

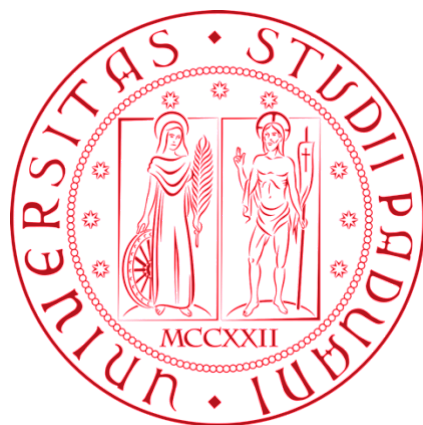
Into the Gray Zone: NATO Deterrence in a Graying and Multipolar World

Mark Olmstead

Università degli Studi di Padova

Prof. Valentine Lomellini

June 23, 2024



INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR
WORLD

Table of Contents

I.	Abstract	3
II.	Introduction	4
III.	Evolution of NATO Operational Domains	
	A. Introduction	9
	B. Land, Sea, and Air	10
	C. Space: The Final Frontier?	12
	D. The Cyber Domain as the Gray Domain	14
IV.	The Gray Zone	
	A. The Graying of Conflicts	18
	B. Russian Operations in the Gray Zone	20
	C. The Stability-Instability Paradox	23
	D. The Russian Calculus	25
	E. The Boiling Frog	30
V.	Deterrence as Punishment - NATO Capabilities	
	A. Deterrence or Compellence	35
	B. Defense Spending: The 2% Folly	36
	C. Military Capabilities	40
	1. The Western Core	43
	2. The Southern Flank	45
	3. The Eastern Flank	46
	4. The Northern Flank	49
	5. Benelux, Balkans, and Canada	51
	6. The United States	52
VI.	Deterrence in the Gray Zone	
	A. Deterrence in the Eastern Flank	55
	B. Strategic Deterrence: The Pivot to China	60
	C. Lessons from the Past: Kosovo, Afghanistan, Iraq, and Libya	
	1. Kosovo	66
	2. Afghanistan	68
	3. Iraq	71
	4. Libya	73
	D. Hybrid Warfare and Strategic Advantage	76
VII.	Relevancy of Interoperability	
	A. The State of Interoperability	82
	B. Revisioning Interoperability	88
	C. From Interoperability to “Gray Deterrence”	93
VIII.	The Multipolar World	
	A. The Further Graying of Conflicts	98
IX.	Conclusion	103
X.	Bibliography	109

I. Abstract

Since the end of the Cold War, the global geopolitical landscape has shifted dramatically toward multipolarity, altering the nature of conflict and threat perception. This paper examines the NATO alliance's capacity to navigate this increasingly complex and ambiguous "gray zone," where traditional distinctions between peace and war are obscured. The research focuses on the implications of this new multipolar context for NATO, particularly in response to gray zone challenges posed by Russia and China.

The study assesses NATO's current deterrent capabilities and explores strategic revisions and solutions aimed at enhancing the alliance's effectiveness in this evolving environment. Proposed solutions emphasize leveraging the strategic advantages of member states, improving interoperability across multiple domains, and fostering deeper integration to proactively address emerging threats.

The analysis highlights the critical need for NATO to adapt to 21st-century warfare dynamics, which now prominently include cyber and space domains, in addition to traditional military confrontations, as evidenced by recent tensions with Russia and China's expansionist policies. The paper argues that strengthening NATO's gray zone deterrence strategies is essential not only for countering immediate threats but also for navigating internal alliance politics and maintaining cohesion.

By enhancing its approach to gray zone deterrence, NATO can transcend its Cold War-era strategies and emerge as a model for a dynamic, flexible defense alliance suited to the complexities of a multipolar and increasingly ambiguous global order. This transformation is pivotal for NATO's relevance and effectiveness in a world where conventional and unconventional threats intersect with unprecedented frequency and intensity.

II. Introduction

“Interoperability is the capstone of NATO theory, but theory is outdated, because now we need to look at the multi-domain.” On a crisp November morning in 2023 I was able to sit down with Colonel Luigi Bramati, Director of the NATO Policing Stability Centre of Excellence in Vicenza, Italy. I was experimenting with ideas about this dissertation and was looking to discuss the future of interoperability within NATO and its future adaptations. This is where I learned from him that the future of NATO is not focused on interoperability at all, but rather revolutionizing the outdated thinking of the Alliance, focusing on the nature of the threats that exist today and in the future, as well as rethinking how the Alliance collaborates, strategizes, and responds among the multiple domains.

He told me, “the multi-domain is the revolution of all the processes. The world is becoming data centric; NATO must become a data-centric structure. Data-centric decision making, data-centric commands,...look at where we have data.” This spurred me to reanalyze the way I perceived the challenges of NATO and the threats of the future. NATO, and the world, has evolved out of the conventional views of the Cold War, a time when two great powers built their own deterrence to signal strength, fought proxy wars, engaged in an arms and space race, over competing ideologies, ending with the collapse of the Soviet Union in 1991, and a United States-led unipolar reality with NATO as the world’s largest defense alliance with no immediate enemy. This led to me to the creation of this dissertation and research question: In a multipolar and graying world, how can NATO adapt its deterrence to address these threats without raising global instability and remain relevant?

The world of today is different from the Cold War or even the immediate post-Cold War era. There has been a rapid rise in “gray zone” strategies and threats that have left states forced to reevaluate and reassess approaches to deterrence, capabilities, resilience, and interoperability. The “gray zone” is known as the place between peace and war, where threats exist, but are hard to define due to difficulties identifying attribution and the sense

of plausible deniability.¹ Furthermore, these gray zone threats do not exist solely in traditional military domains. For most of history the domains of operation have been on land, sea, and eventually air. But in the last decade there has been a rapid expansion of operations domains that include space and cyber. This goes back to what Colonel Bramati stated, that NATO needs to move beyond theory and into navigating the multiple domains around data-centric, and flexible models.

Shifting the paradigm of thought towards deterrence in the gray zone is needed to address the threats where they exist. Gray zone threats can exist across all domains and require an alliance-wide strategy and cohesion in order to stay prominent in a world that is becoming more multipolar. Yet this is easier said than done. Responding to gray zone strategies requires the ability to quickly attribute the aggressor and find a proportional response that does not raise the specter of conflict, creating more instability. President Biden highlighted this difficulty on the eve of Russia's invasion of Ukraine in February 2022. He stated that Russia would pay a "serious and dear price" were it to invade Ukraine, but followed with, "what you're going to see is that Russia will be held accountable if it invades and it depends on what it does. It's one thing if it's a minor incursion, and then we end up having to fight about what to do and not do etc."² It showed that currently NATO does not have an active strategy towards gray zone operations. How does the Alliance respond to threats or conflicts that fall below the level of full war? The Biden Administration later clarified the President's response stating, "The Russians have an extensive playbook of aggression short of military action, including cyberattacks and paramilitary tactics. And [Biden] affirmed today that those acts of Russian aggression will be met with a decisive, reciprocal, and united response."³

NATO knows how to respond to threats in any conventional capacity, yet once the threat falls into the gray zone any strategy becomes subjective, muddled, and scattered. This dissertation will guide through the challenges NATO faces operating in the gray zone,

¹ Stoker, D., & Whiteside, C. (2020). BLURRED LINES: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. *Naval War College Review*, 73(1), 12–48. <https://www.jstor.org/stable/26868211>

² Braw, E. (2022, January). Biden's gray zone gaffe highlights real dilemma. *Defense One*. Retrieved from <https://www.defenseone.com/ideas/2022/01/bidens-gray-zone-gaffe-highlights-real-dilemma/360982/>

³ Ibid

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

particularly through deterrence building. Looking at deterrence through a versatile lens that allows it to be an effective tool across domains, and flexible enough to apply to various threats. It will analyze the role NATO plays in the rapidly changing global dynamics of conflict and how a fluid approach to deterrence is the most efficient and optimal solution.

To begin, this dissertation will analyze the history of operational domains, their evolution, and how NATO can adapt effectively. Warfare has evolved significantly throughout human history, driven by advancements in technology and the expansion of operational arenas. From ancient battlefields to modern cyber conflicts, the fundamental objectives of war remain unchanged, though the theaters of operation have diversified. Recent decades have seen further expansion into new domains such as space and cyberspace, fueled by rapid technological growth. NATO has adapted to these evolving challenges by embracing a multi-domain operational strategy, which includes land, sea, air, space, and cyber. This approach aims to leverage the alliance's collective strengths to enhance deterrence, ensure interoperability, and boost resilience against a spectrum of threats.

Furthermore, this dissertation explores deeper the theory and practice around the gray zone and the complexities of modern hybrid warfare, where the lines between conventional and irregular warfare blur, creating a continuous spectrum of conflict known as the gray zone. This introduction to the realm of gray zone conflict explores NATO's evolving strategy to cope with the indistinct nature of contemporary threats, where adversaries, notably Russia and China, utilize tactics that blend political, military, and informational means to achieve their goals without triggering a full-scale military response, known as the stability-instability paradox. Additionally, these actions challenge NATO's traditional military deterrence creating a situation that follows closely to the boiling frog analogy: slowly escalating tensions that need careful management to prevent sudden, uncontrollable escalations.

In order to determine the future of NATO deterrence it is imperative to analyze and evaluate the current state of the Alliance's defense capabilities. Each member has strengths and weaknesses when it comes to the current state of defense, as well as the debate around boosting capabilities and in what form. This highlights the approach the Alliance takes

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

towards “deterrence by denial”, which denies an adversary the opportunity to begin aggression, which differs from other approaches like compellence which deters aggression after it has started. The necessity for a robust evaluation of NATO's current deterrent capabilities and strategic investments is emphasized, recognizing that the alliance must bolster its defenses, particularly on its Eastern flank, to effectively counter the growing influence and aggression from Russia and the strategic recalibrations necessary for countering China’s rise. This aims to provide a comprehensive assessment of NATO's readiness and strategic positioning, urging an evolution of capabilities and tactics to safeguard against both the visible and the veiled threats of the current geopolitical era.

In the complex arena of contemporary warfare, NATO faces nuanced challenges on its Eastern Flank, particularly from the persistent threats posed by Russia and the strategic machinations of China. The evolution of NATO's deterrence strategy has become imperative, as traditional military approaches must now accommodate the subtleties of gray zone tactics and hybrid warfare, highlighted by the hard lessons learned from engagements in Afghanistan, Iraq, Libya, and Kosovo. The 2014 annexation of Crimea by Russia served as a stark reminder of the need for heightened vigilance and preparedness, catalyzing NATO to bolster defenses from Estonia to Bulgaria and reevaluate its strategic posture against both conventional and non-conventional threats. The strategic lessons from NATO's extensive operational history, including the protracted conflicts in Afghanistan and Iraq, reveal critical insights into alliance dynamics, the importance of cohesive action, and the challenges of political and military integration.

Next, as NATO faces the evolving nature of threats at its borders and beyond, interoperability emerges not merely as a technical or procedural alignment but as a multifaceted strategy vital for the effective execution of collective defense measures. It encompasses technical, procedural, human, and information dimensions, each integral to fostering a cohesive and agile military response under the umbrella of the alliance. The varied military assets and doctrines of NATO's expanded membership, especially with the inclusion of Eastern European states, underscore the urgent need for standardized approaches that respect diverse capabilities and strategic cultures. NATO's pursuit of interoperability is not just about seamless operational integration; it's about transforming

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

the alliance into a more coherent entity capable of preemptive and reactive measures in the murky waters of gray zone tactics.

Challenges to interoperability are multi-dimensional. Technically, the alliance grapples with integrating legacy systems from the Cold War era with cutting-edge technologies like the F-35 jets. Procedurally, there's a continuous effort to synchronize doctrines and operational plans across different military structures, while the human aspect involves enhancing communication and joint decision-making capabilities among forces with different languages and cultural backgrounds.

This concludes with the future of NATO and the evolving nature of threats, especially with an aggressive Russia and growing China. As the global landscape transforms into a multipolar world, NATO faces a spectrum of emergent threats that blur the lines between conventional military engagement and the nebulous realm of gray zone conflicts. As artificial intelligence, robotics, and cyber capabilities advance rapidly, they represent a double-edged sword—offering both immense potential and unprecedented challenges. The thawing Arctic emerges as a new frontier in geopolitical tension, presenting a crucible for conflict over untapped resources and strategic territories, further complicated by the interests of global powers such as China, which assertively seeks a role in Arctic affairs despite its geographical distance from the region. NATO's relevance in this multipolar world hinges on its ability to anticipate and adapt to the gray zone challenges posed by emerging technologies and global power shifts. It will explore how enhancing interoperability and strategic foresight can fortify NATO's deterrence capabilities, ensuring it remains a pivotal force in maintaining international stability amid the complexities of the 21st century.

III. The Evolution of NATO's Operational Domains

Introduction

War has been a part of humanity throughout the history of our existence. Warfare has adapted and evolved over generations with the increase in technology and area. From the Greek Phalanx and chariot of the Shang dynasty to the aerial drones and nuclear weapons of today, the goals of war have stayed the same, but the domain of which they operate has evolved. The very first operational domain was land; the domain of cavalry, artillery, troop columns, forts, and archers. Eventually with the expansion of ship building warfare moved into the domain of the sea; from the Homeric epic *The Odyssey* showing the Greeks versus the Trojans and the power of naval warfare. Naval warfare expanded warfare geographically, allowing quicker access for empires and nations to expand. For most of human history the domains of operation remained on land and sea. It was not until the beginning of the 20th century that air power became the new domain of operation, starting with the Italo-Turkish War in 1911 and expanding with the First World War in 1914.⁴

More recently, the domains have expanded further matching the rate of technological growth. Aerial warfare evolved beyond its potential with the advances in space technology. With humans having access to outer space, tools of war were quick to follow, bringing space into the domains of operation. The United States even became the first country to designate an entire branch of the military to the space domain. Soon after with the advent of the internet, the cyber realm penetrated every part of the globe. Computers became tools and targets of war due to their growing importance to everyday life and the functioning of society. Cyber warfare became the most recent domain of operation and one that has become the most difficult to define and operate.⁵

⁴ Biddle, T. D. (2019). *AIR POWER AND WARFARE: A CENTURY OF THEORY AND HISTORY*. Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep20093>

⁵ Crowther, G. A. (2017). The Cyber Domain. *The Cyber Defense Review*, 2(3), 63–78. <http://www.jstor.org/stable/26267386>

The NATO alliance has prioritized all five of these domains as areas of operation and terms it: the multi-domain. The multi-domain is leveraging power in land, sea, air, space, and cyber in order to establish deterrence, build resilience, facilitate interoperability, and enhance capabilities. Throughout the life of NATO, the domains of operation have remained relatively static and the focus has been on boosting land, sea, and air capabilities to a level that no adversary could ever challenge the alliance. Deterrence by denial has been the center of how NATO has functioned, focusing on building military capabilities in the land, sea, and air domains. This chapter will look at how NATO has developed each domain of operation and analyze how it has adapted and needs to adapt further to the graying of conflict.

Land, Sea, and Air

The land domain is the oldest domain in operation and contains the more traditional elements of warfare even as it has changed over generations. Land power is defined by the United States Army as, “the ability—by threat, force, or occupation—to gain, sustain, and exploit control over land, resources, and people.”⁶ This requires the ability to execute long-term, high-powered operations, often multinational, while consolidating gains, and protecting populations. Land operations are repetitive and continuous and can cover large geographic areas.⁷ The diversity of terrain requires land forces to be able to adapt to any environment whether desert, cold weather, forest, or mountains. Land forces pay special attention to civilian populations as well as resources in the area. Additionally, land forces need to be able to deploy quickly, act with versatility, and sustain operations as long as possible.⁸

Adapting NATO land operations into the modern era requires attention to interoperability, as well as enhancing military capabilities that provide deterrence,

⁶ U.S. Army. (2016). *ADRP 3-0: Operations*. Retrieved from <https://usacac.army.mil/sites/default/files/publications/ADRP%203-0%20OPERATIONS%2011NOV16.pdf>

⁷ Ibid, 9

⁸ Ibid, 10

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

specifically along NATO's Eastern Flank in the Baltic States and Poland. This dissertation will analyze the current military capabilities of each NATO member state, as well as the changes needed to adapt to gray zone strategies, and streamlining the interoperability of a 32-nation defense alliance. The land domain requires a high-functioning interoperability within the alliance, including standardization and infrastructure to give land forces the ability to move rapidly and respond to threats, and for the alliance to work cohesively.

The sea domain is almost as old as the land domain and has evolved into a powerful domain responsible for power projection. The sea domain has worked in tandem with the land domain, and their shared yet unique abilities have been proven as effective models in targeting threats. For example, the Allied invasion of Normandy during World War II in 1944 exemplified the ability of the sea and land domains working within a multinational force to achieve goals. This should be an example and lesson for the future in the era of multi-domain conflicts where the mixture of land, sea, air, space, and cyber will need to work together to facilitate defense and security.

In NATO the naval domain functions as a deterrent through its ability to show its ability to react if needed and demonstrating power in a region if the need to respond arises.⁹ The naval forces of NATO have the flexibility to adapt to low-intensity to high-intensity missions if needed and have sub-surface to above-surface capabilities if faced with conflict.¹⁰ The naval domain has evolved into a portion of the nuclear triad, which offers stealth capabilities to the alliance, as well as the ability to rapidly engage power projection. Similar to the land domain, naval warfare is still important in the modern era but needs to enhance interoperability as well its deterrence capabilities towards every growing threat, specifically China and its expansionist desires.¹¹ Even though land and sea domains are essential to NATO operations, adapting to the ever-evolving technology and threats requires finding new domains to deter future threats.

⁹ NATO. (2023, August 3). *NATO's Maritime Activities*. Retrieved from https://www.nato.int/cps/en/natohq/topics_70759.htm

¹⁰ Ibid

¹¹ Patalano, A. (2024). Naval Power: The Key to Understanding U.S.-China-Russia Relations. *Time*. Retrieved from <https://time.com/6836406/naval-power-us-china-russia/>

The aerial domain is becoming one of the most recognizable areas of operation today. Aerial operations have involved strategic airstrikes, air superiority, bombing campaigns, strategic lift, as well as logistics and supplies.¹² Ever since World War II, warfare has centered around maintaining air supremacy, and having the capabilities of denying air access to adversaries.¹³ With the modern evolution of no-fly zones and air supremacy, air power has been shown to be a centerpiece to any military operation and an important component of multi-domain operations. Additionally, the air domain is only growing in importance and ability. The expansion of unmanned drones has allowed air operations to expand with less risk, forcing militaries around the world to expand their own drone programs and invest in more efficient air defense systems.¹⁴ Air technology has evolved so quickly and so much that it has the capacity to bring humans to space. As a result, satellites and spaceships are becoming components in operational domains, which has resulted in a new domain to be created.

The traditional domains of operation are essential pillars to NATO's deterrence. The ability to deploy quickly, and sustain operations for extended periods of time is essential to proper deterrence. NATO standardization is needed to bring these systems together to operate without interruptions or miscalculations. The graying of conflict only heightens this need, as the threat is harder to define, harder to respond to, and the risks are greater. The two new domains—space and cyber—are emblematic of the graying of conflict, and show how the best deterrence in the future is the ability for the multi-domain to work together.

Space: The Final Frontier?

The United States is currently the only country within NATO (and the world) with a specified and equal branch of the military dedicated to the space domain. Though much of the United States' Space Force roles are just a separation from the previous responsibilities

¹² Francis, E. T. (2020). Air Supremacy in Airpower Doctrine. In *A House Built on Sand: Air Supremacy in US Air Force History, Theory, and Doctrine* (pp. 6–13). Air University Press. <http://www.jstor.org/stable/resrep24881.7>

¹³ Ibid, 17

¹⁴ Ibid, 18

of the US Air Force, it signals a commitment to the importance of the space domain.¹⁵ In 2019 the alliance “adopted NATO’s Space Policy and recognized space as a new operational domain”.¹⁶ The recency and novelty around space policy needs room for further interaction and growth, much of which is restricted by technological developments. But a 21st century space race is occurring whether NATO recognizes it or not, the future competition for information and technology leads to space and it is important to be active in its potential. The creation of the Space Force in the US was a reaction to this, as other actors like Russia and China are actively pushing for a heightened presence in space.¹⁷ Much of the appeal of space as a final frontier for states is the economic advantages it could unleash. China has heavily invested, through its Space Information Corridor and Digital Silk Road, a 30-year plan looking to generate \$10 trillion from cislunar economic and industrial plans.¹⁸

According to the 1967 Outer Space Treaty, states agreed to the peaceful use of space for the common interest of all mankind. It emphasizes the benefit of scientific research and its universal application, but also importantly the agreement towards disarmament by not allowing any nuclear weapons or other weapons of mass destruction in space.¹⁹ But what is not explicitly covered is the potential for economic activity and the exploitation of space resources, which could lead to outer space becoming a frontier for world powers to compete once again, potentially leading to military means.

This opens up outer space as a potential domain of operation, and a priority for NATO. While weapons of mass destruction are not allowed by treaty, the militarization of space for defense purposes is not banned, allowing opportunities for states to bolster deterrence. The side-effect of this is the creation of a potential arms race, emblematic of the

¹⁵ Farley, R. (2020). *Space Force: Ahead of Its Time, or Dreadfully Premature?* Cato Institute. <http://www.jstor.org/stable/resrep28729>

¹⁶ NATO. (2023). NATO - Topic: NATO and the 2030 Agenda for Sustainable Development. https://www.nato.int/cps/en/natohq/topics_175419.htm

¹⁷ Sadat, M. (2020). Space: New Threats, New Service, New Frontier An Interview with Mir Sadat. *Strategic Studies Quarterly*, 14(4), 6–17. <https://www.jstor.org/stable/26956150>

¹⁸ Ibid, 7

¹⁹ Peperkamp, L. (2020). An Arms Race in Outer Space? *Atlantisch Perspectief*, 44(4), 46–50. <https://www.jstor.org/stable/48600572>

space and arms race of the Cold War, yet with more advanced technology.²⁰ The current strategic importance for space is focused around satellites and modern society's reliance on them. Military, economic, scientific, and societal life has become highly dependent on the use of satellites, thus the defense of these systems is of prime importance to the alliance and society at large.²¹ Militarily, much of the future of space warfare is dependent on the expansion of technology, which is not yet achieved, but steadily growing.

The current trajectory for space as a domain of operation is based more on economic, logistic, and intelligence operations rather than actual warfare, but that can quickly change with growth in missile technology.²² Yet due to the reliance on satellite technology to bolster current domains of operation, the true threat comes from cyber-attacks and the alliances' ability to respond. The cyberspace is the true frontier to be explored in the current era, as it has the greatest potential to disrupt all the other domains. The space domain is highly relevant and important and requires a strategic outlook and integration for the future, but paired with the cyber domain, the multi-domain becomes ever more important for NATO to operate and establish a strategic advantage.²³

The Cyber Domain as the Gray Domain

Cyber warfare is growing as a threat faster than states are able to adequately address it. The current state of cyber operations is centered around reactionary operations rather than getting ahead of the threat.²⁴ This causes a unique challenge to deterrence as it becomes difficult for NATO or member states to retaliate or attribute the cyber-attack, leaving the threat in the gray zone for too long and raising the bar of instability. As a result of this uncertainty in the cyber domain NATO has begun to take actions to get ahead of the threat, but still requires more investments to be sustainable and act as a deterrent.

²⁰ Ibid, 48

²¹ Farley, R. (2020). Pp. 3.

²² Sadat, M. (2020). Pp. 13.

²³ Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). THE EVOLUTION OF SPACE AS A CONTESTED DOMAIN. In *ESCALATION AND DETERRENCE: IN THE SECOND SPACE AGE* (pp. 1–9). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23194.3>

²⁴ Shea, J. (2017). How is NATO Meeting the Challenge of Cyberspace? *PRISM*, 7(2), 18–29. <http://www.jstor.org/stable/26470515>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

The cyber domain was added as a NATO operation in 2016 at the Warsaw Summit. This was due to cyberspace attacks within the alliance forcing it to enact cyber defense as a domain of operation. This has now included cyber-attacks as a core task of NATO's collective defense as stated in the Warsaw Summit Communiqué.²⁵ With this elevation of cyber in the domain of collective response it places more emphasis on the challenges of interoperability within NATO, and the need to streamline this communication to respond appropriately to these threats. NATO installed an affiliate center focused on cyber security in Estonia in order to focus on cyber defense research and training so that cyber defense has an elevated status in the NATO structure.²⁶ The cyber domain exploits the idea of the gray zone in modern warfare, which is defined as the ambiguity that exists in modern warfare where attribution is lacking and response is varied. The gray zone as Robert Hoffman defines: "Instead of separate challenges with fundamentally different approaches (conventional, irregular, terrorist), we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously."²⁷ Modern warfare is increasingly becoming hybrid and requires myriad responses and adaptations from NATO in order to navigate this gray zone.

This heightening of gray zone operations has required NATO to prioritize the cyber sphere into offensive capabilities.²⁸ NATO has a reputation of moving major initiatives at a rate of 10-15 years, and as large chunks or platforms. Instead, in regards to cyber capabilities, NATO should transition the culture to become more evolutionary, where it is constantly upgraded with incremental investments in informational technology on a much more frequent basis.²⁹ Since cyber threats are growing quickly and occurring more often, it is important to treat the threats as such, and invest quickly to respond. Debate around the extent of cyber-attacks remains, whether they are as infiltrating as perceived, or just a broader version of espionage and sabotage, regardless, the threat is present and is only

²⁵ NATO. (2016). *Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

²⁶ CCDCOE (n.d.) *About us*. (n.d.). <https://ccdcoc.org/about-us/>

²⁷ Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *Joint Force Quarterly*, 52, 35.

²⁸ Shea, J. (2017). Pp. 21

²⁹ *Ibid*, 21

increasing. US Air Force Lieutenant General VeraLinn Jamieson stated, “Right now, today, in the cyber domain, in information operations, I am not at peace. I am in persistent conflict.”³⁰ Additionally, a Russian diplomat was quoted saying, “The war [in cyberspace] is underway and unfolding very intensively. No matter how hard we may try to say that all this is disguised and that it isn’t that war or this war, in actual fact, military activities in cyberspace are in full swing.”³¹

The potential threat of a cyber-attack on NATO could be immense; a single attack could lead to billions of dollars of economic damage to a member state, or also disrupt the alliance’s logistics and forward operations.³² Compared to the land, sea, air, and even space domains, cyber is not constrained by geography or national borders, therefore it becomes difficult to ascertain whether it is an internal or external security threat.³³ Due to this unique threat and obtuse maneuverability, the cyber domain becomes a main feature of the gray zone, and a primary actor. This additionally allows potential adversaries to exploit the cyber domain in order to test NATO’s deterrence and resilience. Even though cyber-attacks are covered by Article V collective defense, it is still difficult to respond appropriately due to the lack of attribution, and time required to investigate the aggressor’s identity.³⁴

The cyber domain truly represents the gray domain primarily due to the uncertainty it creates around attribution. While attribution is possible to discover, it is complex, and time-consuming, and requires investments in resources that may or may not be readily available.³⁵ Attribution thus becomes a matter of political will, and what resources governments want to invest in order to address it.³⁶ Not only does attribution create a hurdle to deterrence in the gray zone, but also the act of deniability. Even if a state (or non-state actor) is attributed for the attack, they can easily resort to deniability, as often occurs, which

³⁰ Waterman, S. (2019, September 19). Cyber Flight Plan Outlines USAF Efforts to Take on Hybrid Warfare. *Air Force Magazine*. Retrieved from <https://www.airforcemag.com/>

³¹ Tass News Agency. (2021, December 16). Full-blown warfare in cyberspace in progress, says Russian diplomat. Retrieved from <https://tass.com/world/1376491>

³² Ifimie, I. A. (2020). *NATO’s needed offensive cyber capabilities*. NATO Defense College. <http://www.jstor.org/stable/resrep25100>

³³ Ibid, 2

³⁴ Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections*, 15(2), 109–119. <http://www.jstor.org/stable/26326443>

³⁵ Ibid, 114

³⁶ Ibid, 114-115

then minimizes the ability to respond due to the need for overwhelming evidence that will be scrutinized by the international community.³⁷

Furthermore, the cyber-gray domain matrix is exemplified further due to lack of international law addressing the topic, but additionally grays the definition of an attack due to lack of attribution as well as the recipient and extent of the attack. This brings up the concept of state sovereignty and whether a cyber-attack would fit the definition of a conventional attack and its interference to another state's sovereignty.³⁸ Within the alliance structure of NATO it becomes a delicate decision-making process when concocting a response, because it would require support from state's outside the alliance and suitable evidence to show attribution, or else find itself in a quagmire like the Iraq War where there was not sufficient international support for the operation.³⁹

In order to get ahead of the growing gray zone, the NATO alliance needs to make the cyber domain a priority and invest in more strategies and infrastructure to build deterrence and to engage countermeasures. Essentially, this requires a boosting of state capacity, which is a necessity of each member state, but especially those with already established cyber infrastructure like the United States, United Kingdom, France, the Netherlands, and Estonia.⁴⁰ Or using a whole-of-alliance approach where burden-sharing and cross-investments can build the capacity of states with established comparative and strategic advantages. As the world begins becoming more multipolar, the threats will continue to be more diverse and range within a spectrum of conflict creating difficulty for how the alliance can respond. This multipolar world creates a graying of conflict seeking to threaten the status quo, and the use of the cyber domain becoming an increasing instrument in which the alliance needs to adapt.

