2022 CUTTING THE BOW WAVE

COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE

TRANSFORMING ALLIED MARITIME POTENTIAL INTO REALITY

Disclaimer: The opinions, conclusions, and recommendations expressed or implied within are those of the contributors and do not necessarily reflect the views of the U.S. Department of Defense, U.S. Second Fleet, CJOS COE, NATO or any other government agency.
This product is not a doctrinal publication and is not staffed but is the perception of those individuals involved in military exercises, activities and real-world events. The intent is to share knowledge, support discussion and impart information in an expeditious manner.

Front Cover: A U.S. Navy member in Exercise REP(MUS) 21. Courtesy of U.S. Navy
Back Cover: Sundown at sea. A Turkish MEKO Class Frigate. Courtesy of Turkish Navy

Publisher's Note

Cutting the Bow Wave is an annual publication by Combined Joint Operations from the Sea Centre of Excellence, U.S. Second Fleet, in Norfolk, Virginia. For publication purposes, all articles and materials submitted become the sole property of CJOS COE. For copies and information, send request to:

CJOS COE ICO
Bow Wave Editor
7927 Ingersol St., Ste 150
Norfolk, VA 23551

Executive Editor:
Cdre Tom Guy, RN

Managing Editor:
CAPT Rory McLay, RCN

HMS Queen Elizabeth UK Carrier Strike Group manoeuvres with USS Carl Vinson Carrier Strike Group and ships from the JSDMF in the Bay of Bengal. Courtesy of the Royal Navy.

2022 Cutting the Bow Wave – Director's Introduction

Recent events in Eastern Europe have dramatically underscored the vital importance of building and maintaining strong Alliance partnerships as the cornerstone of a successful, deterrent strategy. As we look not only to Europe's eastern flank, but also the pacing threat of an increasingly assertive People's Republic of China, potential threats to the Alliance have manifested in new and sophisticated ways across all domains. Not only have we seen a return to war in Europe, but across the globe, there is a destabilizing erosion of peace and public trust through disinformation campaigns, cyber-attacks and a continued proliferation of high-tech weaponry. The ubiquitous and complex nature of today's challenges demands a level of continuous vigilance that can only be accomplished through the collective efforts of our wide-ranging and steadfast network, across national boundaries, and domains. It is no surprise that the maritime domain, the world's oceans that connect each of our nations, is an intrinsic part of this continuum and is the very realm within which we can assert the deterrence necessary to prevail.

A unique, multi-national organization, CJOS COE supports the Alliance network from a maritime perspective, with the sole focus of providing the best military advice on issues in the maritime domain from tactical to strategic levels. Purposely situated alongside U.S. Second Fleet and Joint Force Command Norfolk, and adjacent to Allied Command Transformation, CJOS COE is a key enabler that drives interoperability, deepens understanding of the maritime domain, enhances multi-domain integration, and supports the development of innovative technologies.

Through the publication of this 'Cutting the Bow Wave,' CJOS COE aims to provide an intellectual catalyst to commands and organizations across the Alliance. It promotes professional discourse on important maritime issues and influencing strategic thinking. Cutting the Bow Wave continues to elevate the conversation on the implications of technology in the maritime domain while enhancing our understanding of potential challenges.

As the Director of CJOS COE, I take great pride in our team's hard work on the most relevant issues facing the Alliance today and I am determined to ensure we continue making a difference. If you have a challenge that you think we can help with, please get in touch.

USS Harry S. Truman (CVN-75), U.S. Navy. Courtesy of U.S. Navy.

Vice Adm. Dwyer is a native of Alameda, California, and a graduate of the California Maritime Academy and U.S. Naval War College, where he holds a Bachelor of Science in Marine Transportation, a Master's in Foreign Affairs and Strategic Studies, and a Master's in Computer Information Science. Dwyer is also a graduate of the NATO Defence College General Flag Officer and Ambassador course.

Vice Adm. Dwyer, a career F/A-18 naval aviator and graduate of the Navy Fighter Weapons School (TOPGUN), has completed eight carrier deployments to the Western Pacific, North Atlantic, Mediterranean, and North Arabian Sea, supporting Operations Southern Watch, Iraqi Freedom, Enduring Freedom, and New Dawn flying over 75 combat missions.

He has previously commanded Strike Fighter Squadron (VFA) 27; Provincial Reconstruction Team Asadabad, Kunar Province, Afghanistan; Fleet Replacement Squadron (VFA) 106, Carrier Air Wing 8, and Carrier Air Wing 17; as a flag officer Dwyer commanded the Theodore Roosevelt Carrier Strike Group (CSG 9), and was the 36th Chief of Naval Air Training (CNATRA).

His major staff assignments include director of Regional Outreach (CJ9) NATO Headquarters, Commander, International Security Assistance Force Kabul, Afghanistan, and director of Aviation Officer Distribution (Pers-43) Naval Personnel Command Millington, Tennessee.

As a flag officer Dwyer served as the chief of staff (CoS) and assistant chief of staff for Strategy, Resources and Plans (N5) for Commander, U.S. Naval Forces Europe and U.S. Naval Forces Africa and for Commander, U.S. 6th Fleet in Naples, Italy, and most recently the Director of Plans and Policy (J5) for U.S. Cyber Command in Fort Meade, Maryland.

Vice Adm. Dwyer assumed duties as Commander, Joint Force Command Norfolk, Commander, U.S. Second Fleet, and Director, Combined Joint Operations from the Sea Centre of Excellence on August 20, 2021.

Dwyer was the 1997 Commander Strike Fighter Wing Pacific Adm. Wesley McDonald Junior Officer of the Year and his personal decorations include the Defense Superior Service Medal, Legion of Merit, Bronze Star, Air Medal Strike/Flight, Combat Action Ribbon, Battle E (three awards) and has accumulated over 3,800 F-18 flight hours, and over 1,100 carrier arrested landings on 12 different aircraft carriers.

A FA-18 Super Hornet is launching from a carrier. Courtesy of U.S. Navy.

2022 Cutting the Bow Wave – Deputy Director's Foreword:

As we started the year, the twin priorities for the Alliance were to 'operationalise' the Concept for Deterrence and Defence of the Euro-Atlantic area (DDA), and to further develop NATO's Warfare Development Agenda (WDA). Even before the turbulent events of recent months I wrote that there was an urgent requirement for clarity in an ever increasingly complex and unclear world. We now face both a dramatically strengthened demand signal and a great will to drive forward our collective warfighting capabilities.

As we look to an effective deterrence posture for the Alliance, we explore what emerging and disruptive technology demands and enables. Complexity and tempo are persistent themes as we investigate how NATO should harness un-crewed systems to best effect, exploit artificial intelligence and quantum computing, and make the most of 5G in the maritime domain. But in simpler, practical terms, the Alliance also needs to understand and agree how it views the totality of its domains, including the security of undersea cable and satellite constellations, which surely deserve the term 'Strategic Lines of Communication'. 'Multi-domain' is an increasingly dominant theme too. As the Deputy Commander of the UK's Strategic Command simply put it: "Joint is no longer enough". Efforts must occur multi-dimensionally and without constraint to artificial lines drawn on charts. Interoperability, integration and interchangeability must always be a high priority; the ability to share information and data effectively must be matched by an understanding of the need to do so, particularly as technological development continues to gather pace.

As domains merge and overlap, and 'multi-domain' concepts dominate, we need to rigorously manage our thinking and ensure coherence in our conceptual development. In this edition, you will see a broad range of open discussion, designed to provoke further thought and debate, much of which will necessarily be conducted more discretely. Our collective ability to fight tonight and tomorrow depends on our informed decisions of today. We look forward to continuing our efforts in turning Allied Maritime potential into reality.

Ice Camp Sargo inside the Arctic Circle during ICEX 2016. Courtesy of NATO

Tom Guy is fortunate to have enjoyed a broad range of rewarding operational, staff and command roles ashore and afloat from the UK to the Far East. Early appointments included a wide variety of ships, from patrol craft to mine-hunters, frigates, destroyers and aircraft carriers, ranging from fishery protection to counter-piracy and UN embargo operations as well as training and operating with a broad range of NATO allies. Having trained as a navigator and diving officer early on, Tom specialised as an anti-submarine warfare officer and then a Group Warfare Officer. He then went on to command HMS Shoreham, a new minehunter out of build, and then HMS Northumberland, fresh out of refit as one of the most advanced anti-submarine warfare frigates in the world. His time as Chief of Staff to the UK's Commander Amphibious Task Group included the formation of the Response Force Task Group and its deployment on Op ELLAMY (Libya) in 2011 and he later had the great privilege of serving as the Captain Surface Ships (Devonport Flotilla).

