UNDERSTANDING THE GRAY ZONE IN THE MARITIME DOMAIN:

A CASE STUDY OF RUSSIA AND NATO IN THE BALTIC SEA

By

By Brandon J. Klewicki

December 2024

Director of Thesis: Dr. Armin Krishnan

Major Department: Department of Political Science

ABSTRACT

This thesis investigates the evolving challenges in the maritime gray zone by conducting a case study on Russia's activities in the Baltic Sea and their impact on NATO and adjacent nations. It argues that Russia has adopted gray zone tactics in the maritime domain against NATO in the Baltic Sea region, and NATO is currently not postured to adequately deter these measures. It analyzes Russia’s clandestine tactics, including the covert transportation of ballistic missiles, deployment of undersea research vessels for malicious purposes, and disruption of maritime traffic using unconventional means in a concerted effort to coerce NATO without breaching the threshold of armed conflict. The study emphasizes the constraints faced by actors in effectively countering these actions, such as legal limitations on maritime operations and barriers to information sharing and cooperation among allied states. The research highlights the pressing need for enhanced coordination, intelligence, surveillance, and reconnaissance strategies to address the escalating gray zone threats in the maritime domain.

Understanding the Gray Zone in the Maritime Domain:

A Case Study of Russia and NATO in the Baltic Sea

A Thesis

Presented to the Faculty of the Department of Political Science

East Carolina University

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Security Studies

By

Brandon J. Klewicki

December 2024

Director of Thesis: Armin Krishnan, Ph. D
Thesis Committee Members:
Hanna Kassab, Ph. D
Austin Matthews, Ph. D
Scott Cuomo, Ph. D

ACKNOWLEDGMENTS

I would first like to thank the Security Studies department at East Carolina University for offering a program with so much flexibility for students like me. To my thesis advisor, Dr. Armin Krishnan, and members of my committee, Dr. Hanna Kassab, Dr. Austin Matthews, and Colonel (USMC) Scott Cuomo, thank you for taking the time from your exceedingly busy schedules to be a part of this endeavor with me. At various stages throughout my time in this program, each challenged my assumptions, forced me to think critically, and most importantly provided honest feedback which was instrumental to my learning. I hope to return this in kind as a valued contributor to the security policy and academic community. To Colonel Cuomo I must also add an additional thank you for the leadership, mentorship, vision, and opportunity he provided during a pivotal stage in my career and personal life. To the countless friends and comrades both at home and abroad who have raised me up, offered a helping hand, or laughed with me during our shared suffering, thank you for being an integral part of who I am. To the Marines and Sailors of Mobile Reconnaissance Company, 2d Light Armored Reconnaissance Battalion, 2d Marine Division, thank you for being with me during what was the greatest privilege of my life.

Lastly, and most importantly, to my wife, Jenna, for enduring and supporting me through many late nights in the office, nights away in the field, deployments overseas, or simply hours at the desk instead of spending time with her and our son, Sam, thank you.

Disclaimer: The following is the work of the author alone, and all analyses, conclusions, and opinions expressed do not reflect any position of the United States Department of Defense nor any branch of the United States government.

TABLE OF CONTENTS

1. INTRODUCTION

In the advent of Russia's invasion of Ukraine in February of 2022, renewed attention was placed on conventional military deterrence. Of course, the invasion of Ukraine actually began in 2014. Russia's annexation of Crimea and the Donbas region, precipitated by the now infamous "little green men" supporting the rebel factions in Ukraine, brought access to the Black Sea via the Sea of Azov and Kerch Strait, as well as their concomitant military and economic advantages (Bush, 2014; CSIS, 2014).[1] The official Kremlin narrative regarding the liberation of native Russians was meant to obscure this geopolitical fact as well as its concern about a growing NATO. The rapidity of the annexation and the resultant campaign of support to the break-away factions offered a politically advantageous method to seize control before the Western world could muster the will and resources to respond.

Russia has adopted gray zone tactics in the maritime domain against NATO in the Baltic Sea region, and NATO is currently not postured to adequately deter these measures. Russia's incrementalistic tactics in eastern Ukraine and the Black Sea in its lead-up to the invasion of Ukraine have ignited fears of similar tactics being employed in the former Soviet satellite region of the Baltic Sea. In the Baltic Sea region, Russia's fears of NATO occupying their borders have been realized. The ascendance of Finland and Sweden to the U.S.-led alliance leaves only Russia's tiny island of Gogland and the culturally significant city of St. Petersburg with access to the Gulf of Finland. Its Kaliningrad enclave, an impressive arsenal notwithstanding, is surrounded by the sea and land by NATO territory. Its Baltic Sea fleet finds itself outmatched by

[1] See, "Crimea's Strategic Value to Russia" by CSIS and "Factbox-Costs and benefits from Russia's annexation of Crimea" by Jason Bush. The Sevastapol Port, previously leased from Ukraine by Russia, offers one of the best harbors from which to project naval power into the Black Sea. Prior to the annexation, this came at a cost around $4 billion dollars per year in lost revenues from gas imports to Ukraine as part of the leasing agreement. Additionally, Russia came into control of an estimated $800 million in energy reserves, Ukrainian state assets, and military equipment. They gained all of this before also embarking on an aggressive effort to commercialize the region.

the NATO alliance. Given these constraints, it is important to understand how else Russia may yet coerce and compete in this region.

Much of the research regarding maritime gray zone activities centers around an increasingly assertive China in the contested South China Sea. While this thesis will reference much of this literature, it will provide crucial context to understanding another critical NATO and U.S. competitor-Russia- and its actions in the Baltic Sea region. These dynamics are important to understand due to the Baltic Sea's economic and strategic importance. To illustrate, in September 2023, 57 percent of Russia's oil exports were shipped from its Baltic Ports (Westgaard, 2023). The Baltic Sea itself accounts for nearly 15 percent of the world's maritime cargo trade (Nordenman, 2018). While there is some peer-reviewed literature which attempts to shed light on the dynamics of gray zone conflict in the maritime domain, this has been largely accomplished by think-tanks and other independent organizations. There is more work to be done in the field of academia.

First, this thesis will begin with the theoretical underpinning of three crucial concepts- maritime security, deterrence theory, and the gray zone. It will then transition to an analysis of the interplay of these concepts, using both theoretical and real-world examples. Next, it will provide an overview of the Baltic Sea region, highlighting its importance to NATO, the states directly surrounding it, and Russia. This will also demonstrate how Russia is engaged in a maritime gray zone campaign by highlighting the asymmetry of interests between Russia and NATO in the region, Russia's disadvantage at greater levels of escalation, ambiguous or non-traditional methods of coercion across multiple domains, and incrementalistic tactics employed by Russia in the region. Lastly, this will conclude with a summary of deterrent measures taken by NATO in the Baltic Sea region and potential methods to enhance gray zone deterrence.

2. LITERATURE REVIEW

The following literature review introduces the concepts of maritime security, deterrence theory, and the gray zone. This includes a discussion regarding the difficulties of achieving deterrence from ambiguous, low-escalatory threshold threats in the maritime domain. Critical to this paper will be an understanding of both the structure of the gray zone and cross-domain deterrence, which will be important for the analysis of the case study.

2.1 MARITIME SECURITY

In military parlance, a domain refers to the space in which operations and effects take place. NATO identifies five domains: maritime, land, air, space, and cyberspace (NATO, 2024). In its 2005 National Strategy for Maritime Security, the U.S. defined the maritime domain as, "all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances" (NMIO, 2005). Effects can originate from one domain for impact in another, and it is important to consider the seams between domains holistically. For example, the airspace above an ocean represents a seam between the air and maritime domains. Likewise, a coast or pier existing at the literal transition point the maritime and land domains, can be exploited via all domains.

Maritime security is a complex and multifaceted concept. The effects of sea, land, air, cyberspace, and space may converge in an ambiguous manner, rendering it difficult to identify the seam where one domain ends and another begins. The securitization of the term itself and lack of international consensus regarding its meaning has given it a "buzzword" quality (Bueger, 2015). However, to be useful in its study and to narrow the focus of this research, it is helpful to think of maritime security as the crossed nexus of human security, national security, economic development, and the marine environment (Bueger, 2015). Maritime security is also primarily

concerned with “illegal and disruptive activities in the maritime domain” (Tallis, 2019). There is also a distinction between naval and maritime strategy in this context. Naval strategy is primarily concerned with the military application of maritime forces to national security objectives. Maritime strategy encompasses a broader range of activities-economic, security-oriented, diplomatic, or otherwise- in furtherance of an actor’s goals (Tallis, 2019). Certainly, naval strategy and the forces involved support and further the maritime strategy, but to focus purely on the military aspect ignores the reality of the range of threats and methods of response in the maritime domain (Tallis, 2019).

Since nearly 90 percent of the global trade may be transported by sea, the importance of maritime security cannot be overemphasized (USAID, 2010). The United States Agency for International Development identifies six functional maritime security areas. These are maritime governance, civil and criminal authority, defense, safety, response and recovery, and economy (USAID, 2010). This broadens the understanding of maritime security to more than naval-military applications. Practices to achieve maritime security include surveillance and information gathering to achieve maritime domain awareness (MDA), defined in the United States “National Maritime Domain Awareness Plan” as “the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States” (Bueger, 2015; NMIO, 2013). It also includes patrols, interdiction, and other law enforcement practices, culminating in prosecution and convictions (Bueger, 2015).

Maritime security issues are often a result of two competing interests- the desire for the actor to control the maritime space nearest to them and the promotion of free maritime shipping (Gheciu & Wohlforth, 2018). Recognized international laws, including the United Nations Convention on the Law of the Sea (UNCLOS), seek to balance these desires. One of the most

important aspects of maritime law is the recognized territorial waters, extending 12 nautical miles from the shoreline, and the exclusive economic zones of coastal nations, extending 200 nautical miles from shore (Kraska & Pedrozo, 2013). Access to resources, fisheries, and power generation in these areas are often the most significant drivers of conflict in the maritime space (Kraska & Pedrozo, 2013). Clear examples of this sort of conflict include the ongoing contestation of the South China Sea by China, Taiwan, Vietnam, Malaysia, and the Philippines (Gheciu & Wohlforth, 2018).

States are also concerned with the protection of critical maritime infrastructure. NATO defines this infrastructure as "ports, navigation, channels, marine terminals, offshore installations, and related communication systems" which play essential roles in global supply chains and trade (Fridbertsson, 2023). In the United States alone, there are more than 1,000 harbors and ports, critical to power projection at sea and abroad (Watts, 2005). This infrastructure services military, economic, diplomatic, and informational roles, and is vulnerable to a wide range of attacks. Offshore wind and energy farms, such as those providing nearly 10 percent of power to Belgium, are projected to increase in use and scope, even while traditional oil rigs and gas lines form the lynchpin of global energy production (Fridbertsson, 2023).

Renewed attention has been paid to the undersea energy and information cables that connect the globe. Attacks on the first data cables began as early as the Spanish-American War (Winkler, 2015).[2] Today, the modernized system of cables is responsible for transporting nearly 95 percent of international digital communications across more than 400 cables (Morcos & Wall, 2021). Since most European data is stored in the United States, the Euro-Atlantic undersea cable

[2] See Reed Winkler's article, "Silencing the Enemy: Cable-Cutting in the Spanish-American War". During the Spanish-American War, a US raiding party utilizing axes, grappling hooks, and wire cutters located and destroyed the cable near the Colorados Point lighthouse in Cienfuegos which connected Cuba to other islands in the West Indies.

route is a critical lynchpin in the global economy. The Mediterranean, Pacific, and Arctic networks intertwine the world information space. These submarine cables are responsible for transferring some $10 trillion daily, not to mention secure diplomatic cables, internet access, and classified military information (Morcos & Wall, 2021).