³⁷ Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38, 30.

³⁸ Hill, A. G. (2019). Analysis. In *The Ultimate Challenge: Attribution for Cyber Operations* (pp. 13–24). Air University Press. <http://www.jstor.org/stable/resrep24884.7>

³⁹ MacAskill, E., & Borger, J. (2004, September 16). Iraq war was illegal and breached UN charter, says Annan. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2004/sep/16/iraq.iraq>

⁴⁰ Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*, 16(2), 5–24. <http://www.jstor.org/stable/26326478>

IV. The Gray Zone

The Graying of Conflicts

For the entire lifespan of NATO interoperability has been the *modus operandi* for targeting intra-organizational reforms and the main focus of cohesion building within the alliance. While incredibly important and a worthwhile pursuit, this dissertation pushes for a transformation of the concept and functionality of interoperability – pushing it to become a component of the multiple domains that NATO needs for its operational strategy. As previously stated the operational domains of NATO are: land, sea, air, space, and cyber. Space and cyber being relatively new additions and showing the rapidly increasing hybrid and irregular warfare the modern world occupies. Even though NATO was founded in the era of conventional warfare the reality has shifted and NATO has been forced to adapt to this new “gray zone” of modern warfare. The gray zone is the area between war and peace, where the lines of conflict are blurred and interpretations of the conflict become subjective because the motives and maneuvers are no longer clear. Gray zones work in tandem with hybrid warfare, but are distinct concepts that require parsing out.

NATO works efficiently within the credence of its founding as a powerful force in conventional warfare. Its deterrence capabilities come from the potential threat of a conventional war and thus outside threats would choose not to challenge this leviathan. Threats to NATO have adapted and challenged the alliance in different ways where the obvious red lines of conflict are blurred and plausible deniability can be leveraged. This is where the gray zone becomes a powerful tool for adversaries to challenge NATO, and where NATO is deficient in suitable and concise strategies to target these threats.⁴¹ NATO needs to recognize these new and diverse threats in doctrine or else perpetually be in an expensive and circular state of adapting to every new threat.⁴²

⁴¹ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

⁴² Gleiman, J. K. (2015). The American Counterculture of War: Supporting Foreign Insurgencies and the American Discourse of War. *Special Operations Journal*, 1(1), 19–36.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

Much of hybrid warfare contributes to the graying of conflict. When state actors' main adversaries are non-state actors, or try to create the appearance of a non-state actor as was seen by Russia in Crimea in 2014, or also the actions of Chinese power projection in the South China Sea. Another aspect is when an adversary may use conventional methods but does so in a clandestine way that avoids attribution and retribution.⁴³ The purpose of which is to create a gray area for the conflict to operate, causing NATO not to respond because plausible deniability prevents attribution. Moreover, this presents an additional challenge and speedbump to NATO's doctrine recognizing that, "prevention represents the best possible means of countering hybrid warfare", due to the difficulty of containing irregular threats after they occur.⁴⁴ For example, irregular warfare occurs when the military and political objectives become interwoven like in Vietnam in the 1960's where winning the support of the native population becomes an important and pivotal goal in fighting.⁴⁵ Therefore it is apparent for NATO to adjust from a solely conventional strategy to one that invests in hybrid threat prevention.

Going forward it becomes necessary for NATO to work towards clarifying the gray zone by adapting to threats that are short of war. The ambiguity that exists around gray zones and the response is also a factor towards the difficulty of creating strategies to prevent or deter conflict. The concept of a gray zone is ever expanding, or "expansive and elusive", as it cannot be agreed on what it actually entails or if it even exists.⁴⁶ Threats around the world and to NATO members have grown increasingly convoluted and within the realm of the gray zone. There was the "little green men" that invaded Eastern Ukraine and Crimea that Russia would not take credit for, there is the threat of ISIL in the Middle-East, Boko Haram in the Sahel and West Africa, the Russian interference in the 2016 United States presidential election, the 2007 cyberattacks against Estonia by Russia,

⁴³ Deep, A. (2015, March 2). *Hybrid War: Old concept, new techniques*. Small Wars Journal. Retrieved February 13, 2024, from <https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques>

⁴⁴ Pindják, P. (2014, November 18). *NATO Review - Deterring hybrid warfare: a chance for NATO and the EU to work together?* NATO Review. <https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html>

⁴⁵ Larson, E. V., Eaton, D., Nichiporuk, B., & Szayna, T. S. (2008). Defining Irregular Warfare. In *Assessing Irregular Warfare: A Framework for Intelligence Analysis* (1st ed., pp. 7–18). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg668a.10>

⁴⁶ Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM*, 7(4), 30–47. <https://www.jstor.org/stable/26542705>

Chinese island building with paramilitary maritime threats, and so many more follow this trend where the line between conflict and interference are blurred and how a victim reacts depends on how the threat was perceived causing future issues. Russia has learned that the best way to respond to multinational organizations like NATO is through these hybrid methods since it cannot challenge NATO conventionally. Putin operates with “a mix of hard and soft power with some military and non-military, choreographed to surprise, confuse and wear down an opponent, hybrid warfare is ambiguous in both source and intent” and by doing so NATO does not have the agility or capacity to respond quickly leaving it at a disadvantage.⁴⁷

Russian Operations in the Gray Zone

Russia has a long history of operating within the gray zone, and as a result NATO should be well adept at being able to identify and respond. Starting from the Soviet era there is a storied and accountable history of using state instruments to influence government officials and individuals. These techniques were known as, “*aktivnyye meropriyatiya* (active measures) and *dezinformatsiya* (disinformation)”.⁴⁸ This was a strategy to combine propaganda created by the Soviet or Russian state with the preexisting narratives in a different country in order to provoke distrust or “smear individuals”.⁴⁹ Much of this was able to play into the hands of the Red Scare during the Cold War that allowed the Soviet Union to play off the fears of the American and European governments around communism, which allowed disinformation measures easier to distribute and create.⁵⁰

From the Soviet or Russian perspective this is a useful strategy because it can start placing divisions in western alliances like NATO or the European Union. The use of disinformation begins to create new narratives over time that make the United States,

⁴⁷ Ibid

⁴⁸ Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4), 50–85. <http://www.jstor.org/stable/26271634>

⁴⁹ Ibid

⁵⁰ Cuordileone, K. A. (2000). “Politics in an Age of Anxiety”: Cold War Political Culture and the Crisis in American Masculinity, 1949-1960. *The Journal of American History*, 87(2), 515–545. <https://doi.org/10.2307/2568762>

primarily, look like an ineffective ally or unreliable partner. In the modern age much of this disinformation has migrated to social media and has been famously successful in its reach and impact. The biggest example of this technique and its pay-off for Russia was with the 2016 United States presidential election.

Social media manipulation and disinformation campaigns by Russia proved to be an influential operation within the hybrid system. Rather than provoking the United States directly the plan was to foment distrust in the population in hopes of boosting Donald Trump during the presidential election as he was viewed as a chaos agent that could help Russia's national interests, specifically disrupting the Western international order, like NATO and the EU. Russia created and funded an organization called the Internet Research Agency designed for "internet trolling" as its influence operation towards the US.

The American Security Project (ASP) investigated the extent of Russian meddling and discovered the Internet Research Agency received \$2.3 million in funding from the Russian government and had a team of 90 workers just on the US influence team alone. The ASP linked content posted on social media and web browsers like Twitter, Facebook, Google, and Bing designed to go viral that would "aggravate tensions across the political spectrum."⁵¹ Beyond social media and the internet the Internet Research Agency also secretly funded groups in the US to organize rallies and protests to create the appearance of discord. One way was to fund Black groups in self-defense classes to create a sense of hostility and fear around racial tensions, and as a way to connect these groups to Black Lives Matter to give the appearance of being violent.⁵² Russia also creates government funded news organizations that produce Russian propaganda for an international audience, like RT (Russia Today) and Sputnik, who publish pro-Russia messages into the West as well as slanted news coverage to create distrust of Western audiences of their own government.⁵³

The American response to this interference highlights the difficult nature around responding to hybrid threats and gray areas. The Obama administration responded in a

⁵¹ Savage, P. (2017). *Russian Social Media Information Operations: How Russia has Used Social Media to Influence US Politics*. American Security Project. <http://www.jstor.org/stable/resrep06042>

⁵² Ibid

⁵³ Ibid

limited way out of fear of sparking a larger cyber conflict with Russia, and also giving a political weapon to Donald Trump who could claim that the Russian interference accusation is an attempt to discredit his campaign by the Democrats.⁵⁴ The Obama administration attempted to placate this worry by releasing the intelligence to Congress in hopes of having a report produced that was bipartisan from Democrats and Republicans, but the Senate Majority Leader at the time, Mitch McConnell, Republican from Kentucky, stated that he will not be a part of the release and will claim partisanship from the administration if it is released.⁵⁵

Forced to deal with the issue alone, President Obama—three weeks before Trump was to be inaugurated—expelled thirty-five Russian “intelligence operatives” and pushed new sanctions on Russian agencies, closed Russian facilities in the US, blocked Russian news sites, and sanctioned individuals believed to be connected.⁵⁶ Retrospectively, these measures did very little to counter the Russian threat, mostly due to the inability for the government to work together to address the issue and without the support of Congress, President Obama was limited in his options.⁵⁷ But the damage was already done and the growing rise of distrust in the United States became evident and the questioning of democratic principles and belief in its own intelligence community questioned. The information warfare that exists is part of a broader hybrid warfare and irregular threats that NATO and member states need to navigate. The Obama administration stated that Russia views information warfare as a “domain of warfare on a sliding scale of conflict that always exists between the US and Russia.”⁵⁸ This raises questions of how NATO should respond to threats, especially with the elevation of cyber as a domain of operation, and whether Article V could be triggered.

⁵⁴ Blackwill, R. D., & Gordon, P. H. (2018). The U.S. Response—Obama, Trump, and Congress. In *Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge* (pp. 10–14). Council on Foreign Relations. <http://www.jstor.org/stable/resrep21423.8>

⁵⁵ Ibid

⁵⁶ Ibid

⁵⁷ Boot, M., Kirkpatrick, J. J., & Bergmann, M. (2019). *Defending America From Foreign Election Interference*. Council on Foreign Relations. <http://www.jstor.org/stable/resrep29933>

⁵⁸ Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4), 50–85. <http://www.jstor.org/stable/26271634>

The Stability-Instability Paradox

Raising a threat from a gray area into a conventional war is not in the interest of an adversary, especially one that knows it exists at a disadvantage from the power it is threatening. This is a major reason NATO was established – deterrence by denial – where NATO is seen as steadfast and strong where other global or regional powers would not threaten due to their power disadvantage. This is where conflicts within the gray area become useful and adversaries looking to threaten or weaken NATO would look to exploit rather than challenging NATO directly. The famous Prussian General Carl von Clausewitz stated, “war is merely the continuation of policy by other means,”⁵⁹ and as the power deficit has existed between NATO and Russia or NATO and China, raising the standard of a conflict as close as they can to conventional war without crossing it would be in their interests to continue their policies and national interests to rebalance global power.

This balancing act within the gray area becomes the main strategy to challenge NATO. How can a state raise the standards of a conflict enough to avoid moving from gray area into direct conflict. States must create gray zone strategies in order to push instability while also making sure the conflict remains stable and not a conventional war. These gray zone strategies look to achieve goals “*without* escalating to overt war, *without* crossing established red lines, and thus *without* exposing the practitioner to the penalties and risks that such escalation might bring.”⁶⁰ Therefore a conflict can be avoided if one actor or state chooses not to escalate, but as a result of not escalating, has now established a new threshold for the conflict to exist. This is because a challenger to the larger power is seeking to change the status quo whereas the larger power wants to preserve the status quo, but the challenger knows the larger power has an advantage at higher levels of conflict, thus

⁵⁹ Clausewitz: *War as Politics by other Means* | *Online Library of Liberty*. (2003). <https://oll.libertyfund.org/pages/clausewitz-war-as-politics-by-other-means>

⁶⁰ Brands, H. (2016, February 5). Paradoxes of the Gray Zone. *Foreign Policy Research Institute*. (emphasis in the original)

incentivizes the challenger to operate at a lower-level conflict, within the gray zone, this being known as the stability-instability paradox.⁶¹

The stability-instability paradox is rooted from the ideas of power transition theory, where cross-benefit analysis of international actors find that the reward to changing the international status quo is higher than maintaining it due to the inequality of power and resource distribution within the current system.⁶² This paradox becomes more apparent between nuclear powers, as in the case of NATO and Russia or NATO and China, due to mutually assured destruction from nuclear weapons direct conflict decreases (stability), but small scale conflicts or indirect conflicts increase (instability).⁶³ Thus NATO needs to focus more on a holistic approach to interoperability and deterrence as a way to navigate the multitude of hybrid conflicts that could be presented in the gray zone.

The growth of this low-level conflict instability comes from the unequal distribution of power and resources at the international level. One state, or alliance, grows faster than others and the old distribution network no longer equalizes benefits like before, so the weaker power seeks a change in the status quo.⁶⁴ This is also true if the power differential is not as large, but the *perception* of the differential exists. Assuming actors are rational, a leader might perceive the power imbalance to be greater than it is or that the distribution of power to be diverging, which can create insecurity.⁶⁵ This has been noted, and stated by Russian President Vladimir Putin, about NATO encroaching closer to Russia.⁶⁶ But the power differential between Russia and NATO is still too great, and works as a deterrence from Russia challenging NATO directly, so as a result Russia felt empowered to invade

⁶¹ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

⁶² Ibid, 25

⁶³ Jervis, Robert (1979). "Why Nuclear Superiority Doesn't Matter". *Political Science Quarterly*. **94** (4): 617–633. doi:10.2307/2149629

⁶⁴ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

⁶⁵ Ibid, 26

⁶⁶ Sullivan, B. (2022, February 24). How NATO's expansion helped drive Putin to invade Ukraine. *NPR*. <https://www.npr.org/2022/01/29/1076193616/ukraine-russia-nato-explainer>

Ukraine conventionally because it believed it had a stronger power differential and could succeed, while also sending a message to NATO.

Since World War II the rate of territorial aggression has decreased mostly due to the high costs accrued. This comes from the higher risks of nuclear aggression, but also from more advanced tactics from insurgents and the technologies associated.⁶⁷ This leads to the increase of gray zone conflicts as countries do not want to take on the excessive costs of adventurism. But the purpose of gray zone strategies and the use of proxies is to convey globally that a state has more power than actuality. Russia chose to invade Ukraine because it is a bordering state that is not within NATO nor the EU, formerly in Russia's sphere of influence and quickly moving away. To bring back its glory and distract from the diverging global powers, Russia invaded Ukraine in hopes of challenging the status quo, have the West take it seriously, and prove that it can succeed outside of the gray zone. But from what has been seen so far, that has not worked in Russia's favor.

The Russian Calculus

Russia has lofty regional goals where it is looking to rebuild and strengthen its sphere of influence in Eastern Europe and Central Asia. In order to obtain these goals Russia needs the economic and military strength to enable this. But Russia does not have the economic might to achieve this, as seen through its gray zone operations, and due to its perception of power imbalances and its perceived need to invade Ukraine. Economically, Russia cannot compete with the United States and the European Union, and would struggle with promoting regional power. Mark Galeotti has observed that Russia is, “a country with an economy somewhere between the size of Italy's and Brazil's [and] is seeking to assert a great power international role and agenda.”⁶⁸ This raises the question of how much can

⁶⁷ Mazarr, M. J. (2015). UNDERSTANDING GRAY ZONE CONFLICT. In *MASTERING THE GRAY ZONE: UNDERSTANDING A CHANGING ERA OF CONFLICT* (pp. 55–78). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep12018.9>

⁶⁸ Galeotti, M. (2015, April 16). "Hybrid War" and "Little Green Men": How It Works and How It Doesn't. *E-International Relations*.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

Russia heat up conflict with NATO in the gray zone before NATO is forced to respond; how much instability can be created to achieve a new level of operation?

Given the power differential between Russia and NATO it becomes curious as to why Russia started a conventional conflict with a NATO-membership seeking country unless Russia had another motive of seeking to change the international status quo, or reclaim past power status. One reason rising or declining powers seek conflict, whether aggressive or gray zone strategies, is due to a slowdown in economic growth⁶⁹, the perseverance of Cold War era alliances⁷⁰, and rising nationalism.⁷¹

Michael Beckley approximates that Russia has gone through two eras of rapid industrial growth that have transitioned to slower growth as well as comparing it to other countries. His research shows that Russia began its first transition starting in 1899, from there the economic growth began to decline for seven years to 50% less than it was the preceding decades. Russia after 1899 then follows an era of revolution, civil war, and expansionism. The next era of Russian economic decline begins in 2007, where the Russian state also pursues expansionism with aggression into Georgia, and then Ukraine.⁷² While Russia's economy is expected to grow over the next few decades it is projected to still be the weakest of the great powers (US, EU, China, and India), much of this is due to being too resource dependent coupled with high levels of inequality.⁷³ On the other hand, Russia is successful in creating perceptions of economic stability through economic capture, where it exerts economic influence over countries like Bulgaria, Latvia, Hungary, Serbia, and Slovakia where 11 to 22 percent of their GDP comes from Russia.⁷⁴ As a result of that, pro-

⁶⁹ Beckley, M. (2023). The Peril of Peaking Powers: Economic Slowdowns and Implications for China's Next Decade. *International Security*, 48(1), 7–46.

⁷⁰ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

⁷¹ Laruelle, M.. (2014). Russian Nationalism and Ukraine. *Current History*, 113(765), 272. Retrieved from https://online.ucpress.edu/currenthistory/article-pdf/113/765/272/412111/curh_113_765_272.pdf

⁷² Beckley, M. (2023). The Peril of Peaking Powers: Economic Slowdowns and Implications for China's Next Decade. *International Security*, 48(1), 7–46.

⁷³ Helm, B., Smeltz, D., & Burakovsky, A. (2020). *US Experts Anticipate Future Decline for Russia Among the Great Powers: They Forecast Diminishing Russian Influence and Stagnating Economic and Military Strength*. Chicago Council on Global Affairs. <http://www.jstor.org/stable/resrep26631>

⁷⁴ Clark, J. P., Pfaff, C. A., Burgess, K. J., Cuccia, P. R., Fleming, A. J., Graham, K. M., Gustafson, J. S., Hillison, J. R., Morrow, C. D., Mowchan, J. A., Thompson, D. C., & Wolfe, A. M. (2020). A STRATEGIC AND OPERATIONAL

Russia sentiments develop in all of these countries due to the economic perceptions in the country that Russia is good for economic growth. Additionally, 4 of these 5 countries are NATO members and, with the exception of Latvia, have started pushing back against material and economic support for Ukraine or look for closer ties with Russia. For example, Bulgaria's Prime Minister has accused the President of doing Russia's bidding⁷⁵, Hungarian Prime Minister Viktor Orban visited Moscow to reaffirm ties with Russia and discuss economic development⁷⁶, and the new Prime Minister of Slovakia, Robert Fico, campaigned on sending no more aid to Ukraine.⁷⁷ Russia's economic capture could lead to further strains on NATO's interoperability and deterrence which requires a reevaluation on its functionality.

Russia cannot rely on its economic capture forever due to other economic indicators that show the fragility of the Russian economy. Being a country that is overly reliant on petroleum and the growing renewable energy market shows limits to Russia's growth. Furthermore, the internal divisions inside Russia are pushing the limits of state capacity in galvanizing resources for a stratified populace. The soft power of Russia is declining and leaving it to be more a regional power to influence its borderlands, rather than globally.⁷⁸ Russia has tried to compete with Western powers for soft power (and hard power) influence throughout the world, but never has been able to compete with the Western alliance system since World War II. The Soviet Union created the Warsaw Pact as a means to counter NATO, but it was less solidified in its goals and operations, as well as lost members like Albania, which resulted in a weaker defense union.⁷⁹ Additionally, with the rise of the

ANALYSIS OF RUSSIA IN 2028. In *STRIKING THE BALANCE: US ARMY FORCE POSTURE IN EUROPE, 2028* (pp. 7–24). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep25429.7>

⁷⁵ Camut, N., Oliver, C. (2023, July 5). Bulgaria PM accuses president of doing Russia's bidding. *Politico*. Retrieved from <https://www.politico.eu/article/bulgaria-nikolai-denkov-pm-russia-influence-rumen-radev/>

⁷⁶ Reuters. (2023, October 17). Russia's Putin holds talks with Hungary's Orban, China. *Reuters*. Retrieved from <https://www.reuters.com/world/europe/russias-putin-holds-talks-with-hungarys-orban-china-2023-10-17/>

⁷⁷ NPR. (2023, October 1). Pro-Russia ex-premier leads party to win Slovakia parliamentary elections. *NPR*. Retrieved from <https://www.npr.org/2023/10/01/1202879797/pro-russia-ex-premier-leads-party-to-win-slovakia-parliamentary-elections>

⁷⁸ Helm, B., Smeltz, D., & Burakovsky, A. (2020). *US Experts Anticipate Future Decline for Russia Among the Great Powers: They Forecast Diminishing Russian Influence and Stagnating Economic and Military Strength*. Chicago Council on Global Affairs. <http://www.jstor.org/stable/resrep26631>

⁷⁹ Kramer, M. (2011). The Demise of the Soviet Bloc. *The Journal of Modern History*, 83(4), 788–854. <https://doi.org/10.1086/662547>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

European Union many former Eastern Bloc countries found Western appeal to be stronger and sought to join the EU over the Russian customs union.

With the creation of NATO in 1949, the military alliance has grown from 12 original members to 32 members today, spanning the North Atlantic into Eastern Europe. As a counterbalance to NATO, the Soviet Union brokered the creation of the Warsaw Pact consisting of 8 countries within the USSR's sphere of influence. The Warsaw Pact ceased to exist with the dissolution of the USSR, and Poland, Romania, Bulgaria, East Germany, Czechia, Slovakia, Hungary, Estonia, Latvia, Lithuania, and Albania joined NATO. The perseverance of NATO through the Cold War and after as it has adapted to the changing international stage has been a lasting problem for Russia as it tries to gain power and disrupt the status quo, forcing it into gray zone strategies.

Russia views the United States as its greatest geopolitical adversary, and as an extension NATO, which it sees as a product of American influence. The United States has been successful in maintaining a global network of alliances, has a leading role in the creation of the World Bank, International Monetary Fund, and the United Nations, as well as having the world's most extensive and capable military in the world.⁸⁰ As a result the United States has been able to leverage its military, institutional, and relational power to its advantage as countries like Russia and China seek to compete and alter this power balance.⁸¹ Conversely, the world has seen much less conventional war occur since the Persian Gulf War, and the United States has shown to be less effective in engaging low-level conflicts as well as having low public support for these campaigns, which emboldens adversaries to seek gray zone conflicts to challenge this power, thus feeding the stability-instability paradox.⁸²

Moreover, Russian nationalism has been fostering the desire for challenging the international system as it exists. Nationalism in Russia is nothing new, as it is for any country, but how it has developed and transformed has pushed it to be expansionary and

⁸⁰ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

⁸¹ Ibid, 27

⁸² Ibid, 28

irredentist, which pushes the state to engage in gray zone strategies to expand nationalism regionally, as well as globally. A glimpse into this comes the day Russia annexed Crimea and President Putin gave a speech linking the Russian people to an ethnic identity. He stated that after the dissolution of the Soviet Union, “the Russian people have become one of the most divided nations in the world, if not the largest.”⁸³ Though not referring to the multiethnic state of Russia itself, but rather the ‘ethnic Russians’ that are living in other countries, and by doing so used a Russian term reserved only for ethnicity and not nationality, showing a change of perception of what is now the newly perceived ethnonationalism.⁸⁴

This now opens the possibility for Russia to rationalize itself as the protector of Russian identity and people and can justify its imperialist excursions into other countries like Ukraine under the guise of protecting the ‘Russian people’. Now Russia can use this as a pretext to challenge other regional and global powers, as well as weaker neighbors, as a way to build back its prestige that it feels was unrightfully taken from it. Russia has already invaded Ukraine and annexed territory, it has threatened Moldova from becoming “anti-Russian” by maintaining 1,500 Russian troops in the unrecognized breakaway region of Transnistria⁸⁵, doubling the amount of troops near the border of Finland and stating the country “will be the first to suffer” if war breaks out with NATO⁸⁶, and also weaponizing immigration through the borders of Estonia and Finland.⁸⁷ All of these are either direct aggression or gray zone strategies used to create instability to further promote Russia’s interests. Russia has the ability to take direct action against non-NATO members like Ukraine, but only resorts to gray zones strategies when dealing with NATO members like Finland and Estonia. The Russian calculus breaks down to increasing the instability through

⁸³ Kolsto, P. (2016). The ethnification of Russian nationalism [PDF]. *The New Russian Nationalism*, 18–45.

⁸⁴ Ibid

⁸⁵ Ibraginova, D. (2023). How Russia Torpedoed its own Influence in Moldova. *Carnegie Endowment for International Peace*. Retrieved from <https://carnegieendowment.org/politika/89731>

⁸⁶ Starcevic, S. (2023, December 28). Russia warns Finland will suffer in latest saber-rattling. *Politico*. Retrieved from <https://www.politico.eu/article/russia-warns-finland-will-suffer-in-latest-saber-rattling/>

⁸⁷ Bryant, M. (2023, November 23). Estonia accuses Russia of weaponising immigration at Europe's borders. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2023/nov/23/estonia-accuses-russia-weaponising-immigration-europe-borders>

low-level conflicts to see how far it can push NATO without stoking the flames of direct conflict.

The Boiling Frog

The current question for the Atlantic alliance is how far has the gray zone developed and what is the current level of instability that could force a broader conflict. As countries like Russia and China continue to push gray zone strategies to test NATO and see how it responds it creates a new level of operation that is more tense but technically still at peace. Consequently, this further pushes the precipice of all-out conflict. Like the boiling frog analogy, the water slowly gets warmer and warmer until it reaches a boiling point and it is too late for the frog to escape and it finds its demise, the alliance is continuously pushed closer to conflict with each passive acceptance of gray zone conflicts which forces the decision of responding to stated red lines or falling to instability.

Furthermore, raising the level of instability moves slowly and undefined that the wider society never realizes there is even a new level of conflict, and so it becomes difficult for states to know how to activate strategies to mitigate the *heating* conflict. NATO is being pushed by gray zone strategies by many international actors trying to find weaknesses in the alliance and ways to disrupt the global status quo. Primarily this is being done by Russia, China, Iran, and North Korea, which all have similar yet distinct reasons to challenge the alliance. NATO is the frog in the progressively increasing boiling water and these countries are the ones turning up the temperature to challenge the alliance.

Russia, as previously discussed, has historically been pushing against NATO and warning against its expansion. NATO-Russia relations have been deteriorating for some time but reached a breaking point with Russia's annexation of Crimea in 2014, and then nearly complete in 2022 with the invasion.⁸⁸ After the invasion of Ukraine in 2022 NATO expanded membership with the addition of Finland and Sweden who felt threatened by an expansionist Russia. Finland and Sweden joining NATO was a major step in each country's

⁸⁸ Rühle, M. (2014). *NATO Enlargement and Russia: Die-Hard Myths and Real Dilemmas*. NATO Defense College. <http://www.jstor.org/stable/resrep10297>

foreign policy as they have been neutral for decades. Russia's decision to invade Ukraine upended the status quo in Europe and allowed for the Baltic Sea to colloquially become a "NATO Lake".⁸⁹ As a result, Finland's Security and Intelligence Service has warned of "increased threats" since joining NATO. Finland closed the border with Russia due to what they claim as "hybrid attacks" by pushing undocumented immigrants into Finland as one of the many gray zone strategies increasing tensions.⁹⁰ In Sweden as well, the government has notified its citizens to prepare for war now that its historical neutrality has ended.⁹¹ Russia is boiling the frog in Europe and looking to test the status quo to see how far it can go while still avoiding attribution. The key to the gray area is ambiguity, especially ambiguity around the final goal, and ambiguity around whether treaties or international norms have been violated.⁹²

This ambiguity is being perpetrated by Russia and probing NATO member states to heighten instability. While Sweden was in the process of acceding into NATO, there was an increase in GPS jamming in the Baltic Sea area. Aircrafts flying around the Baltic region have been experiencing varying degrees of signal interference that "spoof" the signal into misrepresenting an aircraft's true location. While not a new phenomenon it has been occurring almost every day in a significant and widespread way. Analysis into the jamming has shown that it can be traced back to Russian territory based on where aircrafts first experienced the spoofing and from when it ended. While Russia denies any involvement it has come at a conspicuous time when Poland has installed a new American-made air defense system, Sweden was in the process of joining NATO, and Russia's Baltic Fleet has been conducting electronic warfare drills off the coast of Kaliningrad.⁹³ This is a way to

⁸⁹ Deni, J. (2024). Is the Baltic Sea a NATO Lake? *Carnegie Endowment for International Peace*. Retrieved from: <https://carnegieendowment.org/2023/12/18/is-baltic-sea-nato-lake-pub-91263>

⁹⁰ Pohjanpalo, K., Rolander, N., Laikola, L. (2024, February 26). Finland and Sweden join NATO: What it means and how Russia has responded. *Bloomberg*. Retrieved from <https://www.bloomberg.com/news/articles/2024-02-26/finland-and-sweden-join-nato-what-it-means-and-how-russia-has-responded>

⁹¹ O'Dell, H. (2024). Why is Sweden telling its citizens to prepare for war? *Chicago Council on Global Affairs*. Retrieved from: <https://globalaffairs.org/bluemarble/sweden-tells-citizens-prepare-war-russian-aggression-nato-membership>

⁹² Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

⁹³ Goward, D. (2024). As Baltics see spike in GPS jamming, NATO must respond. *Breaking Defense*. Retrieved from: <https://breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond/>

respond to NATO against actions of which Russia does not agree, while also avoiding attribution. This way Russia can increase instability in the gray zone while also avoiding a broader conflict.

