Framework for Analysis*. Boulder, CO: Lynne Rienner.

Cable, James. 1981. *Gunboat Diplomacy*. London: Palgrave Macmillan.

Cable, James. 1985. *Diplomacy at Sea*. London: Palgrave Macmillan.

Chapsos, Ioannis. 2016. "Is Maritime Security a Traditional Security Challenge?" In *Exploring the Security Landscape: Non-Traditional Security Challenges. Advanced Sciences and Technologies for Security Applications*, edited by Masys, Anthony J., 59–78. Cham: Springer. https://doi.org/10.1007/978-3-319-27914-5_4.

Chapsos, Ioannis, and Elizabeth Ann Norman. 2023. "Is Maritime Security Gender-Blind?" *Marine Policy* 147:105399. https://doi.org/10.1016/j.marpol.2022.105399.

Cherp, Aleh, and Jessica Jewell. 2014. "The Concept of Energy Security: Beyond the Four As." *Energy Policy* 75 (C): 415–421. https://doi.org/10.1016/j.enpol.2014.09.005.

Clark, Bryan. 2016. "Undersea Cables and the Future of Submarine Competition." *Bulletin of the Atomic Scientists* 72 (4): 234–237. https://doi.org/10.1080/00963402.2016.1195636.
Collier, Stephen J., and Andrew Lakoff. 2021. *The Government of Emergency: Vital Systems, Expertise, and the Politics of Security*. Princeton: Princeton University Press.
Corbett, Julian S. 2004. *Some Principles of Maritime Strategy*. Mineola, NY: Dover Publications.
Dunn, William N. 2015. *Public Policy Analysis*. London: Routledge.
EEAS. 2021. "*Maritime Security*." https://www.eeas.europa.eu/eeas/maritime-security_en. Retrieved 2023-01-18.
EUGS. 2016. "*EU Global Maritime Strategy*." https://www-coe-civ.eu/kh/a-global-strategy-for-the-european-unions-foreign-and-security-policy Retreived 2023-01-18.
European Union. 2023. "*Maritime Security, EU Updates Strategy to Safeguard Maritime Domain Against New Threats*." https://ec.europa.eu/comission/presscorner/detail/en/ip_23_1483. Retreived 2024-03-22.
Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington, VA: Potomac Institute for Policy Studies.
Hybrid CoE. 2018. "*Network on Maritime Vulnerabilities and Resilience Launched*" https://www.hybridcoe.fi/news/network-on-maritime-vulnerabilities-and-resilience-launched/. Retrieved 2023-01-20
Hybrid CoE. 2023. https://www.hybridcoe.fi/about-us/. Retrieved 2023-02-14.
IMO. 2022. *Our Work, Maritime Security*. https://www.Imo.org/en/ourwork/security/pages/guidemaritimesecuritydefault.aspx. Retrieved 2022-12-19.
IMO (International Maritime Organization). 2023. *Brief History of IMO*. https://www.imo.org/en/About/HistoryOfIMO/Pages/Default.aspx. Retrieved 2023-02-15.
ISA. 2023. "*About ISA*." https://www.isa.org.jm/about-isa. Retrieved 2023-01-16.
James, Kraska, and Raul A. Pedrozo. 2022. *Disruptive Technology and the Law of Naval Warfare*. Oxford: Oxford University Press.
Larsson, L. Oscar. 2024. "Responses to Grey Zone and Hybrid Threats: How much Resilience is enough." In*ISA 2024 Annual Convention April 3rd-6th. Putting Relationality at the Centre of international Studies*, San Fransisco.
Larsson, Robert L. 2006. *Sweden and the NEGP: A Pilot Study of the North European Gas Pipeline and Sweden's Dependence on Russian Energy. No. FOI-R–1984*. Stockholm: Swedish Defence Research Agency.
Leed, Maren. 2015. "Square Pegs, Round Holes, and Gray Zone Conflicts: Time to Step Back." *Georgetown Journal of International Affairs* 16 (2): 133–143. http://www.jstor.org/stable/43773703.
Lohela, Tiia, and Valentin Schatz. 2019. Handbook on Maritime Hybrid Threats—10 Scenarios and Legal Scans. *Hybrid CoE Working Paper 5*. Helsinki: Hybrid CoE. https://www.hybridcoe.fi/wp-content/uploads/2020/07/NEW_Handbook-on-maritime-threats_RGB.pdf .
Luttwak, Edward. 1987. *Strategy: The Logic of War and Peace*. Cambridge, MA: Harvard University Press.
Mahan, Alfred Thayer. 1890. *The Influence of Sea Power Upon History: 1660–1783*. Boston: Little, Brown.
Mahan, Alfred Thayer. 1892. *The Influence of Sea Power Upon the French Revolution and Empire, 1793–1812*. Boston: Little, Brown.
Mälksoo, Maria. 2018. "Countering Hybrid Warfare As Ontological Security Management: The Emerging Practices of the EU and NATO." *European Security* 27 (3): 374–392. https://doi.org/10.1080/09662839.2018.1497984.
NATO. 2021. "*Enlarging NATOs Toolbox*." https://nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html. Retrieved 2023-01-25.
NATO. 2023a. Accessed February 14, 2023 https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html .
NATO. 2023b. "NATO's Capabilities, Other Initiatives, Maritime Security." https://www.nato.int/cps/en/natohq/topics_49137.htm. Retrieved 2023-01-31.