2.2. DETERRENCE THEORY

At its core, deterrence is "the practice of discouraging or restraining someone…from taking unwanted actions, such as an armed attack" (Mazarr M. , 2018). Two general strategies of deterrence emerge within the field of security studies- deterrence by denial, which seeks to deter malign actions through rendering such actions unfeasible, and deterrence by punishment, which threatens severe penalties in retaliation (Mazarr M. , 2018). Traditionally denial is associated with the balance of military forces between actors, but the model can be expanded to the balance of defenses and threats in other domains (Mazarr M. , 2018). Deterrence measures increase the cost against the threat or reduce the perceived gains (Van der Putten, Meijnders, & Rood, 2015). Models of deterrence were developed over three generational "waves." These, as articulated by Robert Jervis, coincided with significant historical events and contexts. The first wave began following the Second World War, after which the development of the atomic bomb shifted strategic thinking from winning wars to preventing them (Jervis, 1979). In the second wave, the focus turned to game theory and bargaining processes, with the analysis turned toward the interplay of how actors attempted to influence the other's actions through threats or promises (Jervis, 1979; Van der Putten, Meijnders, & Rood, 2015). This second wave persisted during the unstable security situation of the Cold War era. Third wave deterrence theorists sought to use empirical evidence over the largely deductive methods of the previous decades (Jervis, 1979). It also counters the previous assumption of rationality between actors, risk-taking behaviors, and

the effects of rewards (Jervis, 1979). In the fourth wave, the era we conceptually exist today, the focus shifts from the calculus between two states to non-traditional threats, non-state actors, asymmetric attacks, and cross-domain effects (Green, Hicks, Cooper, Schaus, & Douglas, 2017).

Earlier this thesis discussed the concept of a domain as it is typically referenced in military terminology. Important to the emerging wave of deterrence and national security are domains that are less about military maneuver and instead refer to a nation's levers of national power: diplomatic, information, economic, and military, commonly acronymized as DIME (CJCS, 2018). The diplomatic instrument of power refers to how a nation engages with or interacts with state and non-state actors (CJCS, 2018). The information instrument is employed to exploit, create, or disrupt the network of knowledge both within and without one's own base or another actor's (CJCS, 2018). The military instrument is the use, possession, or threat of force relative to another actor's applied toward accomplishing national security objectives, and need not include decisive kinetic actions (CJCS, 2018). Lastly, the economic instrument, often considered the "heart of national power," indicates an actor's financial wealth and general prosperity, and can be employed or leveraged in a variety of methods (CJCS, 2018). These domains can become vectors for coercion and therefore domains to implement deterrence.

Effective deterrence, in its simplistic sense, is binary in its identification- an action is either deterred or it is not. To achieve deterrence, the party to be deterred must feel salience from the deterrent threat, clarity in the consequences, timeliness in its execution, credibility in the possibility of attack, and understand the escalation and counter-escalation threshold (Mallory, 2018). Proportionality and capability are essential, as clearly exaggerated or excessive threats are more likely to reduce deterrence rather than enable it (Mallory, 2018). The attacker's and defender's differing intervention thresholds, or the point at which the conflict escalates to a

newer or more lethal level, may be deliberately shrouded in ambiguity and confusion (Mallory, 2018). Deterrence is enhanced when the defender possesses a legitimate retaliatory strike capability, though this can be dissimilar in form to the first-strike and occur in a different domain (Mallory, 2018).

Cross-domain deterrence can be defined as "the use of threats in one domain, or some combination of different threats, to prevent actions in another domain that would change the status quo" (Lindsay & Gartzke, 2019). While in-domain deterrence induces "in-kind" denial or punishment measures, cross-domain deterrence seeks to deter laterally by delivering effects in other domains (Mallory, 2018). Cross-domain deterrence can encompass more than military or kinetic measures. For example, an actor may impose economic sanctions to certain trade sectors or exploit an information system. Dmitry Adamsky (2015) explores the Russian theory of cross-domain deterrence through nuclear and conventional deterrence as well as informational deterrence. Russia's concept of cross-domain deterrence differs from the U.S.'s in its continuity throughout the whole spectrum of war and peace, not resting in the outbreak of hostilities (Adamsky, 2015). This is important to the forthcoming discussion of the gray zone and is critical to analysis of the dynamics in the maritime domain of the Baltic Sea region.

Deterring across domains is challenging for several reasons. First, the signals of escalation are incongruous and have different characteristics (Sweigs & Zilinick, 2019). The costs imposed for conducting an action in one domain, such as through military action, are not necessarily relevant for actions across the economic, information, or diplomatic domains (Green, Hicks, Cooper, Schaus, & Douglas, 2017). Second, the proportionality and credibility of both the threat imposed and the countermeasure may not be synchronous within different domains (Sweigs & Zilinick, 2019). As mentioned, deterrent measures have to come from a place of

credibility without hyperbole and exaggeration, but when employing other instruments of power toward security objectives many traditional deterrent measures can be ineffective (Green, Hicks, Cooper, Schaus, & Douglas, 2017). Lastly, escalation management, though not impossible, requires a shared understanding among belligerents of the "significance of actions across different domains" (Sweigs & Zilinick, 2019). There is an assumption of a shared space of understanding between competitors, a space that is fraught with ambiguity. This ambiguous area will be further discussed in the remainder of the paper.

2.3. THE GRAY ZONE

The US National Defense Strategy defines the gray zone actions as "coercive approaches that may fall below the perceived thresholds for US military action and across areas of responsibility of different parts of the US government" (U.S. Department of Defense, 2022). Government agencies, academic institutions, and journalists have increasingly highlighted the spectrum of conflict that exists between war and peace. It involves state and non-state actors using coercive tools that avoid open warfare, while simultaneously "undermining the security of the target entity" (Atlantic Council's Gray Zone Task Force, 2022; Mazarr, 2015).

This concept has been extensively explored in literature, particularly in Michael Mazarr's seminal work on the topic "Mastering the Gray Zone: Understanding a Changing Era of Conflict" (2015). Mazarr introduces a useful framework for understanding how a gray zone conflict is defined. First, a revisionist actor seeks to change some aspect of the international status quo relating to the distribution of power (Mazarr, 2015). This revisionist actor may be described as a "dissatisfied challenger", and seek to redistribute the balance of prestige and benefit (Brands, 2016; Green, Hicks, Cooper, Schaus, & Douglas, 2017). Second, they engage in patient, gradualist, or incrementalistic campaigns designed to achieve strategic objectives over a

long period of time (Mazarr, 2015). Third, they employ unconventional, ambiguous tools of statecraft which fall short of armed conflict (Mazarr, 2015). Lastly, the revisionist actor perceives relative weakness at higher levels of escalation and, therefore, seeks to complicate the defender's decision-making through actions that, when taken in isolation, may be seen as trivial (Mazarr, 2015). These factors offer a useful starting point for the forthcoming discussion regarding the gray zone.

Hal Brands takes a critical view of the concept of the gray zone in his essay, "Paradoxes of the Gray Zone." Brands highlights the broadening of the concept to such point as to be meaningless, though offers that Mazarr's work is beneficial in providing scope to the idea (Brands, 2016). As Brands states, "'Gray zone' cannot mean everything if it is to mean anything" (Brands, 2016). To understand the debate surrounding the gray zone, it is helpful to introduce terms that are often associated with this space: hybrid warfare and competition. Together with the gray zone, these terms are often conflated or intermingled as different iterations of the same thing. To be helpful for this research, it is important to understand nuances between each. Hybrid warfare may be defined as a military strategy entailing, "an interplay or fusion of conventional as well as unconventional instruments of power and tools of subversion" (Bilal, 2021). Hybrid warfare entails a blend of levers of national power across the DIME spectrum in the pursuit of national security objectives between actors in conflict (Atlantic Council's Gray Zone Task Force, 2022). Competition, meanwhile, "is a fundamental aspect of international relations" wherein actors "protect and advance their own interests" (HQ US Marine Corps, 2020). It is often described as the spectrum of interactions among state and non-state actors from cooperation and collaboration through conflict and armed warfare (Lynch, 2020). Within this hypothetical spectrum, there exists a space which cannot quite be described as peace or cooperation, nor

conflict or war, which is referred to as the gray zone.

Though there may be debate regarding the significance of the differences between hybrid warfare, the gray zone, or competition, the concept of the gray zone is still useful for understanding the sort of low-level conflict to be examined later in this paper. Complementary to Mazarr's work, as defined by Javier Jordan (2020) the gray zone is:

> "[a]n intermediary space separating competition waged in accordance with conventional guidelines governing interstate politics from direct and continued armed confrontation. Gray zone conflict revolves around an incompatibility perceived as relevant at least in the eyes of the aggressor. The strategies are multidimensional and synchronized (hybrid), and implementation is gradual, usually in pursuit of long-term goals."

With this definition, Jordan identifies four critical characteristics for gray zone conflict. The first is ambiguity. This ambiguity can come in the form of the threat or the actual objective (Green, Hicks, Cooper, Schaus, & Douglas, 2017). It also blurs or ignores laws, norms, and established precedents in ways that are difficult to codify, deliberately undercutting confidence in the appropriate response due to the ambiguous legal clarity such an action invokes (Letts, 2024; Green, Hicks, Cooper, Schaus, & Douglas, 2017).

Second, there exists an asymmetry of interests between the two actors, in addition to a power disparity (Mazarr, 2015; Green, Hicks, Cooper, Schaus, & Douglas, 2017; Jordan, 2020). The weaker actor is often able to achieve its objective since the stronger actor may not be willing to take the same risks in securing them (Jordan, 2020). This is also applicable in the context of extended deterrence, wherein one actor's deterrent measures extend to another actor, often an allied nation (Jervis, 1979). Among allies, the interests may not be shared equally nor the

perception of threat and responsibility to support the other (Mazarr, 2015; Green, Hicks, Cooper, Schaus, & Douglas, 2017). For example, in 2020 the U.S. imposed sanctions on the Russian TurkStream and Nordstream pipeline projects. While NATO countries like Turkey, Germany, and France publicly decried the land-grab by Russia, they had significant economic interests with the gas pipeline projects (Belo & Carment, 2020). The deterrent effect of these sanctions was thus reduced when the U.S.'s allies expressed outrage at the unilateral decision by the U.S. government to move forward with the sanctions.

The third characteristic of gray zone conflict is gradualism (Green, Hicks, Cooper, Schaus, & Douglas, 2017; Jordan, 2020; Mazarr, 2015;). Most discussions of the gray zone employ the analogy of "salami slicing" to describe such tactics. A challenger gradually pushes back the boundaries of a deterring actor's red-lines, which is in effect a failure of deterrence (Takahashi, 2018). The aggressor seeks to manipulate the defender's response threshold, thereby minimizing the chance for any serious or comprehensive countermeasure (Jordan, 2020).

Fourth, the actors employ multidimensional or hybrid strategies, which are generally non-military in nature, and are instead economic, informational, or political (Jordan, 2020; Mazarr, 2015). Some refer to this as political warfare, or the wielding of these instruments in such a way to achieve strategic effects without the use of force, while protecting the true purpose of the activity (Letts, 2024; Mazarr, 2015). The critical feature of these strategies is the intent to coerce the opponent or alter the existing dynamic (Jordan, 2020). However, though these levers are often non-kinetic, that does not preclude the use of force if such an action is not perceived to trigger an in-kind or military response (Takahashi, 2018). A challenger employing gray zone strategies will combine political, military, economic, social, and informational tools in unconventional methods to achieve their objectives (Jordan, 2020).