China also engages NATO in gray zone strategies. China has shown magnificent economic and military growth over the past 30 years and is now in a much stronger position to start testing the United States, and NATO, in order to expand its influence. Similar to Russia, China has expansionist goals as it relates to Taiwan, but also desires a sphere of influence in Asia and to prod the US/NATO alliances with Japan and South Korea. Also similar to Russia, China has an aging population, high inequality, and a fervent sense of nationalism that seeks to be promoted.⁹⁴ China's operations in the gray zone are much grayer than Russia's and work in a way that leverages its soft power, while also utilizing shows of military force, covert operations, and cyber tactics. Soft power has even become the defining feature of China's foreign policy.⁹⁵ Since the power dynamic between China and NATO exists, China would be unable to challenge NATO directly to disrupt the global status quo, thus China chose to adapt its foreign policy to circumvent American and NATO influence and sought to expand its soft power in various regions around the world. Soft power is viewed as, "the ability to obtain desired outcomes through attraction rather than coercion, or payment".⁹⁶ China uses its financial power as the world's second largest economy to attract other nations to its influence. It operates the Asian Infrastructure Investment Bank (AIIB) as well as the Belt and Road Initiative (BRI) that support investment projects around the world to help countries with economic development.

Additionally, China uses its soft power leverage to achieve expansionist aims, primarily in the South China Sea. China operates an almost campaign-like gray zone competition that integrates all aspects of national power that has yet to be challenged.⁹⁷

⁹⁴ Zhao, S. (2014). Foreign Policy Implications of Chinese Nationalism Revisited: the strident turn. In *Construction of Chinese Nationalism in the Early 21st Century* (1st ed., pp. 17–36). Routledge. <https://doi.org/10.4324/9781315772172>

⁹⁵ Kalimuddin, M., & Anderson, D. A. (2018). Soft Power in China's Security Strategy. *Strategic Studies Quarterly*, 12(3), 114–141. <http://www.jstor.org/stable/26481912>

⁹⁶ Ibid, 116

⁹⁷ Freier, N. P., Burnett, C. R., Cain, W. J., Compton, C. D., Hankard, S. M., Hume, R. S., Kramlich, G. R., Lissner, J. M., Magsig, T. A., Mouton, D. E., Muztafago, M. S., Schultze, J. M., Troxell, J. F., & Wille, D. G. (2016). ENTER THE DRAGON – CHINA AS A HIGH-END GRAY ZONE REVISIONIST. In *OUTPLAYED: REGAINING STRATEGIC INITIATIVE IN THE GRAY ZONE* (pp. 33–40). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep12061.11>

Even though China is the strongest regional power in the South China Sea region, other Asian countries are not conceding or compromising claims to the sea due to potential untapped resources, shipping routes, or symbolic ideas of national sovereignty.⁹⁸ The reason this becomes so contentious is that there is no international basis to resolve these claims, as the United Nations Convention on the Law of the Sea does not define territorial or economic rights based on different types of land features, thus the only outlet to compromise or negotiate it through bilateral or multilateral talks.⁹⁹ But rather than engaging in these talks China resorts to gray zone strategies that target countries in the region and even the United States.

Tactics China has been utilizing involve border manipulation, economic coercion, co-opting state affiliated businesses, military intimidation, and information operations, in order to exert its influence.¹⁰⁰ Through all of these tactics China is engaging in gradualism, where it adopts a long-term perspective using a multitude of instruments in order to obtain gradual gains that manipulate the opponent's response.¹⁰¹ Gradualism is exactly the strategy that raises the heat of the water where NATO is able to avoid the signs and exist at a new level of insecurity, while not noticing the world has changed all around it. While engaging in the various gray zone strategies, China still is able to brandish an image of soft power through its economic development initiatives and cultural exports. One major policy that demonstrates China's desire to attract influence is through its Belt and Road Initiative that has been deployed to be something similar to a Chinese style Marshall Plan to increase infrastructure and investment around the world and become the modern age Silk Road. Yet since its creation in 2013 it has not been able to accomplish this goal beyond a successful public marketing scheme.¹⁰² Many of the projects are too wide-ranging and exist more to contain India than actually expand infrastructure. Additionally, with too much control by

⁹⁸ Kalimuddin, M., & Anderson, D. A. (2018). Soft Power in China's Security Strategy. *Strategic Studies Quarterly*, 12(3), 114–141. <http://www.jstor.org/stable/26481912>

⁹⁹ Ibid, 118

¹⁰⁰ Jung, C. (2021). *China's Gray Zone Operations in the Yellow Sea*. Daniel K. Inouye Asia-Pacific Center for Security Studies. <http://www.jstor.org/stable/resrep35896>

¹⁰¹ 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. <https://www.jstor.org/stable/26999974>

¹⁰² Nye, J. S. (2020). Perspectives for a China Strategy. *PRISM*, 8(4), 120–131. <https://www.jstor.org/stable/26918238>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

the Chinese Communist Party there is a lack of a flourishing civil society in China to help with these projects compared to Europe or the United States. As a result, participation in the initiative is beginning to decline with Argentina and Italy as examples of countries no longer seeing the benefit of membership.

China uses its soft power as an extension of its gray zone strategy, but also does not shy away from more confrontational approaches to testing the global status quo. With the creation of artificial islands to expand its Exclusive Economic Zone (EEZ), or military drills in the Taiwan Strait, or cyber intrusion into American businesses in order to get ahead on research and development, China seeks to challenge NATO similar to Russia, only in a different manner which requires a different strategic response from NATO.¹⁰³ NATO needs to be attentive and proactive in its responses and how it shapes its deterrence as Russia and China take different paths to reach the same goal. Furthermore, taking into consideration threats from Iran, North Korea, and non-state actors need to be incorporated into the strategy or else the boiling frog will die as the heat has taken over and imminent conflict has succeeded.

¹⁰³ Freier, N. P., Burnett, C. R., Cain, W. J., Compton, C. D., Hankard, S. M., Hume, R. S., Kramlich, G. R., Lissner, J. M., Magsig, T. A., Mouton, D. E., Muztafago, M. S., Schultze, J. M., Troxell, J. F., & Wille, D. G. (2016). ENTER THE DRAGON – CHINA AS A HIGH-END GRAY ZONE REVISIONIST. In *OUTPLAYED: REGAINING STRATEGIC INITIATIVE IN THE GRAY ZONE* (pp. 33–40). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep12061.11>

V. Deterrence through Punishment - NATO Capabilities

Deterrence or Compellence

Gray Zone conflicts and hybrid war are not new to NATO, nor is NATO woefully unprepared to respond. Rather the approach is around adapting the deterrence strategy of conventional warfare to one that can address the multitude of gray zone strategies and the growing threat of hybrid war. As seen, adversaries like Russia, China, Iran, and North Korea, as well as non-state actors, look to assert power to create a new global reality. NATO cannot be caught off-guard to this threat, and thus an analysis of the current state of NATO's deterrence is imperative in order to assess capabilities and future strategies in the changing world.

Hybrid threats are qualitatively different from conventional conflicts, with the diffusion of military technology and the expansion of the information domain; traditional means of counterterrorism and counterinsurgency are not sufficient.¹⁰⁴ Deterrence is the most effective strategy for NATO to take as it is easier to do and accomplishes better results. While deterrence itself is a form of coercion, it is different in the sense that it does not compel a state to act, but focuses on its ability to deter. Deterrence and, as Thomas Schelling coins, "compellence"¹⁰⁵ work differently to achieve similar goals, deterrence seeks to change the consequence of an action so that it prevents a state from seeking that action, whereas "compellence" is initiating an action that can cease if the opponent responds.¹⁰⁶ NATO's current state of operation is around deterrence by denial, in that it is seeking to prevent adversaries from pursuing actions by demonstrating the consequences of an action rather than compelling them to stop. Over the past few years NATO has been

¹⁰⁴ Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM*, 7(4), 30–47. <https://www.jstor.org/stable/26542705>

¹⁰⁵ Schelling, T. C. (1976). *Arms and Influence*. New Haven, CT: *Yale University Press*.

¹⁰⁶ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

working to strengthen its Eastern flank to provide deterrence against Russia, investing more into cyber and hybrid capabilities, and increasing defense budgets. Separately, deterrence against China is still developing and focuses on nuclear deterrence, but in recent years there has been a shift to provide deterrence from China's expansionism. In order to calculate and prescribe the future of NATO deterrence it is imperative to see where NATO currently exists in capacity. The current state of NATO deterrence is optimistic, but there is much more room for growth in the alliance when it comes to defense spending, modernization, and strategic planning.

Defense Spending: The 2% Folly

Since the end of the Cold War the forces of non-US NATO states have declined 40 percent, even with the addition of 16 new member states.¹⁰⁷ After Russia's annexation of Crimea in 2014, NATO announced at the Wales Summit to increase defense spending to 2 percent of GDP for each country, with 20 percent targeted on equipment acquisition. As a result, non-US NATO forces have begun to increase, and increased more rapidly after the 2022 Russian invasion of Ukraine. Moreso, twenty-two member states have begun increasing defense funding with four (Finland, Romania, Hungary, and Slovakia) passing above the 2 percent minimum threshold, making eleven of the thirty-two NATO members at or above this threshold.¹⁰⁸ If trends continue NATO will be able to continue to increase defense expenditures to agreed upon levels that will enhance capabilities and support deterrence efforts.

NATO divides defense spending into four separate categories: equipment, personnel, infrastructure, and "other". The equipment category is broken down even further into procurement of 11 different areas, and research and development spending on

¹⁰⁷ Cancian, M. F., & Saxton, A. (2021). The Current State of NATO Forces and Military Budgets. In *Future NATO Enlargement: Force Requirements and Budget Costs* (pp. 27–34). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep35120.7>

¹⁰⁸ Reuters. (2024). NATO members hike defense spending after Russia's invasion of Ukraine. *Reuters*. Retrieved from <https://www.reuters.com/graphics/USA-ELECTION/TRUMP-NATO/movalqxlzpa/index.html#:~:text=Twenty%2Dtwo%20of%2031%20NATO,goal%20of%202%25%20of%20GDP.&text=NATO%20countries%20aim%20to%20spend,2%25%20of%20GDP%20in%20defense>.

equipment. Personnel spending includes pay and allowances, retirement benefits, and pensions. Infrastructure spending includes national military construction as well as common NATO infrastructure like military bases hosted in other countries, whereas operation and maintenance costs make up most of the “other” category.¹⁰⁹ The 20 percent benchmark for equipment was decided to demonstrate resolve as an alliance and to increase overall capability and modernization, and to decrease the tendency to overspend defense budgets on personnel. While this recent uptick in spending is good and optimistic, there is still much more lost ground to recover from decades of underinvestment, mostly from European members.¹¹⁰ One caveat to mention when analyzing defense spending as a percentage of GDP is that over the long-term states can very well be increasing defense spending, but if it is not increasing faster than its overall economic growth it can be seen as a decrease even if it is a nominal increase from the previous year. Additionally, long-term analyses need to control for the fact that swings in the value of national currencies like the US dollar or the Euro make it difficult to do comparisons as it can mislead the data. Representing defense spending as a percentage of real GDP is more useful as it has less swing when comparing the value of different currencies.¹¹¹

The 2 percent threshold for NATO defense spending was a “gentleman’s agreement” at the 2002 Prague Summit, where NATO members created a guideline for states to aim for 2% of their Gross Domestic Product to be allocated for defense. This was mandated at the 2014 Wales Summit in the aftermath of Russia’s annexation of Crimea, and invasion of eastern Ukraine. As spending rates dropped over the previous decades, and overall armed forces were decreasing significantly, the threshold became a target to help bring back the military capabilities of NATO. The summit communique states:

We agree to reverse the trend of declining defence budgets, to make the most effective use of our funds and to further a more balanced sharing of

¹⁰⁹ HICKS, K. H., RATHKE, J., DANIELS, S. P., MATLAGA, M., DANIELS, L., & LINDER, A. (2018). Current NATO Benchmarks. In *Counting Dollars or Measuring Value: Assessing NATO and Partner Burden Sharing* (pp. 3–8). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep22475.4>

¹¹⁰ Adesnik, D. (2016). *FPI Bulletin: NATO Defense Spending*. Foreign Policy Initiative. <http://www.jstor.org/stable/resrep07277>

¹¹¹ *Ibid*, 1-2

costs and responsibilities... Increased investments should be directed towards meeting our capability priorities, and Allies also need to display the political will to provide required capabilities and deploy forces when they are needed.¹¹²

While this is a mandated threshold to meet, it is not present in the treaty itself and so it lacks an enforcement mechanism to compel states to reach this target. Even after a summit meeting in 2005 the NATO spokesperson stated, it was “not a hard commitment that they [would] do it,” but rather “a commitment to work towards it.”¹¹³ The increase in spending is definitely desired and preferred to overall capability, but it is not the only manner to reach it, and does not represent the true reality.

The 2 percent threshold has evolved into a mantra or political weapon within the alliance to wield against states that others feel are not carrying their commitments. The metric has become a tool used to perceive political willingness and burden-sharing among the alliance. Members that do not reach this goal can be seen as “free-riders”, and it becomes a simple tool of political messaging.¹¹⁴ Former United States President Donald Trump showed how this benchmark could be used for political means and as a way to undermine the alliance, without accounting for overall burden-sharing, its idea as a commitment, and its misleading measurement.

Former President Trump, and at the time of writing this, 2024 United States presidential candidate, has had a rocky relationship with NATO, and is the only American president since the creation of the alliance to have an adversarial relationship with its mission. Much of this comes from the rise of right-wing populism centered on nationalism that is not unique to the United States. Trump’s

¹¹² NATO. (2014). Wales Summit Declaration. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_112964.htm

¹¹³ Appathurai, J. (2005, June 8). Press Briefing by NATO Spokesman, James Appathurai, after the Meeting of the North Atlantic Council at the Level of Defence Ministers. Retrieved from <https://www.nato.int/docu/speech/2006/s060608m.htm>

¹¹⁴ HICKS, K. H., RATHKE, J., DANIELS, S. P., MATLAGA, M., DANIELS, L., & LINDER, A. (2018). Current NATO Benchmarks. In *Counting Dollars or Measuring Value: Assessing NATO and Partner Burden Sharing* (pp. 3–8). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep22475.4>

base of support is very protectionist and isolationist, and playing to these ideologies benefits him. Trump claims that most of NATO is acting as ‘free-loaders’, who are exploiting the generosity of the United States for their own security and are unwilling to contribute the same amount. The former president went as far to say that he would “encourage Russia to do whatever the hell it wants” to NATO countries that do not meet the 2% threshold.¹¹⁵ This is a fundamental misunderstanding of how the alliance works and treats it as if it is a club that requires a membership that the members are not financing.¹¹⁶ This is a misguided way of considering the alliance, where the 2% benchmark has become a scapegoat, rather than motivation for building up deterrence.

Since defense spending is at the will of national governments and not NATO itself, much of this spending is dependent on the politics of each of the 32 countries, a difficult feat considering budget constraints, economic slowdowns, and recovering from the COVID-19 pandemic. The 2% benchmark was created more as a way for European states to build back defense spending, modernization, equipment development, and overall force size that had been dramatically cut since 1991. It is a sign of a country’s commitment to the alliance and building deterrence rather than an established minimum. It is a folly and political trap to consider the 2% threshold as the baseline of NATO contribution because it is a view that lacks nuance and simplifies the actual defense spending that occurs. It shows that a country was able to increase military spending faster than its GDP growth and only looks at the inputs of a country rather than its outputs.¹¹⁷ As previously discussed, NATO defense spending includes equipment, personnel, infrastructure, and more, so if all the increased spending were to go solely into one category it shows an increase of

¹¹⁵ McDonald, A. (2024, March 19). Donald Trump says he won't quit NATO if Europe pays its way. *Politico*. Retrieved from <https://www.politico.eu/article/donald-trump-says-he-wont-quit-nato-if-europe-pays-its-way/>

¹¹⁶ Le Monde. (2024, March 20). Trump describes recent NATO threats as a form of negotiation. *Le Monde*. Retrieved from https://www.lemonde.fr/en/united-states/article/2024/03/20/trump-describes-recent-nato-threats-as-a-form-of-negotiation_6636346_133.html

¹¹⁷ HICKS, K. H., RATHKE, J., DANIELS, S. P., MATLAGA, M., DANIELS, L., & LINDER, A. (2018). Current NATO Benchmarks. In *Counting Dollars or Measuring Value: Assessing NATO and Partner Burden Sharing* (pp. 3–8). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep22475.4>

spending but not necessarily achieving the outputs needed.¹¹⁸ Therefore it would seem more prudent to analyze defense spending as a percentage of government spending, rather than GDP, as it shows a government's willingness to allocate resources.¹¹⁹

While the 2% promise is faulty and misleading it should not distract from the needs of NATO and the hollowing out of European militaries and forces. Recent work has been accomplished in increasing capabilities across Europe, especially since the 2022 invasion, but modernization and capacity building take time and the forecast looks optimistic. Despite the trend of lower force levels and spending, European governments, and Canada, spend more than \$250 billion a year on defense and have tens of thousands of troops deployed with the United States.¹²⁰ Finland and Sweden have joined the alliance and have brought new defense industries, equipment, and force specialization to the alliance. NATO still has the highest military capabilities in the world, as well as power projection, the 2% benchmark is only a political weapon used for internal political messaging rather than a true measurement of NATO member state capabilities and outputs. An Alliance of 32 members has much capability but determining that capability and utilizing its potential for future gray zone operations requires a look at its current state and a sober analysis of strengths and deficiencies among members old and new.

Military Capabilities

Adapting to the different operational domains and the evolution of multi-domain threats requires a look at the capacity of NATO, and its ability to respond. NATO functions primarily through deterrence, whether by denial or punishment, but with the ever-changing global political dynamic, and technology developments

¹¹⁸ Ibid, 6

¹¹⁹ Ibid, 6

¹²⁰ Adesnik, D. (2016). *FPI Bulletin: NATO Defense Spending*. Foreign Policy Initiative. <http://www.jstor.org/stable/resrep07277>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

it requires quick action and change, and cannot be slowed down by aged processes or equipment. The United States Chairman of the Joint Chiefs of Staff Charles Brown famously quips, “accelerate change or lose” when discussing the military and its modernization.¹²¹ While NATO has the largest, most advanced, military alliance in the world it lacks in modernization and deployment due to decades of budget cuts and underfunding. This section will analyze the current state of NATO capabilities to see how they can be adapted to gray zone challenges so that deterrence capability is not lost, and interoperability remains strong.

The NATO Defense Planning Process (NDPP) is a quadrennial report on the capacity and capabilities of allies in NATO, and recommended plans and coordination for multinational military response. The NDPP is what allows NATO to be as adaptable as it currently exists, and to respond effectively in NATO’s three core mission areas: collective defense, crisis response, and collective security.¹²² It creates capability targets for member states to meet and is agreed upon by the entire alliance. It is crucial and effective, that even some allies use it exclusively as their defense planning, and has been a major boost in capacity building in recent years. The NDPP is seen as a more effective means of increasing capabilities within NATO and easier to enact reforms rather than focusing on the 2% spending benchmark. The purpose is to enable burden-sharing across the alliance so that members can target their own advantageous areas and reach the targeted needs of the alliance as a whole.¹²³

The deficits in capabilities are nothing new to NATO in the defense planning process. Navigating the budgetary politics of 32 sovereign countries is never easy and can lead to many falling short of targets. During most of the Cold War, with the exception of the Vietnam War era, NATO countries accepted their capability targets, but with the collapse of the Soviet Union in 1991 NATO

¹²¹ Brown, C. (2020). Accelerate Change or Lose .*Airman Comprehensive Operations and Leadership Exam Booklet*. Retrieved from https://www.af.mil/Portals/1/documents/2020SAF/ACOL_booklet_FINAL_13_Nov_1006_WEB.pdf

¹²² Deni, J. R. (2020). *Security Threats, American Pressure, and the Role of Key Personnel: How NATO’s Defence Planning Process is Alleviating the Burden-Sharing Dilemma*. Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep26532>

¹²³ Ibid, 9

countries saw a steep decline in budgets and overall force structure.¹²⁴ NATO routinely saw targets unallocated since 1991, but that changed in the 2017 NDPP, the first time since the Cold War. This is largely attributed as a response to Russia's invasion of Ukraine in 2014 and the build-up of its military. Much of the emphasis was placed into "heavier and more high-end forces and capabilities, as well as more forces at higher readiness" and a much larger push towards building up cyber defense.¹²⁵ Following the guidance of defense ministers, an algorithm is used to set the Minimum Capability Requirement for each member state relative to each nation's wealth. The United States receives the largest burden covering about 50% of NATO's capabilities, Germany is second, followed by the United Kingdom, France, and so on.¹²⁶ But with the planned investments for NATO and the changing nature of future threats, NATO states need to enhance and streamline their capabilities.

The creation of the 2% benchmark also came with the creation that 20% of defense spending should be equipment. It is a beneficial benchmark to reach because it motivates countries to expand spending beyond personnel, like Greece who spends 3.5% of its GDP on defense, but 53% of the budget is spent on personnel in 2023, down from 77% in 2014, or Italy who spends 1.46% of its GDP on defense but 61% on personnel, down from 76% in 2014.¹²⁷ An important aspect to consider is also countries' needs to adapt budgets to economic downturns like the 2008 recession, and the COVID-19 pandemic. Additionally, a major challenge for NATO members in the Eastern flank is reaching this 20% goal is that much of their current military equipment is outdated Soviet-designed equipment that does not meet full NATO standards, but is also an opportunity to push for upgrading

¹²⁴ Ibid, 9

¹²⁵ Schmitt, G. J. (Ed.). (2020). NATO: THE CURRENT CHALLENGE. In *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners—Second Edition* (pp. 187–224). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep27713.11>

¹²⁶ Ibid, 210

¹²⁷ NATO (2023, July 7). Defence Expenditure of NATO Countries (2014-2023). *NATO Public Diplomacy Division*. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf

equipment.¹²⁸ A recent boost in equipment modernization has been the US-sponsored F-35 Joint Strike Fighter program¹²⁹, which has helped 5 of the 11 countries over the 20% benchmark reach this goal. With NATO countries assisting Ukraine in its fight against Russia, many countries with Soviet weaponry and aircraft were able to donate them to Ukraine and receive updated versions from other NATO states like the US, Canada, France, and the UK.

Similar to the 2% benchmark, the 20% equipment benchmark is faulty in its measurement as well. As it also looks at inputs rather than outputs, where member states can avoid transparency in spending to avoid showing the exact equipment being procured, as well as investing in an overly costly aircraft, for example, that was not actually requested by the NDPP capabilities for each country. This would be efficient if countries had more reporting transparency which would lead to more accountability, but that is an issue easier addressed by national governments through NATO pressure.¹³⁰ These capabilities for NATO demonstrate its resolve and signal the message of deterrence by denial to the rest of the world, therefore it is important to see just where those capabilities lie.

The Western Core: France, Germany, and the United Kingdom

France is one of the more motivated NATO countries in equipment modernization, training, and deterrence. France originally joined the alliance outside the regular command structure and navigated a separate nuclear strategy from the US and the UK, but has since worked closer within the alliance. As one of the three nuclear powers in the alliance it requires much upkeep and works efficiently as a deterrent within Europe. As one of the few in NATO with power projection capabilities, it has shown its commitment to improving its high-intensity fighting

¹²⁸ HICKS, K. H., RATHKE, J., DANIELS, S. P., MATLAGA, M., DANIELS, L., & LINDER, A. (2018). Current NATO Benchmarks. In *Counting Dollars or Measuring Value: Assessing NATO and Partner Burden Sharing* (pp. 3–8). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep22475.4>

¹²⁹ Members include Canada, Denmark, Italy, the Netherlands, Norway, Turkey, the United Kingdom, and the United States. As well as Belgium and Finland looking to join.

¹³⁰ Hicks, K. et. al. (2018), 8

capabilities.¹³¹ Even after major cuts due to the COVID-19 pandemic France was able to maintain its modernization plans, but at the expense of personnel which has significantly declined over the last decade.¹³² After the 2015 terrorist attacks in Paris the government sought to expand its military budget, especially around modernization in all branches of its military. But as France has a history of operating independently from NATO with regards to defense coordination there are still gaps in its long-term land deployment, long-range conventional strike capabilities, as well as the interoperability of its nuclear forces in tandem with the US and the UK.¹³³

Germany is a major contributor to NATO operations but is severely underfunded in regards to readiness and modernization, largely due to cuts after the 2008 financial crisis and the fear of remilitarization after WWII. In 1991 Germany had 476,300 active forces and 1,009,400 reserves, compared to 2021 with 183,500 active forces and 30,500 reserves. Germany also has major declines in artillery, aircraft, armored vehicles, and its naval fleet, prompting concerns about its long-term sustainability and troop deployment capabilities.¹³⁴ Since 2016, there has been a big turnaround in spending, with Germany increasing to meet the moment, but much more needs to be done with modernization. A challenge for Germany still remains that defense spending has been a major political issue ever since World War II, but given Germany's size and location within Europe, it is central to regional security and much more is needed to boost capability.¹³⁵

The United Kingdom has increased spending over the past few years even as it made massive cuts as a result of the 2008 recession. These cuts led to a large

¹³¹ Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

¹³² Morcos, P. (2020). *Toward a New "Lost Decade"?: Covid-19 and Defense Spending in Europe*. Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep26416>

¹³³ Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

¹³⁴ *Ibid*, 33

¹³⁵ Morcos, P. (2020). *Toward a New "Lost Decade"?: Covid-19 and Defense Spending in Europe*. Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep26416>

downturn in overall force size as well as procurement abilities that have lessened its ability to engage in large, high-end operations.¹³⁶ With the departure from the EU, the UK has now sought a larger global presence rather than a focus inside Europe. As a nuclear power the UK does have power projection capabilities, but due to these budget cuts and force decreases it could take until the 2030s and 2040s until the UK is able to sustain large-scale operations. The UK will need to grapple with its desire for a “forward deployed, persistent presence” military, with the reality of a decreased force size of 72,500, which limits its abilities.¹³⁷

The Southern Flank: Italy, Spain, Portugal, Greece, and Turkey

Italy is the major NATO power in the Mediterranean Sea with the most expansive naval fleet in the region. In recent years Italy has invested in modernization and is working on much needed upgrades, like the completion of its third aircraft carrier the *ITS Trieste*.¹³⁸ Additionally, from the 2008 economic crisis and the subsequent austerity, Italy cut much of its defense investment, even while personnel costs are 70% of its budget. The investments that survived the budget cuts in investments were the naval and space operations, but after 2015 equipment investments were prioritized again and are now above 20%, there is still concern about the sustainability of these investments due to the high debt-to-GDP ratio of Italy.¹³⁹

Spain spends considerably less than Italy on defense, but spends a higher proportion on modernization.¹⁴⁰ Similar to the rest of Europe, Spain has seen a large

¹³⁶ Ibid, 4

¹³⁷ Cancian, M. F., & Saxton, A. (2021). The Current State of NATO Forces and Military Budgets. In *Future NATO Enlargement: Force Requirements and Budget Costs* (pp. 27–34). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep35120.7>

¹³⁸ Brimelow, B. (2022, October). Italian military seeking new jets, ships amid rising Mediterranean tension. *Business Insider*. Retrieved from <https://www.businessinsider.com/italian-military-seeking-new-jets-ships-amid-rising-mediterranean-tension-2022-10>

¹³⁹ Cancian, M. F., & Saxton, A. (2021). The Current State of NATO Forces and Military Budgets. In *Future NATO Enlargement: Force Requirements and Budget Costs* (pp. 27–34). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep35120.7>

¹⁴⁰ Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

decrease in force and equipment size but is beginning to turn that around. Portugal has the opposite problem of Spain, where it has relatively higher rates of defense spending overall, but very minimal investments in modernization.¹⁴¹

Greece is a moderate military power and has utilized its economic recovery on defense spending and modernization, mostly from perceived threats from Turkey.¹⁴² Greece spends large amounts on personnel expenses but has been decreasing over the years with investments in equipment. Greece hosts an American base on the island of Crete, as well as strong relations with France. The forces of Greece are very well-trained in spite of the economic troubles it has been facing.¹⁴³ Greece has turned around its shipbuilding industry with the assistance of France signals Greece's desire to become an arms and logistics supplier, especially within the alliance.¹⁴⁴

Turkey is also a moderate power like Greece, but with a much larger active-duty base. Turkey has the second largest active-duty force in NATO after the United States, with 355,200 active duty and 378,700 in reserves.¹⁴⁵ Turkey is pushing for a much larger role in the Middle East and placing much of its power projection into the region. As well as control over the Bosphorus Strait, Turkey is aiming to leverage its regional power capabilities. As will be covered later, Turkey adopted the Russian made S-400 Air Defense system which is incompatible with NATO equipment causing a challenge to alliance interoperability.