Shore appointments have included the Strategy area in the MOD, a secondment to the Cabinet Office, Director of the Royal Naval Division of the Joint Services Command and Staff College, and the role of DACOS Force Generation in Navy Command Headquarters. He has held several Operational Staff appointments, including service in the Headquarters of the Multi National Force Iraq (Baghdad) in 2005. Other operational tours have included the Balkans and the Gulf, both ashore and afloat. In 2016-17 he was the Deputy UK Maritime Component Commander in Bahrain, working alongside the U.S. Fifth Fleet Headquarters. He assumed the role of Deputy Director of the Combined Joint Operations from the Sea Centre of Excellence in Norfolk, VA, in September 2017.

A graduate of the UK's Advanced Command and Staff Course and the U.S. Capstone Course , with a Master's Degree from Kings College, Tom is a Younger Brother of Trinity House and a keen yachtsman (qualified as an Offshore Yachtmaster), as well as being a classic car and bike enthusiast. He is married to Katie who is a sailing instructor and they have two grown up children, both of whom are also keen sailors.

The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) was established in May 2006. Representing 13 nations, CJOS is the only Centre of Excellence in the United States, and one of 28 NATO accredited Centres worldwide, representing a collective wealth of international experience, expertise, and best practices.

Independent of the NATO Command structure, CJOS COE draws on the knowledge and capabilities of sponsoring nations. U.S. Second Fleet, and neighboring U.S. commands to promote "best practices" within the Alliance. CJOS COE also plays a key role in aiding NATO's transformational goals, specifically those focused on maritime-based joint operations. We enjoy close cooperation with Allied Command Transformation (ACT), other NATO commands, maritime COEs, and national commands.

Comprised of 25 permanent staff, CJOS COE is highly flexible and responsive to its customers' needs. The Centre cooperates, whenever possible, with industry and academia to ensure a comprehensive approach to the development of concept and doctrine.

REQUEST FOR SUPPORT

NATO Organizations should submit Requests for Support (RfS) via the TRANSNET website for inclusion into the CJOS program of work. Individual nations or institutional stakeholders who wish to submit a request may contact CJOS COE directly and submit a request to the Directorate Coordinator. The CJOS Program of Work (PoW) is on an annual cycle. Request for the 2023 PoW should ideally be submitted by 15 August 2022. If the requests are approved by the Steering Committee, they will be included in the 2023 PoW. We also are available to take emergent request as an Out of Cycle RfS. If submitting an out of cycle request via TRANSNET, there must be also an email directly to CJOS COE for timely acceptance and work to begin on the project.

Our aim is to be a pre-eminent source of innovative military advice on combined joint operations from the sea. Our strength lies in our diverse staff spanning 13 different nations from multiple military branches. We continue to improve our products and services by collaborating with institutions, universities and other organizations that are leaders in their fields of expertise. We take full advantage of our location in Norfolk, VA and the numerous universities, and research facilities in our area. We also have a unique tie to the United States Navy's Fleet Forces Command, SECOND Fleet and NATO's Joint Force Command Norfolk.

If you are interested in receiving project support from our staff, simply submit a request to CJOS COE as described above via the following link https://portal.transnet.act.nato.int/Pages/home.aspx . TRANSNET accounts can be requested from the TRANSNET website, or you can visit our website at www.cjoscoe.org . RfS' can be submitted to any staff member or the Directorate Coordinator at:

Email: USFF.CJOS.COE@NAVY.MIL or Phone: +01-757-836-2611

Hope to hear from you soon!

WHAT IS CJOS COE?

The Combined Joint Operations from the Sea Centre of Excellence is a preeminent, independent, multinational source of innovative advice and expertise on all aspects of maritime operations, charged with developing and promoting maritime concepts and doctrine in order for NATO, Sponsoring Nations, Allies and other international partners and organizations to optimize the efficient delivery of Maritime Effect.

CJOS COE MISSION

To support the sponsoring Nations (SN) and NATO in improving their ability to conduct Allied combined joint operations from the sea in order to counter current and emerging maritime global security challenges

CJOS COE VISION

Working closely with partners and stakeholders from international militaries, governments, non-governmental agencies, industry and academic communities of interest, CJOS COE aims to be the Alliance's source of expertise in the conduct of combined and joint operations in the maritime environment.

NATO HQ. Courtesy of NATO.

CJOS COE WILL ACCOMPLISH ITS MISSION:

- Through the development of innovative concepts and doctrine thus supporting transformation of NATO to meet the demands of future operations in the maritime domain.
- By identifying and resolving obstacles to a networked response to maritime security challenges.
- By applying the principles of Smart Defense and pooling subject matter experts.
- Through broad intellectual engagement thereby supporting the Connected Forces Initiative.

DILEMMAS OF DETERRENCE IN AN ERA OF EMERGING DISRUPTIVE TECHNOLOGY

PROFESSOR JAMES HENRY BERGERON
POLITICAL ADVISOR, ALLIED MARITIME COMMAND

Although the variables may be changing. . . deterrence remains concerned with the comprehensive impact of all military capabilities that shape an adversary's risk calculus.

The issue of Emerging and Disruptive Technologies (EDT) has been trending in NATO of late. The 2019 NATO Leaders Meeting in London set out an EDT Roadmap.[1] The NATO 2030 Report cited EDT as a major area for focus and investment. In February 2021, Defence Ministers agreed in general terms on coordinating investment in EDT, strengthening relationships with private sector innovation hubs and creating foreign export protection mechanisms.[2] NATO has set a headmark of developing policies on seven key EDT areas: AI, Data, Autonomy, Biotechnology, Hypersonic Technology, Quantum Physics-based technologies, and Space. The Ministers also announced plans to complete specific artificial intelligence (AI) and Data strategies by summer 2021. The AI Strategy was released in August 2021.[3]

On 1 March 2021, NATO's Advisory Group on Emerging and Disruptive Technologies released its first annual report with recommendations to create an internal agency based on the U.S. Defense Advanced Research Projects Agency (DARPA) that would group together existing centres, invest in new technology, and collaborate with Allied innovation hubs in the public and private sectors. This would be backed by a NATO investment bank to fund innovation in EDT. Those recommendations were approved at the Brussels Summit.[4]

Seen through a NATO institutional prism, an important if understated concern with EDT is its potential disruption of allied cohesion and interoperability. As some move forward with embracing advanced EDT, the U.S. in particular, there is a concern that other allies may not be able to keep up, and that the ability to communicate and operate together at the 'speed of relevance' will be impaired. The Alliance efforts look forward to setting NATO standards and encouraging technology sharing, as well as playing a collective role in fostering innovation.

Seen through a NATO and allied external prism, of course, EDT is seen as a part of 'Great Power Competition', and particularly for NATO, through the lens of deterrence of aggression. MARCOM is engaged in this transformation, particularly in underwater autonomy. Building on the success of the Portuguese-hosted REP(MUS) exercise series, MARCOM is building DYNAMIC MESSENGER, an opportunity to incorporate experimentation in underwater autonomy into a conventional exercise. MARCOM has also begun to seriously explore the implications for EDT in the future of naval warfare and Alliance security. In September 2021, MARCOM held its 4th Sea Power Conference with the University of Plymouth. The theme, 'Operating in an All-Domain Grey Zone,' focused on many of the challenges of an EDT era, including deterrence management, space, cyber, advanced technologies, and the lawfare related to them.

EDT has been described in terms of technology advantages to protect and advance, or of challenges to counter, and there is a small but growing literature on the implications of EDT for deterrence. This article explores that third dimension, the implications of EDT for deterrence in the concrete situation in which we find ourselves.

As an opening point, the term 'disruptive' in EDT is not particularly useful. All major technological breakthroughs are disruptive of what went before. When Jackie Fisher built HMS DREADNOUGHT, that was certainly an application of a disruptive technology. There is a parallel to the use of 'asymmetric' in the 00's as almost a term of abuse. In both cases, a threat was perceived to status quo advantages.