2.4 DETERRENCE IN THE MARITIME GRAY ZONE

In traditional deterrence study, the baseline for understanding deterrence in the maritime domain would involve the balance of two actors' naval forces. If one possesses a larger, more capable navy, the other would be less inclined to aggression. This could also lead to the classic security dilemma and an arms race dynamic in which the less capable navy is grown to counter or overpower the other nation's navy. This endless feedback loop can result in the paradoxical result of making conflict more likely. The modern environment is characterized by deniability and ambiguity, making it difficult for states to respond in a proportional and effective manner. The opacity of these threats leads to increased suspicion and can trigger defensive measures that might be perceived as aggressive by the states involved, thereby escalating tensions (Tang, 2009). However, since escalation does not always result in open conflict, it is worth examining other methods by which states compete in the maritime domain.

Lukas Milveski (2024) offers a concept for understanding the difficulties of deterrence in the gray zone. To start, he posits that the west assumes the gray zone is a shared space, bounded by the same shared set of rules by all actors operating within its conceptual guidelines (Milveski, 2024). However, this assumption is faulty, as not all actors may recognize the concept itself nor the boundaries (Milveski, 2024). Though competing in the gray zone offers opportunities to compete and subvert below the threshold of armed conflict, there are limits to its application. For any concept of strategy to be useful, it should lead to a method or definition of victory (Milveski, 2024). The best strategy also generates competitive options or redefines the parameters of the competition itself (Milveski, 2024). Actors are therefore incentivized to be the ones defining these parameters, especially when competing against a more powerful rival.

China for example, has sought to redefine the status quo in the South China Sea and broader Pacific. Its maritime militia and distant water fishing fleets secure forward access and extend its global economic reach (Luo & Panter, 2021). Gradually deploying more and more of these assets into disputed regions and increasingly stressed fishing zones, these maritime militia forces act as "frontline responses to maritime disputes and contingencies" and erode U.S. relationships with allies (Luo & Panter, 2021). "Little blue men," or non-uniformed special operations forces and intelligence agents aboard these craft, conduct a blend of reconnaissance and wartime support operations from these vessels (Larsson, 2024). Struggling to justify the employment of an already stretched-thin U.S. Navy against these fleets of small merchant and fishing vessels, it may appear this strategy is working in China's favor. This strategy, however, is undergirded by the idea that in the event of war with the U.S., these militias could be relied upon in combat. In fact, a survey of the captains and sailors of these ships shows a very low likelihood or inclination to support wartime operations, when the meager pay from the Chinese Communist Party can do little to justify the high risk undertaken by these poorly trained militias (Luo & Panter, 2021). Additionally, they are hamstrung by ambiguous command relationships and internal service disputes regarding their use (Luo & Panter, 2021). Still, whether this fleet is critical in supporting a hypothetical invasion of Taiwan remains to be seen, but what is clear is the prominence placed by Chinese political and military leadership on overall strategy (Luo & Panter, 2021).

As Bueger (2024) asserts, the role that military forces can in turn play in countering these actions is limited. Often, the control and safety of maritime infrastructure within a territory and exclusive economic zones is under civil authorities (Bueger, 2024). For China, maritime law enforcement vessels not only execute these tasks, but they also fill roles in intelligence and

coercion. Increasingly, commercial fishing vessels are playing a larger role intimidating other nations in disputed waters (Erickson, Hickey, & Holst, 2019). The use of these assets allows the Chinese Communist Party to exert influence without the escalation inherent with the passage of warships. Alongside these law enforcement vessels is China's "second navy," the Chinese Coast Guard (CCG). Featuring the largest coast guard fleet in the world, its vessels are outfitted with high-pressure water cannons, interceptor boat launch and recovery apparatuses, and helicopter landing pads to not only conduct traditional activities of coastal water patrol and navigation but also exert influence at increasingly extended ranges from China's territorial and exclusive economic zones (Erickson, Hickey, & Holst, 2019). Since the world's coast guards are generally regarded internationally as protective and rescue forces, bound by both laws and internalized codes of conduct to help all those at sea regardless of flag or affiliation, the CCG maintains "cover" for espionage and coercion (Erickson, Hickey, & Holst, 2019). By employing the CCG for limited power projection, China can preserve its equally formidable Navy for major combat operations and wartime activities, avoiding the climb up the escalation ladder (Erickson, Hickey, & Holst, 2019).

That there are limits to the employment of military force to deter gray zone threats in the maritime domain does not mean that the possession of a strong military posture is unimportant. Rather, it is the key reason an actor would seek to employ such measures in the first place. A cornerstone of gray zone deterrence should be the risk for decisive escalation, and if this is taken away there is no longer a need for gray zone tactics (Takahashi, 2018). In a sense, the existence of a gray zone implies that "hostilities" have already begun, even if hostilities in this sense does not include armed conflict (Larsson, 2024). Clearly, China has deliberately chosen low-escalation threshold tactics to avoid direct confrontation with the U.S., just as the U.S. and its

allies have opted not to respond with the use of lethal force owing to the highly capable Chinese Navy (Hicks, et al., 2019).

One of the most prominent theoreticians of naval strategy, Alfred Thayer Mahan, offers a conception for understanding great power competition in the maritime domain, but he falls short of offering a sound understanding for a country's navy in countering gray zone threats (Landreth, 2020). States may employ deniable measures or non-state actors, as illustrated through Iran's supply of autonomous surface vessels to the Houthis in 2017 to attack a Saudi frigate (Landreth, 2020). Or they may utilize transnational criminal organizations to manufacture and deliver drugs into competitor nations. China, for instance, has been implicated in the funding and manufacture of opiates and heroin for distribution into the U.S. supply chain, resulting in more deaths per year than the September 11, 2001 terror attacks in New York (Landreth, 2020).

As previously discussed, military navies struggle to deal with these types of threats. This is often related to a lack of legal authorities, technical capabilities, and training compared to maritime police forces and coast guards (Landreth, 2020). Even if navies were more empowered to act in countering these types of threats, the cost balance associated with the deployment of military assets against these relatively low-end and cheap threats is prohibitive. As the U.S. discovered in Afghanistan, an F-22 is more than capable of destroying a heroin processing facility, but the cost of a precision air-to-ground missile, flight hours, and targeting assets to achieve this effect generally offsets whatever wartime benefit the destruction aimed to achieve (Landreth, 2020). Now include the potential for misestimation, misidentification, and misinterpretation of adversary intentions, the cost-benefit analysis changes from an economic matter to an evaluation of the risks of escalation versus acquiescence.

The challenges in countering and understanding gray zone operations in the maritime domain relates to the increased layer of ambiguity as it relates to enforcement of the law in the world's oceans. As Larsson (2024) states, "the sea constitutes a domain over which there is little political control." The 1982 United Nations Convention on the Law of the Sea (UNCLOS) provides a basic legal framework for global governance and policy regarding maritime safety and navigation. However, for this charter to be effective it must be recognized and enforced by the parties of which it is comprised. Even other governing bodies, such as the International Maritime Organization (IMO), struggle to appropriately handle gray zone threats due to the political sensitivities of ascribing blame to specific nations for coercive actions in the maritime domain (Larsson, 2024).

In the maritime gray zone, deciding on a strategy of deterrence of denial or punishment can be challenging. Signaling to the actor to be deterred what exactly would compel punishment on the part of the defender is a gambit of cost-benefit analysis between both parties- who is willing to sacrifice what, and for what end (Green, Hicks, Cooper, Schaus, & Douglas, 2017). Gray zone strategies specifically blur these lines. Punishment in conventional deterrence typically involves the threat of massive military retaliation in the event of attack, but in the gray zone it could also involve loss of reputation or prestige. However, the dilemma for the defender is the opposite effect, wherein a military response to a limited, non-military threat reduces its own influence and credibility (Green, Hicks, Cooper, Schaus, & Douglas, 2017). Denial strategies seek to prevent the adversary from ever achieving its objectives since the cost to do so would be more than it could bear (Green, Hicks, Cooper, Schaus, & Douglas, 2017). At issue here is the tactic of salami-slicing, and the incongruent interest in achieving the objective on the part of the attacker and denying it on the part of the defender (Jordan, 2020; Green, Hicks,

Cooper, Schaus, & Douglas, 2017; Mazarr,2015). As demonstrated by China, it is hard to deny the harassment of every Philippine vessel through armed escort of each ship or defense of each contested fishery.

3. THE CASE STUDY

Sea blindness, in research, political, and theoretical measures, can be understood as, "the inability to understand the sea or to recognize its importance to national and international well-being" (Larsson, 2024). State actors may combine effects across all domains, but adverse actions in the maritime domain can wreak havoc due to the sheer volume of economic output affected. There is much literature discussing the Russian gray zone conflict in Ukraine. Additionally, much of Russia's geopolitical and national security strategy has pivoted toward the Arctic, and within the maritime domain toward its Northern sea route.[3] This in turn has pivoted much of the foregoing discussion of subsurface reconnaissance and para-militarization of Russia's maritime ambitions toward this region. However, it still possesses a national security interest in the Baltic Sea, which will be further analyzed.

This section will first explain why Russia would adopt a gray zone strategy to compete with NATO in the maritime domain by demonstrating that Russia is a dissatisfied challenger, faces a disadvantage at increased levels of escalation, and perceives an asymmetry of interests between its ambitions in the region and NATO's (Mazarr M. J., 2015) (Green, Hicks, Cooper, Schaus, & Douglas, 2017) (Jordan, 2020). It will also explore the different tactics used by Russia which coincide with previously identified tenets of the gray zone: ambiguity, multidimensional tactics, and gradualism (Jordan, 2020) (Mazarr M. J., 2015). Lastly, this thesis will discuss both the deterrence challenges and measures of NATO in the region to provide recommendations for the implementation of maritime gray zone deterrence. In the gray zone between Russia and NATO in the Baltic Sea region, the critical questions are regarding the commitment of NATO to the area's defense, Russia's desire for the restoration of its historical holdings, and its desire to

[3] See "Maritime Doctrine of the Russian Federation" translated by Davis and Vest. Russia has placed significant focus on the maritime routes in the Arctic Sea, and has made significant territorial and access claims contested by many Western nations.

probe NATO's weaknesses (Murphy & Schaub, 2017). This section will explore the second and third questions to begin, and end with an examination of NATO's defenses in this arena.

3.1. RUSSIA'S DISSATISFACTION WITH THE STATUS QUO AND ASYMMETRY OF INTERESTS IN THE BALTIC SEA REGION

To understand why Russia would be motivated to employ gray zone tactics in the Baltic Sea region, it is important to consider both the theoretical and the tangible. This section will first demonstrate two conditions Russia meets which encourages it to employ a gray zone strategy. First, it intends to alter the status quo, and second, it perceives a comparative disadvantage at greater levels of escalation (Jordan, 2020; Malyarenko & Kormych, 2023; Mazarr, 2015). It will conclude by showing that Russia may be capitalizing on the belief that its interests for subversion and influence in the region are greater than NATO's interests in defending against it.

Russia can be classified as a dissatisfied challenger. President Putin famously proclaimed in his 2005 address to the nation that the dissolution of the Soviet Union was the, "greatest geopolitical catastrophe of the century."[4] During the downfall of the Soviet Union in the late eighties and early nineties, Russia would lose five of its satellite states in the Baltic Sea region: East Germany, Poland, Lithuania, Latvia, and Estonia (Savitz & Winston, 2024). Current strategic documents reflect a desire to renew Russia's power in the world. Russia's 2023 *Foreign Policy Concept* offers a framework to understand how and why the Kremlin would seek to engage in a gray zone strategy. The document alludes to the "special responsibility" Russia feels it has to create a multi-polar world (Buchanan, 2023). They view European states' "aggressive policy toward Russia" as an extension of U.S. hegemony (Ministry of Foreign Affairs of the

[4] See, "Annual Address to the Federal Assembly of the Russian Federation". He goes on to say, "for the Russian people, it became a genuine tragedy. Tens of millions of our fellow citizens and countrymen found themselves beyond the fringes of Russian territory."