¹⁴¹ Ibid, 40

¹⁴² Ibid, 37

¹⁴³ Ibid, 37

¹⁴⁴ Plakoudas, S. (2021). The recent turnaround of the Greek defense industry. *Newlines Institute*. Retrieved from <https://newlinesinstitute.org/strategic-competition/regional-competition/the-recent-turnaround-of-the-greek-defense-industry/>

¹⁴⁵ Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

The Eastern Flank: The Bucharest Nine¹⁴⁶

The countries along the Eastern flank sought NATO membership after the dissolution of the Soviet Union and the collapse of the Warsaw Pact. NATO membership, along with EU membership, was seen as a way to move away from communist oppression and begin democratic liberalization, which was eventually accepted in the late 1990's.¹⁴⁷ Since then, Poland has focused on high levels of defense spending over the years and has relatively high levels of overall and modernization spending. It is still in need of converting to Western weapons systems and structures, but has been moving fast in this regard.¹⁴⁸ Poland has been converting its air fleet from former Soviet made designs to the American F-16 and F-35s. It has strong connections with the Visegrad Group¹⁴⁹, as well as the rest of the Bucharest Nine. Poland lacks a missile defense system, and its land-based air defense systems are outdated Russian models, thus it requires a faster transition to Western systems in order to enhance interoperability for overall deterrence capability.

Czechia has long-term defense plans to be completed by the 2030s, but has been lacking in sufficient funding to reach these goals. It only has minimal defense capabilities that need to be enhanced to be considered capable from outside threats, and its air defense is reliant on other nations in the alliance.¹⁵⁰ Slovakia has been looking to modernize as well, and has invested in new F-16 aircrafts, but similar to Czechia it requires support from others in the alliance in face of an attack, as it lacks the air defense or modernized force capabilities to push back.¹⁵¹

After the collapse of the Soviet Union the armed forces of Hungary also drastically fell to 27,800 active duty. Most of the Hungarian equipment is Warsaw

¹⁴⁶ The Bucharest Nine consists of Poland, Czechia, Slovakia, Estonia, Latvia, Lithuania, Hungary, Romania, and Bulgaria

¹⁴⁷ Shiffrinson, Joshua R. (2020). "NATO enlargement and US foreign policy: the origins, durability, and impact of an idea". *International Politics*. 57 (3): 342–370. doi:[10.1057/s41311-020-00224-w](https://doi.org/10.1057/s41311-020-00224-w). hdl:[2144/41811](https://hdl.handle.net/2144/41811)

¹⁴⁸ Ibid, 34

¹⁴⁹ The Visegrad Group consists of Poland, Czechia, Slovakia, and Hungary

¹⁵⁰ Ibid, 35

¹⁵¹ Ibid, 34

Pact-era except for Leopard tanks and Gripen C/D fighters from Germany and Sweden, respectively. Spending levels are adequate, but the armed forces lack an air defense, missile defense, and one brigade sized land force, thus requiring Hungary to rely on neighbors and other alliance members for support.¹⁵²

Similar to the other nations in the Eastern Flank, Romania has an abundance of Soviet-era weaponry and equipment that needs to be modernized. It has relatively high levels of defense spending, but low levels of modernization. The Soviet-era weaponry is immense, but lacks the long-term sustainability needed for effective deterrence. It has been shifting slowly to Western made weapons with its acquisition of patriot missiles and F-16 aircrafts. It has much larger capability than other countries in the Bucharest Nine, but still lacks warfighting capabilities.¹⁵³

Bulgaria has maintained decent defense spending and modernization, but similar to its neighborhood peers it has an abundance of Soviet-era weaponry that is quickly aging or obsolete. It does have air defense capabilities, but they also are outdated and require a higher degree of maintenance. For these reasons, Bulgaria lacks the capability to be interoperable fully with NATO, and needs to hasten its modernization.¹⁵⁴

Security in the Baltic states is a NATO priority (along with Poland), and is the main beneficiaries of Operation Enhanced Forward Presence. Due to this, the Baltic states are too small in comparison to Russia and would require higher NATO presence for deterrence and support. The capabilities that do exist are minimal, but not weak. Estonia is key to NATO cyber defense operations and intelligence, but lacks the hard artillery and equipment needed to pushback against an invasion. Latvia has fewer active-duty forces than Estonia, but slightly higher naval capabilities, but overall, not sufficient for deterrence. Lithuania has a geographic challenge of the Suwałki Gap which has Russia on its eastern and western borders forcing the country into two fronts if invaded. As future chapters will expand on,

¹⁵² Ibid, 35

¹⁵³ Ibid, 35

¹⁵⁴ Ibid, 36

deterrence in the gray zone and traditional domains of operation involve the heightened alliance presence in the Baltic states due to historical and capability reasons of the region.

The Northern Flank: Norway, Sweden, Finland, Denmark, and Iceland

The Northern Flank of NATO shares the longest land border with Russia with 1,537 kilometers (951 miles). Additionally, the Northern Flank is pivotal towards NATO's Arctic policy in countering Russia. All the countries of the Northern Flank have strong ties with each other and mutual support that enhances the deterrence of the region. Norway, Denmark, and Iceland are founding members of NATO in 1949, whereas Finland joined in 2023, and Sweden in 2024, bringing the entire Nordic region into the NATO alliance.

Norway does not have a large defense expenditure, but it does use advanced equipment, with a modernized Air Force using F-35 aircrafts, new German submarines, but with very limited forces, especially in regards to its strategic position, long coastline, and border with Russia. To compensate for its lack of forces and lack of air and missile defense, Norway has close ties with the United States with whom it relies on for power projection. Norway has a comparative advantage with Arctic conditions and cold-weather warfare. Norway is a NATO leader in alliance-wide military drills called "Nordic Response", which occurs every other year. It allows Norwegian troops to train allies in cold-weather fighting, utilizing skis, snowmobiles, and snowshoes, as well as how to survive in the cold wilderness, and treat cold related injuries like frostbite.¹⁵⁵

Denmark is located at a geopolitically strategic location as the entrance to the Baltic, and with the rest of the NATO countries in the Baltic region, it has the potential to apply a lot of pressure on Russia from this position. On the other hand, Denmark has about half of its total active forces than existed in 1991, and does not

¹⁵⁵ NATO. (2024). NATO conducts major air and missile defense exercise. *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/news_223083.htm#:~:text=Since%20then%2C%20the%20exercise%20has,from%20more%20than%2014%20countries.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

have a significant air and missile defense system necessary for strategic deterrence. Denmark, like much of NATO Europe, has plans for modernization, but it is a lengthy process to get operational.¹⁵⁶ Sweden is NATO's newest member but contributes well to the overall effectiveness of the alliance. Sweden has a small force, but is considered highly-trained and is considered sufficiently modernized. Sweden has high equipment capabilities, with a very large Navy and coastal defense system. It has acquired Patriot air defense systems and anti-ballistic missile systems. Sweden's main challenge is the operational defense of the island of Gotland due to its location in the Baltic Sea, as it would be a major target in any conflict with Russia.¹⁵⁷

Finland joined the alliance in 2023 and is now the NATO country with the longest land border with Russia. Finland has a long history of having a large reserve military, and provides NATO with one of the largest wartime strengths with 280,000 troops, and 900,000 that have received military training.¹⁵⁸ Finland's long border with Russia and its proximity to St. Petersburg, places NATO's northern flank as a lynchpin of deterrence against Russia. Also, in the last year Finland has signed a defense compact with the United States that allows the sales of American F-35 aircrafts to Finland to modernize its Air Force, and allows the US military into Finland at the request of the government according to the limits prescribed in the agreement.¹⁵⁹ Finland has significant artillery, but still lacks sufficient air and missile defense systems.¹⁶⁰

Iceland and Greenland (through extension of Denmark) are also NATO members, but neither have established militaries. Iceland has a Coast Guard and

¹⁵⁶ Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

¹⁵⁷ Ibid, 28

¹⁵⁸ Moyer, J., (2024). Finland's Remarkable First Year in NATO. *Wilson Center*. Retrieved at: <https://www.wilsoncenter.org/article/finlands-remarkable-first-year-nato#:~:text=NATO%20remains%20popular%20in%20Finland,contributions%20to%20Ukraine%20not%20included.>

¹⁵⁹ Ibid

¹⁶⁰ Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

police force, while Greenland relies on Denmark for defense. Iceland provides the alliance with air access and refueling, while Greenland has agreed to allow the American Thule Space Force base to continue to operate providing NATO access to the Arctic.

Benelux, Balkans, and Canada

As smaller countries wedged between the larger powers of Germany and France the Benelux nations of the Netherlands, Belgium, and Luxembourg have combined interoperability with themselves and Germany in order to enhance capabilities and deterrence. The Netherlands has decreased its forces by two-thirds over the last 30 years, and operates as a mixed combat support contingent of the alliance as it could not operate as an independent force.¹⁶¹ The capabilities of Belgium are even less, as its defense spending is very minimal and lacks adequate numbers of armor, and too small a force to contribute to forward area combat. It additionally lacks the capability to sustain its already small Air Force, or the funds to modernize. It also does not have significant missile defense systems.¹⁶² Luxembourg is too small to analyze effectively to overall capability as it has a military force size of around 900 troops, but does offer logistics and training for NATO.¹⁶³

The Balkans nations in NATO consist of Slovenia, Croatia, Albania, Montenegro, and North Macedonia. Slovenia, Croatia, Montenegro, and North Macedonia were part of Yugoslavia and retained much of their equipment from there. They have limited fighting experience and very limited defense capabilities. Slovenia has begun spending more on defense, but still comparatively little on modernization. Croatia has also begun spending much more on defense since 2014, but its resources still remain limited. Montenegro has moderate levels of defense spending, but its forces are only designed for national defense, and not power

¹⁶¹ Ibid, 32

¹⁶² Ibid, 32

¹⁶³ NATO. (2024). Luxembourg. *Supreme Headquarters Allied Powers Europe - NATO*. Retrieved from: <https://shape.nato.int/luxembourg>

projection. North Macedonia has made significant increases to defense spending and modernization, but lacks overall force size, with only land-based forces. Albania has also begun modernizing its forces and equipment and has been making a concerted effort to move away from its Russian systems to Western based systems.¹⁶⁴

Canada, as the only other North American member of NATO besides the US, has positioned itself as a major actor in Arctic security and defense. Canada has recently made large investments in Arctic security as it will become more prevalent as climate change progresses. With Russia also looking to expand its presence into the Arctic, Canada could potentially become a frontline in a future conflict. Canada has consistently been behind the NATO average in defense spending, but has announced plans to greatly expand its investments and modernization, focusing on its submarine fleet. Canada is also looking to set up a Cyber Command to target potential threats in the cyber domain and adapt to the irregular threats in the gray zone. While the new investments look promising, Canada is still faced with recruitment and force size problems as it has been declining over the past few decades.¹⁶⁵ Since 2008 Canada has begun major modernization plans for its Air Force, Navy, and its partnership with the United States through the North American Aerospace Defense Command (NORAD).

The United States

During the Cold War the United States and the Soviet Union exerted resources to challenge one another through military deterrence, as well as nuclear deterrence. With the collapse of the Soviet Union and the end of the Cold War, the United States was faced with the question of cutting down on its defense or maintaining it for the future, as it is now the sole global superpower. The United States decided not to cut down on defense, but rather find a new way to *transform*

¹⁶⁴ Ibid, 36-37

¹⁶⁵ Ritchie, S. (2024, April 8). Canada unveils updated defence policy, plan to spend \$73B over 20 years on renewing military capacity. *The Canadian Press*. Retrieved from: <https://www.ctvnews.ca/politics/canada-unveils-updated-defence-policy-plan-to-spend-73b-over-20-years-on-renewing-military-capacity-1.6837383>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

the military into future threats and adapt to the changing nature of conflict.¹⁶⁶ This does not distract from the conventional capabilities of the US military, which is the largest and most expansive of the NATO alliance. According to the United States Department of Defense for fiscal year 2024, the United States allocated \$841.4 billion towards defense, or 2.7% of GDP.¹⁶⁷ American nuclear weapon supply is beginning to age and the new budget has acquired funds for nuclear modernization as the strongest aspect of deterrence. The United States' nuclear triad consists of 400 intercontinental ballistic missiles from land positions, 14 Ohio-Class Ballistic Missile Submarines (SSBNs) from stealth positions in the sea, and 46 B-52H Stratofortress aircraft with 20 B-2A Spirit aircraft providing deterrence by air.¹⁶⁸ The American nuclear arsenal is the largest deterrence tool for NATO, as well as the arsenals from the UK and France.

The United States has 1,379,800 active personnel in addition to 849,850 in reserves, as well as the world's largest Air Force, and the world's largest Naval fleet, with 11 aircraft carriers and 75 destroyers. The United States is capable of global power projection and has 38 named military bases around the world, with many more military installations beyond that.¹⁶⁹ The US Air Force is slowing down in aircraft procurement, with the fleet aging quicker than its being modernized. Yet there is still great investment in the next generation of fighter jets, that is helping boost modernization efforts.¹⁷⁰ The Navy is consistent with goals and modernization and sees an increase in unmanned undersea vessels for future plans.¹⁷¹ The US Army has remained relatively consistent over the years in terms of modernization

¹⁶⁶ Ahn, K. H., & Shin, S. J. D. B. C. (2019). The US Military. In *F-35 JSF and Military Transformation: American Militarism during the Post-Cold War Era* (pp. 18–36). Asan Institute for Policy Studies. <http://www.jstor.org/stable/resrep20918.7>

¹⁶⁷ U.S. Department of Defense. (2023). FY 2024 Budget Request Overview Book. Retrieved from https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request_Overview_Book.pdf

¹⁶⁸ U.S. Department of Defense. (2024). America's Nuclear Triad. Retrieved from <https://www.defense.gov/Multimedia/Experience/Americas-Nuclear-Triad/>

¹⁶⁹ Stevenson, J. (2022). *Overseas bases and US strategy: Optimising America's Military Footprint*. International Institute for Strategic Studies.

¹⁷⁰ Cancian, M. (2021, November 30). U.S. Military Forces in FY 2022: Air Force. *Center for Strategic and International Studies*. Retrieved from <https://defense360.csis.org/u-s-military-forces-in-fy-2022-air-force/>

¹⁷¹ Cancian, M. (2021, November 2). U.S. Military Forces in FY 2022: Navy. *Center for Strategic and International Studies*. Retrieved from <https://defense360.csis.org/u-s-military-forces-in-fy-2022-navy/>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

and recruitment, with recent cuts to modernization programs, but with promises from Congress to fund them back.¹⁷²

Another area where the United States has an advantage that contributes to overall capability, is the logistics operations of the military. The US military has airlift potential just for logistics and supplies, as well as utilizing its extensive global military installation network to access weapons and equipment. The US Navy has 31 fast combat ships with 1.29 million tonnages of supplies dedicated to maintaining supply lines in combat and in the face of threats.¹⁷³ The supply lines are so successful that the US military can backfill a fast-food restaurant like Taco Bell or Burger King to troops in combat situations.¹⁷⁴

The capabilities of NATO militaries are vast and efficient. Even with the expansion of the alliance into former Warsaw Pact members and the Western Balkans, the alliance has the capacity to modernize and improve interoperability in order to develop effective deterrence in the face of graying and hybrid threats. The alliance can work to integrate deterrence further and build its interoperability with systems, equipment, infrastructure, and command. Nowhere is this need greater than boosting deterrence and readiness efforts along the Eastern Flank of NATO.

¹⁷² Cancian, M. (2021, October 21). U.S. Military Forces in FY 2022: Army. *Center for Strategic and International Studies*. Retrieved from <https://defense360.csis.org/u-s-military-forces-in-fy-2022-army/>

¹⁷³ Sawant, M. (2021). Why China Cannot Challenge the US Military Primacy. *Journal of Indo-Pacific Affairs*. Retrieved at: <https://www.airuniversity.af.edu/JIPA/Display/Article/2870650/why-china-cannot-challenge-the-us-military-primacy/>

¹⁷⁴ Quadri, Z. (2022). TGI Fridays In Kandahar: Fast Food, Military Contracting, and Intimacies of Force in the Iraq and Afghanistan Wars. *Journal of Transnational American Studies*, 13(1). <http://dx.doi.org/10.5070/T813158582> Retrieved from <https://escholarship.org/uc/item/7188527q>

VI. Deterrence in the Gray Zone

Deterrence in the Eastern Flank

The 2014 Russian invasion of Ukraine and annexation of Crimea was the catalyst for NATO to begin taking the Russian threat more seriously. The Eastern Flank of the NATO alliance from Estonia down to Bulgaria has been reinforced and continues to be enhanced in order to heighten deterrence against Russia. The strongest sense of deterrence, currently, against Russia is Article V of the North Atlantic treaty and its collective defense obligation. Article V is far from the only deterrence NATO is implementing in the Eastern Flank, with the creation of the Very High Readiness Joint Task Force, and increased defense spending alliance-wide, NATO is looking to build its deterrence by denial in hopes of preventing conflict from occurring. However, conventional threats are not the only problem the alliance faces in the East, the gray zone strategies Russia employs also need to be countered in order to prevent a new level of global instability.

As discussed previously, NATO has high military capabilities and the ability to project power wherever needed. It has advanced equipment, weaponry, and economic potential. Deficits exist within the alliance in terms of modernizing equipment—especially in the Eastern members—as well as internal political disputes that hamper decision making. All considered, the alliance still functions greatly at overall deterrence and readiness, but key challenges exist that need to be addressed.

The Warsaw Summit in 2016 created the alliance's commitment to bolstering the Eastern borders with the creation of the enhanced Forward Presence (eFP), promising to base NATO troops on a rotating basis in Estonia, Latvia, Lithuania, and Poland. This deployment began in 2017 and is voluntary by nations, fully sustainable, and coordinated with home-base defense forces. Participating nations include Canada, Germany, the United Kingdom, the United States, and

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

additional NATO members¹⁷⁵ supplement these main forces by also contributing to forward presence in the Baltic States.¹⁷⁶ There has been debate within NATO about how much of a presence is required and if it should be large in order to display a resolved appearance of deterrence-by-denial or rather, a smaller presence that signals that a multinational contingency is united to invoke Article V if needed from potential Russian provocation.¹⁷⁷ Ultimately, NATO chose the second option, but has left room to increase presence if Russia signals a desire to escalate.

With enhanced Forward Presence NATO perceives it more like an insurance policy in the Eastern Flank, or a “tripwire”, as the forces are much smaller than the Russian forces that would be sent to invade, and instead it is used as a way to save time for larger reinforcements to come to aid, rather than pushback.¹⁷⁸ Enhanced Forward Presence offers NATO the opportunity to deter Russia, even from gray zone strategies, if implemented correctly. Navigating the multinational command structures and bureaucracy is challenging, thus, “with clear responsibilities, pre-delegated authority and maximally harmonised rules of engagement”, NATO can secure the Eastern states and deny Russian gray zone adventurism and conventional threats.¹⁷⁹

Potential areas of conflict can arise in the Eastern member states that require diverse responses from NATO. Beyond just conventional invasion by Russia, NATO needs to prepare for the gray zone challenges as well, and have maneuverable plans to adapt and respond. One area that offers a unique challenge to NATO is the Suwałki Gap, which is the land that connects Poland and Lithuania,

¹⁷⁵ Contributing members to Canadian-led forces in Latvia include: Albania, Czechia, Italy, Poland, Slovakia, Slovenia, and Spain. Contributing members to German-led forces in Lithuania include: Belgium, Czechia, Iceland, Luxembourg, the Netherlands, and Norway. Contributing members to the UK-led forces in Estonia include: Denmark and Iceland. And contributing members to the US-led forces in Poland include: Romania, Croatia, and the UK.

¹⁷⁶ Shalamanov, V., Anastasov, P., & Tsvetkov, G. (2019). Deterrence and Defense at the Eastern Flank of NATO and the EU: Readiness and Interoperability in the Context of Forward Presence. *Connections*, 18(1/2), 25–42. <https://www.jstor.org/stable/26948847>

¹⁷⁷ Dempsey, J. (2017). *NATO'S EASTERN FLANK AND ITS FUTURE RELATIONSHIP WITH RUSSIA*. *Carnegie Endowment for International Peace*. <http://www.jstor.org/stable/resrep12934>

¹⁷⁸ Leuprecht, C. (2019). *The enhanced Forward Presence: innovating NATO's deployment model for collective defence*. NATO Defense College. <http://www.jstor.org/stable/resrep19859>

¹⁷⁹ *Ibid*, 5

and separates the Russian exclave of Kaliningrad from Belarus. NATO understands the importance of this gap, hence why in 2016 it deployed battlegroups to Orzysz, Poland and Rukla, Lithuania as a defensive posture to deter Russia from invading and opening new, free, access to the Baltic Sea.¹⁸⁰ Russia has always seen the separation of Kaliningrad as one of its biggest weaknesses, creating a sense of insecurity and vulnerability. Particularly, Russia is concerned about threats to command, control, and communication between mainland Russia and Kaliningrad that could potentially prevent air traffic access.¹⁸¹ Russia and Belarus even operated a military drill in 2017 that mimicked a potential invasion of Kaliningrad, highlighting how obtaining land access to connect to Belarus is one of Russia's core defensive interests.¹⁸² Additionally, any invasion of the Baltic states would entail forces from Kaliningrad as well as the bordering mainland regions of Russia, which would completely overwhelm the stationed NATO forces.

Traversing through the gray zone, Russia has other strategies it is engaging in order to test the resolve in the Eastern Flank, in particular, expanding the cyber domain operations. Back when Vladimir Putin became Prime Minister of Russia in 1999, he pushed for information warfare to be a major plank in national security policy.¹⁸³ It faced its first test back in 2007 when Russia engaged in a large cyber-attack in Estonia. As a result, Estonia has put itself at the forefront of cybersecurity and hybrid warfare in NATO.¹⁸⁴ As discussed in the last chapter, Russia also seeks to promote misinformation and propaganda in NATO states to affect elections like in the US, the Netherlands, and France. As a response, NATO installed "sovereign

¹⁸⁰ Challis, B. (2020). Security Risks: between Russia and NATO. In *Belarus beyond 2020: Implications for Russia and the West* (pp. 3–6). European Leadership Network. <http://www.jstor.org/stable/resrep25716.4>

¹⁸¹ Ibid, 4

¹⁸² Ibid, 4

¹⁸³ Dempsey, J. (2017). *NATO'S EASTERN FLANK AND ITS FUTURE RELATIONSHIP WITH RUSSIA*. Carnegie Endowment for International Peace. <http://www.jstor.org/stable/resrep12934>

¹⁸⁴ Ibid, 11

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

cyber effects” into alliance operations, which allow offensive cyber operations to be conducted from individual member states.¹⁸⁵

NATO states have been taking concrete steps to push back on these techniques, for example, Germany created a new Cyber and Information Space Command to be staffed by 13,500 soldiers and civilians.¹⁸⁶ But more needs to be done to push back against these threats, especially in the Eastern states that are at the frontlines of these operations. Cyber operations can impact air traffic control (as seen in the signal jamming in the Baltic Sea), communications, power grids, transportation systems, and banking. These gray zone strategies are designed to raise deniability and attribution and test the obligations in the alliance so that Russia can escalate to higher level provocations.¹⁸⁷ NATO needs to assume that Russia will not change its attitude toward the alliance and thus needs to take necessary steps that increase its deterrence capacity.

A speedbump to these steps is the infrastructure logistics in the Eastern Flank that prevent quick maneuvering and readiness. Like any multinational and multilateral institution NATO lacks the ability to move quickly. Ironically, during the Cold War, NATO did not have this problem and was able to move troops, tanks, and equipment easily throughout Western Europe.¹⁸⁸ Due to the present fear of a possible Soviet invasion or attack, the trains were designed for large tank movements, the roads were well kept, and bridges were in great shape in the need of getting fresh troops and weaponry to the front lines. This changed when the Soviet Union collapsed in 1991 and with the creation of the Schengen System, which allows goods and people to pass freely through Europe, does not apply to military equipment.¹⁸⁹ On top of that, the movement of military equipment requires going

¹⁸⁵ Schmitt, G. J. (Ed.). (2020). NATO: THE CURRENT CHALLENGE. In *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners—Second Edition* (pp. 187–224). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep27713.11>

¹⁸⁶ Dempsey, J. (2017). *NATO'S EASTERN FLANK AND ITS FUTURE RELATIONSHIP WITH RUSSIA*. *Carnegie Endowment for International Peace*. <http://www.jstor.org/stable/resrep12934>

¹⁸⁷ Ibid, 12

¹⁸⁸ Ibid, 10

¹⁸⁹ Ibid, 10

through red tape and bureaucracy in order to get the permissions to travel, and then the state of the actual infrastructure to transport this equipment comes into question.

Moving this equipment into Eastern Europe adds to this challenge as much of the infrastructure is less developed than in Western Europe, and as more recent members to NATO, does not have the history of moving military equipment and personnel quickly. To fix this problem NATO countries should create their own version of a military Schengen Area, where personnel and equipment do not need to go through border controls or checks. Doing so would require political will and a new treaty, where many countries would be less open to liberalizing the movement of military equipment. Another problem in the Eastern Flank is there lacks a central command like the Atlantic Command during the Cold War. It was designed to plan, command, and execute on a short notice, but was disbanded in 2003, re-establishing a central command in the Eastern border states could help fill the gap in alliance readiness.¹⁹⁰

The immediate need in NATO is to bolster the Eastern Flank and streamline the obstacles of enhanced Forward Presence. Building up deterrence along the Suwałki Gap is pivotal to territorial integrity as well as preventing Russia additional access to the Baltic Sea. Building up cyber defense and other hybrid techniques from Russia should also remain a top priority for the Atlantic alliance. Once these strategies have been implemented, NATO can then work and strategies the differences within the alliance and the different schools of thought about countering Russian aggression.¹⁹¹ Disagreements in the alliance center around how much of a future threat Russia will be, if it contains itself to just Ukraine, or adventures further into Europe, as well as disagreements about the priorities of the Southern Flank and migration, or energy security, and terrorism. Where the alliance does agree is the growing threats from China, and how NATO should adapt to the reality of multilateral and multi-domain threats.

¹⁹⁰ Ibid, 11

¹⁹¹ Ibid, 16

Strategic Deterrence: The Pivot to China

While Russia is much more conventional in its geopolitical interests, while still possessing an arsenal of gray zone strategies to challenge the status quo; China has been incredibly consistent in its approach to the gray zone and working as a revisionist actor that pushes to challenge Western spheres of influence while also obfuscating the perceived redlines.¹⁹² China has developed a trademark in its activities in the gray zone, as shown by Lyle J. Morris, et. al. at the RAND Corporation, it primarily uses measures involving “the use of civilian tools (e.g., fishing vessels), paramilitary tools (e.g., *a maritime militia*, or a group of civilian fishermen who receive military training and coordinate their actions under state and military guidance), and government vessels (e.g., coast guards)”¹⁹³, in order to assert control in an area and demonstrate power. While the strategies used by China are evident, the prioritization of the Chinese threat to NATO is an open debate in the alliance, and the steps desired to address it are asymmetrical.

The path forward for NATO in relation to the rise of China is one of strategic deterrence, with a focus on China’s activities in the gray zone, utilizing the wider alliance network, as well as enhancing its own strategies in the gray zone. First, it is important to analyze the gray zone strategies China is using and how they are integrated into a larger state-organized strategy to raise the specter of instability in order to gain more global legitimacy. Second, it is important to weigh the relation to NATO and why NATO needs to play a role in countering the gray zone strategies of China through strategic deterrence. Lastly, a look into the future possibilities of unchecked or balancing of power is needed and what role NATO plays in that future.

¹⁹² Freier, N. P., Burnett, C. R., Cain, W. J., Compton, C. D., Hankard, S. M., Hume, R. S., Kramlich, G. R., Lissner, J. M., Magsig, T. A., Mouton, D. E., Muztafago, M. S., Schultze, J. M., Troxell, J. F., & Wille, D. G. (2016). ENTER THE DRAGON – CHINA AS A HIGH-END GRAY ZONE REVISIONIST. In *OUTPLAYED: REGAINING STRATEGIC INITIATIVE IN THE GRAY ZONE* (pp. 33–40). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep12061.11>

¹⁹³ Morris, L. J., & Binnendijk, A. (2019). *Gaining competitive advantage in the gray zone: Response Options for Coercive Aggression Below the Threshold of Major War*. RAND Corporation.

In the disputed islands around the East China Sea and the South China Sea, China has been using civilian fishing vessels to assert control over the territory and resources. China has also been using its Coast Guard to push its jurisdiction there, which has gone as far as resulting in death.¹⁹⁴ By overwhelming the area with a Chinese civilian and government presence, China is seeking to legitimize its claim of the land by denying access to other states with a similar claim. China, at this time, does not seek to spark a larger military conflict as not to provoke the United States or NATO, so it resorts to these gray zone strategies that subtly hint to the possibility of military escalation.