Deterrence is usually described as being of two types: deterrence by punishment and deterrence by denial.[5] The first approach promises unacceptable retaliation should an adversary cross the policy red line that deterrence is intended to prevent. This is a popular notion of nuclear deterrence and it remains relevant at the highest end of conflict. But increasingly over the years, deterrence by denial has achieved emphasis in Western military circles, possibly prominence. For the nuclear powers, the two are linked in ways that foster, if not mandate, Grey Zone or indirect manoeuvre, or an attack only on non-nuclear others, as in Ukraine, as the only feasible major use of the Military Instrument of Power.

This argument rests on the premise that Mutual Assured Destruction remains the prime factor in shaping deterrence and defining the limits of 'competition' between the nuclear powers and, to a degree, between middle non-nuclear powers tied to nuclear alliances. But what that means for conventional conflict has always been subject to debate. At the height of the Cold War, it was widely assumed that a Soviet invasion of Western Europe would lead to a nuclear exchange between the U.S. and Soviet homelands. The shift from conventional to nuclear conflict was viewed as likely to be inevitable. NATO also threatened first use of nuclear weapons if necessary to stop Russian aggression, even as Moscow does today against NATO and very recently over their aggression in Ukraine.

As early as 1954, the British military thinker Basil Liddel-Hart argued that a nuclear weapon would never be used against anything but the threat of another nuclear weapon.[6] In other words, nuclear competition existed in a sealed bubble and was separate from conventional conflict. Now if that were true, then the world has, for many decades, been 'safe' for great power conventional conflict. Yet it has not happened and recent history indicates that the desire on all sides to manoeuvre beneath the assumed escalation threshold is as strong as ever. Why? Arguably, due to uncertainty on all sides that conventional conflict would not escalate out of control, combined with the lack of truly vital state interests being challenged. But, as a result, deterrence needs to be considered in the systemic context of mutual deterrence, a deterrent equilibrium, possibly even competitive deterrence.

In a situation where unacceptable nuclear retaliation, commanded by both sides, would still destroy themselves and much of the world, manoeuvre strategies for advantage, beneath the believed threshold of kinetic escalation between nuclear states and alliances, are pursued as a form of political or strategic capital in pursuit of important state interests. The cyber and electronic warfare realms, hypersonics, space, AI, Data, autonomy, and quantum technologies are all becoming primary fields for this activity.

NATO's Airborne Warning and Control System (AWACS) Aeroplanes Courtesy of NATO

Does the emergence of EDT destabilise or undermine our assumptions about the viability of deterrence? And the role of deterrence in peacetime or 'Grey Zone' times? There is a growing literature on this. Recently Brad Roberts provided an excellent review of EDT scholarship on the question of its deterrent impact, with the general result that scholars profoundly disagree over the impact that EDT will have.[7] Some see it as stabilizing, others as profoundly destabilising. Roberts points out that studies of the role of EDT in conflict predominate in current research.[8] Explorations of its use in crisis management are less and EDT in peacetime rivalry is the least developed of all.[9]

What Deterrence Requires

The practical application of a deterrent strategy in our era has depended on a few key factors.

Deterrence requires a mutually understood sphere of activity by an adversary that is acceptable, even if unwelcome, and a sphere that crosses the 'redline' into triggering a response. Ideally all sides share a strategic appreciation of where these lines exist. Things get tricky when strategic appreciations differ.

Deterrence requires knowledge of adversary capabilities. Recall Dr Strangelove's response to the Russian ambassador on the Doomsday Machine that they kept secret: 'Why didn't you tell us?' This is the first Essential Dilemma of the era of EDT for deterrence strategies. With new technology, there is the motivation to surprise as well as the desire to deter. A compromise between these goals might involve broadcasting successes in some EDT fields, while holding others back. High energy weapons, hypersonics might fall more easily into the first category; AI, data, cyber, space, Electromagnetic Pulse (EMP) employment and quantum breakthroughs might better fit the second. But the tension remains, evidenced recently by the November 2021 Russian destruction of a satellite in orbit, demonstrating a key capability.[10]

This also raises the distinction between the application of EDT in 'peacetime' or non-crisis situations, and their employment at the juncture of crisis-to-conflict. The dynamics are quite different. In Grey Zone manoeuvre, surprise is not the aim, the purchase of political capital is, at the expense of signalling a capability (or intent to acquire one) and allows a potential adversary to work on a counter. The Russian satellite shoot-down is enlightening here. By contrast, the application of EDT as a strategic shock in crisis may have operational advantages, possibly decisive ones, but also risks losing control of escalation. There was a notable NBC report on 24 February that President Biden had been briefed on major offensive cyber options against Russia as the war in Ukraine was beginning.[11] The White House immediately rejected the claim as 'wildly off base'.[12]

It may well have been, but the episode also illustrates the difficult linkage between surprise and escalation with EDTs.

Deterrence depends on time. There needs to be enough time to process decision-making through the adversary's administrative and political processes, but not so much time that a counter-strategy for escalation can be offered. And not so little as to encourage a 'use it or lose it' response.

Further, systemic deterrence requires a relationship between time and counter-strategies that encourages restraint now in hopes of reversing the deterrent advantage in the future. There is an 'OODA loop' effect where each side chills action by the other, all seeking advantage, the technology takes time to develop and deploy, and the challenges are chronic enough for long-term strategic decision making. They do not arrive so quickly or in such numbers to prevent a deterrent counter-strategy; they do not take so long that one believes they have an enduring advantage. This takes the form of competition over innovation, production, and military posture for deterrent advantage.

Application to the Era of EDT

Applying this thinking to EDTs – A few case examples raise interesting questions for deterrence.

1. Command and Control: As Chris Dougherty points out, wargame after wargame of U.S.-Russia and U.S.-China confrontations posits the conflict to begin with an attack on C2 to dissemble the effectiveness of the command structure and sever the links with deployed forces.[13] There is a first mover advantage here, especially where a first mover like Russia also seeks to adopt a short-war strategy, a one-two week conflict window followed by a negotiated settlement in their favour.

Implications of EDT here are mixed. In the Grey Zone, it does not appear that the use of cyber disruption in non-crisis situations breaks the deterrent threshold for a kinetic response, so long as the damage resulting is itself data and not physical damage. Consider SolarWinds.[14] Does 'what happens in Cyber stay in Cyber'? The Colonial Pipeline software hack could have been the limiting case here with its resulting shutdown of the pipeline by Colonial as a precaution, but it was not.[15] The attribution problem was in play, with the U.S. government pointing the finger at Russian cyber-criminals, but not the Russian state. In the crisis or acute situation, the result could be different. Physical retaliation might be more likely if an attack was against dual use C3I systems, where a debilitating strike could have both conventional and nuclear response implications.

Location also matters. In the Grey Zone, an element of protection seems to exist in the reluctance of great powers to strike each other's homelands. But that could be less of a concern with C2 nodes based elsewhere. Chris Dougherty tells of a wargame where air C2 was relocated from USAFE to the Continental U.S. to raise the stakes for pre-emption and retaliation.[16] There is also a logic in dispersing C2 across the territory of several allies, as with the NATO Command Structure, to confound attempts by an adversary to focus its attack and limit the conflict. Interestingly, that protection might be at its weakest in deployed command and control systems aboard ship or in the air in the global commons.

There is also a human dimension to C2, and an aspect of EDT that has not been much addressed. This is the 'Havana Syndrome' reports of U.S. State Dept and other officials falling ill with numerous debilitating and long lasting symptoms. Little is known (or acknowledged) by governments, although the CIA has issued an interim report discussing most cases but considering foreign involvement in about two dozen incidents since 2016.[17] From public sources, it appears that the likely explanation of the most suspicious cases is some form of microwave radiation targeting the individuals in civilian environments. Most of the literature pointed the finger of suspicion at Russia, although governments have yet to attribute blame.

'Havana' attacks differ from cyber attacks or AI-enabled disruption of headquarters. Like bioweapons – the Skripal case in the UK – this is a kinetic attack on people in a national territory. It crosses the red line for a response, although not necessarily a military response. That may be partly due to the unwillingness of allied governments to respond in kind to such an unorthodox and illegal form of attack.