Russian Federation, 2023). In their view, it is the "US policy of power-domination," which threatens global stability and equitable distribution of power (Ministry of Foreign Affairs of the Russian Federation, 2023).

Russia is often described as a revisionist power (Murphy & Schaub, 2017), seeking to alter the balance of power in the world from the unipolarity of the United States to one of bipolarity or multipolarity, with themselves exerting influence, prestige, and power on par with the U.S. (Green, Hicks, Cooper, Schaus, & Douglas, 2017). Aggrieved by continued NATO expansion, U.S.-led sanction regimes, and a perceived strategy of continued Russian containment, Russia's dissatisfaction encourages it to alter the status quo in its favor (Green, Hicks, Cooper, Schaus, & Douglas, 2017; Ministry of Foreign Affairs of the Russian Federation, 2023). It sees the Western world in decline and an opportunity to establish itself as a regional and world power (Ministry of Foreign Affairs of the Russian Federation, 2023).

In July of 2022, one year prior to the Concept for Foreign Policy, Russian President Vladimir Putin approved the 2022 Maritime Doctrine of the Russian Federation. It was the first update of this form since 2015. It's important to understand this document to gain insight into Russia's priorities regarding maritime space. Within the maritime space, they identify the US dominated world order and control of the seas as the greatest threat to their prosperity and wellbeing (Davis & Vest, 2022). This document highlights the strategic importance that Russia places on its conceptual "World Ocean," emphasizing among other things the development of the Russia's maritime potential, ensuring sovereignty, access to global lines of communications, environmental protection, and the preservation of human life at sea (Davis & Vest, 2022). This serves as the foundation for the World Ocean reference again in its Foreign Policy Concept, calling for the need to protect its "sovereign rights on the continental shelf" (Ministry of Foreign

Affairs of the Russian Federation, 2023). It also delineates between "vital, important, and others" regarding which specific maritime zones in the world it considers in order of priority, conferring the Baltic Sea important status (Davis & Vest, 2022). The Maritime Doctrine also highlights the U.S.'s "strategic course" and "global influence" over the world's oceans as its main challenge to national security and development in this domain (Davis & Vest, 2022). It further explains the U.S.'s and NATO's expanded military infrastructure and network, emphasizing the pivotal role force continues to play in international relations (Davis & Vest, 2022). Another threat is described by the document as "attempts by a number of states to change existing legal regulations" regarding the legal use of maritime spaces (Davis & Vest, 2022).

The document also explains other risks to Russia's maritime dominance relating to ship numbers, access, and composition of the naval and merchant fleets. It admits to insufficient numbers of commercial ships bearing the Russian flag, dependence on foreign trade to maritime means, and sanctions limiting investment in maritime technologies and shipbuilding (Davis & Vest, 2022). Unlike the U.S., with its large network of overseas bases and ports, Russia lacks a significant number of "friendly" installations to make harbor (Davis & Vest, 2022). The doctrine makes specific reference to procedures and laws governing the employment or conscription of civilian maritime vessels for wartime purposes. However, it explicitly calls for the improvement of "the procedure for the conscription and use of transport, fishing, and specialized vessels of all forms" for the military forces conducting special operations outside of war (Davis & Vest, 2022). This in effect gives legal authority and precedent for the Russian intelligence and military forces to employ civilian vessels for gray zone operations, part of a series of tactics employed by Russia which will be discussed in a forthcoming section.

If Russia were to deploy military force in pursuit of its objectives, it perceives itself to be at a relative disadvantage to NATO. With the recent addition of Finland and Sweden to NATO, Russia is geographically flanked to the west by NATO countries and territory. The entirety of the Baltic Sea is just slightly larger than the state of California (Savitz & Winston, 2024), encompassing the Gulf of Bothnia between Finland and Sweden, the Gulf of Finland between Finland and Estonia, and the entrance to the sea via the Straits of Denmark. The Swedish island territory of Gotland lies just west of the center of the Baltic. Together with the Danish island of Bornholm and Finnish island of Aland, these three terrain features are considered key terrain for any conventional military conflict in the region owing to their forward position within the sea (Murphy & Schaub, 2017). Dotting the waters is the Swedish and Finnish Archipelagoes, through which transit can be treacherous for larger vessels (Savitz & Winston, 2024). The average depth is only 200 feet, and very few ports to accommodate ships with drafts greater than 13 meters (Savitz & Winston, 2024). Complicating the UNCLOS, the entirety of the sea is comprised of the adjoining states' territorial waters and exclusive economic zones, allowing only for the innocent passage of foreign vessels (Pawlak, 2024). Further constricting traffic is the presence of ice for extended periods of the year (Savitz & Winston, 2024).

With the ascendance of Finland and Sweden to the alliance the Baltic Sea has been commonly called "the NATO Lake" (Messmer, 2024). However, Russia still maintains significant interests and defense capabilities in the region. Of particular concern to NATO is the robust anti-access and area denial "bubbles" originating in its Kaliningrad enclave and western military region (Pawlak, 2022). This refers to its large stores of precision missiles, rocket and conventional artillery, and other military assets in the region which can range the entirety of the Baltic Sea and beyond (Savitz & Winston, 2024). Russian Federation Navy's (RFN) Baltic Sea

fleet also possesses more naval surface combatants than the rest of the NATO Baltic Sea states combined (Savitz & Winston, 2024), and has demonstrated a willingness to use force as evidenced by its invasion of Ukraine and other expeditions abroad (van Tol, Bassler, Kjellstrom Elgin, & Hacker, 2022).

Russia's capable military in the region aside, from a military perspective altering the status quo in the Baltic Sea region would be incredibly challenging. The status quo in this instance is that in the event of an attack on one of the NATO countries, this would invoke Article 5 of the NATO charter for collective defense (NATO, 2023). To allay Baltic state fears of a *fait accompli* as seen in Crimea or instead a rapid and overwhelming invasion by Russia, 12 NATO nations have contributed elements deployed to the Enhanced Forward Presence battle groups of roughly battalion to brigade size forces to each of the countries on its eastern flank (Winnerstig, 2017). These ground forces, even bolstered by the host nation's military, are more reflective of the "trip wire" strategy, trading space for time in the event of an invasion to muster the full military capacity of the NATO alliance (Winnerstig, 2017). The navies comprising the Baltic Sea states, meanwhile, are predominantly patrol and coastal defense ships, and possess extensive mining capabilities (Savitz & Winston, 2024). Sweden and Finland also feature sleek, fast amphibious assault craft, in addition to the former's advanced submarines which are highly capable of maneuvering in the shallow confines of the Baltic (Savitz & Winston, 2024). Robust air and land-based platforms also contribute to NATO's maritime defense in the region (Savitz & Winston, 2024).

This paper previously discussed the collapse of the Soviet Union and Russia's historic holdings in the Baltic Sea region. Despite the Baltic States NATO membership status, Russia still may believe it has a greater interest in regaining or influencing these regions than NATO has in

defending them. Take for example the demographic make-up of the Baltic States. Estonia's and Latvia's population is comprised of 25 percent and 27 percent, respectively, ethnic Russian-identifying people (Brauss & Racz, 2021). These people are often vectors utilized by Russia to sow disinformation and doubt in the governments of their former client states, though surveys have shown that among this minority population they still hold stronger allegiance to their current states (Brauss & Racz, 2021). Narratives regarding the protection of the Russian people are commonplace, and were used in the build-ups to Russia's military invasions of Georgia and Ukraine (Brauss & Racz, 2021). Even under the blanket of NATO's collective defense structure, Russia exploits doubts regarding Article 5 commitments to the region. Murauskaite et al. (2019) provides insights into the extended deterrence dilemmas faced by Baltic states in countering Russian gray zone influence. Through surveys and simulations, the authors found that in a hypothetical gray zone crisis in the Baltic States, the U.S. and its allies may still be reluctant to respond through conventional military means (Murauskaite, et al., 2019) This is not in itself a shocking revelation, as the employment of these tactics are meant to remain below the threshold for collective defense. However, the erosion of the red-lines separating acceptability and counter-action over an extended period of time is the concerning factor, and will be discussed further in the next sections.

3.2. RUSSIA'S GRAY TACTICS

The following section will examine the ambiguous, deniable, cross-domain tactics employed by the Russian Federation in the Baltic Sea region. This includes an overview of militarized civilian vessels and the erosion or outright violation of international laws and norms in the maritime domain. Following this, this paper will show how Russia may be "salami-slicing" the boundaries of the Baltic Sea while gradually testing or pushing-back previously

established “red-lines.” Lastly, this thesis will analyze the strategies employed by the NATO states surrounding the Baltic Sea to counter these threats.

3.2.1. MULTI-PURPOSE SHIPS AND AMBIGUITY

Merchant vessels operating for military purposes are not necessarily an indicator of gray zone activity. Many nations, Russia and the US included, have provisions allowing for the incorporation of civilian fleets for military purposes in times of war. What is reflective of gray zone spectrum actions is the dual, ambiguous purposes a vessel may serve under the circumstances, exploiting seams between international laws. Take for example the use of the *Sparta IV* cargo vessel used to transport arms between Russia and Syria. Russia has levied accusations against Ukraine of unjustifiably targeting *Sparta IV*, resulting in the unsuccessful attack by an unmanned surface vessel against its military escort ships (Palmer, Duff, Jun, & Bermudez, 2023). There is strong evidence linking the *Sparta IV* to weapons deliveries to the Assad regime, as well as resupply of Russian forces in the Black Sea (Palmer, Duff, Jun, & Bermudez, 2023).

This ship, to be classified as a military target, must meet one of three criteria. It must make a direct contribution to military action, be under the control of the state for government service, or traveling in a convoy with military vessels (Palmer, Duff, Jun, & Bermudez, 2023). The movement of the *Sparta IV*, while under western sanctions, does not meet thresholds for armed response by the sanctioning countries. The tactics that vessels like the *Sparta IV* employ to avoid detection, such as switching its on-board automatic identification system (AIS) or spoofing its location, have become common practice for Russian-affiliated vessels (Palmer, Duff, Jun, & Bermudez, 2023). These actions in times of war would constitute a basic force protection measure. What’s highlighted here is the deliberate exploitation of a seam between laws of armed

conflict and international maritime law. The IMO dictates the use of AIS on most cargo and shipping vessels, though allows for deviations where its employment may compromise the safety of the ship (International Maritime Organization, 2015).[5] However, the employment of these tactics is increasingly commonplace by Russian research vessels and cargo ships. This allows deniability in attribution for coercive or malign actions.

If the breach international norms or established bounds of competition are commonplace in the gray zone, then perhaps there is no asset more capable of this than Russia's class of containerized munitions. Revealed in 2010, the Club-K missile system disguises multiple variants of Russia's formidable missile arsenal as little more than a commercial shipping container. These systems are configurable to a variety of platforms both on land and sea, and come with incorporated command and control systems, targeting suites, and other support apparatuses designed for concealment with the lethal payloads (IISS, 2020). The concept of containerized munitions is not necessarily new, and several countries have similar designs to enable modularity and flexibility for future warships.[6] Russia has revealed several conceptual renderings of Club-K containers being placed aboard future naval vessels (Vavasseur, 2020). These designs include payloads not limited to missiles, such as helicopter loading bays, medical centers, and ancillary power systems (IISS, 2020).

That Russia has designed a weapon meant to evade detection is not the central issue. What is notable is that Russia has designed a weapon that can very easily be outfitted to civilian transport vessels. It would not be difficult to surmise that the system was designed to

[5] See https://www.imo.org/en/OurWork/safety/navigation/ais.aspx. Interestingly, the IMO published a statement regarding the detrimental effect on navigation safety and security by publishing AIS data on the Internet, going so far as to say these platforms undermine its purpose.