Similar to the Soviet Union during the Cold War, China seeks to gain global legitimacy as a growing power, and even a superpower. China already has a rapidly growing and diverse economy, sizable population, expansive geography, advanced military, and strong soft power projection¹⁹⁵. The current objective is demonstrating this power projection through gray zone strategies, as previously stated, the stability-instability paradox demonstrates how China is unable to challenge the United States and NATO directly, therefore it resorts to regional displays of power to create new levels of normal. The first strategy, and most obvious, is military intimidation, whether large or small-scale.¹⁹⁶ China has done this by amassing troops near contested borders, large-scale exercises close to Taiwan, threatening military action against Vietnam for approving oil drilling, or provocative actions against the US military in the EEZ.¹⁹⁷ These strategies are more blatant and provocative and raise the visibility of gray zone strategies and are thus used sparingly. China uses other strategies much more often with attribution hazier.

The next strategy China engages to assert regional dominance is through paramilitary activities that blur the distinction between military and civilian.¹⁹⁸

¹⁹⁴ Ibid, 28

¹⁹⁵ Kalimuddin, M., & Anderson, D. A. (2018). Soft Power in China's Security Strategy. *Strategic Studies Quarterly*, 12(3), 114–141. <http://www.jstor.org/stable/26481912>

¹⁹⁶ Morris, L. J., & Binnendijk, A. (2019). Pg. 30.

¹⁹⁷ Ibid, 31-32

¹⁹⁸ Ibid, 33

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

China uses maritime law enforcement that challenges the conventions of maritime law. The law enforcement uses techniques like ramming, shouldering, and water cannons to dispel foreign civilian vessels from the area. The use of a coast guard to use the tactics blurs the line of the role of law enforcement in peacetime and potential military action.¹⁹⁹ Additionally, China also uses civilian vessels for this same purpose but they are crewed by Navy reservists or those with naval military training creating a type of maritime militia that confuses the boundary of what is state or civilian action.²⁰⁰ Furthermore, China uses state-owned or state-affiliated businesses to advance Chinese interest in disputed areas by licensing oil drilling, or dredging to create artificial islands.²⁰¹

The creation of these artificial islands is used to demarcate borders and manipulate them in order to compel international legitimacy to Chinese expansion. After the creation of an artificial island, China is able to redraw its boundaries and economic zones, even placing these new borders on its passport so that foreign governments are compelled to stamp these passports with the new borders.²⁰² Similar to Russia, China also utilizes the information warfare space in order to create misinformation in the region to bring legitimacy to its actions. China does this through discrediting other states' claims to the disputed area through information campaigns and even disrupting the communications of other states' vessels through cyber campaigns against the Philippines and Japan, for example.²⁰³

Less tangible actions have been through China leveraging its legal, diplomatic, and economic power to achieve its aims. China has regulated fishing in the South China Sea in order to force foreign vessels to receive licenses to fish in the area around the pretext of preserving marine life, as well as ignoring

¹⁹⁹ Morris, L. J. (2017, March 8). The Era of Coast Guards in the Asia Pacific Is upon Us. Asia Maritime Transparency Initiative, *Center for Strategic and International Studies*.

²⁰⁰ Ibid, 34

²⁰¹ Ibid, 34

²⁰² Blanchard, B., & Mogato, M. (2012, November 28). China decries attempts to 'read too much into' passport map row. *Reuters*.

²⁰³ Piiparinen, A. (2015, September 18). The Chinese Cyber Threat in the South China Sea. *The Diplomat*.

international rules around fishing and economic rights of the sea.²⁰⁴ Another useful gray zone tool is economic coercion to influence its behavior around disputed areas, but also around human rights abuses. It has issued travel bans in South Korea to try to prevent US missile defense systems from being installed, banning rare earth metal imports to Japan after a fishing dispute, as well as other import bans with the Philippines and Norway, imposing export fees on Mongolia after allowing a visit from the Dalai Lama, or limiting Chinese workers or tourists to certain countries over disputes in these areas.²⁰⁵

The actions have mostly gone unchecked and have allowed China to dominate these regions and “achieve warlike aims without resorting to warlike violence”.²⁰⁶ In 2012, United States President Barack Obama outlined in the “Defense Strategic Guidance”, a new American pivot to the Asia-Pacific region due to the heavy economic and security interests. NATO first acknowledged China as an important topic at the 2019 London Summit when it argued that China's “growing influence and international policies present both opportunities and challenges that we need to address together as an Alliance.”²⁰⁷ Dealing with the rise of China requires a delicate approach from NATO, and challenging the gray zone strategies imperative to maintaining international stability. A rising China does not necessarily mean conflict or a decline of Western power. Similar to the “Thucydides Trap” about the cause of the Peloponnesian War which revolved around the growing power of Athens and the fear that provoked from Sparta.²⁰⁸ The metaphor is useful because even though China is growing and it is sparking fear in the West, but even if the growing China variable is unavoidable, the Western response is the most important as it can avoid conflict like the one between Athens and Sparta.

²⁰⁴ Morris, L. J., & Binnendijk, A. (2019). Pg. 38.

²⁰⁵ Ibid, 39

²⁰⁶ Freier, Et. al. (2016). Pg. 33.

²⁰⁷ Simón, L. (2023, November 23). NATO's China and Indo-Pacific conundrum. *NATO Review*. Retrieved from: <https://www.nato.int/docu/review/articles/2023/11/22/natos-china-and-indo-pacific-conundrum/index.html>

²⁰⁸ Nye, J. S. (2020). Perspectives for a China Strategy. *PRISM*, 8(4), 120–131. <https://www.jstor.org/stable/26918238>

NATO deterrence against China does not contain the same urgency from the alliance as it does with Russia. Russia directly invaded a NATO ally, as well as continuously provoked the alliance through different gray zone approaches. China on the other hand, does not directly instigate NATO, but rather seeks a sphere of influence in Asia, and raises tensions with neighboring countries instead. This is why a strategic deterrence is needed for China, as it is using this regional display of power to create a greater power advantage in order to then challenge NATO from a stronger position. The current challenge to the alliance is the displaced urgency on addressing China, thus creating an “alliance security dilemma”.²⁰⁹ China presents a more immediate challenge to the United States than the European NATO members, and this imbalance of threat perception can create a security dilemma within the alliance through either entrapment or abandonment.²¹⁰ Entrapment exists when an ally is dragged into a conflict over another ally’s interest that it does not share or only shares partially. Abandonment in the alliance security dilemma exists when there is a defection from realignment or dealignment from a conflict.²¹¹ With regard to China and NATO what is most likely to occur is entrapment especially in light of dueling hot conflicts between Russia and with China.

Conversely, what makes NATO unique to this security dilemma is the nature of alliance compared to other alliances historical or contemporary. NATO exists as a “tight alliance” due to the existence of Article V and its collective defense commitment.²¹² Meaning that in the face of threats from either Russia or China, the alliance requires deliberation and weighing of mutual priorities when crafting deterrent responses. Additionally with a tight alliance it requires joint military drills, integrated operations, rotational deployments, and access agreements to not only signal to others in the alliance but to the adversaries as well.²¹³ In regards to China,

²⁰⁹ Snyder, G. H. (1984, July). The Security Dilemma in Alliance Politics. *World Politics*, 36(4), 466.

²¹⁰ Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

²¹¹ Ibid, 44

²¹² Ibid, 45

²¹³ Ibid, 45

NATO has begun showing a more concerted effort to challenge its expansionist aims rather than its economic growth. The biggest concern for NATO is China's competition and interference with key NATO allies like Japan, South Korea, Australia, and New Zealand.²¹⁴ This was expanded at the 2021 Brussels Summit, where NATO allies agreed, "China's stated ambitions and assertive behaviour present systemic challenges to the rules-based international order and to areas relevant to Alliance security".²¹⁵ Much of this is due to the continuing military connection between China and Russia, and both of their involvements in cyberspace and disinformation, thus raising the need to address China even higher within the alliance.

Moving forward NATO has a challenge of balancing both threats from China and Russia making it imperative to deter any possible conflict as the consequences would be dire. The main goal currently is bolstering the alliances in the region, and working to support their right to territorial integrity. The United States has already had a sustained military presence in the region, but could be supplemented by NATO members and regional allies like Australia and Japan.²¹⁶ Similar to Russia, China continues to make more enemies in the region than friends, which works in NATO's favor and should prompt NATO to work closer with less-allied nations like Mongolia, Thailand, Cambodia, and Indonesia. Furthermore, as contrasted with Russia, China has not engaged so adversarial with NATO, offering more time for potential diffusion of tensions and cooperation. Even with Russia and China both wanting to challenge the Western-led status quo, China offers an opportunity for, as Joseph Nye coins, a "cooperative rivalry"²¹⁷ where the differences between Russia and China are made more aware and spheres of influence are balanced by empowering neighboring countries with economic growth and soft power. This strategic deterrence avoids future conflict and presents the

²¹⁴ Simón, L. (2023, November 23). NATO's China and Indo-Pacific conundrum. *NATO Review*. Retrieved from: <https://www.nato.int/docu/review/articles/2023/11/22/natos-china-and-indo-pacific-conundrum/index.html>

²¹⁵ Ibid

²¹⁶ Freier, Et. al. (2016). Pg. 39.

²¹⁷ Nye, J. S. (2020). Perspectives for a China Strategy. *PRISM*, 8(4), 120–131. <https://www.jstor.org/stable/26918238>

alliance with new opportunities. The pivot to China can offer success if done properly without miscalculations and adequate planning for strategic advantage.

Historically NATO countries have made many mistakes on how it treats perceived threats, and mistakes in the heat of conflict. Similar to how NATO has treated China, and even Russia, in the past has taught lessons for how to approach them in the future. Beyond these two global powers, NATO has involved itself into conflicts with Libya, Iraq, Afghanistan, Bosnia and Herzegovina, and Kosovo where important goals were achieved and made beneficial impacts, but also mistakes occurred that have tarnished parts of NATO's reputation and its mandate for future threats.

Lessons from the Past: Kosovo, Afghanistan, Iraq, and Libya

Kosovo

The breakup of Yugoslavia led to the first war and genocide in Europe since World War II. In 1991 Slovenia was the first to declare independence, followed by Croatia, and then Bosnia and Herzegovina in 1992. Due to the ethnic diversity of Bosnia and Herzegovina, primarily Bośniak, Serb, and Croat, the independence from Yugoslavia was not equally desired by the population resulting in the predominantly Serbian controlled Yugoslav government under Slobodan Milošević to invade Bosnia to prevent its independence.

By 1996, the Dayton Accords were signed and the war in Bosnia ended, but the conflict in Kosovo was still ongoing from the Serbs. Kosovo was an ethnically Albanian autonomous province in Serbia. By this point the conflict in Kosovo began heating up as the Kosovo Liberation Army (KLA) returned to Kosovo to regain autonomy from Serbia after Milošević scapegoated the Albanian population as enemies to the Serbians. Violence breaks out and the international community becomes concerned hoping to avoid a Bosnia 2.0, which just ended a few years

earlier.²¹⁸ For fear of repeating these events the international community sought to look for possible ways to intervene to stop the fighting. Eventually NATO started making plans (against the wishes of Russia) to intervene militarily to force Milošević to stop. NATO began airstrikes against strategic Serb locations, and eventually Serb forces to escalate a ceasefire. After a 78-day campaign, the Serbs agreed to surrender and pulled out of Kosovo, meeting NATO's demands.²¹⁹

NATO's first miscalculation was its perception that the intervention would only require a couple of days. The 78-day conflict was a result of misjudging the culture and history of Serbia and Kosovo and understating the importance of Kosovo to Serbian identity and history.²²⁰ NATO was able to prevent the mass killing of Kosovar Albanians and by doing so created a blueprint for successful interventions in the future. However, the intervention into Kosovo highlighted a major deficiency in the model of NATO, that was also seen in Afghanistan and Libya, in that NATO deliberations to reach consensus and strategy can become an obstacle to successful missions.

In organizing plans to intervene in Kosovo many NATO members caveats and preferences began to slow down the process, even during the airstrikes.²²¹ The main difference among the allies was the pace and the intensity of the operation and the potential use of ground forces. Debating the details of the intervention helped draw it out when more decisive action on heightened airstrikes and the threat of ground invasion would have made Milošević capitulate sooner.²²² The lesson to take from this is that in the face of a more capable adversary these lengthy deliberations

²¹⁸ Gromes, T. (2019). NATO'S KOSOVO INTERVENTION IN OVERVIEW. In *A HUMANITARIAN MILESTONE?: NATO'S 1999 INTERVENTION IN KOSOVO AND TRENDS IN MILITARY RESPONSES TO MASS VIOLENCE* (pp. 3–8). Peace Research Institute Frankfurt. <http://www.jstor.org/stable/resrep19997.5>

²¹⁹ Johnson, D. E. (2007). Kosovo, 1999. In *Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era* (pp. 65–90). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg405af.11>

²²⁰ Ibid, 65

²²¹ Pettyjohn, S. L., & Wasser, B. (2022). A Framework for Integrated Deterrence with Allies and Partners. In *No I in Team: Integrated Deterrence with Allies and Partners* (pp. 10–19). Center for a New American Security. <http://www.jstor.org/stable/resrep46863.7>

²²² Ibid, 16

would have more deleterious outcomes that could cause higher casualties or lose a war.²²³

Afghanistan

Fifty years after its creation, for the first time ever, NATO had found itself conducting an operation outside of Europe.²²⁴ The attacks on September 11, 2001 in the United States sparked the first time Article V was invoked by a NATO member, prompting a collective response against Al-Qaeda in Afghanistan. It was not an easy decision for the alliance, as some members did not think NATO should leave its mandate in Europe and pursue operations around the world. Moreso, behind the scenes the United States did not fully plan to incorporate the alliance with its response in Afghanistan; there was no intention to incorporate NATO directly through its collective assets to command structure. Deputy Secretary of Defense Paul Wolfowitz stated the day before the operation in Afghanistan:

“We think we had a collective affirmation of support with what they said with Article Five, and if we need collective action we’ll ask for it. We don’t anticipate that at the moment ... We need cooperation from many countries but we need to take it in appropriately flexible ways”.²²⁵

Already showing the first failure of the operation as it relates to NATO by not fully incorporating it as a NATO mission, but as a US mission with NATO support, leading to future fragmentations, miscommunications, and misplacements of goals.

One of the first differences that appeared in the alliance was the overall objective of the mission. The American objective, through Operation Enduring Freedom (OEF) was to ‘disrupting, dismantling, and defeating Al-Qaeda and

²²³ Ibid, 16

²²⁴ Hoehn, A. R., & Harting, S. (2010). A Greater Role for NATO in Afghanistan. In *Risking NATO: Testing the Limits of the Alliance in Afghanistan* (pp. 25–40). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg974af.11>

²²⁵ Wolfowitz, P. (2001, September 26). Press Conference, NATO HQ. Quoted in Kreps, S. E. (2011). *Coalitions of Convenience: United States Military Interventions after the Cold War* (pp. 95–96). Oxford University Press.

Taliban’, but many of the European members were much more broad and included nation-building as a postwar objective.²²⁶ And then two years into the war the reality in Afghanistan turned from a commitment to stabilization and reconstruction in limited areas to the security of the entire country.²²⁷ The responsibilities of NATO grew over time adding to the vagueness of the mission and its goal, ultimately leading the alliance into a fragmented security force of an entire country. The responsibilities were also delegated to various members of the alliance where security of different provinces was left in charge of either the US, UK, Germany, France, Italy, or the Netherlands contributing to this fragmentation.²²⁸

Furthermore, the disagreements in the alliance and moving forward without a united objective further exacerbated the operation. When the United States Congress authorized the use of force in 2001 it was not specified solely to Afghanistan; it was open-ended in terms of geography and timeline, giving fear to some European partners that this could pull NATO into perpetual conflict in the ‘War on Terror’, and specifically the not-so-secret destination of Iraq, next.²²⁹ This prompted an existential crisis for NATO at the time. Without the Cold War motive that fueled the resolve of NATO in the past, what future does the alliance have? Afghanistan offered an opportunity to address this question, but with conflicting views throughout its timeline. The NATO Secretary General in June 2002 George Robertson stated that NATO is not seeking “out of area” roles for the alliance, and that NATO has always been a “defence alliance, and we remain a defence alliance”²³⁰, but in September, three months later, Robertson discussed refocusing

²²⁶ Berdal, M. (2016). A Mission Too Far?: NATO and Afghanistan, 2001–2014. In D. MARSTON & T. LEAHY (Eds.), *War, Strategy and History: Essays in Honour of Professor Robert O’Neill* (pp. 155–178). ANU Press.

<http://www.jstor.org/stable/j.ctt1dgn5sf.16>

²²⁷ Hoehn, A. R., & Harting, S. (2010). Pp. 29.

²²⁸ Ibid, 33

²²⁹ Hoehn, A. R., & Harting, S. (2010). Redefining NATO’s Role: 9/11 to Afghanistan. In *Risking NATO: Testing the Limits of the Alliance in Afghanistan* (pp. 13–24). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg974af.10>

²³⁰ Robertson, G. (2002, June 6). NATO Secretary General, transcript of press conference. Brussels: NATO Headquarters.

NATO's priorities on terrorism and the dangers of weapons of mass destruction, opening up the possibility of placing NATO on the offensive.²³¹

With NATO becoming the primary security force in the country, it had to make a switch from military operations to civilian, engaging the police forces to bring stability. This brings to light the challenges Col. Luigi Bramati, Director of the NATO Policing Stability Centre of Excellence discussed with me, primarily around the areas of information jealousy, and the failure of systems to communicate with each other. As a multinational force, jealousy of information is a natural side-effect, he explains. With a multitude of different regulations from each country, and since policing is within the jurisdiction of each member state making the streamlining of information difficult. In the nature of a graying world of conflict, much of the incoming threats, according to Bramati, under the radar of collective defense, and thus local law enforcement and intelligence are the ones to pick it up, and without being able to connect the dots with one another it becomes difficult to move forward together as an alliance towards these ambiguous gray threats.

An example of information jealousy, or even information distrust, in Afghanistan was noted how Turkey made NATO cooperation difficult when it came to sharing intelligence within the NATO-EU collaborations because it would block intelligence to be shared with Afghan forces because the EU would have the same access to it, and as some EU members are not members of NATO—specifically Cyprus—Turkey would prevent its release.²³² Since intelligence gathering is a responsibility of individual member states, there is no NATO-wide intelligence agency, so sharing information comes down to a country's ability to trust more on a bilateral relationship rather than a multilateral way. As a result of this natural tendency, intelligence sharing slows down and centers around assurances not to be shared again, protection of sources, and possible *quid pro quos*.²³³

²³¹ Hoehn, A. R., & Harting, S. (2010). Pp. 18.

²³² Hoehn, A. R., & Harting, S. (2010). Pp. 36.

²³³ Ballast, J. (2017). *Trust (in) NATO: The future of intelligence sharing within the Alliance*. NATO Defense College. <http://www.jstor.org/stable/resrep10248>

The lesson learned from Afghanistan in this regard showed the need to centralize intelligence as best it could, and restructure intelligence from being less US-centered to being truly multilateral.²³⁴ And has the 2021 withdrawal showed, NATO needs to work together in all actions, as the US-centered evacuation was mired in rushed decision-making and flawed design.²³⁵ During the conflict in 2006 the alliance created the NATO Intelligence Fusion Centre (NIFC) with a designated “intelligence chief” in order to help make intelligence a more centralized effort and make the process more streamlined. Col. Bramati recognized these issues as well and mentioned that the regulations that existed during the wars in Afghanistan and Iraq led to mismatched intelligence sharing, and so reforms were made to enhance the system and make it more collaborative. This will be imperative to adapting NATO to the future of domain operations, and the rising trend of hybrid warfare.

Iraq

The lessons from Afghanistan can be replicated in Iraq, but also expanded. Afghanistan showed that “military force can initially bring violence down, but it cannot ensure lasting peace alone.”²³⁶ Iraq differs from the war in Afghanistan since NATO was not directly involved and only the UK and Poland assisted the US in its operation. Specifically, France and Germany were against any type of invasion of Iraq. Although at the request of United States President George W. Bush, NATO states did offer assistance in training the Iraqi Armed Forces and the police force, but NATO made it important to mention that this was solely a US-led mission.²³⁷ Subsequently, in 2018, after the rise of ISIL in Iraq and Syria, NATO launched the

²³⁴ Gordon, J. S. (2017). Intelligence sharing in NATO. *Atlantisch Perspectief*, 41(6), 15–19. <https://www.jstor.org/stable/48581386>

²³⁵ NATO. (2021). *Afghanistan lessons learned*. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/12/pdf/2112-factsheet-afgh-lessons-en.pdf

²³⁶ Schmitt, G. J. (Ed.). (2020). NATO: THE CURRENT CHALLENGE. In *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners—Second Edition* (pp. 187–224). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep27713.11>

²³⁷ Clausen, M.-L., & Albrecht, P. (2022). DISTANCE EXEMPLIFIED – NATO IN IRAQ. In *EXPLORING DISTANCE IN SECURITY FORCE ASSISTANCE: THE CASE OF NATO MISSION IRAQ* (pp. 11–19). Danish Institute for International Studies. <http://www.jstor.org/stable/resrep43420.7>

NATO Mission Iraq (NMI) to scale up its training and advisory efforts.²³⁸ The purpose of this mission is to help the Iraqi defense and police forces target ISIL and establish stability in the country. After working with the Iraqi Ministry of Defense, NMI noticed the rampant and bloated corruption and switched from purely advisory to a longer-term strategy of system reform and internal influence.²³⁹

Col. Bramati highlighted this point in our discussion about NATO assistance in Iraq. Some of the confusion that exists in NMI comes back to the culture of the NATO countries themselves and their own perceptions of policing and the military. As previously touched upon, the United States and a country like Italy organize the police and military differently. In the United States, law enforcement is primarily local or state, even though the FBI exists, there is clear delineation between the powers and responsibilities of federal, state, and local police. Furthermore, the military is completely separate from policing and is only called upon to assist the police in a state of emergency, otherwise the responsibilities are separated as the police in the US cannot act as a paramilitary.

Since the US-led operation brought with it a US-centered perception of military and policing, it neglected the potential for the two to work together. The military was seen as leading the role of neutralizing threats and the police were seen as the ones to provide the service of law enforcement. According to Col. Bramati, without sufficient and comprehensive plans beforehand, many of the miscommunications and implementation gaps could have been avoided in Iraq, when it came to military and police training. This shows the need to change the notion of collective defense to not only be around territorial deterrence and defense, but to incorporate cooperative security and crisis management as key components to strategic deterrence and the transition to threats in the gray zone.²⁴⁰

²³⁸ Ibid, 13

²³⁹ Ibid, 13

²⁴⁰ Dresen, R. (2023). *NATO's Strategic Concept from theory to practice: NATO Mission Iraq*. NATO Defense College. <http://www.jstor.org/stable/resrep48882>

Libya

The United Nations Security Council authorized military intervention into Libya in 2011, allowing NATO to implement a no-fly zone and launch attacks against the Libyan government led by Muammar Gaddafi. Seven months later, rebel forces conquered the country and killed Gaddafi.²⁴¹ This was initially seen as a success by Western media as an organic overthrow of a dictator and a transition to democracy, but a retrospective analysis shows this was not necessarily the case, and the handling by NATO shows mistakes and lessons to be taken from the intervention.

The intervention by NATO into Libya was successful, but also mired in miscalculations that sparked disunity and destruction. It is important to highlight both the successes and the mistakes made in Libya to inform future operations of NATO, especially how they can be used to strengthen operations through the expanding domains and gray areas of conflict.

The successful lessons to be taken from Libya center around NATO's ability to adapt quickly and restructure mid-conflict if needed. A major concern among NATO leaders in 2010 was about NATO's ability to move on from Afghanistan and adjust to a new Strategic Concept that could transition smoothly. The intervention into Libya occurred soon after in 2011 and NATO was able to commit forces again within four months with agility, showing the alliance's flexibility to adjust to conflicts.²⁴² The intervention demonstrated that the alliance is capable of uniting for a goal and is best suited for these operations as the EU's common defense policy and collective defense obligations do not have the capacity to work quickly and engage in large operations.²⁴³

Additionally, the intervention was able to help reintegrate France into the alliance when it rejoined NATO's integrated military structures in 2009. The

²⁴¹ Kuperman, A. J. (2013). A Model Humanitarian Intervention? Reassessing NATO's Libya Campaign. *International Security*, 38(1), 105–136. <http://www.jstor.org/stable/24480571>

²⁴² Wilson, D. M. (2011). *Learning from Libya: The Right Lessons for NATO*. Atlantic Council. <http://www.jstor.org/stable/resrep03354>

²⁴³ Ibid, 2

intervention demonstrated the importance of France in the alliance since it essentially served as the lead nation of the operation, showing that working through the alliance serves a greater legitimacy than working around it.²⁴⁴ The alliance has the potential to work effectively with the right planning, sufficient flexibility, and unity in purpose and Libya helped demonstrate that.

Unfortunately, there were also miscalculations and mistakes made in Libya that require analysis to help the alliance be better prepared for future operations and threats. The primary mistake in Libya was extending the mission beyond the scope established by the UN Security Council of civilian protection, and covertly setting a separate goal of toppling the Gadaffi regime. By looking to support the rebels in their political aims there became a blurring of the objective and it extended the conflict longer than needed, which ultimately required a long-term stabilization force in the country.²⁴⁵

When the United States turned over primary control of the operation to the British and French, the objectives of the intervention were muddled, going beyond the original scope. For future operations, especially in the gray zone, the United States needs to take a more central role in the planning and execution as it is the only member with the capacity and capabilities to engage long-term and financially burdensome operations.²⁴⁶ The portions of the intervention led by the French and Italian forces were successful initially but they quickly were shown to not have the longevity to last more than a few weeks. The French, Italian, and even British forces were required to rely on the United States forces for weaponry, logistics, and finances to continue their operations.²⁴⁷

By changing the control of the intervention to the European powers it changed the trajectory from a few weeks, to a few months due to the lack of planning, resources, and finances. As previously discussed about military

²⁴⁴ Ibid, 2

²⁴⁵ Kuperman, A. J. (2013). Pp. 123.

²⁴⁶ Brzezinski, I. (2011). Lesson From Libya: NATO Alliance Remains Relevant. *National Defense*, 96(696), 18–19. <https://www.jstor.org/stable/27019211>

²⁴⁷ Ibid, 1

capabilities, the European forces do not have the same capabilities as the Cold War era and until major investments are made, the US cannot back away from leading operations. In order to achieve the political aims of toppling Gadaffi, the intervention was extended further leading to more violence in the country resulting in more civilian casualties.²⁴⁸ The debate around whether this political goal was necessary is beyond the scope of this paper, but it certainly added to lessons for the alliance in strategic planning that need to be adapted in the future.

When operating in the multidomain of future gray zone conflicts NATO needs to focus on its ability to center its strategic planning, integrate deterrence, and enhance capabilities across the alliance to enable more equitable and efficient burden-sharing. The lessons from Libya have shown that the US currently has most of the capacity within the alliance, moving forward the other states need to develop capabilities for long-term and hybrid threats for greater effectiveness towards future threats.

In order to inform the future, NATO needs to take the lessons from mistakes and successes of past operations to adapt to the changing reality of a multipolar world. From this chapter, using the lessons from the past, it is my assessment that Afghanistan has shown that strategic objectives are required for a long-term operation, and utilizing the whole-of-organization approach to conflict is needed. The multitude of threats and challenges that arose were not suited for NATO's structure, and required higher flexibility to adjust to the changing reality on the ground. Iraq demonstrated that alliance politics need to be paramount to operations and taking into account the different cultures, histories, and advantages of member states enhances the alliance as a whole. Adapting the alliance structure to speed and collaboration will strengthen NATO in the future when gray zone challenges become more evident. Burden-sharing and capabilities are still key to any NATO operation as Libya has shown, and European allies need to begin boosting capabilities to adapt to these future challenges so as not to become over reliant on

²⁴⁸ Kuperman, A. J. (2013). Pp. 132.

the United States. Moreso, as shown in Kosovo, strategic planning and quick deliberation are needed more than ever. Hybrid warfare is becoming more likely over time and NATO needs to adapt to these challenges and do so quickly or else it could fall behind to being a 20th century military alliance.

Hybrid Warfare and Strategic Advantage

Hybrid warfare within the gray zone is not necessarily a new or modern feature to the nature of war and conflict. Sun Tzu wrote in *The Art of War*, “to subdue the enemy without fighting is the acme of skill.”²⁴⁹ If an actor is able to discover means to neutralize an adversary without the use of a military it would be the most beneficial solution, thus showing why states resort to this strategy to challenge the global power structure. As a form of deterrence, a state would be mistaken to focus solely on conventional threats as this focus would obscure the complexity of threats and oversimplify the challenges.²⁵⁰ The alliance needs to be strategic about deterrence from hybrid threats by adapting to the continuum of conflict, or as Prussian war theorist Carl Von Clausewitz argued, war is an ever-evolving, interactive phenomenon.²⁵¹

NATO, as a product of the Cold War, has had a long focus on conventional and interstate warfare. As such, no other state would seek war with NATO due to this heavy advantage. This is why creating a strategic advantage in the gray zone is paramount to future NATO strategy in hybrid deterrence. This requires a need of understanding the complexity of conflict and how it exists within the continuum of conflict, in order to generate workable solutions. The continuum of conflict portrays a range of potential conflicts compared against an increasing level of violence to

²⁴⁹ Sun Tzu. (1963). *The Art of War* (S. Griffith, Trans.). New York: Oxford University Press.