There is also the knowledge and attribution problem again, as with cyber and AI-disruptions. The second Essential Dilemma of EDT for deterrence is the tension between signalling ownership of an 'attack' or even a capability for an attack, to benefit from its deterrent effect, and not providing so much evidence that attribution, retaliation, and escalation inevitably follows. The middle ground arguably pursued by Moscow in Crimea, with the Skripals and other ill fates met by former spies, SolarWinds, and other hacking efforts, might be called 'implausible deniability'. The political benefit of such acts requires that the adversary does attribute the act to the antagonist, but not too easily or clearly or formally.

There is also a diplomatic dimension of such pseudo-ambiguous strategies: implausible deniability creates wiggle room where states or parts of an alliance are not keen on a confrontation and are looking for a plausible or face-saving reason not to respond. 'We can't be sure' works well as a STRATCOM play in this regard, even if, inside government, they are relatively sure who the culprit is.

2. Autonomous systems and drones: There has been a revolution in land warfare over the past two years,

or perhaps it would be more accurate to call it a new form of air-land battle: the remarkably successful applications of drones on the battlefield in Syria, Libya, the recent Azerbaijan-Armenia conflict and in Ukraine. We have also seen their use in the Middle East and the Gulf. In the land domain, the impact on deterrence does not appear to be very great, as these forces were deployed in conflicts that were ongoing. They changed the tactical picture and perhaps the operational outcome, but did not alter or undermine strategic deterrent effects, although these were not contests between nuclear powers. One potential counter-example is Russian anger at Turkish drones sold to Ukraine and used to respond to insurgent attacks across the line of control in the Donbas. This could have been a factor in Russia's decision to escalate its armed aggression in eastern Ukraine into full scale war.

The situation may be different at sea or in the air, and when used outside of an existing conflict. Horowitz, Scharre and Fitzgerald expressed the concern that autonomy may allow leaders to take escalatory risks they otherwise would not, given the lack of human lives at stake.[18] But this dynamic cuts both ways – the adversary may also be ready to act against autonomous systems in ways they would not consider against a manned system. If that is so, there may be a deterrent equivalence at play, almost parallel to Liddle-Hart's remark about the Bomb, and some conclusions from non-kinetic cyber-attacks. Are drones and autonomous systems 'fair game' for action by great powers on a shared understanding that this exists below the threshold of escalation? Does 'what happens in unmanned stay in unmanned'? Practice is not yet firm on the point, but there are hints in that direction.

3. Artificial Intelligence, Mass and Speed: The application of AI can be expected to have divergent effects on the deterrent balance, depending on the nature of the systems being enhanced. An AI or autonomy-enhanced mine clearance capability favours the defence and arguably bolsters deterrence by denial. So do ASW gliders or underwater acoustic sensors, possibly the development of quantum-based radars that might pierce the oceans. But one counter that AI or autonomy might enable could be 'chaff', a bewildering number of false contacts hiding the real mine or the actual submarine. One might hypothesize that greater transparency, detection or autonomy, in and of themselves, are not destabilising for deterrence, although they might alter the balance of military power.

US deploys THAAD to Romania
Courtesy of U.S. Navy.

By contrast, AI-enabled hypersonic weapons or cruise missiles tend to favour the offence. They dramatically shorten the time for response, putting a strain on decision-makers, particularly in large alliances. Their potential dual nuclear or conventional nature creates a problem for knowledge as well as time. This can foster 'use it or lose it' first strike responses if one party believes that the other has deliberately crossed the threshold of aggression. It means that, as Michael Horowitz has pointed out, in conflict states can win faster, but they can also lose faster.[19] It may be that the speed factor is destabilising for deterrence.

However, the other side of AI is its potential automaticity. To turn again to Dr Strangelove, the perverse logic of the film's Soviet Doomsday Machine was that computers and sensors would automatically respond to an attack: it removed the human factor from a retaliatory response. In current conditions, adversaries will always consider the coherence of opposing C2 and the willingness of governments, administrations and the military to carry out nuclear orders from the top. Those dynamics do change when the C2 chain is simplified. In one sense, deterrence may be strengthened if there is less scope for C2 breakdown. But on the other, some important political, military and human checks and balances against first nuclear use may be weakened.

Implications for Deterrence and the Grey Zone Threshold

Looking at the problem from the perspective of the Grey Zone in which the great powers find themselves – arguably confined up until now – does EDT disrupt or destabilise our system of deterrence? And if so, in whose favour?

As we are only in the beginning of this era of EDT, it is hard to draw conclusions. But I would offer the following tentative ones:

What we have seen to date is a tendency towards parallelism in deterrent posturing, not crossover or horizontal escalation. Non-kinetic and non-human attacks seem to imply non-kinetic and non-human responses. The wild card may be at the individual human level, whether biological and EW based, where the individual nature of attacks has led to a characterisation more akin to secret service activities and public responses (or non-responses), rather than state on state conflict. Thus, nukes for nukes, cyber for cyber, and possibly a growing willingness to attack each other's drones. This is not a disruption of the escalatory threshold so much as a reimagining of what exists below it (Electromagnetic Pulse could be the exception here).

Certain aspects of EDT do challenge stable deterrence – the shortening of decision-making cycles with hypersonics and machine learning, the risk of a perishable first mover advantage in the use of AI, cyber or quantum technologies to disable command and control, disaggregate the force and deny (particularly to the U.S.) its current advantages in all domain force integration. At present, however, all players in this technological competition have a reasonable shot at success. Overmatch across all of these fields is not pre-ordained for anyone. As a result, it is likely that the great powers will not abandon their escalatory thresholds in the short or medium term by the lure of an EDT advantage alone, even if any of them could claim it. That advantage is likely to be short-lived, in any case. The perverse implication is that strategic stability is maximized if none of the main players succeed too well or fail too badly.

Last, there remains scope for mutual restraint and the equivalent of arms control-like agreements to suppress some of the more destabilising aspects of EDT. That will not be easy, however. Different players may see themselves as having advantages or lead times that they might not want to sacrifice.

Conclusion

Ultimately, the foundations and debates of deterrence theory appear to remain relevant, although the variables may be changing, or afforded differing weights. Deterrence remains concerned with the comprehensive impact of all military capabilities that shape an adversary's risk calculus. It is always to be measured from their perspective. Note that they therefore have an uncomfortable purchase on the purse strings of Allied defence budgets.

From a NATO perspective, AI and machine learning may be the biggest institutional challenge. As foreshadowed by BMD, the speed of response required in an AI-enabled conflict would shorten the scope for complex political negotiations and compromises that are at the heart of Alliance politics. That strikes at allied cohesion, which is a central element in deterrence. But it is not a new one: at the height of the Cold War, the North Atlantic Council was expected to meet within one hour if necessary to authorise Article V collective defence responses to a Soviet attack.

There are some solutions. One would be to follow the BMD model and shift politics onto pre-agreed authorisations, metrics, and criteria for the use of force in defence against, or responding to, an AI-enabled or hypersonic attack, or the crippling of C2 systems. The level of delegation required to be effective could be extremely high, possibly down to the CIC of a warship, and possibly beyond that, taking the human out of the immediate response loop entirely. This level of automation might enhance deterrent credibility but needs to be balanced against effective constraints on irrational or impulsive nuclear use. A second option would be the tacit acceptance that only a few allies, at present, are capable of operating in most EDT environments and would need to be depended upon as first responders. And the third option, as promoted in the NATO 2030 report and being pursued in Brussels, is to work on ways to agree on sharing of EDT and counter-EDT capabilities and techniques as widely as possible within NATO. This would ensure a more united and cohesive Alliance.