[6] See "China's Container Missile Deployments Could Violate the Law of Naval Warfare" by Raul Pedrozo and "US Navy Tests Sea-Based Containerized Missile Launcher" by Inder Bisht. The outward purpose of these containerized missiles is to enable modularity aboard military ships. However, the proliferation of these systems may be more indicative of a new type of arms race, a discussion beyond the scope of this paper.

intentionally conceal itself among civilian traffic. The developer of the Club-K demonstrated this very thing in a promotional video introducing the system in 2010, displaying a graphical rendering of the launch of these missiles from trains, trucks, and cargo ships (Stott, 2010). These tactics, wherein the actor deliberately "induces trust on the part of an adversary in order to injure, kill, or capture them" (Clarke, 2011), may constitute perfidy and is banned under international humanitarian law. It is important to distinguish between military deception, which is completely lawful and normal in times of war, and the intent such a weapon system may have to exploit the protected status conferred upon it by potential adversaries should it be transported aboard commercial vessels (Clarke, 2011).

In the tight confines of the Baltic Sea, flagged Russian Federation vessels are relatively easy to track and naturally garner most of the surveillance assets available to NATO forces in the region. The "gray fleet," however, describes those ships with business structures obscuring their national origins and ownership, allowing them to skirt sanctions through bearing "flags of convenience" (Braw, 2024).[7] Windward AI produced a comprehensive report on the activities of the Russian gray fleet, explicitly analyzing the ships suspected of transporting sanctioned Russian crude oil products through a convoluted series of port transfers under ostensibly legal circumstances (Windward, 2024). Many of the ships transporting Russian crude oil products originate in the Baltic Sea, making the long trek down the Baltic and up the North Sea to Russia's arctic ports (Braw, 2024). They manipulate the GPS location on the automated identification system aboard the ship (Windward, 2024), and are often the subject of maritime safety and navigation violations (Braw, 2024).

[7] See, "Worse than Pirates: Russian Shadow Fleet Brings Disaster" by Elisabeth Braw. Flag of convenience refers to the practice of registering the ships in countries with lower standards for insurance and policy compliance, if any exist. Braw specifically references countries like Swaziland and Gabon with low expertise in maritime affairs.

Russian vessels conducting paramilitary gray zone actions in the Baltic Sea is not an unknown phenomenon. The *Sibirjakov* hydrographic survey vessel conducts subsurface exploratory activities, equipped with a host of sensors to provide detailed analysis of the submarine layer (US Army, 2024). While operating under ostensibly civilian research purposes, an ongoing investigative journalism report has revealed evidence via collected transmissions, open-source satellite imagery, and AIS history-or its lack thereof- to place the *Sibirjakov* and several other Russian ships at the epicenter of a massive intelligence collection operation (Pointer, 2024). This ship, and vessels like the *Admiral Vladimirsky*, were noted to be loitering over the Balticconector cable in the months preceding the 2023 sabotage attack (Pihl, 2024). On 10 October 2023, Finland reported an apparent sabotage on its Balticconnector undersea gas line and high-speed undersea data cables running beneath the Gulf of Finland to Estonia (Armstrong & Sri-Pathma, 2023). On 17 October 2023, Sweden discovered that one of their undersea gas lines was likely attacked (Associated Press, 2023). Russia vehemently denied all accusations of its involvement, and it was revealed that one of their data cables was damaged (Trevelyn, 2023). On 26 October 2023, Finland reportedly recovered an anchor near the damaged site allegedly belonging to the *NewNew Polar Bear*, a Chinese-owned container ship. Speculation has turned to a plausible accusation that this ship's anchor was dragging on the bottom of the seabed (Baker & Spohr, 2023). Additional investigation is ongoing to determine intentionality, but the confluence of NATO's two greatest geopolitical rivals in the region is cause for suspicion, as are indications of Russian complicity and cooperation in this incident (Baker & Spohr, 2023).

Though attribution for this incident is still unclear, what is known is that Russia's Main Directorate for Deep Sea Research (GUGI) manages vessels to conduct deep-sea research, oceanographic surveys, and intelligence gathering functions. Ships like the *Yantar* and *Admiral*

Vladimirisky have well-documented histories scouting NATO critical maritime infrastructure and are equipped with a host of sensors and surveillance technologies (Kaushal, 2023). These vessels also act as "mother ships" for smaller submersibles capable of clandestine insertion, including remotely piloted or autonomous underwater vehicles and small, three-man submarines (Lobner, 2018).

Russia conducts maritime special operations across two main organizations, the RFN and GUGI. Through its Ministry of Defense and its subordinate military intelligence agency, the GRU, the RFN and GUGI execute clandestine operations in the maritime domain (Kaushal, 2023). The GUGI operates largely independent from the RFN, though draws heavily from submarine and specialized diving units to fill its ranks (Kaushal, 2023). Smaller submersible vessels such as the *Losharik* can be launched from surface or subsurface-based motherships, such as the nuclear-powered submarine *Belgorod* or research ship *Yantar* (Kaushal, 2023). Incursions by these small submersibles and specialist divers into the territorial waters of the countries adjoining the Baltic Sea have been documented, and for quite some time. In 1983, an unidentified submarine was spotted in the middle of the Hårsfjärden Naval Base in Sweden. An investigation of the seabed indicated an imprint matching the dimensions of a Triton 2 mini-submarine employed by Russian naval special forces, or Spetsnaz, out of its Primorsk base north of Kaliningrad (Jansson, 2016). In the same year, three divers quickly escaped into the Baltic waters around the Swedish archipelago after they were spotted near a beach, with a follow-on investigation once again implicating the Spetsnaz (Jansson, 2016).

The use of military assets, submarines included, to conduct reconnaissance is not indicative of gray zone strategy. These vignettes of Russian subsurface intrusion in the Baltic Sea are not provided to denigrate the common practice by the world's militaries of hiding

submarines off adversaries' and allies' coasts to gather intelligence.[8] Instead, it demonstrates the capability and use of the submarine domain for gray zone operations. Unlike the Chinese maritime militias filling dual roles in commercial and paramilitary operations, the operatives of the GUGI are well-compensated and highly trained (Kaushal, 2023). As discussed, gray zone operations can be identified through the blending and disguise of military assets and operations with civilian means. The GUGI retains the capability to execute and has been implicated in these operations.

The use of multi-role ships, deceptive shipping practices, and sanctions evading are not in themselves gray zone actions. What is emphasized is the objective these assets are pursuing, in this case security related, and the ambiguity relating to the legal status proportional response to these measures (Green, Hicks, Cooper, Schaus, & Douglas, 2017; Letts, 2024). The implementation of sanctions on Russian oil is an example of an attempt to achieve cross-domain deterrence. The economic instrument of power in this case is wielded to punish Russia for its aggression in Ukraine, but by employing the gray fleet, Russia undermines the deterrent value that sanctions are meant to impose. This cross-domain coercion, whereby Russia undercuts the economic lever of power without wielding its military strength, reduces the alliance's security (Adamsky, 2015). In the next section, the thesis will show how Russia deploys cross-domain levers of power in a concerted effort to undercut maritime security in the Baltic Sea.

[8] See “Submarine Intrusions in Swedish Waters: Past and Present” by Nils-Ove Jansson. In a slightly more comical incursion, a Swedish fisherman claimed to collide with a submarine, casting him from his boat. He was able to briefly grab hold of both the submarine and his vessel before the submarine departed and he made his way to shore to report the incident. Owing to his bad reputation, initially he was not believed until he described the exterior of the sub as “like the skin of an orange”, which accurately describes the sonar-reducing coating of many submarines.

3.2.2. RUSSIA IS SALAMI-SLICING THE BALTIC SEA

As discussed, gray zone campaigns seek gradual, incremental gains rather than rapid and massive advances. This includes the erosion of established norms and territorial boundaries, factors for which Russia has previously undermined in its long campaign in Ukraine. To illustrate, in September of 2003, barely 10 years after the collapse of the Soviet Union, Russia began constructing a dam between its coast and the tiny Tuzla Island near the Kerch Strait (Malyarenko & Kormych, 2023). After Ukrainian protest, both countries signed an agreement regarding the Sea of Azov and Kerch Strait, critically containing language that "the Sea of Azov and the Kerch Strait have historically been inland waters of the Russian Federation and Ukraine" (Malyarenko & Kormych, 2023). Only relatively recently has Ukraine publicly decried the shabby dam building as little more than a tool to gain this concession (Malyarenko & Kormych, 2023).

Russia also displays incrementalistic, salami-slicing tactics in the Baltic Sea. This is both in incursions into NATO waters, harassment of civilian and military vessels akin to the Chinese maritime militia as well as political-influence operations meant to destabilize and re-establish normative behaviors (Lagrone, 2016; Reuters, 2014). For instance, a now-deleted official Russian government document showed a proposal redefining the sea borders in the eastern part of the Gulf of Finland and in the vicinity of the Kaliningrad enclave (Aliyev, 2024). According to the draft decree, the current maritime borders established in 1985 were based on outdated nautical charts, and do not "allow the establishing of the external boundary of Russia's internal waters and does not take into account the practice of establishing baselines by other states" (Hartog, 2024). The changes were to take effect in January of 2025 (Hartog, 2024). For its part, Russian state-run news agencies ran reports following the redaction discrediting Russian

intentions to redraw the borders, and an unnamed Russian political source was cited as saying there is no intention to redraw the border (Hartog, 2024). A day after the government redacted the document, Russian border guards removed a series of navigation buoys in the Narva River separating Russia from Estonia on the Estonian side (Aliyev, 2024). Since this incident, Estonia reported a marked increase of border violations and apprehensions (ERR, 2024). While most of these incidents are rather benign, the Head of the Border and Migration Supervision Department at the Police and Border Guard Board's East Prefecture in Estonia has claimed that the majority of the illegal crossings have taken place in areas where Russia moved these markers (ERR, 2024).[9] This event is significant due to the still unratified agreement on the Treaty on the Delimitation of Maritime Areas of Narva Bay and the Gulf of Finland between Estonia and Russia (Schaub, Murphy, & Hoffman, 2017).

It remains to be seen if Russia will try to enforce these borders in 2025. If it does, it may likely result in a similar situation as China's actions in the South China Sea in the form of increased civilian and military vessels patrolling the newly claimed territory. This could in turn fuel low-level tensions and raise the risk of escalation through increase Russian and NATO interactions at sea. This speculation aside, the fact that the Russian ministry published this information is indicative of an intentional act. In a government where policy making is tightly controlled and the flow of information even more so, the mere act of the publication and redaction can be viewed as an attempt to sow confusion and ambiguity regarding Russian intentions (Aliyev, 2024).

[9] See, "Removal by Russia of Narva River buoys leads to surge in border violations" by ERR. Many fishermen have inadvertently crossed the line and were swiftly redirected toward their respective countries. However, the Estonian border guard still decries these encounters for the drain on scant resources.

Regardless of Russian intent, this is largely viewed by NATO as a deliberate provocation to induce uncertainty and undermine confidence in the alliance (Bornio & Szacawa, 2024). For the NATO Baltic Sea states, they may now feel increased pressure to patrol these areas more intensely, or otherwise invest security assets in areas Russia never intended to lay claim to. It is also plausible that the document was released as a way to normalize the idea of Russian sovereignty over this disputed maritime territory, in the same way China's artificial reefs, forward military bases, and assertive maritime militias stake its claim in the South China Sea. Moreover, the establishment of a new maritime boundary or exclusive economic zone would give access not only for maritime maneuver, but also to the airspace extending above it thereby increasing the range of aerial reconnaissance and strike craft for Russia (Kalm, 2024).