²⁵⁰ Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM*, 7(4), 30–47. <https://www.jstor.org/stable/26542705>

²⁵¹ Ibid, 32

illustrate how conflict does not exist on a black-white dichotomy, but rather a spectrum of low-level unarmed measures, to large-scale conventional war.²⁵²

This dissertation so far has documented various methods and means that adversaries have been testing the NATO alliance through gray zone strategies and hybrid threats. Responding to these threats and building infrastructure to respond to future threats within the alliance framework is necessary for security and deterrence. NATO must get ahead of hybrid threats and create an advantage in deterrence, which first requires laying out the principles necessary to create a plan going forward.

First, it is not enough to simply mitigate losses; advantage requires a forward-thinking strategy. It needs to incorporate an ability to respond quickly to provocation, lead through the multilateral process, understand the local culture and government, and respond appropriately to the nature of the threat.²⁵³ Under these principles a strategy for NATO can be created that not only mitigates the current threats but allows future operations in the gray zone that put the alliance at an advantage.

Placing hybrid threats along the continuum of conflict is much easier said than done. The spectrum includes threats that can be classified as persistent, moderate, or aggressive, each with specific characteristics for classification. But not all hybrid threats can be cleanly placed in any category and thus the nature of responding requires a human element that could lead to an over- or under-response.²⁵⁴ An aggressive threat would require an immediate deterrence, a moderate threat would require active deterrence over a period of time, and persistent threats would allow living with them but also competing against. Overall, these types of threats will need different tools over a different time frame, in addition to

²⁵² Ibid, 32

²⁵³ Morris, L. J., & Binnendijk, A. (2019). *Gaining competitive advantage in the gray zone: Response Options for Coercive Aggression Below the Threshold of Major War*. The RAND Corporation.

²⁵⁴ Ibid, 137

having an alliance-wide ability to decide on redlines that cannot be crossed without a prompt response.²⁵⁵

NATO has already been establishing mechanisms to respond to hybrid threats in the gray zone. It is already becoming apparent that these adaptations and processes will need to become a permanent feature to the alliance structure. Firstly, the efforts to consolidate information sharing and overcome the political and logistical obstacles that exist with the creation of the Joint Intelligence and Security Division (JSID) has begun helping to streamline intelligence sharing. This has also been adapted into military operations by incorporating hybrid operations into military drills. Although not as apparent, these operations are important in case of military threats with gray zone elements to promote the alliance's ability to respond effectively.²⁵⁶ Furthermore, NATO has been making a concerted effort to build up resilience abilities in case of gray zone attacks, primarily around energy supplies, uncontrolled movement of peoples, critical government services, food and water resources, dealing with mass casualties, as well as communication and transportation systems.²⁵⁷

These measures alone are not enough and need to be prioritized further and adapted to the specific hybrid threats the alliance is facing. Russia has already created a strategic plan against NATO called, “strategy of active defense”, with the goal of destabilizing allies, disrupting the decision-making process, and inhibiting NATO's military options for defense.²⁵⁸ Russia has already begun using tactics in Ukraine, seeking to expand its sphere of influence in order to place itself in a higher position of power vis-à-vis NATO, known as “simmering borscht”.²⁵⁹ In the event of a more heated confrontation, Russia would resort to a variety of cyber-attacks

²⁵⁵ Ibid, 137-138

²⁵⁶ Ozawa, M. (2021). Adapting NATO to grey zone challenges from Russia. In T. Tardy (Ed.), *NATO 2030: new technologies, new conflicts, new partnerships* (pp. 19–32). NATO Defense College. <http://www.jstor.org/stable/resrep29562.8>

²⁵⁷ Ibid, 26

²⁵⁸ Schmitt, G. J. (Ed.). (2020). NATO: THE CURRENT CHALLENGE. In *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners—Second Edition* (pp. 187–224). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep27713.11>

²⁵⁹ Hoffman, F. G. (2018)

that give it a strategic advantage conventionally. This requires NATO to enhance the resilience of its cyber capabilities as there is a capability gap among member states in countering cyber threats.²⁶⁰

In order for this to be accomplished NATO must develop a strategic concept that can be deployed in the face of hybrid threats. Based on the severity of threats, a strategic concept helps identify the threat, as well as the appropriate alliance-wide response that enhances deterrence and resilience. The first step, as laid out by Morris and Binnendijk of the RAND Corporation, to this concept is setting the strategic context. The gray zone challenges are part of a larger geopolitical competition that rely on local factors for success. This requires boosting resilience in states that would receive the brunt of gray zone threats, like the Baltic States and Poland, as well as boosting a narrative around the world about how these threats undermine the international rules-based order.²⁶¹ Setting this context will require reaffirming alliance solidarity and resolve, working with other regional actors like the EU and ASEAN, and promoting more military training and drills with a focus on hybrid threats and operations.²⁶²

The next step is to increase deterrence of highly destabilizing gray zone threats. This requires having publicly stated redlines that would prompt a response to NATO and showing the resolve to follow through. Furthermore, this requires publicly defining what gray zone threats could be used that would prompt a response, as is the nature of the continuum of conflict. Russia has already shown it is willing to use hybrid tactics to achieve geopolitical gains that enable it to make even more aggressive moves later on. In 2014, with the “little green men” in Crimea which allowed Russia to avoid attribution, to later annexing Crimea, and then ultimately invading Ukraine altogether, showed that NATO was unwilling to offer a strong deterrent message to aggressive gray zone strategies resulting in a higher level of global instability.²⁶³ An example of a future aggressive gray zone strategy

²⁶⁰ Ozawa, M. (2021).

²⁶¹ Morris, L. J., & Binnendijk, A. (2019). Pp. 139-140.

²⁶² Ibid, 140

²⁶³ Ozawa, M. (2021). Pp. 21.

from Russia would be paramilitary aggressive within a NATO state like the Baltics. Establishing redlines increases the deterrence threshold and sends a strong message to Russia against heightening the conflict.²⁶⁴

Next, NATO needs to address moderate gray zone threats by dissuading their use over time. These types of threats normally have a higher difficulty of attributing blame or do not rise to the level of threat that needs an immediate response, which could include large-scale disinformation campaigns, or threats against civilian actors in international waters. Once identified as a moderate threat the appropriate action to respond is through dissuasion, which includes addressing the security concerns of the potential aggressor.²⁶⁵ This requires taking into account the concerns of Russia and China within the framework of international norms and rules, in order to not be perceived as aggressive as well. But in addition, this will need consistent global pressure on gray zone aggression and building a global coalition against these measures, making aggressors pay a greater price diplomatically.²⁶⁶ This also needs to be followed up with increasing costs if aggression continues to persist, through the means of possible sanctions or other economic measures.

Lastly, as the domains of operation continue to evolve into space and through cyber, it remains paramount that NATO invest further in cyber deterrence and space operations. Cyber defense and counterintelligence will need to be scaled up and expanded across the alliance if any serious deterrence is to take place. Ultimately a lack of clarity in addressing hybrid threats in the gray zone can become problematic which is why I propose prioritizing resources to address the threats as they exist and as they will exist in the future. It is impossible to know what future threats will exist, as this dissertation has shown, preparing the infrastructure to quickly adapt to these threats lessens the need to respond militarily, and enhances

²⁶⁴ Morris, L. J., & Binnendijk, A. (2019). Pp. 145.

²⁶⁵ Ibid, 149

²⁶⁶ Ibid, 150

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

deterrence in the gray zone. Working alongside a modernized interoperable strategic plan and the NATO alliance can adapt to the new challenges when they appear.

VII. The Relevancy of Interoperability

The State of Interoperability

Interoperability has always been an evolving concept in the NATO lexicon, it is malleable enough to be bent into many boxes of usage. In the most general sense, it has been defined by NATO as, “the ability for Allies to act together coherently, effectively and efficiently to achieve tactical, operational and strategic objectives.”²⁶⁷ Interoperability is broken down into four different dimensions: technical, procedural, human, and information.²⁶⁸ NATO maintains a Standardization Office (NSO) in order to facilitate interoperability among the dimensions but many challenges arise outside the NSO’s ability. Navigating the armed forces of 32 countries can be difficult. From the technical dimension it is noted by NATO that equipment standardization is not necessary as long as “that equipment can share common facilities and is able to interact, connect and communicate, exchange data and services with other equipment.”²⁶⁹ However, challenges still arise from the diversity of equipment, especially from Eastern European states joining NATO still utilizing former Soviet equipment. Competition exists among national and regional military industries, as well as technology not being shared within the alliance, all of which leads to standardizing equipment being the most impactful, yet most difficult to implement in terms of NATO interoperability.²⁷⁰ NATO has been making progress in this regard, the F-35 program being an example, but more work is required.

The 2018 NATO Summit in Brussels resulted in the continued effort of NATO member-states to reduce their dependence on Russian equipment, specifically stating the Alliance is, “working to address, as appropriate, existing dependencies on Russian-sourced legacy military equipment through national efforts and multinational cooperation.”²⁷¹

²⁶⁷ NATO. (2023). NATO. Interoperability: connecting forces. https://www.nato.int/cps/en/natohq/topics_84112.htm

²⁶⁸ Ibid

²⁶⁹ Ibid

²⁷⁰ Maranian, S. J. (2015). *NATO Interoperability: Sustaining Trust and Capacity within the Alliance*. NATO Defense College. <http://www.jstor.org/stable/resrep10254>

²⁷¹ NATO. (2018). NATO Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_156624.htm

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

Achieving this goal becomes more difficult as many former Warsaw Pact members cannot bear the costs of modernization creating complications on whether to support NATO interoperability or to meet their own baseline capability targets.²⁷² Additionally, as NATO expands east and south it requires suitable infrastructure that can accommodate NATO equipment causing logistical problems in military readiness and ground reinforcement.²⁷³ Much of this came from lack of foresight from NATO itself in welcoming new members, and did not anticipate how much infrastructural capacity would be needed, including the logistical challenges from administrative constraints needed for border crossings.²⁷⁴ It is also not only the former Warsaw Pact members with these logistical challenges either. A 2017 RAND study evaluated the abilities of the United Kingdom and France to respond to threats and found it would take a few weeks to over a month to send and sustain a brigade for forward employment.²⁷⁵

Many of these obstacles toward interoperability are due to its evolving nature and NATO lagging to keep up. The perception of what is considered a threat and how to respond plays a major role in where NATO can act together coherently. Additionally, the relationship between member states leads to credibility and cohesion in making future plans together. The purchase of the Russian S-400 air defense system by Türkiye highlights this potential disconnect. This created tension within the Alliance due to incapability for the Russian designed system to integrate within the NATO system and showing Türkiye's willingness to go against the Alliance if needed. The United States even suggested to Türkiye to donate the system to Ukraine for air defense but Türkiye stated that this proposal

²⁷² Clark, J. P., Pfaff, C. A., Burgess, K. J., Cuccia, P. R., Fleming, A. J., Graham, K. M., Gustafson, J. S., Hillison, J. R., Morrow, C. D., Mowchan, J. A., Thompson, D. C., & Wolfe, A. M. (2020). A STRATEGIC AND OPERATIONAL ANALYSIS OF EUROPE IN 2028: DEFINING ALLIES AND PARTNERS. In *STRIKING THE BALANCE: US ARMY FORCE POSTURE IN EUROPE, 2028* (pp. 25–40). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep25429.8>

²⁷³ Ibid

²⁷⁴ Scaparrotti, C. M., Bell, C. B., Schroeder, W., Starling, C. G., & Rodihan, C. (2020). Enhancing Deterrence and Readiness: The Role of Military Mobility. In *MOVING OUT: A Comprehensive Assessment of European Military Mobility* (pp. 6–9). Atlantic Council. <http://www.jstor.org/stable/resrep24666.5>

²⁷⁵ Shurkin, M. (2017). *The Abilities of the British, French, and German Armies to Generate and Sustain Armored Brigades in the Baltics* (No. RR-1556-OSD). RAND Corporation. https://www.rand.org/pubs/research_reports/RR1556.html

interfered with their sovereignty.²⁷⁶ Before making this proposal the United States removed Türkiye from the F-35 program due to fears that this technology might be compromised by Russia obtaining some valuable information on the stealth program.²⁷⁷ Further, Türkiye is looking to become a regional power that is not beholden to US or NATO influence and through buying the S-400 air defense system it can signify its independence.²⁷⁸ Interoperability becomes more than a technical or structural challenge when internal politics and different perceptions of threats are in play.

The next portion of NATO's interoperability goals lies within procedural interoperability, which as NATO states, includes uniform implementation of doctrines and procedures.²⁷⁹ Difficulties in procedural interoperability come from enacting agreed-upon doctrines, as well as facilitating the capabilities of NATO states to implement the policies in order to have effective deterrence. Effectiveness in procedural interoperability is measured by how well it can align its resources for sustainment, operational reach, and freedom of movement.²⁸⁰ NATO addresses this through standardization agreements among the member states. Since every country has different ways to implement directives, the challenges to interoperability come from streamlining the requirements and bureaucratic differences of countries.²⁸¹

One method NATO has employed to respond to its deterrence deficit in regards to interoperability was the creation of Operation Enhanced Forward Presence, at the 2016 Warsaw Summit. Enhanced Forward Presence is the rotating of NATO militaries in the Baltic states and Poland in order to enact a new strategy of deterrence by denial against Russia, and its annexation of Crimea in 2014. The summit communique details the operation as, "enhanced forward presence will comprise multinational forces provided by

²⁷⁶ Aydoğan, M. (2023, May 7). Türkiye rejected US proposal to send Russian S-400 defense system to Ukraine: Foreign minister. *AA News*. Retrieved December 30, 2023, from <https://www.aa.com.tr/en/turkiye/turkiye-rejected-us-proposal-to-send-russian-s-400-defense-system-to-ukraine-foreign-minister/2891323>

²⁷⁷ Atlamazoglou, C. (2023, July 9). Turkey isn't getting much use out of its Russian-made missile-defense system, but that's not why Erdogan is keeping it around. *Business Insider*. <https://www.businessinsider.com/turkey-russia-s400-too-politically-costly-to-get-rid-of-2023-7?r=US&IR=T>

²⁷⁸ Ibid

²⁷⁹ NATO. (2023). NATO. Interoperability: connecting forces. https://www.nato.int/cps/en/natohq/topics_84112.htm

²⁸⁰ Gamble, D., & Letcher, M. (2016, September). *The Three Dimensions of Interoperability for Multinational Training at the JMRC*. US Army. Retrieved February 1, 2024, from <https://alu.army.mil/alog/2016/SEPOCT16/PDF/173432.pdf>

²⁸¹ Ibid

framework nations and other contributing Allies on a voluntary, sustainable, and rotational basis. They will be based on four battalion-sized battle groups that can operate in concert with national forces, present at all times in these countries, underpinned by a viable reinforcement strategy.”²⁸² Increasing multinational operations, training/exercises, and similar equipment is one way to boost interoperability at a targeted level rather than in a general sense.²⁸³

Procedural interoperability requires prior assumptions for member countries that have higher capacities when working with those with lower capacities. Boosting these efforts could take extended efforts over long periods of time so often countries like the United States need to “meet partners halfway” in capacity building and learn to adapt for future operations.²⁸⁴ To adapt to this reality the structure and design of enhanced Forward Presence was built to be more versatile and fluid in face of threats. The decision was to have individual battalions integrated into their respective host country brigade who then fell under the command of the Supreme Allied Commander Europe (SACEUR).²⁸⁵ This design is to give more flexibility to multinational brigades in the event a crisis begins with Russia. If an invasion occurs NATO has the tool to bypass the political command of NATO from the North Atlantic Council by having a country like the United States, UK, or Canada take control of the intervention while awaiting a decision.²⁸⁶ Through reducing procedural obstacles the enhanced Forward Presence has evolved interoperability in the face of immediate threats.

NATO spans 32 countries with 28 different languages of which only English and French are official, requires interoperability at the human level to require intergovernmental and interpersonal effectiveness. Human interoperability aligns the terminology and training required for ease of communication. It is about harmonizing language, relationships, and

²⁸² NATO. (2016). NATO Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_133169.htm

²⁸³ Pernin, C. G., & Lerario, M. (2019). *Targeted interoperability: A New Imperative for Multinational Operations*.

²⁸⁴ Ibid

²⁸⁵ Leuprecht, C. (2019). *The enhanced Forward Presence: innovating NATO's deployment model for collective defence*. NATO Defense College. <http://www.jstor.org/stable/resrep19859>

²⁸⁶ Ibid

education that influence the human dimension.²⁸⁷ Maintaining these relationships is vital to functionality of NATO, especially in times of conflict. The most vital component to this is when equipment is needed to cross borders or needs access to specific infrastructure, then the human dimension becomes paramount. The human dimension is where this potential friction can be reduced and leveraged to promote efficiencies.²⁸⁸ Challenges in the human dimension can derail any operation and is the one dimension that needs constant education and development. The biggest friction that exists right now is the cultural misalignment among member states where structural differences manifest themselves into cultural differences that ultimately impact interoperability.

As part of my discussion with Colonel Luigi Bramati, the Director of the NATO Policing Stability Centre of Excellence in November of 2023 he was able to provide me with useful insight about this human dimension and how it can become an interoperability issue through multiple domains. While this point was highlighted previously in regards to NATO operations in Iraq, it can also be applied to the importance of cultural understanding within the human dimension of interoperability.

The American police system is primarily localized, focusing on enforcement of local laws, while state and federal roles are more distinct and do not typically overlap. In contrast, Italian police, including the paramilitary Carabinieri, can address crimes at any level, limited only by resources, not jurisdiction. Unlike Italy, the U.S. lacks a direct equivalent to the Carabinieri, with the FBI handling only federal issues. The human dimension of interoperability becomes apparent in the world of stability policing due to the structural differences of NATO units' home countries. Since the American system of policing does not have a strategic posture and is seen as a local actor, the roles of paramilitary police forces from other countries might be overlooked and be placed only in military roles, where policing becomes an oversight. Learning from past operations in human interoperability needs a focus of cultural understanding and trust for multinational

²⁸⁷ Gamble, D., & Letcher, M. (2016, September). *The Three Dimensions of Interoperability for Multinational Training at the JMRC*. US Army. Retrieved February 1, 2024, from <https://alu.army.mil/alog/2016/SEPOCT16/PDF/173432.pdf>

²⁸⁸ Ibid

forces to resolve technical challenges.²⁸⁹ NATO requires focus on joint exercises that capture “institutional memory” with personnel, especially on a rotating basis.²⁹⁰

The last dimension of interoperability as listed by NATO is informational interoperability as “a critical transversal element”.²⁹¹ Much of the information dimensions comes down to the exchange and storage of data and information. Going back to the 1999 NATO Summit in Washington, the idea of interoperability in information was first proposed, “Alliance forces must be adequate in strength and capabilities to deter and counter aggression against any Ally. They must be interoperable and have appropriate doctrines and technologies”.²⁹² Much of information interoperability relies on the IT technology and data storage of NATO as a whole and the individual member states, but this paper will focus more on the exchange of information and how effective interoperability in this dimension only improves NATO’s posture within the multidomain future. Effective information exchange requires similar protocols, exchange of free-form or standardized information, and physical, syntactic, and semantic levels of information exchange.²⁹³

My conversation with Col. Bramati additionally focused on the importance of information exchange and how it is one of the pivotal aspects of NATO interoperability in the future. A hypothetical that was highlighted was how the police information at local levels could be used and exchanged to help track patterns with international implications. Local police pick up crime statistics in their area and begin noticing patterns that point to an adversarial foreign actor as the cause, but with only local knowledge the cause would not be apparent, but with information exchange these patterns could be shared and analyzed and thus the true cause could be identified. With the increase of hybrid threats the need for rapid and efficient information exchange becomes more important to target emerging threats and adapt quickly. The information dimension is only one aspect of the evolving

²⁸⁹ Pernin, C. G., & Lerario, M. (2019). *Targeted interoperability: A New Imperative for Multinational Operations*.

²⁹⁰ Ibid

²⁹¹ NATO. (2023). NATO. Interoperability: connecting forces. https://www.nato.int/cps/en/natohq/topics_84112.htm

²⁹² NATO. (1999). NATO Summit Declaration. <https://www.nato.int/docu/pr/1999/p99-064e.htm>

²⁹³ Szeleccki, S. (2019). Interpreting the interoperability of the NATO’s communication and information systems. *Scientific Bulletin*, 24(1), 95–107. <https://doi.org/10.2478/bsaft-2019-0011>

nature of interoperability and requires all to work together in the modern age of international security.

Interoperability is an important component to building deterrence within NATO. All the dimensions that contribute to interoperability also contribute towards targeting gray zone threats. Through the cyber domain specifically, information sharing becomes an important tool towards enhancing the alliance and solidifying an alliance-wide deterrence structure. Moving forward into this future of multipolarity the NATO alliance must adapt how it operates interoperability to meet this 21st century reality and focus on the changing domains of operation, and identifying gray zone threats through a strategic advantage.

Revisoning Interoperability

The Cold War notion of interoperability does not meet the needs of NATO missions today and is not sufficient towards addressing the rising level of instability brought by gray zone threats. Interoperability within NATO needs to evolve beyond the standardization of equipment and become flexible and dynamic, with the decision-making capabilities to match. This involves revisoning interoperability to meet the needs of multi-domain threats and operations, as well as targeting it to enhance the alliance capabilities. Building this interoperability is important to the alliance and addressing the multitude of threats along the continuum of conflict. These changes in built interoperability would be more tactical, while encompassing more multinational partners.²⁹⁴ Unfortunately to accomplish these goals the alliance needs to deal with the costs of this transformation which could cause a potential obstacle. Beyond just being tactically or operational more effective, a new revisoning of interoperability can also add strategic benefits to the alliance as a whole, as well as the individual member states.²⁹⁵

With the increase of multi-domain operations so too has the confusion to act collectively in a multinational alliance. This confusion not only exists horizontally among

²⁹⁴ Pernin, C. G., & Lerario, M. (2019). *Targeted interoperability: A New Imperative for Multinational Operations*. RAND Corporation.

²⁹⁵ Ibid, 41

member state interoperability, but also vertically among levels of government, and transformatively among the multiple domains of operation.²⁹⁶ Therefore creating a 32 multinational consensus among a defense alliance can cause hindrance to interoperability, showing the need for a deeper integration. But member states have the benefit of close cooperation with one another in order to bridge this cultural and political divide. As stated by Karlijn Jans, this closer cooperation “is underpinned by a mutual understanding of political intent, decision-making and authorization; secure capital-to-capital communications; and familiarity established through political-level training and exercises”.²⁹⁷ The need moves beyond a static sense of interoperability of cooperation and more into an integrated approach that enhances the multi-domain operations. In practice this means engaging all levels of conventionally understood interoperability: strategic, operational, tactical, and technological.²⁹⁸ But as technology is rapidly increasing and as an extension gray zone operations through cyber are becoming a bigger threat, the technological level is becoming a much larger aspect of interoperability, and one with greater challenges. Much of these challenges come from the difficulties surrounding information and intelligence sharing, where potential threats can escape detection and fall into the bureaucratic trap.²⁹⁹

This revisioning of interoperability allows it to function strategically, and operate more effectively at a tactical level. This requires every member state to work within close cooperation at *each* domain of operation, by increasing the number of tactical drills, trainings, and strategizing. Each domain requires similar inputs like equipment, infrastructure, intelligence, and investment. Finding ways to integrate further the multinational aspects, by leveraging strategic advantages that exist within the alliance would promote overall effectiveness. But beyond effectiveness at tactical or operational levels, streamlining interoperability among domains would promote a strategic benefit as

²⁹⁶ Ellison, D., & Sweijts, T. (2024). *Empty Promises?: A year inside the world of Multi-Domain Operations*. Hague Centre for Strategic Studies. <http://www.jstor.org/stable/resrep58469>

²⁹⁷ Jans, K. (2019). Strengthening NATO's readiness through coalitions. *King's College News Centre*.

²⁹⁸ Hura, M., McLeod, G. W., Larson, E. V., Schneider, J., Gonzales, D., Norton, D. M., Jacobs, J., O'Connell, K. M., Little, W., Mesic, R., & Jamison, L. (2000). *Interoperability: A continuing challenge in coalition air operations*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR1235.html

²⁹⁹ Dengg, A. (2001). Challenges of Intelligence Sharing in Combating Terrorism: An Academic Point of View. *commitment*, 3, 3.

well.³⁰⁰ It has the ability to develop more intimate knowledge, bring forces together with shared experiences, and builds trust that is much needed in the face of real threats.³⁰¹

In the face of gray zone threats the key is through deterrence and identifying the threats before or as they occur in order to respond appropriately and proportionally. In order to have effective deterrence there is a need for the intelligence to be accurate and shared appropriately and strategically. But as NATO is only a defense alliance there are still challenges that come to intelligence sharing, even if efforts are being made to address it. Much of this comes down to the fact that there are important trade-offs to intelligence sharing. Characteristically, there are games around trust, risk mitigation, national interest, deception, and quid pro quo.³⁰² Sharing any intelligence requires a large amount of trust with an ally. The trust formula comes down to: does the importance of the intelligence outweigh the potential to compromise a source?³⁰³ This is part of the reason why intelligence-specific alliances exist outside of NATO, for example the Five Eyes intelligence alliance among the United States, United Kingdom, Canada, Australia, and New Zealand, which contains three NATO members and two non-NATO members, which agree to share signal intelligence. This alliance has very close historical and cultural ties, which establishes trust and less fear around compromising intelligence sources.

For NATO to develop more effective deterrence in the gray zone a higher standard of intelligence sharing is essential. An impediment to this is the European structure around intelligence gathering and sharing. While it is primarily a national priority and responsibility, the European Union is also a major actor in the gathering and distribution of intelligence through agencies like Europol, Eurojust, and Frontex.³⁰⁴ Although many EU members are also members of NATO, the EU itself is not a member of NATO, and a few EU members are not members to NATO, causing some issues around intelligence gathering, especially around trust and perceptions of jurisdiction.

³⁰⁰ Pernin, C. G., & Lerario, M. (2019). Pp. 41.

³⁰¹ Ibid, 41

³⁰² Ballast, J. (2017). *Trust (in) NATO: The future of intelligence sharing within the Alliance*. NATO Defense College. <http://www.jstor.org/stable/resrep10248>

³⁰³ Ibid, 2

³⁰⁴ Ibid, 3

Interoperability can be more than just tactical military standardization. Too often the conventional wisdom surrounding interoperability is centered on the traditional domains of land, sea, and air, and their capacities in military operations. While these are incredibly important components to interoperability, the expanding domains of operation and the threat from gray zone strategies requires a bending of convention and requires a much deeper integration of interoperability and cooperation, which requires integration at the institutional level as well.³⁰⁵ This means allowing NATO members into the national decision-making centers so that information is shared quicker and trust is established. Strategic and policy integration are important aspects of building deterrence capabilities, but do come with risks that member states may not be open to. Institutional integration differs from tactical integration because it requires an agreement on shared principles and rules that guide interactions and decisions, but also around research and development and capacity building among member states.³⁰⁶

These aspects of deeper integration can be easily achieved and slowly scaled-up in order to create liaisons in decision-making processes, but again, at an institutional level, information sharing still creates the biggest obstacle to interoperability in any alliance. Institutional integration can help alleviate problems and deficiencies that exist at national levels by allowing assistance from other member states to address specific problems. Rather than focusing on alliance-wide deficiencies, it is more pertinent to address member-specific lacks in capacity where member states create credible force plans, programs, and priorities, that highlight their different capabilities.³⁰⁷ With an integrated approach different member states can assist others in areas they have a comparative advantage and others lack and are seeking to improve while building stronger relationships in the process.

NATO has already made important steps to increasing integration that boosts interoperability around intelligence sharing. The creation of the Joint Intelligence and

³⁰⁵ Pettyjohn, S. L., & Wasser, B. (2022). A Framework for Integrated Deterrence with Allies and Partners. In *No I in Team: Integrated Deterrence with Allies and Partners* (pp. 10–19). Center for a New American Security. <http://www.jstor.org/stable/resrep46863.7>

³⁰⁶ Ibid, 13

³⁰⁷ Cordesman, A. H., & Hwang, G. (2022). Focusing on the Right Strategic Priorities for NATO. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 3–7). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.2>

Security Division (JISD) demonstrates this commitment and shows the first steps necessary to integrating military, civilian, internal, and external intelligence, but full integration is a slow process that needs to be delicate to the reasonable hesitations of member states.³⁰⁸ The best and most reliable approach to building integration is through the creation of bilateral intelligence sharing agreements within the alliance that can build much larger alliance-wide intelligence networks. Intelligence sharing is centered around trust, which is a process that cannot be rushed, and so the easiest, though time-consuming, process of member-to-member agreement is the most effective method.³⁰⁹ Additionally, the creation of JISD comes at the risk of redundancy with intelligence gathering and may over-saturate the intelligence community if not organized correctly.³¹⁰ Therefore maintaining the sovereignty of national control of intelligence is still important and utilizing the JISD as a tool to facilitate intelligence sharing is the most effective strategy.

Interoperability is and will always be an essential part of NATO's functionality. Interoperability has evolved beyond just equipment standardization and training drills and has been thrust into the 21st-century gray zone. The gray zone requires interoperability to adapt to space and cyber if it wants to remain a pivotal force in deterrence, and needs to find an integrated approach that enables closer cooperation and communication among the alliance. Achieving this requires more effective ways to share intelligence along different channels and levels of government, as well as through ways that build trust and risk mitigation. This process must then undergo more institutional integration where alliance actors are present in decision-making centers that boost multilateralism to build legitimacy on a global stage. Balancing the bilateral means of intelligence with stranger integration, the alliance can move beyond responding to gray zone threats and move into creating "gray deterrence", where flexibility, trust, and maneuverability counter gray zone strategies before they can occur.