1 See Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in London 3-4 December 2019, available at https://www.nato.int/cps/en/natohq/official_texts_171584.htm.
2 See 'New focus on emerging and disruptive technologies helps prepare NATO for the future' 3 March 2021, available at https://www.nato.int/cps/en/natohq/news_181901.htm.
3 See Press Release, NATO releases first-ever strategy for Artificial Intelligence, 22 October 2021, available at https://www.nato.int/cps/en/natohq/news_187934.htm?selectedLocale=en.
4 See Brussels Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 14 June 2021 pp. 37, available at https://www.nato.int/cps/en/natohq/news_185000.htm.
5 The classic work is Glenn H. Snyder, Deterrence by Denial and Punishment (Princeton: Center of International Studies, January 1959). See also André Beaufre, Deterrence and Strategy (New York: Praeger, 1965), Thomas Schelling, The Strategy of Conflict (Cambridge: Harvard University Press, 1980)
6 Basil Liddell Hart, Strategy, (London: Faber and Faber, 1954 and 1967), Preface.
7 Brad Roberts, Emerging and Disruptive Technologies, Multi-domain Complexity, and Strategic Stability: A Review and Assessment of the Literature (Centre for Global Security Research, Lawrence Livermore National Laboratory, February 2021) available at https://cgsr.llnl.gov/content/assets/docs/EDT_ST2_BHR_2021.3.16.pdf.
8 Id.
9 Id.
10 BBC News, "Russian anti-satellite missile test draws condemnation", 16 November 2021, available at https://www.bbc.co.uk/news/science-environment-59299101.
11 NBC News, "Biden has been presented with options for massive cyberattacks against Russia", 24 February 2022 available at https://www.nbcnews.com/politics/national-security/biden-presented-options-massive-cyberattacks-russia-rcna17558.
12 Reuters, "White House denies report on Biden being presented with cyberattack options against Russia", 24 February 2022, available at https://www.reuters.com/world/europe/biden-presented-with-options-cyberattacks-against-russia-nbc-news-2022-02-24/.
13 Chris Dougherty, More than Half the Battle: Information and Command in a New American Way of War (Centre for a New American Security, 21 May 2021) available at https://www.cnas.org/publications/reports/more-than-half-the-battle.
14 Reuters, "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft" 15 February 2021 available at https://www.reuters.com/article/us-cyber-solarwinds-microsoft-idUSKBN2AF03R.
15 New York Times, "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity", 14 May 2021,
Updated 8 June 2021, available at https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html.
16 Supra, n. 14 at p. 24.
17 BNBC News, "CIA says 'Havana Syndrome' not result of sustained campaign by hostile power" 20 January 2022, available at https://www.nbcnews.com/politics/national-security/cia-says-havana-syndrome-not-result-sustained-global-campaign-hostile-rcna12838.
18 Michael C. Horowitz, Paul Scharre, and Ben FitzGerald, Drone Proliferation and the Use of Force: An
Experimental Approach. (Washington, DC: Center for a New American Security, 2017), p. 8. Available at http://drones.cnas.org/wp-content/uploads/2017/03/Drone-Proliferation-and-the-Use-of-Force-ProliferatedDrones.pdf.
19 Michael C. Horowitz, "When speed kills: Lethal autonomous weapon systems, deterrence and stability." Journal of Strategic Studies 42(6) (2019) pp. 782.
20 The views expressed herein are those of the author alone and do not necessarily reflect the position of NATO or of any ally.

TASK FORCE ARCTIC: AN "APPROPRIATE" MEASURE

LT (USN) ELISABETH MADRELL
CDR (USN) TRACY REYNOLDS

The international community must act to counter the unilateral Russian restriction on freedom of movement in the Northern Sea Route.

In 2021, Russia assumed chairmanship of the Arctic Council, an Arctic intergovernmental forum, professing their commitment of "actively fostering peaceful, progressive and sustainable development in the region and strengthening cooperation among Arctic States, indigenous Permanent Participants and Observers."[1] Unsurprisingly, Russia has not acted in congruence to this mission statement. In the past two years, Russia has expanded their maritime claims in the Arctic and imposed restrictions on sovereign vessels, a violation of maritime law. Russian political, legal, and military aggression in the Arctic demands a renewed, multinational effort to secure the region. A cooperative task force, modeled on various Combined Maritime Forces and organized to counter Arctic-specific concerns, would serve to both counter increased Russian activity and encourage further regional cooperation and safety. There are many factors, both positive and negative, that support the establishment of an Arctic-focused task force, but, for the purposes of this article, recent Russian activity will be the main focus point.

The Arctic can be defined in many ways including its physical location and environment, climate, socio-economic layout, political characteristics, or even its specific legal framework (or lack thereof). Each perspective is critical in order to understand and assess the motivations and actions of Arctic stakeholders, friendly and adversarial, and further determine how to cooperate with, or combat them, as needed. Geographically, the U.S. defines the Arctic by statute as the area north of the Arctic Circle at 66.5 degrees[2], which is then split into three Arctic regions: The North American Arctic (NAA) comprised of Canada, the U.S., and Greenland; the European Arctic (EA) comprised mainly of the aquatic region from Greenland to Scandinavia; and the Asian Arctic, comprised of Russia. The physical environment is complex – from albedo effects on solar radiation absorption,[3] to the Arctic permafrost and its patterned ground polygons,[4] hummocks,[5] frost boils,[6] rolling pingos,[7] and thermokarst.[8] From a climatological standpoint, the Arctic is warming twice as fast as the rest of the globe, severely impacting everything from the phytoplankton food chain to the national security interests of the greatest world powers.[9] From a socio-economic standpoint, roughly ten percent of the Arctic's four million inhabitants are Indigenous Peoples, some of whom continue their traditional ways of life.[10] For example, there are an estimated 80,000 Sámi spread throughout Finland, Sweden, Norway, and Russia, and approximately 2,600 of them practice traditional reindeer husbandry today.[11]

Most pertinent to the national security analysis are the political and military stakeholders and legal frameworks by which they conduct themselves. Established by the Ottawa Declaration in 1996, the Arctic Council is comprised of the eight Arctic states including the U.S., Canada, Denmark, Russia, Norway, Finland, Sweden, and Iceland. It is the premier and cooperative forum for addressing sustainable development and environmental protection of the Arctic.[12] However, there is a notable exception to the Arctic Council's mission: military security.[13] In the interest of ensuring peaceful settlement of disputes, given their overlapping claims in the Central Arctic Ocean, Canada, Denmark, Norway, Russia, and the U.S. signed the Ilulissat Declaration in May of 2008, declaring:

> The Arctic Ocean stands at the threshold of significant changes. Climate change and the melting of ice have a potential impact on vulnerable ecosystems, the livelihoods of local inhabitants and indigenous communities, and the potential exploitation of natural resources. By virtue of their sovereignty, sovereign rights and jurisdiction in large areas of the Arctic Ocean the five coastal states are in a unique position to address these possibilities and challenges...[T]he law of the sea provides for important rights and obligations concerning the delineation for the outer limits for the continental shelf, the protection of the marine environment,

including ice-covered areas, freedom of navigation, marine scientific research, and other uses of the sea. We remain committed to this legal framework and to the orderly settlement of any possible overlapping claims. This framework provides a solid foundation for responsible management by the five coastal States and other users of this Ocean through national implementation and application of relevant provisions. We therefore see no need to develop a new comprehensive international legal regime to govern the Arctic Ocean. We will keep abreast of the developments in the Arctic Ocean and continue to implement appropriate measures.

Russia's recent territorial claims in the Arctic and violations of maritime law clearly represent significant developments, requiring appropriate measures. One such measure could be the establishment of a multinational task force squarely focused on cooperative security and safety in the Arctic.

A Maritime Law Primer

Before reviewing violations of maritime law, it is important to provide a cursory review of it. Put simply, maritime law governs the use of oceans and seas. Although there are myriad controlling national and international bodies of law, the primary codified international source is the United Nations Convention on the Law of the Sea (UNCLOS). Signed in 1982, after nearly ten years of negotiations, the treaty addresses a broad range of maritime issues such as freedom of navigation, dispute resolution, and a framework for maritime claims.[14] As of 2016, UNCLOS has been ratified by 162 parties.[15] While the U.S. has not officially ratified UNCLOS, it does adhere to UNCLOS in so far as it is a reiteration of customary international law. The U.S. infuses domestic interpretation of customary international law as it relates to the law of the sea within U.S. military doctrine, training, operational planning, and mission execution.[16] In contrast, Russia ratified UNCLOS, yet continues to violate UNCLOS through maritime claims and restriction of navigation. These two foundational points of maritime law serve as a launch point for assessing the severity of Russian aggression in the Arctic.