3.3. NATO AND GRAY ZONE DETERRENCE

This thesis has so far examined Russia's reasoning, intent, and capability to conduct gray zone maritime operations in the Baltic Sea region and will now turn to a discussion of NATO in this arena. To counter the deployment of these multifaceted, ambiguous, and incrementalistic tactics by Russia, NATO has implemented several measures to varying degrees of success. Deterrent measures in this region are mainly focused to its landward borders with Russia, with particular attention paid to the "Suwalki Gap" separating the Baltic States from the rest of NATO (van Tol, Bassler, Kjellstrom Elgin, & Hacker, 2022). To this end, substantial efforts have been made by NATO to create integrated defense concepts rather than separate national plans (van Tol, Bassler, Kjellstrom Elgin, & Hacker, 2022). However, to defend the region against the gray zone tactics deployed by Russia in the region, several issues arise.

As Russia continues to make small-scale, deniable incursions across NATO's threat perception thresholds, NATO could in effect be desensitized to the tactics and fail to respond

before a *fait accompli* is complete or another aspect of the status quo is altered (Murauskaite, et al., 2019). To illustrate the conundrum, take a hypothetical scenario wherein Russia chooses to enforce its redrawn maritime boundaries between it and Estonia with sea mines (Duenow, 2022). NATO could respond with conventional military force, striking the mine-laying ships in a clear escalation; it could undertake anti-sea mining measures which may instead be viewed more defensively; or, it may do nothing, in which case the de facto border has in effect been redrawn despite whatever protest it may solicit. Now, imagine these vessels conducting the mining are ostensibly civilian research vessels.[10] The law of armed conflict makes these vessels legitimate targets in war, but in this case, NATO is faced with the question of whether it is in fact at war. Complicating these variables further is the incongruity of interests within NATO, and the individual national politics which could supersede any Article 5 response (Murauskaite, et al., 2019).

Though NATO conducts extensive bilateral maritime patrols and exercises in the region, these military responses to what is often not a military problem require non-military solutions to solve. NATO's very framework is predicated on conventional military deterrence, leaving a seam which Russia can exploit (Murphy & Schaub, 2018). NATO adopted the Alliance Maritime Strategy in 2011 and has continued to revise and update this document iteratively over the years. It has also established combined naval headquarters and coordination cells. However, this is still primarily aimed at collective deterrence against conventional naval forces and does little to enable coalition operations to protect against gray zone threats (Larsson, 2024; Schaub, Murphy, & Hoffman, 2017). Most concerningly, NATO's official position leaves the primary responsibility for response to gray zone threats on the targeted country (Hansen, Musser, &

[10] See, "Sea of Peace or Sea of War" by Murphy and Schaub. In 1984, the Libyan navy used a civilian vessel to lay mines in the Red Sea, damaging twenty ships transiting the Suez Canal.

Villasenor, 2021; NATO, 2024). As previously discussed, sub-lethal threshold actions leave ambiguity and uncertainty surrounding appropriate responses. For example, should a Russian "gray" ship collide with a flagged NATO ship, resulting in no onboard casualties but extensive hull damage, it is not clear the sort of response this should engender (Schaub, Murphy, & Hoffman, 2017). Alternatively, if the same ship were to be scuttled to block the entrance to the port of Riga at the Daugava river, as Russia did in its 2014 annexation of Crimea to trap the Ukrainian navy in Sevastapol, under non-wartime conditions, it is hard to say if this could be seen as an escalation (Savits, 2021). Owing to the purposefully deceitful origin of the ship, attribution could further complicate NATO's response.

As illustrated, NATO's official doctrine within the 2022 Strategic Concept and Alliance Maritime Concept are primarily oriented on conventional deterrence from military threats. To its credit, and recognizing the evolving security environment, NATO adopted the Concept for Deterrence and Defense of the Euro-Atlantic Area in 2020, acronymized as DDA or referred to as its "deter and defend" strategy (Covington, 2023). While it emphasizes deterrence in peacetime through the integration of all elements of national power, most of the discussion focuses on military force dispositions and operations (Covington, 2023). This is accomplished through what the alliance calls "vigilance activities", which includes collective military exercises and combined patrol operations (Monaghan, Dahlstrand, and Moller, 2024). The concept of the gray zone or even hybrid threats is addressed in terms of the application of military forces, but it does not clearly delineate how other measures or intelligence systems should be synchronized to counter these threats (Monaghan, Dahlstrand, and Moller, 2024).

Deterrence failures in the gray zone are often failures of attribution, undermining the bedrock of the actor's fear of retaliation (Stuckenberg, 2019). Within the Baltic Sea, millions of

tons of cargo are traded each year via large container ships. Tracking and identifying the contents of each vessel moving within this corridor is exceedingly difficult under the best of circumstances, a task with more urgency when these ships may be carrying ballistic missiles or conducting reconnaissance. To this end, NATO has attempted to develop shared intelligence and sensor data information sharing systems (Schaub, Murphy, & Hoffman, 2017), such as NATO's Digital Ocean Initiative to integrate an array of technologies and sensors to enhance MDA (Bueger, 2024). Sharing this information swiftly and precisely through a shared common operating picture allows national leaders the time and space necessary to coordinate responses (Stuckenberg, 2019). To counter the threats posed to the network of underseas cables, NATO established the Critical Undersea Infrastructure Coordination Cell in its Brussels headquarters in 2023 and tasked it with identifying vulnerabilities and improving information sharing, but they remain inhibited by national policies and lack of common systems (Bueger, 2024). It remains to be seen if these efforts enhance NATO's ability to deter and counter Russia's gray zone activities in the maritime domain.

4. RECOMMENDATIONS AND CONCLUSION

Despite the challenges of deterrence in the gray zone, several strategies and polices offer promising solutions. Critically, nations must be able to identify that gray zone tactics are being employed as part of a concerted campaign rather than simply seeing the individually weak signals of which they are comprised (Hicks, et al., 2019). This requires the development of modern, persistent, and advanced intelligence apparatus's that can expose these actions and their instigators in real-time, thus denying the ambiguity and deniability they rely upon (Hicks, et al., 2019). This risks the attacker's reputation and prestige vice the defender's (Green, Hicks, Cooper, Schaus, & Douglas, 2017). A model of deterrence by detection comprised of persistent, low-cost, and interoperable intelligence, surveillance, and reconnaissance (ISR) networks could enable defenders to identify and respond to emerging low-intensity threats prior to them coalescing into larger incursions (Mahnken, Sharp, & Kim, 2020). Adversaries would be less likely to commit opportunistic actions if they are being surveilled and their actions being broadcast publicly to the world (Mahnken, Sharp, & Kim, 2020). Backed by credible combat deterrent measures, illuminating malign actions prior to increased hostilities at a minimum buys time and space for policy makers (Sharp, Mahnken, & Sadov, 2023).

This model has already been employed in the Pacific region in conjunction with U.S. allies in their ongoing competition against China. As outlined in a comprehensive report by the Center for Strategic and Budgetary assessments, deterrence by detection includes the integration of full spectrum ISR capabilities with nascent technology like artificial intelligence (Mahnken, Sharp, Bassler, & Durkee, 2021). It speaks to a "neighborhood watch" concept, which would integrate the ISR complexes of the Philippines, Australia, the U.S., and their other allies to generate risk of discovery for China regarding its malicious activities in the region (Mahnken, Sharp, Bassler, & Durkee, 2021). Reaffirming its belief in the utility of this model, on May 3,

2023 the Philippine and U.S. Secretaries of Defense established Bilateral Defense Guidelines which prioritized shared ISR systems and information sharing procedures (U.S. DOD, 2023).

There are two steps NATO may undertake to deter Russia's gray zone actions in the maritime domain. First, NATO must create a fully synchronized, combined operating picture in pursuit of complete MDA in the Baltic Sea. The Digital Ocean Initiative and the Critical Undersea Coordination Cell are excellent programs in this regard, but NATO still must overcome national information-sharing policies inhibiting shared MDA. Overcoming challenges of attribution will require more than object-locating sensors, but will also require shared cyber and signals intelligence to ascertain the intentions and actions of gray and dark vessels. It is not enough to know where a vessel is in the maritime domain- NATO must maintain full awareness of the origins of each vessel, its actions, and its contents (Mahnken, Sharp, & Kim, 2020). This denies Russia the ability to conceal the actions of the GUGI, its military, and intelligence services, enhancing deterrence. A studies have reinforced that capabilities such as unmanned aerial and subsurface drones and electronic surveillance systems which may or not be known to the adversary has a strong deterrent effect in the gray zone (DSB, 2016; Mahnken, Sharp, & Kim, 2020; Sharp, Mahnken, & Sadov, 2023). The deterrent value is induced in the risk of attribution of coercive measures, and the use of non-lethal or non-kinetic means minimizes the risk for escalation (DSB, 2016). For example, employing a small, unmanned surface vessel to trail a Russian research ship instead of a naval vessel would provide a visible sign to Russia that it is being observed while reducing the risk of negative public perceptions regarding the employment of military assets for this purpose.

Second, NATO must develop a clear strategy which denotes its red-lines and response thresholds. The current NATO deterrent posture is based on, "an appropriate mix of nuclear,

conventional and missile defence capabilities" (NATO, 2022). However, countering threats to the maritime security of the Baltic Sea region will require a clear signal from the alliance regarding its deterrence posture across the entirety of the diplomatic, information, military, and economic spectrum. The policy must communicate what the alliance will and will not tolerate, and under what conditions, and what the aggressor risks losing should it cross these boundaries (Green, Hicks, Cooper, Schaus, & Douglas, 2017). The Article 5 commitment is not enough to deter Russia's gray zone actions in the Baltic Sea region, and NATO should instead adopt a model of deterrence by detection across the DIME spectrum, expanding its intelligence collection systems to illuminate these threats (Mahnken, Sharp, & Kim, 2020). NATO must also adopt an allied approach to dealing with hybrid threats, not simply allow allied countries to react to individual episodes of coercion (DSB, 2016; Sharp, Mahnken, & Sadov, 2023). Since one of the critical vulnerabilities surrounding the credibility of NATO is the viability of the extended deterrence conferred by membership, NATO would benefit by exhibiting collective defense strategies to gray zone actions. It will also require NATO to adopt plans that are not wholly dependent on the U.S. should it be focused on operations in the Pacific or other regions of the world (Westgaard, 2023). With the addition of Sweden to the alliance, NATO now has one of the most capable submarine forces for operations in the unique environment of the Baltic sea (Kalm, 2024). In the gray zone, where a blend of military and non-military means are necessary to deter threats, it will be vital to incorporate these and other assets into a coherent strategy to deny Russia the use of its coercive tactics.

Russia has adopted gray zone tactics in the maritime domain against NATO in the Baltic Sea region, and NATO is currently not postured to adequately deter these measures. This thesis provided a broad overview of the concept of the gray zone in the maritime domain. This included

a discussion on the challenges of deterrence and attribution. It then examined these dynamics within the context of Russia's actions in the Baltic Sea region, highlighting its strategic thinking and methods by which it executes maritime gray zone actions, owing to the imbalance of power in the region and the asymmetry of interests between it and NATO. These methods are ambiguous, multidimensional, and incrementalistic, bearing the hallmarks of a concerted campaign to threaten and coerce NATO without breaching the level of armed conflict. Finally, it examined the deterrence dilemma in the maritime domain faced by NATO in the region, and methods by which it may continue to compete with and deter Russia. While more must be done to understand the complexities of the gray zone and maritime domain, policymakers and academia can no longer afford to be "sea-blind." Comprehensive security strategies will require practitioners to become more comfortable engaging in the maritime domain beyond the simple examination of naval force comparisons and instead enter the complex arena of the gray zone.