NATO. 2023c. "*NATO and European Union Launch Task Force on Resilience of Critical Infrastructure*." https://www.nato.int/cps/en/natohq/news_212874.htm. Retrieved 2024-03-29.
O'Keefe, David. 2020. *One Day in August: Ian Fleming, Enigma, and the Deadly Raid on Dieppe*. London: Icon Books.
Oscar, Larsson, and J. J. Widen. 2022. "The European Union As a Maritime Security Provider - the Naval Diplomacy Perspective." *Studies in Conflict & Terrorism* 1–23. https://doi.org/10.1080/1057610X.2022.2058863.
Ozava, Marc. 2021. Report NATO 2030: Adapting NATO to Grey Zone Challenges from Russia
Rowlands, Kevin. 2019. *Naval Diplomacy in the 21st Century: A Model for the Post-Cold War Global Order*. London: Routledge.
Sari, Aurel. 2020. "Legal Resilience in an Era of Grey Zone Conflicts and Hybrid Threats." *Cambridge Review of International Affairs* 33 (6): 846–867. https://doi.org/10.1080/09557571.2020.1752147.
Sartori, Nicolò. 2010. "The Militarization of Energy: A Sustainable Challenge for the EU." In *European Security and Defence Forum Workshop "A New European Security Architecture."*, 1–19.,London: Chatham House.
Singh, Abhijit. 2018. Deciphering Grey-Zone Operations in Maritime-Asia. ORF Special Report # 71, August 2018
Smith, Justin O. 2011. "Maritime Interdiction in Sri Lanka's Counterinsurgency." *Small Wars & Insurgencies* 22 (3): 448–466. https://doi.org/10.1080/09592318.2011.581490.
Speller, Ian. 2019. *Understanding Naval Warfare*. 2nd ed. Abingdon and New York: Routledge.
Subhayn, Chattopadhyay, Ingesson Tony, Rinaldi Alberto, Larsson Oscar, J. J. Widen, Almqvist Jessica, and Gisselsson David. 2024. "Weaponized Genomics: Potential Threats to International and Human Security." *Nature Reviews. Genetics* 25: 1–2. 10.1038/s41576-023-00677-8.
Thornton, Rod. 2015. "The Changing Nature of Modern Warfare." *The RUSI Journal* 160 (4): 40–48. https://doi.org/10.1080/03071847.2015.1079047.
Treverton, Greg. 2018. "The Intelligence Challenges of Hybrid Threats: Focus on Cyber and Virtual Realm." Stockholm: Center for Asymmetric Threat Studies (CATS), working paper.
Wirtz, James J. 2017. "Life in the 'Gray Zone': Observations for Contemporary Strategists." *Defense and Security Analysis* 33 (2): 106–114. https://doi.org/10.1080/14751798.2017.1310702.
Yanow, Dvora. 2000. *Conducting Interpretive Policy Analysis*. Vol. 47. London: Sage.
Yergin, Daniel. 2011. *The Prize: The Epic Quest for Oil, Money and Power*. New York: Simon and Schuster.