³⁰⁸ Gordon, J. S. (2017). Intelligence sharing in NATO. *Atlantisch Perspectief*, 41(6), 15–19. <https://www.jstor.org/stable/48581386>

³⁰⁹ Ballast, J. (2017).

³¹⁰ de Graaff, B. (2017). NATO intelligence: At the crossroads of informal intelligence sharing and institutional streamlining. *Atlantisch Perspectief*, 41(6), 4–5. <https://www.jstor.org/stable/48581383>

From Interoperability to “Gray Deterrence”

Deterrence is built through capabilities, communication, and integrity, but also enhanced through interdependence and acceptance of each other's norms.³¹¹ It is important to build “broad deterrence” according to Joseph Nye, which demonstrates that an attack not only would hurt the victim but also the attacker.³¹² When interoperability works effectively across the different domains and is implemented institutionally, the interdependence of the alliance increases and the deterrence capabilities also increase, which begin to push back against gray zone threats. Gray zone threats require shifting the paradigm on what deterrence works, and how building alliance interoperability assists. The principle of interoperability essentially comes down to specific means in which multinational militaries can exchange services with each other with the least amount of resistance.³¹³ Yet, within the gray zone, that principle is not sufficient and needs to be enhanced to apply to the ever-changing continuum of conflict.

At a baseline it is important to begin strategic level deterrence during peacetime, in order to build shared understandings of threats, as well as roles and responsibilities of member states.³¹⁴ From a shared viewpoint can the alliance move as a collective unit towards creating means of deterrence in the gray zone. Much of the conventional understanding of deterrence relates to “top-down” approaches, while incredibly important within interoperability, training, and operations; it does not fully address the complexity of gray zone threats and how to effectively deter them.³¹⁵ Identifying gray zone threats and crafting means to deter them through the alliance also requires “bottom-up” strategies, like a deep understanding of local politics that can make their way to the national level, can help

³¹¹ Veebel, V., & Ploom, I. (2018). The deterrence credibility of NATO and the readiness of the Baltic States to employ the deterrence instruments. *Lithuanian Annual Strategic Review*, 16(1), 188.

³¹² Nye, J. S. (2016). Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), 44-71.

³¹³ Pernin, C. G., & Lerario, M. (2019). *Targeted interoperability: A New Imperative for Multinational Operations*. RAND Corporation.

³¹⁴ Pettyjohn, S. L., & Wasser, B. (2022). A Framework for Integrated Deterrence with Allies and Partners. In *No I in Team: Integrated Deterrence with Allies and Partners* (pp. 10–19). Center for a New American Security. <http://www.jstor.org/stable/resrep46863.7>

³¹⁵ Matisek, J. W. (2017). Shades of Gray Deterrence: Issues of Fighting in the Gray Zone. *Journal of Strategic Security*, 10(3), 1–26. <http://www.jstor.org/stable/26466832>

understand the developing threats earlier and create cohesive plans to deter them.³¹⁶ This creates what is known as a “gray deterrence”, in which creative means are used by the Alliance to deter gray actors undermining the Alliance’s interest. By doing so NATO would be able to “capitalize on gray actor’s rational political objective calculations by changing their interpretation of the cost-benefit analysis.”³¹⁷ Rather than using military means to deter, gray deterrence would focus on changing the political or informational outcomes, so that gray zone threats are met with gray zone responses.

The concept of a *gray deterrence* is relatively new and has not become an official doctrine of a state, alliance, or international actor. As a developing concept it is expanding, and seeking a set definition, aim, and implementation strategy that can be tested or challenged. As a result, examining the effectiveness of this theory is beyond the scope of this dissertation. Nevertheless, the principles guiding the need for a new deterrent strategy are apparent, as well as reinforcing the multiple layers of interoperability within the alliance to create an effective deterrent strategy. Deterrence is more than just signaling to the government or non-state actor organization, but is also about signaling to the population as well, and navigating the cultural and social side where conflicts and threats can originate or be proliferated. Deterrence now is becoming an ever-growing definition as well as encompassing ever-evolving strategies that blur the intended goals and means. This places a burden on deterrence responsibilities, as explained by Tim Sweijs et al, that make these requirements almost impossible to meet.³¹⁸

Therefore, a framework and prescribed strategies are required to develop this new deterrence. A strategic framework would help differentiate different strategies that exist throughout the gray zone, as well as across the multiple domains of operation, and leverage and reinforce the interoperability of the alliance. The framework, as created by Sweijs et al, is broken down into five strategies: cooperation, persuasion, protection, coercion, and control. The strategies are also listed according to how escalatory they are, from

³¹⁶ Ibid, 14

³¹⁷ Ibid, 14

³¹⁸ Sweijs, T., Zilincik, S., Bekkers, F., & Meessen, R. (2021). Strategic Framework to Counter Hybrid Action. In *A Framework for Cross-Domain Strategies Against Hybrid Threats* (pp. 15–26). Hague Centre for Strategic Studies. <http://www.jstor.org/stable/resrep27705.7>

cooperation being the least escalatory, to control being the most. The framework helps manage each crisis at its level of escalation and creates measures to seek de-escalation across multiple domains.³¹⁹

The first strategy of cooperation seeks to improve political relations by creating mutually beneficial policies. It seeks to maximize mutual gains while also avoiding reciprocal losses. It can present itself in multiple ways, like entanglement, conciliation, and accommodation. Entanglement entails developing interdependencies that would make hostile actions costly.³²⁰ Similar to how after World War II with the creation of the European Coal and Steel Community combined the coal and steel markets—ingredients for war—to entangle the economies of previously warring states as a way to build cooperation in the future. Conciliation seeks to create win-win situations in negotiations by removing the key obstacles to an agreement, and accommodation which would require concessions from either side. Cooperation works because it demonstrates good faith between two parties, but without demonstrations from either side it can also easily escalate.³²¹

The next strategy is the use of persuasion to promise positive incentives or rewards to gain cooperation. Persuasion can be material or non-material in its means. Material means would be economic incentives or tangible rewards, whereas non-material means would be status, prestige, or reassurances. Persuasion and cooperation work well together and both require a sense of goodwill in order to be effective.³²² In order to operate effectively in the gray zone, building goodwill is an effective deterrence that can help de-escalate future threats, but should not be the only means to use gray deterrence, as more escalatory means are necessary.

Recent deterioration of treaties like New SALT, the Open Skies treaty, and the Intermediate-Range Nuclear Forces Treaty between the NATO states, primarily the United States, and Russia, have shown that after a quick escalation from one side, cooperation and persuasion are less effective and other strategies are needed. This is where gray deterrence is needed with conventional deterrence, as both are needed to work hand-in-hand as an

³¹⁹ Ibid, 22

³²⁰ Ibid, 18

³²¹ Ibid, 18

³²² Ibid, 19

effective deterrent strategy. Conventional deterrence will always exist and it is incumbent on the NATO interoperable system to facilitate its continuance, but gray deterrence needs to be scaled up to work the informational operation as a means to “deny, discredit, and delegitimize” an adversary’s presence in the informational domain.³²³

Extending beyond cooperation and persuasion are more conventional means of deterrence. Protection is focused on building a state’s ability to defend itself. Coercion works the opposite of persuasion where it utilizes punishment as a form of deterring a threat. And protection is an “offensive use of force”, that denies an adversary the ability to make strategic choices.³²⁴ As these focus on more conventional means to build deterrence, the interoperability involved is similar to the traditional approach NATO has been taking. In order to restructure interoperability to focus on the informational and cultural sphere, efforts are needed to “gray” the thinking around what deterrence means and how an alliance can navigate its interoperability. This shift requires a multi-domain interoperability which prioritizes the deterrent capabilities of the alliance. China and Russia have already stated intentions to exploit the gray zone to reach these goals. Russian General Gerasimov stated about the pursuit of ‘gray wars’ and overcoming international pressures:

“Asymmetrical actions have come into widespread use, enabling the nullification of an enemy's advantages in armed conflict. Among such actions are the use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected.”³²⁵

If NATO wants to be ahead of the gray zone, especially as the world becomes increasingly multipolar, then it needs to take the steps to get ahead of gray

³²³ Matissek, J. W. (2017). Pp. 19

³²⁴ Sweijts, T., Zilincik, S., Bekkers, F., & Meessen, R. (2021). Pp. 21.

³²⁵ Gerasimov, V. (2013, February 27). The value of science is in foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military-Industrial Kurier*.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

zone operators and adapt its interoperability to include informational, human, and cultural domains so its conventional deterrence advantages are not nullified.

Deterrence in today's multipolar world requires adaptations beyond traditional methods to address ambiguous "gray zone" threats effectively. Joseph Nye's concept of "broad deterrence" emphasizes the mutual disadvantages that would result from conflict, suggesting that both attacker and defender stand to lose. Interoperability across NATO's member states enhances deterrence by enabling coordinated responses across multiple domains, which is vital against non-traditional threats like cyber-attacks and political destabilization. Such threats demand innovative deterrence strategies, which include strengthening alliances and improving capabilities in cyber and space domains.

Traditional "top-down" deterrence approaches, which focus on military and strategic alignment, are insufficient alone to counter gray zone activities. Instead, "bottom-up" strategies that involve understanding local political dynamics and crafting localized responses are crucial. This dual approach leads to what is termed "gray deterrence," a strategy that aims to alter adversaries' cost-benefit analyses by leveraging political and informational tactics over direct military action.

As gray zone challenges grow, especially from actors like Russia and China who exploit these realms, NATO must adapt its interoperability to include more than just military strategies. As such, NATO should have an advantage in this field as it is a multinational alliance, and can leverage its diversity to establish creative and effective interoperable tools to power deterrence. Similar to the United States utilizing the Native American code talkers to use little-known indigenous languages to get around German spies, NATO today can leverage its multi-cultural identity to enhance its interoperability.³²⁶ This involves a shift to encompass informational and cultural tactics, ensuring that its conventional strengths are not undermined in increasingly complex international conflicts.

³²⁶ Lyle, Amaani (June 28, 2015). "Word Power: How Code Talkers Helped to Win Wars". *archive.defense.gov*. Washington, D.C.: U. S. Department of Defense.

VIII. The Multipolar World

The Future of Graying Conflicts

After the Cold War NATO experienced an identity crisis that forced a restructuring and repositioning of priorities and targets. With the Russian threat minimized in the short-term this allowed the defense alliance to cut military spending and decrease personnel, development, and spending. This new posturing altered the idea of interoperability and military readiness. The United States began shifting its attention to the Balkans, Afghanistan, and the Middle East, bringing with it the attention of NATO. This new priority was shifted towards counterterrorism measures and stabilization forces, but at the neglect of logistics and infrastructure in Europe that would benefit deterrence.³²⁷

With the invasion of Ukraine by Russia and a growing and assertive China the need for another reevaluation of NATO and its ability to respond and communicate is necessary. The challenges of today show the short-sightedness of the previous restructuring and how security in Europe and of NATO allies requires a new perspective and approach to an increasingly multipolar world and a power dynamic that is quickly changing.

The future of multipolarity also comes with new global threats that need to be addressed at the global level, or can be leveraged against adversaries for geopolitical advantage. The future challenges exist around expanding technologies like Artificial Intelligence (AI) and robotics, climate change, the emergence of the Arctic as a realm of operation, and the shifting of alliances. These challenges will all lead to conflicts and threats that will only become grayer and require the flexibility and versatility to adapt in order to stay relevant.

The AI and robotics revolution that is fast approaching has been described as analogous to the Cambrian Explosion where the Earth experienced the most rapid burst of

³²⁷ Scaparrotti, C. M., Bell, C. B., Schroeder, W., Starling, C. G., & Rodihan, C. (2020). Enhancing Deterrence and Readiness: The Role of Military Mobility. In *MOVING OUT: A Comprehensive Assessment of European Military Mobility* (pp. 6–9). Atlantic Council. <http://www.jstor.org/stable/resrep24666.5>

evolution and biodiversity.³²⁸ Currently, the United States is the largest investor and power in AI-technology, with China looking to become a competing power in this field. Russia also seeks to expand its AI-technology capabilities, but still lags behind significantly.³²⁹ Although, in recent years China and Russia have begun a partnership around technology sharing and development, where Russia is seeking to substitute western-made technology with Chinese-made instead. Additionally, while there has been no military integration as of yet, there has been information sharing in regards to space technology, air defense systems, nuclear submarines, and hypersonic technologies.³³⁰ But lack of trust still remains which has kept the technological partnership from advancing, particularly around China's desire to pursue interests in the Arctic, Russia's loose threats around nuclear weapon usage with the war in Ukraine, and fears around China using bilateral military-technology trade to contain Russia in order to subdue competition in the Asia-Pacific region.³³¹

Climate change becomes a potential threat towards the future of the alliance due to its impact on the Arctic region and the changing geopolitical landscape it could create. Currently the Arctic region consists of NATO members Canada, United States, Iceland, Denmark (Greenland), Norway, Sweden, and Finland, and non-NATO member Russia. While the Arctic region currently has an overwhelming NATO presence, there are still differing perspectives around the future of the regions, especially as it becomes more open due to climate change.³³² Even China, which does not border the Arctic, views itself as an actor in the region, under the rule of "exceptionalism" as termed by the Arctic Council, based on a speech by Mikhail Gorbachev, where he stated the Arctic should be a "zone of peace", for states to exist, thereby allowing China to claim an interest in the region.³³³

³²⁸ Kasapoğlu, C., & Kırdemir, B. (2019). *WARS OF NONE: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CONFLICT*. Centre for Economics and Foreign Policy Studies. <http://www.jstor.org/stable/resrep21050>

³²⁹ Ibid, 2

³³⁰ Sendstad, C., Hakvåg, U., Nouwens, M., Schwartz, P., Hart, B., Lin, B., Wilson, R. S., Julienne, M., Pynnöniemi, K., & Patalano, A. (2022). Russian Views on Sino-Russian Military- Technical Cooperation. In M. Bergmann & A. Lohsen (Eds.), *Understanding the Broader Transatlantic Security Implications of Greater Sino-Russian Military Alignment* (pp. 6–12). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep45513.4>

³³¹ Ibid, 10

³³² CHARRON, A., Bacon, P., Burton, J., Charron, A., Deni, J. R., Gaub, F., Kertysova, K., Lazarou, E., Lindstrom, G., Mustasilta, K., Portela, C., Rebegea, C., & Stanley-Lockman, Z. (2020). Arctic security: NATO and the future of transatlantic relations. In S. R. Soare (Ed.), *TURNING THE TIDE: How to rescue transatlantic relations* (pp. 137–152). European Union Institute for Security Studies (EUISS). <http://www.jstor.org/stable/resrep36312.13>

³³³ Ibid, 139

NATO deterrence is needed in order to push-back on the multipolarity in the region, and is another example where informational interoperability as well as gray zone deterrent strategies would be effective in this push-back. However, NATO currently does not have a strategic doctrine on how it views the region nor a consensus on how it should be perceived strategically.³³⁴ With a mixture of Arctic and non-Arctic states within the Alliance, the perceptions of the region vary, even as far as the future effects climate change will have. But there is also room for reconciliation on this front, where the alliance can move forward collectively. Due to higher ship traffic and potential trade routes developing, a multilateral code of conduct would be needed in order to avoid miscommunications or displays of power.³³⁵ This could help ease tensions and lower the threshold of conflict to the cooperation level in hopes of reducing the gray zone potentials that could be created.

Conflicts can gray economically too. The economies of the world are becoming more globalized, increasing the interdependencies among states, which potentially calm tensions or spark them as it challenges the balance of power in its goal towards multipolarity.³³⁶ However, the growing interdependence of economies and rapid globalization is creating a backlash, especially in Western countries, which can further challenge the future polarity of the world. Former President Donald Trump rescinded the United States from the Trans-Pacific Partnership trade agreement, further isolating the United States from multilateral involvement³³⁷, as well as withdrawing the US from the Paris Climate Agreement (in which President Biden reversed), highlighting the United States' indecisiveness around world leadership and participation. On the other hand, the European Union sees itself as a member of the global polarity, but without projection of military strength it is difficult to consider its position. Currently the European Union has all but four member states as members of NATO, and thus its global power projection remains in an alliance with the United States and Canada. Therefore, transatlantic solidarity

³³⁴ Ibid, 142

³³⁵ Ibid, 148

³³⁶ Burrows, M. J. (2017). *Western Options in a Multipolar World*. Atlantic Council.

<http://www.jstor.org/stable/resrep16818>

³³⁷ Ibid, 3

becomes even more important due to the reliance and cooperation NATO and the EU need from each other.

The Alliance will be challenged within the gray zone well into the future. The nature of threats and response is changing and requires the political will and flexibility to counteract these threats. While it is impossible to predict the future, the rapid increase in technology will play a role, and being ahead of this curve is paramount to any deterrence policy or strategy. The Alliance also needs to juggle the current geopolitical threat from Russia in Ukraine and its desires to move beyond those borders, as well as a rapidly growing China that is on track to be the world's largest economy with a desire to expand its global influence and build legitimacy.³³⁸

Additionally, in a world with nuclear weapons, any discussion of polarity needs to address this variable. The dynamics of a multipolar or unipolar world can change dramatically in the face of nuclear war or a nuclear attack. The Russian General Gerasimov also notes. "a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war."³³⁹ Highlighting how quickly a conflict can change and the defense calculus upended with the introduction of new variables. NATO deterrence in a graying and multipolar world is achievable but needs to meet the demands of the world as it is and what it will become.

As NATO faces evolving challenges in a multipolar world, the need for dynamic and flexible strategies becomes a priority. The alliance's ability to adapt its deterrence to encompass not only traditional military threats but also emerging gray zone activities is crucial for its continued relevance and effectiveness. Moreover, the economic interdependencies and the shifting geopolitical landscapes necessitate a robust, multilayered strategy that considers both political and military dimensions. To navigate these complexities, NATO must enhance its interoperability and develop comprehensive gray zone deterrent strategies that address both current and potential future threats. Additionally,

³³⁸ Liu, M. (2020). China's road to power: what does it really want?: A Chinese perspective on a rising China. *Atlantisch Perspectief*, 44(3), 4-8. <https://www.jstor.org/stable/48600549>

³³⁹ Gerasimov, V. (2013, February 27). The value of science is in foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military-Industrial Kurier*.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

as global power dynamics shift, particularly with the rise of China and the persistent challenges posed by Russia, NATO's response must be cohesive yet adaptable to the diverse needs and perspectives within the alliance.

IX. Conclusion

The shifting paradigms of NATO's deterrence strategy amidst the complexities of a graying and multipolar world present challenges but also opportunities for the Alliance to address. The essence of modern conflict pivots significantly on the integration and manipulation of the 'gray zone'—a nebulous theater where state and non-state actors exploit ambiguities and the blurred lines between war and peace. So, in a multipolar and graying world, how can NATO adapt its deterrence to address these threats without raising global instability and remain relevant? Given the changed nature of the world and international system, NATO has needed to adapt and reform its deterrence structure in order to maintain stability, which, as demonstrated in this dissertation, around creating a strategic advantage in the gray zone, building capabilities in the multiple domains of operation, and synchronizing the structure of the alliance to allow easier facilitated interoperability among states and within states.

NATO's operational domains have drastically expanded and evolved, reflecting the shifting landscape of modern warfare and the alliance's need to adapt to an increasingly multipolar world. From traditional battlegrounds of land, sea, and air to the pioneering frontiers of space and cyber, each domain presents unique challenges and necessitates a tailored approach to ensure comprehensive deterrence and defense. The land domain, with its historic significance, continues to demand high levels of interoperability and rapid deployment capabilities to counter threats, particularly along NATO's Eastern Flank. The sea domain, crucial for power projection and deterrence, must address challenges posed by burgeoning naval powers like China. Meanwhile, the air domain's evolution, driven by technological advances in drone warfare and aerial surveillance, underscores the necessity for maintaining air supremacy in contemporary conflict scenarios.

The introduction of space as an operational domain marks a proactive step towards securing orbital assets critical for communication and surveillance, acknowledging the increasing militarization of space by global powers such as Russia and China. Concurrently, the cyber domain emerges as the quintessential gray domain where warfare is undefined by traditional metrics and blurred by issues of attribution and sovereignty. The

intricacies of cyber warfare, where attacks can destabilize economies and disrupt societal infrastructure without a clear aggressor, epitomize the challenges NATO faces in the digital age.

Moving forward, NATO must enhance its multi-domain interoperability and strategic foresight to effectively navigate the complexities of gray zone threats and the uncertainties of a multipolar world. This entails not only bolstering traditional military capabilities but also embracing advanced technologies and developing robust cyber defenses to protect against and deter hybrid warfare tactics. As the nature of conflict continues to evolve, NATO's ability to adapt and innovate across all operational domains will be paramount in upholding its strategic objectives and maintaining global stability in the face of emerging global threats.

It is evident that the alliance must rigorously adapt its strategies to counteract the complexities introduced by the gray zone. As highlighted, the gray zone blurs the traditional boundaries of warfare, where state and non-state actors employ tactics that exploit the ambiguities of international law and the thresholds of war. These tactics, ranging from the deployment of "little green men" in Ukraine to the strategic use of disinformation and cyber-attacks, challenge NATO's conventional military superiority by operating beneath the threshold of overt war. The examples of Russian interference in the 2016 U.S. election and Chinese island-building in the South China Sea illustrate how adversaries leverage gray zone tactics to achieve their geopolitical objectives without provoking a direct military response from NATO. These actions, while not outright acts of war, destabilize the international order and test the resolve and agility of NATO's response mechanisms.

NATO's recognition of cyber and space as operational domains is a step toward addressing these threats, yet the alliance's response must be more dynamic and encompass a wider range of non-military tools to effectively counter hybrid warfare. The adoption of a more nuanced approach that includes both prevention and rapid response strategies is crucial. Enhanced interoperability, intelligence sharing, and strategic communication within the alliance are key to thwarting gray zone tactics. Additionally, the alliance needs to continuously update its collective defense doctrine to reflect the evolving nature of conflict,

where cyber-attacks and political warfare are as significant as traditional military threats. As the chapter discusses, the stability-instability paradox underpins much of the rationale behind adversaries' use of gray zone tactics; thus, understanding this dynamic is essential for NATO as it seeks to maintain global stability and deter aggression.

By adapting conventional deterrence strategies, NATO aims to counter the assertive actions of adversaries such as Russia, China, Iran, and North Korea, as well as non-state actors. This adaptation involves a focus on deterrence by denial, which seeks to prevent adversaries from pursuing actions by demonstrating the consequences of their actions. NATO has made strides in strengthening its capabilities, particularly in response to threats from Russia, with investments in cyber and hybrid capabilities, as well as increased defense budgets.

One key aspect of NATO's capability enhancement strategy is defense spending, with the 2% of GDP target established at the 2014 Wales Summit serving as a guideline for member states. While progress has been made, particularly with 22 member states increasing defense funding, challenges remain in achieving full compliance with the target. The 2% threshold, while important for signaling commitment, should not be viewed as the sole measure of NATO contributions, as it overlooks nuances in defense spending and capabilities. Moreover, NATO's deterrence capability is not solely reliant on defense spending but also on modernization efforts and interoperability among member states. The NATO Defense Planning Process (NDPP) plays a crucial role in coordinating multinational military responses and setting capability targets. While challenges persist in meeting these targets, particularly in the Eastern Flank, NATO members have shown a willingness to invest in modernization and enhance interoperability.

Furthermore, the deterrence strategies extend in multiple theaters and contain lessons from past operations. The reinforcement of NATO's Eastern Flank following the 2014 Russian invasion of Ukraine demonstrates the alliance's heightened focus on both traditional and gray zone deterrence strategies. The establishment of the Very High Readiness Joint Task Force and the increased deployment of NATO forces under the enhanced Forward Presence initiative reflect a strategic adaptation aimed at deterring Russian advances through a robust military presence and rapid response capability. These

efforts are supplemented by NATO's commitment to counter the less visible but equally challenging gray zone threats such as cyber warfare and misinformation, which require both technological advancement and strategic communication.

The pivot to China further illustrates NATO's recognition of the shifting global power dynamics and the need for strategic deterrence in multiple arenas. As China employs a range of gray zone tactics to expand its influence in the South China Sea and beyond, NATO is challenged to respond not just with military might, but with a comprehensive strategy that includes diplomatic and economic tools, highlighting the complex nature of modern global threats.

Lessons from past conflicts in Afghanistan, Iraq, Libya, and Kosovo have been crucial in shaping NATO's current strategies. These engagements underscore the importance of clear objectives, unified command, and the integration of civil and military efforts to achieve sustainable peace. The experiences have also stressed the importance of agility and adaptation in NATO's approach to conflict management, particularly in dealing with non-conventional warfare and building resilience against hybrid threats. The concept of strategic advantage in gray zone warfare calls for a nuanced understanding of the continuum of conflict, as NATO must navigate a landscape where military force alone is insufficient to secure long-term peace. The alliance's strategic advantage will depend on its ability to effectively blend military, technological, and diplomatic resources to deter adversaries and prevent the escalation of conflicts into full-scale wars.

NATO's focus on enhancing interoperability has elucidated that while technical, procedural, human, and information interoperability play crucial roles, they also encounter significant obstacles. For instance, the technical challenges of integrating diverse military technologies, highlighted by the ongoing dependency on Russian equipment among Eastern European members, emphasize the need for strategic standardization within the alliance.

Additionally, the procedural dimension, as exemplified by initiatives like the Enhanced Forward Presence, underscores NATO's efforts to align doctrines and practices across diverse military cultures. However, this alignment is often hampered by varying national defense policies and capabilities, necessitating a more nuanced approach to collective defense. The human aspect of interoperability, crucial for the seamless

integration of forces during operations, faces hurdles such as language barriers and cultural differences, which can impede effective communication and operational cohesion. The example of the diverse implementation strategies of the S-400 system by Türkiye illustrates how internal politics and divergent threat perceptions can further complicate interoperability. Information interoperability, though essential for effective command and control across NATO forces, is often restricted by the varied capability of member states to secure and share intelligence securely and promptly. This is critical in an era where information dominance is often a precursor to battlefield success.

As NATO navigates the complexities of a multipolar world characterized by shifting power dynamics and emerging gray zone conflicts, it is imperative that the alliance reassesses and adapts its strategies to meet the evolving challenges. The chapter underscores the necessity for NATO to reevaluate its deterrence capabilities in response to the multifaceted threats presented by significant actors like Russia and China, alongside technological advancements in AI and robotics, and the strategic importance of the Arctic due to climate change. Moreover, the growing economic interdependencies and the potential for economic conflicts to become gray zones require NATO to refine its approach towards economic security and political stability. The lessons from past restructuring efforts reveal the importance of maintaining a robust logistical and infrastructural readiness within Europe, which is essential for ensuring timely and effective responses to threats.