Bibliography

Adamsky, D. (2015, November). Cross-Domain Coercion: The Current Russian Art of Strategy. *Proliferation Papers, 54*. Retrieved from https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/pp54adamsky.pdf

Aliyev, N. (2024, August 15). *Does Russia want to revise its water border with the Nordic and Baltic states?* Retrieved from International Centre for Defence and Security: https://icds.ee/en/does-russia-want-to-revise-its-water-border-with-the-nordic-and-baltic-states/

Atlantic Council's Gray Zone Task Force. (2022, December 22). *Scoping the gray zone: Defining terms and policy priorities for engaging competitors.* Retrieved from Atlantic Council Scowcroft Center for Strategy and Security: https://www.atlanticcouncil.org/wp-content/uploads/2022/12/Scoping-the-Gray-Zone_Strategic-Insights-Memo.pdf

Belo, D., & Carment, D. (2020). Gray-zone conflict management: Theory, Evidence, and Challenges. *The Air Force Journal of European, Middle Eastern, and African Affairs, 1*(1), 1-38. Retrieved from https://www.airuniversity.af.edu/JEMEAA/Display/Article/2213954/gray-zone-conflict-management-theory-evidence-and-challenges/

Bilal, A. (2021, November 30). *Hybrid Warfare- New Threats, Complexity, and 'Trust' as the Antidote.* Retrieved from NATO Review: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Bornio, J., & Szacawa, J. D. (2024, June 5). *Finland's response to the Russian Federation's provocations regarding the change of maritime borders in the Baltic Sea*. Retrieved from Institute of Central Europe: https://ies.lublin.pl/en/comments/finlands-response-to-the-russian-federations-provocations-regarding-the-change-of-maritime-borders-in-the-baltic-sea/

Brands, H. (2016, February 5). *Paradoxes of the Gray Zone.* Retrieved from Foreign Policy Research Institute: https://www.fpri.org/article/2016/02/paradoxes-gray-zone/

Brauss, H., & Racz, A. (2021). *Russia's Strategic Interests and Actions in the Baltic Sea Region.* German Council on Foreign Relations. Retrieved from https://www.academia.edu/44926390/Russias_Strategic_Interests_and_Actions_in_the_Baltic_Region

Braw, E. (2024, January 11). *Russia's growing dark fleet: Risks for the global maritime order*. Retrieved from Atlantic Council: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/russias-growing-dark-fleet-risks-for-the-global-maritime-order/#the-shadow-fleet-and-sanctions

Braw, E. (2024, July 22). *Worse Than Pirates: Russian Shadow Fleet Brings Disaster*. Retrieved from Center for European Policy Analysis: https://cepa.org/article/worse-than-pirates-russian-shadow-fleet-brings-disaster/

Buchanan, E. (2023, October 2). *It's Russia's (Maritime) World-We're Just living in It*. Retrieved from RUSI: https://rusi.org/explore-our-research/publications/commentary/its-russias-maritime-world-were-just-living-it

Bueger, C. (2015, December). What is Maritime Security? *Marine Policy, 53*, 159-164. doi:http://dx.doi.org/10.1016/j.marpol.2014.12.005

Bueger, C. (2024, January 19). *NATO's Contribution to the Critical Maritime Infrastructure Protection*. Retrieved from NATO Center for Maritime Strategy: https://centerformaritimestrategy.org/publications/natos-contribution-to-critical-maritime-infrastructure-protection/

Bush, J. (2014, April 8). *Factbox-Costs and benefits from Russia's annexation of Crimea*. Retrieved from Reuters: https://www.reuters.com/article/world/uk/factbox-costs-and-benefits-from-russias-annexation-of-crimea-idUSBREA370NY/

CJCS. (2018, April 25). *Joint Doctrine Note 1-18 Strategy.* Retrieved from Joint Chiefs of Staff: https://www.jcs.mil/Portals/36/Documents/Doctrine/jdn_jg/jdn1_18.pdf

Clarke, R. (2011). *The Club-K Anti-Ship Missile System: A Case Study in Perfidy and its Repression*. Retrieved from Inter-American Court of Human Rights: https://corteidh.or.cr/tablas/r30494.pdf

Covington, S. (2023, August 2). *NATO's Concept for Deterrence and Defence of the Euro-Atlantic Area (DDA).* Retrieved from Belfer Center for Science and International Affairs, Harvard: https://www.belfercenter.org/publication/natos-concept-deterrence-and-defence-euro-atlantic-area-dda

CSIS. (2014, March 18). *Crimea's Strategic Value to Russia*. Retrieved from Center for Strategic and Security Studies: https://www.csis.org/blogs/post-soviet-post/crimeas-strategic-value-russia

Davis, A., & Vest, R. (2022). *Maritime Doctrine of the Russian Federation.* US Naval War College, Russia Maritime Studies Institute. Newport, Rhode Island: US Naval War College. Retrieved from https://dnnlgwick.blob.core.windows.net/portals/0/NWCDepartments/Russia%20Maritime%20Studies%20Institute/20220731_ENG_RUS_Maritime_Doctrine_FINALtxt.pdf?sv=2017-04-17&sr=b&si=DNNFileManagerPolicy&sig=2zUFSaTUSPcOpQDBk%2FuCtVnb%2FDoy06Cbh0EI5tGpl2Y%3D

Derleth, J. W. (2023, January 13). *Great Power Competition, Irregular Warfare, and the Gray Zone.* Retrieved from Irregular Warfare Center: https://irregularwarfarecenter.org/wp-content/uploads/20230111_Perspectives_No_2.pdf

DSB. (2016). *Summer Study on Capabilities for Constrained Military Operations.* DOD, Office of the Under Secretary of Defense for Acquistion, Technology, and Logistics, Washington, D.C.

Duenow, V. (2022, April 18). *Baltic Sea Mining as an Extension of the Russian Gray Zone*. Retrieved from Foreign Policy Research Institute: https://www.fpri.org/article/2022/04/baltic-sea-mining-as-an-extension-of-the-russian-gray-zone/

Erickson, A. S., Hickey, J., & Holst, H. (2019). Surging Second Sea Force: China's Law-Enforcement Forces, Capabilities, and Future in the Gray Zone and Beyond. *Naval War College Review, 72*(2, Article 4). Retrieved from https://digital-commons.usnwc.edu/nwc-review/vol72/iss2/4

ERR. (2024, September 09). *Removal by Russia of Narva River buoys leads to surge in border violations*. Retrieved from news.err.ee: https://news.err.ee/1609471447/removal-by-russia-of-narva-river-buoys-leads-to-surge-in-border-violations

Fridbertsson, N. T. (2023). *Protecting Critical Maritime Infrastructure-The Role of Technology.* Copenhagen, Denmark: NATO Parliamentary Assembly-Science and Technology Committee. Retrieved from file:///C:/Users/bklew/Downloads/032_STC_23_E_rev_2_fin__CRITICAL_MARITIME_INFRASTRUCTURE__FRIDBERTSSON_REPORT1_sFDLYEDDXLBV4IEbElKeeiH08_99720.pdf

Gheciu, A., & Wohlforth, W. C. (2018). Maritime Security. *The Oxford Handbook of International Security*.

Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In M. Green, K. Hicks, Z. Cooper, J. Schaus, & J. Douglas, *Countering Coercion in Maritime Asia:The Theory and Practice of Gray Zone Deterrence* (pp. 21-50). Center for Strategic and International Studies.

Hansen, D., Musser, M., & Villasenor, B. (2021). *The Rhetoric vs the Reality: Understanding NATO's Capacity to Address Russian Gray-zone Conflict.* Retrieved from The Civil Affairs Association: https://www.civilaffairsassoc.org/post/the-rhetoric-vs-the-reality-understanding-nato-s-capacity-to-address-russian-gray-zone-conflict

Hartog, E. (2024, May 22). *Russia mysteriously deletes threat to redraw Baltic Sea border*. Retrieved from Politico: https://www.politico.eu/article/russia-defense-ministry-change-baltic-sea-border-finland-latvia/

Hicks, K. H., Friend, A. H., Federici, J., Shah, H., Donahue, M., Conklin, M., . . . Sheppard, L. (2019, July). *By Other Means: Part 1: Campaigning in the Gray Zone.* Center for Strategic and International Studies. Lanham, Boulder, New York, London: Rowman & Littlefield. Retrieved from Center for Strategic and International Studies: https://csis-

website-prod.s3.amazonaws.com/s3fs-public/publication/Hicks_GrayZone_interior_v4_FULL_WEB.pdf

HQ US Marine Corps. (2020, December 14). *MCDP 1-4 Competing.* Retrieved from marines.mil: https://www.marines.mil/Portals/1/Publications/MCDP%201-4.pdf?ver=fGwjmqkxGvv0GPe0mPgdqw%3D%3D

IISS. (2020, June 26). *Further testing of the containerized missile system*. Retrieved from iiss.org: https://www.iiss.org/online-analysis/online-analysis/2020/06/mdi-testing-containerised-missile-system

International Maritime Organization. (2015, December 2). *Resolution A. 1106(29) Revised Guidelines for the Onboard Operational Use of Shipborne Automatice Identification Systems (AIS).* Retrieved from International Maritime Organization: https://www.imo.org/en/OurWork/safety/navigation/ais.aspx

Jansson, N.-O. (2016, January-March). Submarine Intrusions in Swedish Waters: Past and Present. *Kungl, 1*, 52-59. Retrieved from https://kkrva.se/hot/2016:1/jansson_subm_instrusions.pdf

Jervis, R. (1979, January). Deterrence Theory Revisited. *World Politics, 31*(2), 289-324. doi:10.2307/2009945

Jordan, J. (2020). International Competition Below the Threshold of War: Toward a Theory of Gray Zone Conflict. *Journal of Strategic Security, 14*(1), 1-24. doi:https://doi.org/10.5038/1944-0472.14.1.1836

Kalm, H. (2024, May 29). *NATO's Path to Securing Undersea Infrastructure in the Baltic Sea*. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/research/2024/05/nato-baltic-sea-security-nord-stream-balticconnector?lang=en

Kaushal, S. (2023, May 25). *Stalking the Seabed: How Russia Targets Critical Undersea Infrastructure.* Retrieved from RUSI: https://rusi.org/explore-our-research/publications/commentary/stalking-seabed-how-russia-targets-critical-undersea-infrastructure

Kraska, J., & Pedrozo, R. (2013). *International Maritime Security Law.* Brill/Nijhoff. doi:978-90-04-23357-7

Lagrone, S. (2016, April 13). *Video: Russian Fighters Buzz USS Donald Cook in Baltic Sea*. Retrieved from USNI News: https://news.usni.org/2016/04/13/video-russian-fighters-buzz-uss-donald-cook-in-baltic-sea

Landreth, J. M. (2020, July-August). *Sea Power in the Gray Zone.* Retrieved from Defense Acquisition University: https://www.dau.edu/sites/default/files/Migrate/DATLFiles/July_Aug2020/Landreth.pdf

Larsson, O. L. (2024, May 30). Sea blindness in grey zone preparations. *Defence Studies, 24*(3), 399-420. doi:10.1080/14702436.2024.2359913

Letts, D. (2024). 12. The Maritime Domain. In M. R. Sari, *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies* (pp. 251-270). Oxford Academic.

Lindsay, J. R., & Gartzke, E. (2019). *Cross-Domain Deterrence: Strategy in an Era of Complexity.* Oxford, New York, US: Oxford Academic. doi:https://doi.org/10.1093/oso/9780190908645.001.0001

Lobner, P. (2018, May 21). *You Need to Know About Russia's Main Directorate of Deep-Sea Research (GUGI)*. Retrieved from The Lyncean Group of San Diego: https://lynceans.org/all-posts/you-need-to-know-about-russias-main-directorate-of-deep-sea-research-gugi/

Luo, S., & Panter, J. G. (2021). China's Maritime Militia and Fishing Fleets: A Primer for Operational Staffs and Tactical Leaders. *Military Review, 101*, 6-21. Retrieved from https://www.researchgate.net/publication/357031819_China's_Maritime_Militia_and_Fishing_Fleets_A_Primer_for_Operational_Staffs_and_Tactical_Leaders

Lynch, T. F. (2020, November 4). 1. Introduction. In *Strategic Assessment 2020: Into a New Era of Great Power Competition.* Washington, D.C.: National Defense University. Retrieved from National Defense University Press: https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404286/1-introduction/

Mahnken, T. G., Sharp, T., & Kim, G. B. (2020). *Deterrence by Detection: A Key Role for Unmanned Aircraft Systems in Great Power Competition.* Center for Strategic and Budgetary Assessments.