Maritime law and claims do not begin in the sea, but on land. The first general provision of UNCLOS related to the legal status of territorial seas is "the sovereignty of a coastal State extends, beyond its land territory and internal waters and, in the case of an archipelagic State, its archipelagic waters, to an adjacent belt of sea, described as the territorial sea."[17] Therefore, if a coastal state can extend its maritime claims, it can potentially control, on varying levels, the activities within Russian waters. This principle is key to understanding not only the importance of why maritime claims must be valid, but also the motivations behind a State's campaign for sovereignty within the maritime domain.

A U.S. Marine takes cover after landing in Keflavik, Iceland. Courtesy of NATO.

Russia's Excessive Maritime Claims Violate UNCLOS

As the ice caps melt, the race for Arctic resources is on and Russia isn't wasting time claiming all it can in violation of current maritime boundaries. In 2008, former Russian President Dmitry Medvedev stated "our foremost goal is to transform the Arctic into Russia's resource base in the 21st century. In order to fulfill this task, we should first resolve a number of special issues. The main issue is to ensure and firmly defend Russia's national interests in that region."[18] In 2021, Russia expanded its UN maritime claim to cover nearly 70 percent of the Arctic seabed and reach Canada's and Greenland's exclusive economic zones (EEZ).[19] The claim expands Russia's current ownership by approximately 705,000 square kilometers.[20] While Russia is seeking legal approval from the Commission of the Limits of the Continental Shelf (CLCS), the UN body charged with establishing the limits of coastal state continental shelves, the results of a ruling against Russian interests might have little to no impact on Russian aggression. One need only look to Russia's neighbor, the People's Republic of China (PRC), for an example of an UNCLOS signatory disregarding an international body's determination that is contrary to national interests.

In 2016, the Permanent Court of Arbitration (PCA), an international dispute resolution forum, ruled in favor of a Philippine claim against the PRC regarding the PRC's excessive and expansive maritime claims in the South China Sea.[21] There were fifteen maritime claims and the PCA ruled in favor of the Philippines on almost all of them.[22] As an UNCLOS signatory, the PRC is bound by this ruling. However, following the tribunal's decision, the PRC made no effort to abide by the ruling and has "advanced a new articulation of its maritime claims in the South

China Sea."[23] Generally, the PRC claims the following: its sovereignty over maritime features, i.e. island groups such as the Paracel Islands; proper drawing of straight baselines to encapsulate island groups; nearly the entire South China Sea as its territorial waters; and its "historic right" to the South China Sea.[24] The latter, while a principle on land, has no basis in international maritime law, customary or codified. The U.S. Department of State stated,

> These expansive maritime claims are plainly inconsistent with international law as reflected in the Convention...The overall effect of these maritime claims is that the PRC unlawfully claims sovereignty or some form of exclusive jurisdiction over most of the South China Sea. These claims, especially considering their extensive geographic and substantive scope, gravely undermine the rule of law in the oceans and numerous universally recognized provisions of international law reflected in the Convention.[25]

Russia, ever watchful, has no doubt assessed both the PRC's and international community's reaction to the PCA's decision, especially its limited impact to the status quo of daily life in the South China Sea. Various sovereign states have issued harsh words against the PRC and continued to conduct freedom of navigation operations (FONOP), but this has done arguably little to shift the PRC's agenda. Due to the economic and security concerns of the Arctic, it would behoove Arctic stakeholders to leverage the established frameworks to institute a multinational task force to maintain the status quo and the peaceful and open use of the Arctic.

Nato Forces in Arctic Conditions
Courtesy of NATO.

Russia's Restrictions on the Northern Sea Route Violate the Law of the Sea

There are three primary sea lanes through the Arctic: the Northern Sea Route (NSR) running roughly along the Russian Arctic coast; the Northwest Passage running along the North American Arctic coast; and the Transpolar Sea Route running directly through middle of the Arctic from the tip of Alaska to the southeast of Greenland. While the Transpolar route is limited by ice most of the year, the other two are quickly becoming navigable year around. These routes have two major global impacts: economic and military. The economic impact cannot be understated. Using the Arctic routes, the distance from Northern Europe to China would be about 40% shorter than traveling via the Suez Canal and about 60% shorter than that of the Cape of Good Hope.[26] This translates to a major reduction in fuel, manpower, and transportation costs.[27]

As for understanding Russia's military motivation for securing complete control of the NSR, it is important to briefly review one of the deepest wounds in the side of Mother Russia – its defeat in the Russo-Japanese war.[28] In 1904, conflict arose between Japan and Russia over the ownership of areas of present-day China and Korea. The brutal land and sea conflict led to the deployment of the Russian Baltic Fleet to reinforce the Far East Fleet at Port Arthur. Due to several mishaps during planning, treaties limiting the movement of closer Russian fleets, and an accidental attack on British ships, the Baltic Fleet was forced to take lengthy routes through the Suez Canal and around Cape Hope.[29] The latter route, taken by the larger battleships, was 18,000 miles long and had very few re-supply options.[30] The tired Baltic Fleet arrived nine months later, met Japanese-conquered Port Arthur, and much of the remaining Russian Fleet was decimated soon after.[31] The defeat secured Japanese maritime superiority in the Pacific for decades, and left an indelible scar on Russia, one she never wishes to reopen.

In order to arguably assert dominance over the economic and military NSR goldmine, Russia began mandating non-Russian vessels request passage by providing the vessel name, parameters, crew information, and board a Russian maritime pilot.[32] Russia claims the NSR is within its territorial waters and protecting it is squarely within UNCLOS. It should be noted the UNCLOS Article cited is specifically focused on environmental concerns related to marine pollution.[33] Russia's citation of an UNCLOS article that, on its face, appears applicable to environmental concerns is noteworthy. At a minimum, this seems a misinterpretation of UNCLOS. At a maximum, some might argue this is a violation of international law particularly as it applies to sovereign-immune foreign warships. Further, Russia claims the mandated coordination is necessary for Russian forces to quickly respond to those stranded in need within the Arctic ice.

This is not without merit, and they have indeed saved many vessels in the past.[34] Even if Russia is acting with the safety of others in mind, the international community must act to counter the unilateral Russian restriction on freedom of movement in the NSR.

The total and impediment-free use of the NSR allows Russian assets to reach anywhere in the Northern Hemisphere in a matter of days. Every base will act as an east-to-west maneuver arm and Russia will never again need to take nine months to reach its opposite coast. It will enjoy maritime superiority by virtue of its land mass and position alone. The global impact, especially from a military standpoint, must not be underestimated or ignored. While other countries will continue to need carriers to expand their maritime presence, Russia can act as one massive carrier. With geographic distances obviously playing an important logistic part, the international community cannot deny that Russia's land mass fronting the Arctic is a distributive advantage. Taken in conjunction with the melting ice caps, Russia will soon have an even easier journey across the top of the world to both the Atlantic and the Pacific. This increased access only bolsters the demand for an Arctic-focused task force.

A Cooperative Solution – Task Force: Arctic

"Look at me. Look at me. I am the Captain now" is a quote many know from the film Captain Phillips, which is based on the true story of a 2009 Somali pirate attack on a U.S. cargo ship. In 2008, there were a reported 111 piracy incidents near the coast of Somalia and Gulf of Aden, including 42 hijacked vessels.[35] In response to these attacks, the UN unanimously passed a security resolution establishing Combined Task Force 151 (CTF 151) to "deter, disrupt and suppress piracy."[36] To accomplish its mission, the 30 partner nations focus on "intelligence collection and building pattern-of-life analysis of pirates, and coordination, tactical de-confliction, and synchronization of multinational counter-piracy operations."[37] CTF 151 is not isolated or autonomous, rather it is bolstered by current international constructs.[38] The mission is supported by the European Union (EU) and the North Atlantic Treaty Organization (NATO) along with at least six other international operations.[39]

CTF 151 sits surrounded by these various institutions and focuses on information sharing and de-confliction across disparate groups. Voluntary cooperation and coordination is the key to CTF 151's communication sharing system. Unclassified chat communication systems available through an Internet connection tie together the entirety of merchant vessels, independent naval forces, and task force vessels in transits through pirate infested waters.