To conclude answering my research question; the alliance must develop a cohesive strategy that includes both traditional military deterrence and innovative gray zone deterrent strategies, emphasizing interoperability and information sharing across its members. As NATO looks to the future, it will be crucial to integrate these diverse strategies to manage the risks and leverage the opportunities presented by the increasingly interconnected and technologically advanced global landscape. This strategic integration will enable NATO to continue playing a pivotal role in maintaining international peace and security in the face of rapidly evolving global threats. NATO remains relevant for the future, and can own the information, cyber, space, and gray zones by being the leader in each space, and getting ahead of the gray zone challenges rather than putting out the fires

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

when they occur. Again, as General Clausewitz stated, “war is merely the continuation of policy by other means,” and NATO can prevent the war with the right policy.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

X. Bibliography

- Adesnik, D. (2016). *FPI Bulletin: NATO Defense Spending*. Foreign Policy Initiative. <http://www.jstor.org/stable/resrep07277>
- Ahn, K. H., & Shin, S. J. D. B. C. (2019). The US Military. In *F-35 JSF and Military Transformation: American Militarism during the Post-Cold War Era* (pp. 18–36). Asan Institute for Policy Studies. <http://www.jstor.org/stable/resrep20918.7>
- Appathurai, J. (2005, June 8). Press Briefing by NATO Spokesman, James Appathurai, after the Meeting of the North Atlantic Council at the Level of Defence Ministers. Retrieved from <https://www.nato.int/docu/speech/2006/s060608m.htm>
- Atlamazoglou, C. (2023, July 9). Turkey isn't getting much use out of its Russian-made missile-defense system, but that's not why Erdogan is keeping it around. *Business Insider*. <https://www.businessinsider.com/turkey-russia-s400-too-politically-costly-to-get-rid-of-2023-7?r=US&IR=T>
- Aydogan, M. (2023, May 7). Türkiye rejected US proposal to send Russian S-400 defense system to Ukraine: Foreign minister. *AA News*. Retrieved December 30, 2023, from <https://www.aa.com.tr/en/turkiye/turkiye-rejected-us-proposal-to-send-russian-s-400-defense-system-to-ukraine-foreign-minister/2891323>
- Ballast, J. (2017). *Trust (in) NATO: The future of intelligence sharing within the Alliance*. NATO Defense College. <http://www.jstor.org/stable/resrep10248>
- Beckley, M. (2023). The Peril of Peaking Powers: Economic Slowdowns and Implications for China's Next Decade. *International Security*, 48(1), 7–46.
- Biddle, T. D. (2019). *AIR POWER AND WARFARE: A CENTURY OF THEORY AND HISTORY*. Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep20093>
- Blackwill, R. D., & Gordon, P. H. (2018). The U.S. Response—Obama, Trump, and Congress. In *Containing Russia: How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge* (pp. 10–14). Council on Foreign Relations. <http://www.jstor.org/stable/resrep21423.8>
- Blanchard, B., & Mogato, M. (2012, November 28). China decries attempts to 'read too much into' passport map row. *Reuters*.
- Boot, M., Kirkpatrick, J. J., & Bergmann, M. (2019). *Defending America From Foreign Election Interference*. Council on Foreign Relations. <http://www.jstor.org/stable/resrep29933>
- Brands, H. (2016, February 5). Paradoxes of the Gray Zone. *Foreign Policy Research Institute*.
- Braw, E. (2022, January). Biden's gray zone gaffe highlights real dilemma. *Defense One*. Retrieved from <https://www.defenseone.com/ideas/2022/01/bidens-gray-zone-gaffe-highlights-real-dilemma/360982/>
- Brimelow, B. (2022, October). Italian military seeking new jets, ships amid rising Mediterranean tension. *Business Insider*. Retrieved from <https://www.businessinsider.com/italian-military-seeking-new-jets-ships-amid-rising-mediterranean-tension-2022-10>
- Brown, C. (2020). Accelerate Change or Lose. *Airman Comprehensive Operations and Leadership Exam Booklet*. Retrieved from https://www.af.mil/Portals/1/documents/2020SAF/ACOL_booklet_FINAL_13_Nov_1006_WEB.pdf
- Bryant, M. (2023, November 23). Estonia accuses Russia of weaponising immigration at Europe's borders. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2023/nov/23/estonia-accuses-russia-weaponising-immigration-europe-borders>
- Brzezinski, I. (2011). Lesson From Libya: NATO Alliance Remains Relevant. *National Defense*, 96(696), 18–19. <https://www.jstor.org/stable/27019211>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

Burrows, M. J. (2017). *Western Options in a Multipolar World*. Atlantic Council. <http://www.jstor.org/stable/resrep16818>

Camut, N., Oliver, C. (2023, July 5). Bulgaria PM accuses president of doing Russia's bidding. *Politico*. Retrieved from <https://www.politico.eu/article/bulgaria-nikolai-denkov-pm-russia-influence-rumen-radev/>

Cancian, M. (2021, November 30). U.S. Military Forces in FY 2022: Air Force. *Center for Strategic and International Studies*. Retrieved from <https://defense360.csis.org/u-s-military-forces-in-fy-2022-air-force/>

Cancian, M. (2021, October 21). U.S. Military Forces in FY 2022: Army. *Center for Strategic and International Studies*. Retrieved from <https://defense360.csis.org/u-s-military-forces-in-fy-2022-army/>

Cancian, M. (2021, November 2). U.S. Military Forces in FY 2022: Navy. *Center for Strategic and International Studies*. Retrieved from <https://defense360.csis.org/u-s-military-forces-in-fy-2022-navy/>

Cancian, M. F., & Saxton, A. (2021). The Current State of NATO Forces and Military Budgets. In *Future NATO Enlargement: Force Requirements and Budget Costs* (pp. 27–34). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep35120.7>

CCDCOE (n.d.) *About us*. (n.d.). <https://ccdcoc.org/about-us/>

Challis, B. (2020). Security Risks: between Russia and NATO. In *Belarus beyond 2020: Implications for Russia and the West* (pp. 3–6). European Leadership Network. <http://www.jstor.org/stable/resrep25716.4>

CHARRON, A., Bacon, P., Burton, J., Charron, A., Deni, J. R., Gaub, F., Kertysova, K., Lazarou, E., Lindstrom, G., Mustasilta, K., Portela, C., Rebegea, C., & Stanley-Lockman, Z. (2020). Arctic security: NATO and the future of transatlantic relations. In S. R. Soare (Ed.), *TURNING THE TIDE: How to rescue transatlantic relations* (pp. 137–152). European Union Institute for Security Studies (EUISS). <http://www.jstor.org/stable/resrep36312.13>

Clark, J. P., Pfaff, C. A., Burgess, K. J., Cuccia, P. R., Fleming, A. J., Graham, K. M., Gustafson, J. S., Hillison, J. R., Morrow, C. D., Mowchan, J. A., Thompson, D. C., & Wolfe, A. M. (2020). A STRATEGIC AND OPERATIONAL ANALYSIS OF RUSSIA IN 2028. In *STRIKING THE BALANCE: US ARMY FORCE POSTURE IN EUROPE, 2028* (pp. 7–24). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep25429.7>

Clausen, M.-L., & Albrecht, P. (2022). DISTANCE EXEMPLIFIED – NATO IN IRAQ. In *EXPLORING DISTANCE IN SECURITY FORCE ASSISTANCE: THE CASE OF NATO MISSION IRAQ* (pp. 11–19). Danish Institute for International Studies. <http://www.jstor.org/stable/resrep43420.7>

Clausewitz: War as Politics by other Means | *Online Library of Liberty*. (2003). <https://oll.libertyfund.org/pages/clausewitz-war-as-politics-by-other-means>

Cordesman, A. H., & Hwang, G. (2022). Looking at European Trends by Sub-Region and Country. In *NATO and the Ukraine: Reshaping NATO to Meet the Russian and Chinese Challenge* (pp. 25–40). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep39637.11>

Crowther, G. A. (2017). The Cyber Domain. *The Cyber Defense Review*, 2(3), 63–78. <http://www.jstor.org/stable/26267386>

Cuordileone, K. A. (2000). “Politics in an Age of Anxiety”: Cold War Political Culture and the Crisis in American Masculinity, 1949-1960. *The Journal of American History*, 87(2), 515–545. <https://doi.org/10.2307/2568762>

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). Hybrid War: High-tech, Information and Cyber Conflicts. *Connections*, 16(2), 5–24. <http://www.jstor.org/stable/26326478>

Deep, A. (2015, March 2). *Hybrid War: Old concept, new techniques*. Small Wars Journal. Retrieved February 13, 2024, from <https://smallwarsjournal.com/jrnl/art/hybrid-war-old-concept-new-techniques>

Dempsey, J. (2017). *NATO'S EASTERN FLANK AND ITS FUTURE RELATIONSHIP WITH RUSSIA*. Carnegie Endowment for International Peace. <http://www.jstor.org/stable/resrep12934>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

Dengg, A. (2001). Challenges of Intelligence Sharing in Combating Terrorism: An Academic Point of View. *commitment*, 3, 3.

Deni, J. R. (2020). *Security Threats, American Pressure, and the Role of Key Personnel: How NATO's Defence Planning Process is Alleviating the Burden-Sharing Dilemma*. Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep26532>

Deni, J. (2024). Is the Baltic Sea a NATO Lake? *Carnegie Endowment for International Peace*. Retrieved from: <https://carnegieendowment.org/2023/12/18/is-baltic-sea-nato-lake-pub-91263>

Dresen, R. (2023). *NATO's Strategic Concept from theory to practice: NATO Mission Iraq*. NATO Defense College. <http://www.jstor.org/stable/resrep48882>

Ellison, D., & Sweijts, T. (2024). *Empty Promises?: A year inside the world of Multi-Domain Operations*. Hague Centre for Strategic Studies. <http://www.jstor.org/stable/resrep58469>

Farley, R. (2020). *Space Force: Ahead of Its Time, or Dreadfully Premature?* Cato Institute. <http://www.jstor.org/stable/resrep28729>

Fitton, O. (2016). Cyber Operations and Gray Zones: Challenges for NATO. *Connections*, 15(2), 109–119. <http://www.jstor.org/stable/26326443>

Francis, E. T. (2020). Air Supremacy in Airpower Doctrine. In *A House Built on Sand: Air Supremacy in US Air Force History, Theory, and Doctrine* (pp. 6–13). Air University Press. <http://www.jstor.org/stable/resrep24881.7>

Freier, N. P., Burnett, C. R., Cain, W. J., Compton, C. D., Hankard, S. M., Hume, R. S., Kramlich, G. R., Lissner, J. M., Magsig, T. A., Mouton, D. E., Muztafago, M. S., Schultze, J. M., Troxell, J. F., & Wille, D. G. (2016). ENTER THE DRAGON – CHINA AS A HIGH-END GRAY ZONE REVISIONIST. In *OUTPLAYED: REGAINING STRATEGIC INITIATIVE IN THE GRAY ZONE* (pp. 33–40). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep12061.11>

Galeotti, M. (2015, April 16). "Hybrid War" and "Little Green Men": How It Works and How It Doesn't. *E-International Relations*.

Gamble, D., & Letcher, M. (2016, September). *The Three Dimensions of Interoperability for Multinational Training at the JMRC*. US Army. Retrieved February 1, 2024, from <https://alu.army.mil/alog/2016/SEPOCT16/PDF/173432.pdf>

Gerasimov, V. (2013, February 27). The value of science is in foresight: New challenges demand rethinking the forms and methods of carrying out combat operations. *Military-Industrial Kurier*.

Gleiman, J. K. (2015). The American Counterculture of War: Supporting Foreign Insurgencies and the American Discourse of War. *Special Operations Journal*, 1(1), 19–36.

Gordon, J. S. (2017). Intelligence sharing in NATO. *Atlantisch Perspectief*, 41(6), 15–19. <https://www.jstor.org/stable/48581386>

Goward, D. (2024). As Baltics see spike in GPS jamming, NATO must respond. *Breaking Defense*. Retrieved from: <https://breakingdefense.com/2024/01/as-baltics-see-spike-in-gps-jamming-nato-must-respond/>

Green, M., Hicks, K., Cooper, Z., Schaus, J., & Douglas, J. (2017). Deterrence Theory and Gray Zone Strategies. In *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence* (pp. 21–50). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23165.6>

Gromes, T. (2019). NATO'S KOSOVO INTERVENTION IN OVERVIEW. In *A HUMANITARIAN MILESTONE?: NATO'S 1999 INTERVENTION IN KOSOVO AND TRENDS IN MILITARY RESPONSES TO MASS VIOLENCE* (pp. 3–8). Peace Research Institute Frankfurt. <http://www.jstor.org/stable/resrep19997.5>

Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). THE EVOLUTION OF SPACE AS A CONTESTED DOMAIN. In *ESCALATION AND DETERRENCE: IN THE SECOND SPACE AGE* (pp. 1–9). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep23194.3>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

- Helm, B., Smeltz, D., & Burakovsky, A. (2020). *US Experts Anticipate Future Decline for Russia Among the Great Powers: They Forecast Diminishing Russian Influence and Stagnating Economic and Military Strength*. Chicago Council on Global Affairs. <http://www.jstor.org/stable/resrep26631>
- HICKS, K. H., RATHKE, J., DANIELS, S. P., MATLAGA, M., DANIELS, L., & LINDER, A. (2018). Current NATO Benchmarks. In *Counting Dollars or Measuring Value: Assessing NATO and Partner Burden Sharing* (pp. 3–8). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep22475.4>
- Hill, A. G. (2019). Analysis. In *The Ultimate Challenge: Attribution for Cyber Operations* (pp. 13–24). Air University Press. <http://www.jstor.org/stable/resrep24884.7>
- Hoehn, A. R., & Harting, S. (2010). Redefining NATO's Role: 9/11 to Afghanistan. In *Risking NATO: Testing the Limits of the Alliance in Afghanistan* (pp. 13–24). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg974af.10>
- Hoehn, A. R., & Harting, S. (2010). A Greater Role for NATO in Afghanistan. In *Risking NATO: Testing the Limits of the Alliance in Afghanistan* (pp. 25–40). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg974af.11>
- Hoffman, F. G. (2009). Hybrid Warfare and Challenges. *Joint Force Quarterly*, 52, 35.
- Hoffman, F. G. (2018). Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges. *PRISM*, 7(4), 30–47. <https://www.jstor.org/stable/26542705>
- Hura, M., McLeod, G. W., Larson, E. V., Schneider, J., Gonzales, D., Norton, D. M., Jacobs, J., O'Connell, K. M., Little, W., Mesic, R., & Jamison, L. (2000). *Interoperability: A continuing challenge in coalition air operations*. Santa Monica, CA: RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR1235.html
- Ibragina, D. (2023). How Russia Torpedoed its own Influence in Moldova. *Carnegie Endowment for International Peace*. Retrieved from <https://carnegieendowment.org/politika/89731>
- Ifimie, I. A. (2020). *NATO's needed offensive cyber capabilities*. NATO Defense College. <http://www.jstor.org/stable/resrep25100>
- Jans, K. (2019). Strengthening NATO's readiness through coalitions. *King's College News Centre*.
- Jervis, Robert (1979). "Why Nuclear Superiority Doesn't Matter". *Political Science Quarterly*. 94 (4): 617–633. doi:10.2307/2149629
- Johnson, D. E. (2007). Kosovo, 1999. In *Learning Large Lessons: The Evolving Roles of Ground Power and Air Power in the Post-Cold War Era* (pp. 65–90). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg405af.11>
- 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. <https://www.jstor.org/stable/26999974>
- Jung, C. (2021). *China's Gray Zone Operations in the Yellow Sea*. Daniel K. Inouye Asia-Pacific Center for Security Studies. <http://www.jstor.org/stable/resrep35896>
- Kalimuddin, M., & Anderson, D. A. (2018). Soft Power in China's Security Strategy. *Strategic Studies Quarterly*, 12(3), 114–141. <http://www.jstor.org/stable/26481912>
- Kasapoğlu, C., & Kırdemir, B. (2019). *WARS OF NONE: ARTIFICIAL INTELLIGENCE AND THE FUTURE OF CONFLICT*. Centre for Economics and Foreign Policy Studies. <http://www.jstor.org/stable/resrep21050>
- Kolsto, P. (2016). The ethnification of Russian nationalism [PDF]. *The New Russian Nationalism*, 18–45.
- Kramer, M. (2011). The Demise of the Soviet Bloc. *The Journal of Modern History*, 83(4), 788–854. <https://doi.org/10.1086/662547>
- Kuperman, A. J. (2013). A Model Humanitarian Intervention? Reassessing NATO's Libya Campaign. *International Security*, 38(1), 105–136. <http://www.jstor.org/stable/24480571>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

- Larson, E. V., Eaton, D., Nichiporuk, B., & Szayna, T. S. (2008). Defining Irregular Warfare. In *Assessing Irregular Warfare: A Framework for Intelligence Analysis* (1st ed., pp. 7–18). RAND Corporation. <http://www.jstor.org/stable/10.7249/mg668a.10>
- Laruelle, M. (2014). Russian Nationalism and Ukraine. *Current History*, 113(765), 272. Retrieved from https://online.ucpress.edu/currenthistory/article-pdf/113/765/272/412111/curh_113_765_272.pdf
- Le Monde. (2024, March 20). Trump describes recent NATO threats as a form of negotiation. *Le Monde*. Retrieved from https://www.lemonde.fr/en/united-states/article/2024/03/20/trump-describes-recent-nato-threats-as-a-form-of-negotiation_6636346_133.html
- Leuprecht, C. (2019). *The enhanced Forward Presence: innovating NATO's deployment model for collective defence*. NATO Defense College. <http://www.jstor.org/stable/resrep19859>
- Liu, M. (2020). China's road to power: what does it really want?: A Chinese perspective on a rising China. *Atlantisch Perspectief*, 44(3), 4–8. <https://www.jstor.org/stable/48600549>
- Lyle, Amaani (June 28, 2015). "Word Power: How Code Talkers Helped to Win Wars". *archive.defense.gov*. Washington, D.C.: U. S. Department of Defense.
- MacAskill, E., & Borger, J. (2004, September 16). Iraq war was illegal and breached UN charter, says Annan. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2004/sep/16/iraq.iraq>
- Maranian, S. J. (2015). *NATO Interoperability: Sustaining Trust and Capacity within the Alliance*. NATO Defense College. <http://www.jstor.org/stable/resrep10254>
- Matissek, J. W. (2017). Shades of Gray Deterrence: Issues of Fighting in the Gray Zone. *Journal of Strategic Security*, 10(3), 1–26. <http://www.jstor.org/stable/26466832>
- Mazarr, M. J. (2015). UNDERSTANDING GRAY ZONE CONFLICT. In *MASTERING THE GRAY ZONE: UNDERSTANDING A CHANGING ERA OF CONFLICT* (pp. 55–78). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep12018.9>
- McDonald, A. (2024, March 19). Donald Trump says he won't quit NATO if Europe pays its way. *Politico*. Retrieved from <https://www.politico.eu/article/donald-trump-says-he-wont-quit-nato-if-europe-pays-its-way/>
- Morcos, P. (2020). *Toward a New "Lost Decade"?: Covid-19 and Defense Spending in Europe*. Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep26416>
- Morris, L. J. (2017, March 8). The Era of Coast Guards in the Asia Pacific Is upon Us. Asia Maritime Transparency Initiative, *Center for Strategic and International Studies*.
- Morris, L. J., & Binnendijk, A. (2019). *Gaining competitive advantage in the gray zone: Response Options for Coercive Aggression Below the Threshold of Major War*. The RAND Corporation.
- Moyer, J., (2024). Finland's Remarkable First Year in NATO. *Wilson Center*. Retrieved at: <https://www.wilsoncenter.org/article/finlands-remarkable-first-year-nato#:~:text=NATO%20remains%20popular%20in%20Finland,contributions%20to%20Ukraine%20not%20included.>
- NATO. (1999). NATO Summit Declaration. <https://www.nato.int/docu/pr/1999/p99-064e.htm>
- NATO. (2014). Wales Summit Declaration. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_112964.htm
- NATO. (2016). *Warsaw Summit Communiqué issued by NATO Heads of State and Government (2016)*. NATO. https://www.nato.int/cps/en/natohq/official_texts_133169.htm
- NATO. (2018). NATO Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_156624.htm

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

- NATO. (2021). *Afghanistan lessons learned*. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2021/12/pdf/2112-factsheet-afgh-lessons-en.pdf
- NATO (2023, July 7). Defence Expenditure of NATO Countries (2014-2023). *NATO Public Diplomacy Division*. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/2023/7/pdf/230707-def-exp-2023-en.pdf
- NATO. (2023). NATO. Interoperability: connecting forces. https://www.nato.int/cps/en/natohq/topics_84112.htm
- NATO. (2023, August 3). *NATO's Maritime Activities*. Retrieved from https://www.nato.int/cps/en/natohq/topics_70759.htm
- NATO. (2024). NATO conducts major air and missile defense exercise. *NATO*. Retrieved from https://www.nato.int/cps/en/natohq/news_223083.htm#:~:text=Since%20then%2C%20the%20exercise%20has,from%20more%20than%2014%20countries.
- NPR. (2023, October 1). Pro-Russia ex-premier leads party to win Slovakia parliamentary elections. *NPR*. Retrieved from <https://www.npr.org/2023/10/01/1202879797/pro-russia-ex-premier-leads-party-to-win-slovakia-parliamentary-elections>
- Nye, J. S. (2016). Deterrence and Dissuasion in Cyberspace. *International Security*, 41(3), 44-71.
- Nye, J. S. (2020). Perspectives for a China Strategy. *PRISM*, 8(4), 120–131. <https://www.jstor.org/stable/26918238>
- O'Dell, H. (2024). Why is Sweden telling its citizens to prepare for war? *Chicago Council on Global Affairs*. Retrieved from: <https://globalaffairs.org/bluemarble/sweden-tells-citizens-prepare-war-russian-aggression-nato-membership>
- Ozawa, M. (2021). Adapting NATO to grey zone challenges from Russia. In T. Tardy (Ed.), *NATO 2030: new technologies, new conflicts, new partnerships* (pp. 19–32). NATO Defense College. <http://www.jstor.org/stable/resrep29562.8>
- Patalano, A. (2024). Naval Power: The Key to Understanding U.S.-China-Russia Relations. *Time*. Retrieved from <https://time.com/6836406/naval-power-us-china-russia/>
- Peperkamp, L. (2020). An Arms Race in Outer Space? *Atlantisch Perspectief*, 44(4), 46–50. <https://www.jstor.org/stable/48600572>
- Pernin, C. G., & Lerario, M. (2019). *Targeted interoperability: A New Imperative for Multinational Operations*. RAND Corporation.
- Pettyjohn, S. L., & Wasser, B. (2022). A Framework for Integrated Deterrence with Allies and Partners. In *No I in Team: Integrated Deterrence with Allies and Partners* (pp. 10–19). Center for a New American Security. <http://www.jstor.org/stable/resrep46863.7>
- Piiparinen, A. (2015, September 18). The Chinese Cyber Threat in the South China Sea. *The Diplomat*.
- Pindják, P. (2014, November 18). *NATO Review - Deterring hybrid warfare: a chance for NATO and the EU to work together?* NATO Review. <https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html>
- Pohjanpalo, K., Rolander, N., Laikola, L. (2024, February 26). Finland and Sweden join NATO: What it means and how Russia has responded. *Bloomberg*. Retrieved from <https://www.bloomberg.com/news/articles/2024-02-26/finland-and-sweden-join-nato-what-it-means-and-how-russia-has-responded>
- Prier, J. (2017). Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly*, 11(4), 50–85. <http://www.jstor.org/stable/26271634>
- Quadri, Z. (2022). TGI Fridays In Kandahar: Fast Food, Military Contracting, and Intimacies of Force in the Iraq and Afghanistan Wars. *Journal of Transnational American Studies*, 13(1). <http://dx.doi.org/10.5070/T813158582> Retrieved from <https://escholarship.org/uc/item/7188527q>

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

- Reuters. (2023, October 17). Russia's Putin holds talks with Hungary's Orban, China. *Reuters*. Retrieved from <https://www.reuters.com/world/europe/russias-putin-holds-talks-with-hungarys-orban-china-2023-10-17/>
- Reuters. (2024). NATO members hike defense spending after Russia's invasion of Ukraine. *Reuters*. Retrieved from <https://www.reuters.com/graphics/USA-ELECTION/TRUMP-NATO/movalqxlzpa/index.html#:~:text=Twenty%2Dtwo%20of%2031%20NATO,goal%20of%202%25%20of%20GDP.&text=NATO%20countries%20aim%20to%20spend,2%25%20of%20GDP%20in%20defense.>
- Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, 38, 30.
- Ritchie, S. (2024, April 8). Canada unveils updated defence policy, plan to spend \$73B over 20 years on renewing military capacity. *The Canadian Press*. Retrieved from: <https://www.ctvnews.ca/politics/canada-unveils-updated-defence-policy-plan-to-spend-73b-over-20-years-on-renewing-military-capacity-1.6837383>
- Robertson, G. (2002, June 6). NATO Secretary General, transcript of press conference. Brussels: NATO Headquarters.
- Rühle, M. (2014). *NATO Enlargement and Russia: Die-Hard Myths and Real Dilemmas*. NATO Defense College. <http://www.jstor.org/stable/resrep10297>
- Sadat, M. (2020). Space: New Threats, New Service, New Frontier An Interview with Mir Sadat. *Strategic Studies Quarterly*, 14(4), 6–17. <https://www.jstor.org/stable/26956150>
- Savage, P. (2017). *Russian Social Media Information Operations: How Russia has Used Social Media to Influence US Politics*. American Security Project. <http://www.jstor.org/stable/resrep06042>
- Sawant, M. (2021). Why China Cannot Challenge the US Military Primacy. *Journal of Indo-Pacific Affairs*. Retrieved at: <https://www.airuniversity.af.edu/JIPA/Display/Article/2870650/why-china-cannot-challenge-the-us-military-primacy/>
- Scaparrotti, C. M., Bell, C. B., Schroeder, W., Starling, C. G., & Rodihan, C. (2020). Enhancing Deterrence and Readiness: The Role of Military Mobility. In *MOVING OUT: A Comprehensive Assessment of European Military Mobility* (pp. 6–9). Atlantic Council. <http://www.jstor.org/stable/resrep24666.5>
- Schelling, T. C. (1976). *Arms and Influence*. New Haven, CT: *Yale University Press*.
- Schmitt, G. J. (Ed.). (2020). NATO: THE CURRENT CHALLENGE. In *A Hard Look at Hard Power: Assessing the Defense Capabilities of Key US Allies and Security Partners—Second Edition* (pp. 187–224). Strategic Studies Institute, US Army War College. <http://www.jstor.org/stable/resrep27713.11>
- Sendstad, C., Hakvåg, U., Nouwens, M., Schwartz, P., Hart, B., Lin, B., Wilson, R. S., Julienne, M., Pynnöniemi, K., & Patalano, A. (2022). Russian Views on Sino-Russian Military- Technical Cooperation. In M. Bergmann & A. Lohsen (Eds.), *Understanding the Broader Transatlantic Security Implications of Greater Sino-Russian Military Alignment* (pp. 6–12). Center for Strategic and International Studies (CSIS). <http://www.jstor.org/stable/resrep45513.4>
- Shalamanov, V., Anastasov, P., & Tsvetkov, G. (2019). Deterrence and Defense at the Eastern Flank of NATO and the EU: Readiness and Interoperability in the Context of Forward Presence. *Connections*, 18(1/2), 25–42. <https://www.jstor.org/stable/26948847>
- Shea, J. (2017). How is NATO Meeting the Challenge of Cyberspace? *PRISM*, 7(2), 18–29. <http://www.jstor.org/stable/26470515>
- Shiffrinson, Joshua R. (2020). "NATO enlargement and US foreign policy: the origins, durability, and impact of an idea". *International Politics*. 57 (3): 342–370. doi:10.1057/s41311-020-00224-w. hdl:2144/41811
- Shurkin, M. (2017). *The Abilities of the British, French, and German Armies to Generate and Sustain Armored Brigades in the Baltics* (No. RR-1556-OSD). RAND Corporation. https://www.rand.org/pubs/research_reports/RR1556.html
- Simón, L. (2023, November 23). NATO's China and Indo-Pacific conundrum. *NATO Review*. Retrieved from: <https://www.nato.int/docu/review/articles/2023/11/22/natos-china-and-indo-pacific-conundrum/index.html>
- Snyder, G. H. (1984, July). The Security Dilemma in Alliance Politics. *World Politics*, 36(4), 466.

INTO THE GRAY ZONE: NATO DETERRENCE IN A GRAYING AND MULTIPOLAR WORLD

- Starcevic, S. (2023, December 28). Russia warns Finland will suffer in latest saber-rattling. *Politico*. Retrieved from <https://www.politico.eu/article/russia-warns-finland-will-suffer-in-latest-saber-rattling/>
- Sullivan, B. (2022, February 24). How NATO's expansion helped drive Putin to invade Ukraine. *NPR*. <https://www.npr.org/2022/01/29/1076193616/ukraine-russia-nato-explainer>
- Sun Tzu. (1963). *The Art of War* (S. Griffith, Trans.). New York: Oxford University Press.
- Stevenson, J. (2022). *Overseas bases and US strategy: Optimising America's Military Footprint*. International Institute for Strategic Studies.
- Stoker, D., & Whiteside, C. (2020). BLURRED LINES: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. *Naval War College Review*, 73(1), 12–48. <https://www.jstor.org/stable/26868211>
- Sweijts, T., Zilincik, S., Bekkers, F., & Meessen, R. (2021). Strategic Framework to Counter Hybrid Action. In *A Framework for Cross-Domain Strategies Against Hybrid Threats* (pp. 15–26). Hague Centre for Strategic Studies. <http://www.jstor.org/stable/resrep27705.7>
- Szeleccki, S. (2019). Interpreting the interoperability of the NATO's communication and information systems. *Scientific Bulletin*, 24(1), 95–107. <https://doi.org/10.2478/bsaft-2019-0011>
- Tass News Agency. (2021, December 16). Full-blown warfare in cyberspace in progress, says Russian diplomat. Retrieved from <https://tass.com/world/1376491>
- U.S. Army. (2016). *ADRP 3-0: Operations*. Retrieved from <https://usacac.army.mil/sites/default/files/publications/ADRP%203-0%20OPERATIONS%2011NOV16.pdf>
- U.S. Department of Defense. (2023). FY 2024 Budget Request Overview Book. Retrieved from https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2024/FY2024_Budget_Request_Overview_Book.pdf
- U.S. Department of Defense. (2024). America's Nuclear Triad. Retrieved from <https://www.defense.gov/Multimedia/Experience/Americas-Nuclear-Triad/>
- Veebel, V., & Ploom, I. (2018). The deterrence credibility of NATO and the readiness of the Baltic States to employ the deterrence instruments. *Lithuanian Annual Strategic Review*, 16(1), 188.
- Waterman, S. (2019, September 19). Cyber Flight Plan Outlines USAF Efforts to Take on Hybrid Warfare. *Air Force Magazine*. Retrieved from <https://www.airforcemag.com/>
- Wilson, D. M. (2011). *Learning from Libya: The Right Lessons for NATO*. Atlantic Council. <http://www.jstor.org/stable/resrep03354>
- Wolfowitz, P. (2001, September 26). Press Conference, NATO HQ. Quoted in Kreps, S. E. (2011). *Coalitions of Convenience: United States Military Interventions after the Cold War* (pp. 95–96). Oxford University Press.
- Zhao, S. (2014). Foreign Policy Implications of Chinese Nationalism Revisited: the strident turn. In *Construction of Chinese Nationalism in the Early 21st Century* (1st ed., pp. 17–36). Routledge. <https://doi.org/10.4324/9781315772172>