Mahnken, T. G., Sharp, T., Bassler, C., & Durkee, B. (2021). *Implementing Deterrence by Detection: Innovative Capabilities, Processes, and Organizations for Situational Awareness in the Indo-Pacific Region.* Center for Strategic and Budgetary Assessments. Retrieved from https://csbaonline.org/uploads/documents/CSBA8269_(Implementing_Deterrence_By_Detection)_FINAL_web.pdf

Mallory, K. (2018, April 12). *New Challenges in Cross-Domain Deterrence.* Retrieved from RAND: https://www.rand.org/pubs/perspectives/PE259.html

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

Matisek, J. W. (2017, Fall). Shades of Gray Deterrence: issues of Fighting in the Gray Zone. *Journal of Strategic Studies, 10*(3), 1-26. Retrieved from https://www.jstor.org/stable/26466832

Mazarr, M. (2018). *Understanding Deterrence.* RAND. Retrieved from www.rand.org: https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf#:~:text=Deterrence%20is%20the%20practice%20of%20discouraging%20or%20restraining,efort%20to%20force%20an%20actor%20to%20do%20something.

Mazarr, M. J. (2015). *Mastering the Gray Zone: Understanding a Changing Era of Conflict.* US Army War College: Strategic Studies Institute/ Monographs, Books, and Publications. Retrieved from https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1427&context=monographs

Messmer, M. (2024, April 22). *The Baltic Sea is far from a 'NATO lake'- the alliance must strengthen its defences.* Retrieved from Chatham House: https://www.chathamhouse.org/2024/04/baltic-sea-far-nato-lake-alliance-must-strengthen-its-defences

Milveski, L. (2024, February 15). When does gray zone confrontation end? A conceptual analysis. *Joint Forces Quarterly, 112*, 4-11. Retrieved from https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3678004/when-does-gray-zone-confrontation-end-a-conceptual-analysis/

Ministry of Foreign Affairs of the Russian Federation. (2023, March 31). *The Concept of the Foreign Policy of the Russian Federation (English Translation).* Retrieved from www.mid.ru: https://www.mid.ru/en/foreign_policy/fundamental_documents/1860586/

Monaghan, S., Dahlstrand, K., & Moller, S. (2024, May 20). *Understanding NATO's Concept for Deterrence and Defense of the Euro-Atlantic Area.* Retrieved from Center for Strategic and Budgetary Assessments: https://csbaonline.org/research/publications/understanding-natos-concept-for-deterrence-and-defense-of-the-euro-atlantic-area

Morcos, P., & Wall, C. (2021, June 11). *Invisible and Vital: Undersea Cables and Transatlantic Security.* Retrieved from Center for Strategic and International Studies: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Murauskaite, E., Quinn, D., Thompson, C. P., Ellis, D. H., Wilkenfield, J., & Gartzke, E. (2019, November 14). Extended Deterrence Dilemmas in the Grey Zone: Trans-Atlantic Insights on Baltic Security Challenges. *Journal on Baltic Security, 5*(2), 5-16. doi:https://doi.org/10.2478/jobs-2019-0006

Murphy, M. N., & Schaub, G. (2017, March 29). *The Baltic: Grey-Zone Threats on NATO's Northern Flank*. Retrieved from Center for International and Maritime Security: https://cimsec.org/baltic-grey-zone-threats-natos-northern-flank/

Murphy, M., & Schaub, G. (2018). Sea of Peace or Sea of War-Russian Maritime Hybrid Warfare in the Baltic Sea. *Naval War College Review, 71*(2), 122-148. Retrieved from

https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1738&context=nwc-review

NATO. (2022, June 29). *NATO 2022 Strategic Concept.* Retrieved from NATO.int: https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

NATO. (2023, Jul 04). *Collective defence and Article 5*. Retrieved from NATO: https://www.nato.int/cps/en/natohq/topics_110496.htm

NATO. (2024, May 07). *Countering hybrid threats*. Retrieved from NATO: https://www.nato.int/cps/en/natohq/topics_156338.htm

NATO. (2024). *Multi-Domain Operations.* Retrieved from NATO Allied Command Transformation: https://www.act.nato.int/activities/multi-domain-operations/

NMIO. (2005, September). *The National Strategy for Maritime Security.* Retrieved from nmio.ise.gov: https://nmio.ise.gov/Portals/16/Docs/National%20Strategy%20for%20Maritime%20Security.pdf?ver=2015-12-04-123608-170

NMIO. (2013, January). *National Maritime Domain Awareness Plan.* Retrieved from National Maritime Intelligence-Integration Office: https://nmio.ise.gov/Portals/16/National%20MDA%20Plan%202023%20%28U%29.pdf

Palmer, A., Duff, D., Jun, J., & Bermudez, J. S. (2023, August 24). *A Wolf in Ship's Clothing: Russia's Militarization of Civilian Vessels in the Black Sea*. Retrieved from CSIS.org: https://www.csis.org/analysis/wolf-ships-clothing-russias-militarization-civilian-vessels-black-sea

Pawlak, J. (2022, September 5). *No, Don't Call the Baltic a 'NATO Lake'.* Retrieved from RUSI: https://rusi.org/explore-our-research/publications/commentary/no-dont-call-baltic-nato-lake

Pawlak, J. (2024, May 21). *Charting the Challenges in the Baltic Sea*. Retrieved from War on the Rocks: https://warontherocks.com/2024/05/charting-the-challenges-in-the-baltic-sea/

Pihl, A. (2024, September 25). *What are Russian research vessels doing in the Baltic Sea?* Retrieved from ERR News: https://news.err.ee/1609470505/what-are-russian-research-vessels-doing-in-the-baltic-sea

Pointer. (2024, September 24). *Russian Spy Vessels (translated from website)*. Retrieved from pointer.com: https://pointer.kro-ncrv.nl/rusland-bespioneert-systematisch-onze-wateren

Reuters. (2014, May 30). *Lithuania accuses Russia of Harassing ships in Baltic Sea*. Retrieved from Reuters: https://www.reuters.com/article/idUSKBN0EA27T/

Ryzhenko, A. (2022, October 4). Nord Stream Explosions: Russian Sabotage in the Baltic? *Eurasia Daily Monitor, 19*(146). Retrieved from https://jamestown.org/program/nord-stream-explosions-russian-sabotage-in-the-baltic/

Savits, S. (2021, December). Blockship Tactics to Trap Enemy Fleets. *147*(12). Retrieved from US Naval Institute: https://www.usni.org/magazines/proceedings/2021/december/blockship-tactics-trap-enemy-fleets

Savitz, S., & Winston, I. (2024). *A Brief Naval Overview of the Baltic Sea Region.* RAND Corporation. Retrieved from https://www.rand.org/pubs/perspectives/PEA2111-1.html

Schaub, G. J., Murphy, M., & Hoffman, F. G. (2017). Hybrid Maritime Warfare: Building Baltic Resilience. *The RUSI Journal*, 32-40.

Sharp, T., Mahnken, T. G., & Sadov, T. (2023). *Extending Deterrence by Detection: The Case for Integrating Unmanned Aircraft Systems Into the Indo-Pacific Partnership for Maritime Domain Awareness.* Center for Strategic and Budgetary Assessments.

Siebold, S. (2023, May 3). *NATO says Moscow may sabotage undersea cables as part of war on Ukraine*. Retrieved from Reuters: https://www.reuters.com/world/moscow-may-sabotage-undersea-cables-part-its-war-ukraine-nato-2023-05-03/

Stott, M. (2010, April 26). *Deadly new Russian weapon hides in shipping container.* Retrieved from Reuters: https://www.reuters.com/article/world/deadly-new-russian-weapon-hides-in-shipping-container-idUSTRE63P2XB/

Stuckenberg, D. J. (2019). *Re-orienting NATO deterrence: The Reality of Strategic Gray Zone Threats.* Retrieved from NATO STO: https://www.airuniversity.af.edu/AUPress/Display/Article/2905307/maj-david-j-stuckenberg/

Sweigs, T., & Zilinick, S. (2019). *From Deterrence to Cross Domain Deterrence.* Hague Center for Strategic Studies. Retrieved from http://www.jstor.org/stable/resrep24191.5

Takahashi, S. (2018). Development of gray-zone deterrence: concept building and lessons from Japan's experience. *The Pacific Review, 31*(6), 787-810. doi:https://doi.org/10.1080/09512748.2018.1513551

Tallis, J. (2019). *The War for Muddy Waters: Pirates, Terrorists, Traffickers, and Maritime Insecurity.* Naval Institute Press.

U.S. DOD. (2023, May 23). *Fact Sheet: U.S.-Phillipines Bilateral Defense Guidelines*. Retrieved from defense.gov: https://www.defense.gov/News/Releases/Release/Article/3383607/fact-sheet-us-philippines-bilateral-defense-guidelines/

US Army. (2024, October). *Sibirykov-Class (Project 865 Class) Russian Hydrographic Survey Vessel*. Retrieved from odin.tradoc.army.mil:

https://odin.tradoc.army.mil/exports/pdf/c75671650bffb9cd372c3b46f84c81ef9bfbf737.pdf

USAID. (2010, December). *Maritime Security Sector Reform.* Retrieved from www.usaid.gov: https://www.usaid.gov/sites/default/files/2022-05/Maritime-Security-Sector-Reform_FINAL.pdf

Van der Putten, F.-P., Meijnders, M., & Rood, J. (2015). *Deterrence: Deterrence as a Security Concept against Non-Traditional Threats: In-Depth Study Clingendael Monitor.* Clingendael Institute. Retrieved from https://www.clingendael.org/sites/default/files/pdfs/deterrence_as_a_security_concept_against_non_traditional_threats.pdf

van Tol, J., Bassler, C., Kjellstrom Elgin, K., & Hacker, T. (2022). *Deterrence and Defense in the Baltic Region.* Center for Strategic and Budgetary Assessments. Retrieved from https://csbaonline.org/research/publications/deterrence-and-defense-in-the-baltic-region

Vavasseur, X. (2020, August 03). *Russian Navy to Begin Trials of Modular Systems for Surface Vessels*. Retrieved from www.navalnews.com: https://www.navalnews.com/naval-news/2020/08/russian-navy-to-begin-trials-of-modular-systems-for-surface-vessels/

Watts, R. (2005). Maritime Critical Infrastructure Protection: Multi-Agency Command and Control in an Asymmetric Environment. *Homeland Security Affairs* .

Westgaard, K. (2023, December 21). *The Baltic Sea Region: A Laboratory for Overcoming European Security Challenges*. Retrieved from CSIS: https://carnegieendowment.org/research/2023/12/the-baltic-sea-region-a-laboratory-for-overcoming-european-security-challenges?lang=en

Winkler, J. R. (2015, November 6). *Silencing the Enemy: Cable-Cutting in the Spanish-America War*. Retrieved from warontherocks.com: https://warontherocks.com/2015/11/silencing-the-enemy-cable-cutting-in-the-spanish-american-war/

Winnerstig, M. (2017, November). *The Baltic Sea Area: a New Geopoltical Focal Point.* Retrieved from Swedish Defence Research Agency: Strategic Outlook 7: https://www.foi.se/rest-api/report/FOI%20Memo%206210