CTF 151 is an unequivocal success as there hasn't been a successful piracy incident for four years and, in December 2021, the UN voted to phase out the international mission.[40] CTF 151 is a premier example of mission-focused international cooperation and provides a framework for the same in the Arctic. The establishment of a Task Force: Arctic (TFA) could provide a dedicated and stable pathway for critical information sharing and coordination, and, most importantly, it could be a platform for the "consolidations of international effort free of political mandate or military intent"[41] throughout the Arctic region.

TFA would counter the two cited areas of Russian overreach and misapplication of international law without the need to militarize the region. First, it would provide an international cooperation venue that, as demonstrated by CTF-151, has already shown the ability to solve international problems. TFA would directly address Russia's stated concerns over the safety of vessels afloat in the Arctic region. It would present a capability to encourage and ensure information sharing and coordinate polar rescue. Similar safety constructs exist in polar regions which are particularly prone to dangerous conditions. The Polar Code, for example, is shipping related, specifically addresses safety coordination, and could provide a framework to support TFA.[42] Russia, as a permanent member of the UN Security Council (UNSC), might use its veto power to forever prevent the creation of TFA; however, presenting such an option shows a unified international community and provides Russia an opportunity to either live up to their UNCLOS signatory obligations, or openly defy them and risk continued international scorn.

In the best-case scenario, if TFA made it past the UNSC, a strong and vigilant international presence would likely influence adherence to international laws, standards, rules, and norms in the Arctic maritime environment. Also, TFA's mission could include monitoring and tracking infringements upon international law and increase transparent communication with the international community. TFA could work in close coordination with the International Maritime Community and other Arctic or Artic-interested nations to facilitate and coordinate search and rescue missions.

Even in the worst case where Russia, as a permanent member of the UNSC, vetoes a resolution to establish a TFA, such a resolution still represents significant success. International coordination, negotiation, communication, and consensus must take place among Arctic and Arctic-interested nations to draft a resolution

in support of TFA. This type of work among sovereign nations sends a strong message regarding the importance of international organizations and the rule of law.

TFA would not solve all of the Arctic's geopolitical or national security concerns; however, it could play an important role in supporting a rules-based order in a vulnerable and potentially volatile area. TFA would create a framework aligned with international laws, standards, rules, and norms; an environment that Russia could join and fully take part in along with the rest of the international community. However, such cooperation would be unambiguously contingent on a decisive shift in Russian aggression and international relations, especially in light of Russia's violent invasion of Ukraine in 2022. Russia would then be a welcomed TFA partner and have the opportunity to collaborate with sovereign nations interested in a rules based order. Ultimately, the proposal of a cooperative, multinational task force in the Arctic, such as TFA, would be a concrete step to enable Arctic peace.

DISCLAIMER: Elisabeth Maddrell is a Lieutenant in the U.S. Navy. Tracy Reynolds is a Commander in the U.S. Navy. All views expressed in this article are the participant's own and do not represent the official view of the U.S. government, the Department of Defense, or the Department of the Navy.

1 "The Russian Chairmanship of the Arctic Council Begins Under the Theme 'Responsible Governance for a Sustainable Arctic'" Artic Council, last modified 28 June 2021, https://arctic-council.org/news/russian-chairmanship-begins-under-theme-responsible-governance-for-a-sustainable-arctic/
2 15 U.S.C. § 4111 (1984)
3 "Albedo Effect" Norwegian Polar Institute, https://www.npolar.no.en/fact/albedo, "Albedo is an expression of the ability of surfaces to reflect sunlight (heat from the sun). Light-coloured surfaces return a large part of the sunrays back to the atmosphere (high albedo). Dark surfaces absorb the rays from the sun (low albedo)."
4 "Ground Polygons" Wikipedia. A ground polygon is a geometric shape "found anywhere that freezing and thawing of soil alternate." https://www.wikipedia.org/wiki/Patterned_ground
5 "Hummuck" National Snow & Ice Data Center. A hummock is "a smooth hill of ice that forms on the sea ice surface." https://nsidc.org/cryosphere/glossary/term/hummock
6 ."Frost Boils" Wikipedia. Frost boils are "small circular mounds of fresh soil material formed by frost action." https://www.wikipedia.org/
7 "Pingo" Britannica. A pingo is "a dome-shaped hill formed in a permafrost area when the pressure of freezing groundwater pushes up a layer of frozen ground." .https://www.brittanica.com/science/pingo
8 "Thermokarst" Wikipedia. Thermokarst "is a terrain-type, charaterised by very irregular surfaces of marshy hollows and small hummocks formed as ice-rich permafrost thaws." https://www.wikipedia/ord/wiki/Theraokarst
9 "Arctic Report Card: Update for 2021," National Oceanic and Atmospheric Administration https://www.arctic.noaa.gov/Report-Card/Report-Card-2021
10 "Arctic People," Arctic Council, https://arctic-council.org/explore/topics/arctic-peoples
11 "The Sami," Northern Norway, https://nordnorge.com/en/tema/the-sami-are-the-indigenous-people-of-the-north
12 "Arctic Region," U.S. Department of State, https://www.state.gov/key-topics-office-of-ocean-and-polar-affairs/arctic/
13 Id.
14 United Nations Convention on the Law of the Sea "UNCLOS." https://www.unclos.org/
15 Id.
16 The Commander's Handbook on the Law of Naval Operations, August 2017
17 "UNCLOS," United Nations Convention on the Law of the Sea, https://www.unclos.org/
18 Kennedy Cameron, "Examining the Russian Federations Claim to Extend Their Exclusive," last modified, May 6 2020, https://jsis.washington.edu/news/examining-the-russian-federations-claim-to-extend-their-exclusive-economic-zone-within-the-arctic/
19 "Partial Revised Submission by the Russian Federation," Commission on the Limits of the Continental Shelf, last modified August 3, 2021, https://www.un.org/depts/los/clcs_new/submissions_rus.rev1.htm
20 Martin Breum, "Russia Extends its Claim to the Arctic Ocean Seabed," April 4 2021, https://arctictoday.com/russia-extends-its-claim-to-the-arctic-ocean-seabed
21 "The South China Sea Arbitration," Permanent Court of Arbitration, July 12, 2016, https://docs.pca-cpa.org/2016/07.PH-CN-20160712-Press-Release-No-11-English.pdf
22 Id.
23 "Limits in the Seas No. 150," U.S. Dept. of State. January 2022, https://state.gov/wp-content/uploads/2022/01/LIS150-SCS.pdf
24 Id.
25 Id.
26 "Northern Sea Route: The Shortcut Between Asia and Europe," Arctic Bulk, www.arcticbulk.com/article/186/NORTHERN_SEA_ROUTE
27 Id.
28 Christopher Hoitash, "The Bear Steams East: the Amazing Journey of the Russian Baltic Fleet to the Pacific," War History Online, July 14, 2018, https://www.warhistoryonline.com/history/bear-steam-east-russian-fleet.html
29 Id.
30 Id.
31 Id.
32 "Russia Imposes Foreign Sailing Restrictions on Northern Sea Route," Warsaw Institute, 08 March 2019, https://warsawinstitute.org/russia-imposes-foreign-sailing-restrictions-northern-sea-route/
33 UNCLOS, Article 134
34 "Russia Sends Icebreaker to Rescue Ships Stranded in Arctic," N World, November 23, 2021, www.thenationalnews.com/world/2021/11/23/russia-sends-nuclear-powered-icebreakers-to-rescue-at-least-18-ships-stranded-in-the-arctic.
35 International Chamber of Commerce. "Pirate Attacks off Somalia Already Surpasses 2008 Figures." https://www.icc-ccs.org/index.php/33
36 "CTF 151: Counter-Piracy" Combined Maritime Forces. Last modified 18 November 2021. https://combindedmartimeforces.com/ctf-151-counter-piracy/?amp
37 Tracy Reynolds, "Counter-Piracy as a Model for an Arctic Task Force: An Opportunity for International Cooperation," 6 March 2016, https://www.fletchersecurity.org/the-arctic-spotlight-web-exclusive
38 Reynolds, "Counter-Piracy."
39 Id.
40 The Maritime Executive. "U.N. Security Council Explores Ending Somalia Anti-Piracy Resolution," last modified December 10, 2021. https://www.maritime-executive.com/article/u-n-security-council-exlore
41 Reynolds, "Counter-Piracy."
42 International Maritime Organization. "Shipping in Polar Waters" https://www.imo.org/en/MediaCentre/HotTopics/Pages/Polar-default.aspx

THE NATO SUPPORTED – SUPPORTING RELATIONSHIP CONCEPT

CDR (RNoN) PER CHRISTIAN GUNDERSEN

"...two key truths of Command and Control. First, when C2 is working properly you don't even notice, but everyone immediately knows if it's bad. Second, it's wicked hard![1]" - *Lt Gen Thomas J. Sharpy (USAF ret.)*

NATO Command and Control

Command and control (C2) is a key *Joint Function*[2] of military operations, closely related to the more civilian expression *Leadership and Management*. NATO defines C2 as "The authority, responsibilities, and activities of military commanders in the direction and coordination of military forces and in the implementation of orders related to the execution of operations."[3] Simply put, it tells us who has the formal authority to do what with whom. C2 touches on many aspects of military activity. The topic is extensive, complex, and contentious. Not surprisingly, C2 is a central theme during the planning and execution of NATO operations at all levels.

From Cold War to Coalition Operations

In the 1950s, NATO established a set of standard command terms to describe the authority and limitations of command relationships from *Full Command to Tactical Control* that have changed very little since then.[4] Over the same period, NATO has changed significantly. The fixed command structure of the Cold War, consisting of 33 headquarters in the late 1980s[5], has been reduced to 11.[6] Furthermore, the introduction of *Out of Area Operations and Coalition Operations* during the 1990s revealed discrepancies in how allied and partner nations understood NATO's C2 doctrine. Critical questions, like who has the authority to do what, when, where, and with whom, drove challenging discussions within the alliance from the political strategic level in the allied capitals to the tactical level on the ground. Examining the early years of the KFOR operation from 1999 and ISAF 2001-2014, most would agree NATO struggled with C2. Bluntly put, there was a lack of *Unity of Command*.[7] In KFOR, "the NATO commander lacked the necessary leverage and control, so nations reserved the right to dictate how, where, and when their contributing forces would be employed and deployed."[8] With ISAF, multilateral cooperation was neither straightforward nor guaranteed. Participating countries differed significantly in what they were willing to do and how and where they were willing to do operations. Some nations refused to participate in dangerous or offensive combat missions, while others changed tactical objectives with each new commander.[9] Lacking Unity of Command, and in the face of increasingly complex C2 relationships during coalition operations, NATO adopted the *Supported-Supporting Relationship Concept* more than a decade ago. The aim was to establish a more flexible arrangement to enable cooperation and coordination across the *Chain of Command*[10] during allied operations. Although the concept is not entirely new, this article aims to describe the NATO *Supported-Supporting Relationship Concept* and discuss the advantages and challenges associated with this concept. Arguably, there is a requirement for some clarification, even if the concept has been utilized on several occasions in the Alliance already.

NATO 1957 Summit. Courtesy of NATO.

The Supported-Supporting Relationship Concept

The NATO Supported-Supporting Relationship Concept is not a command relationship; nevertheless, it complements NATO C2. The concept facilitates mutual reinforcement and enables close coordination between different commanders and forces across the command structure, often limited in time, space, force size, and scope. The relationship is typically established when subordinating one unit to another would be undesirable, inappropriate, or impractical. The aim is to maintain flexibility and focus, creating *Unity of Effort*[11] and complementing each other by coordinating the overall means required throughout a campaign or operation. Higher Command designates subordinate commanders as Supported or Supporting Commanders and, in principle, several Supported Commanders may exist simultaneously. Mainly described in NATO's Joint Doctrine, this concept is primarily intended to be used at the operational level but may also be applied at the tactical level. However, it must be noted that even though some similarities exist, the concept is not interchangeable with tactical support, such as the *Direct and Indirect Support* within allied armies or the Support Situations within allied navies.[12]

As described in NATO doctrine, Supported Commanders have authority and are accountable for achieving the objectives of a phase, warfare function, mission, or task. In a specific geographic area, Supported Commanders may have overall responsibility for planning and execution of a mission. This includes specifying and incorporating the support required from designated Supporting Commands.

Multinational Operations. Courtesy of NATO.

The Concept Applied During Phasing

Typically, a campaign or operation is divided into phases and sub-phases, arranged to ensure *Unity of Effort* and clarify priorities across the force at any specific time. For NATO, the *Supported-Supporting Relationship Concept* is viewed as "an effective means of weighting the phases and sub-phases."[13] As the main effort is likely to change across different phases, the concept enables the Force Commander to synchronize activities, ensuring that the entire force remains focused and flexible throughout the mission. For example, if the main effort is the redeployment of forces, it could be appropriate to designate the Commander of the Joint Logistic Support Group as the Supported Commander during this specific phase of the campaign.[14] Doctrinally, this Commander is responsible to the Force Commander for coordination and execution of operational-level logistic support using assigned national, host nation, and/or commercial resources. The Joint Logistics Support Group, in this case, is best suited to coordinate logistic resources and networks across the Joint Operations Area, regardless of the level of control specified in a redeployment phase.

A Functional Approach

With a functional application of the concept within a joint force, Component Commanders may receive and provide support for different missions, functions, or operations simultaneously. As described in the U.S. Joint Publication 3.0, within a Joint Force, a Special Operations Component Commander may be supported for a direct-action mission while simultaneously supporting a Land Component Commander for a raid. Similarly, a Maritime Component Commander may be supported for a sea control mission while simultaneously supporting an Air Component Commander to achieve air control throughout the operations area.[15]

A Geographical Application

Regarding a geographical allocation of the concept, Force Commanders are usually the Supported Commanders synchronizing maneuver with information, intelligence, fires, protection, sustainment, and supporting activities within their designated Area of Operations (AO). To facilitate this integration and synchronization, they have the authority to designate target priority, effects, and timing of fires within their Areas of Operations.[16] An example could be a Land Component Commander designated as the Supported Commander for all operations within a designed land

area and a Maritime Component Commander for all operations within a designated ocean area. At the same time, both commanders could simultaneously be supporting commands for each other across their respective boundaries.

Trust and Close Cooperation

An effective Supported-Supporting relationship is based on mutual trust, respect, and close dialog between the Commanders and their staffs, ensuring that the Supported Commander gains a clear understanding of the overall support the Supporting Commander will be providing within means and capabilities. A practical solution for ensuring close cooperation and information sharing is detailing liaison officers (LNOs) across the commands, especially from supporting to supported command staffs. The importance of assigning LNOs is by no means a new thought. However, in reference to the Supported-Supporting Relationship Concept, they translate requirements, communicate capabilities and find solutions to ensure Supported Commander expectations are met.

Advantages and Opportunities

Even if some of the advantages have already been mentioned above, it is important to acknowledge flexibility as the principal advantage of this concept. During a phased operation, if the main effort and objectives change, (e.g., from a shaping operations phase to an offensive operations phase) the Supported and Supporting Commanders may also change. The concept enables forces to offer and receive support across the chain of command, usually without delay.

Mission Command[17] is the default leadership philosophy in NATO. As described by NATO Doctrine, "A commander's responsibility for mission accomplishment is total, but delegation of authority to subordinates and their responsibility to act in support of the Higher Commander's intentions are included in the principle of decentralization."[18] Mission Command provides Subordinate Commanders freedom of action to execute operations according to the Commander's intent. Furthermore, it encourages initiative through decentralized decision-making. Mutual trust between the command levels is key. The same can be said for the Supported-Supporting Relationship Concept. In principle, it is about delegating authority and responsibilities to subordinate commands, providing a convenient and flexible tool between the command levels and across the chain of command. However, it is worth mentioning that even if the concept is not a command relationship, Higher Command may have to intervene to provide orders and adjustments as required. One can imagine any number of situations where subordinate commands disagree on priorities which require intervention or adjudication, especially when there are gaps between support required and support offered.

Utilizing the Supported-Supporting Relationship Concept may open opportunities for closer integration between different national forces and services by focusing on possibilities more than limitations. During recent NATO operations, numerous allied nations have provided forces to NATO operations with national limitations, often called caveats. This became especially apparent during the ISAF years, but was also documented during NATO operations in Bosnia, Kosovo,[19] and later in Libya.[20] In 2006, U.S. General James L. Jones, Supreme Allied Commander Europe, reported 102 national caveats, about 50 of which he deemed as operationally significant.[21] The problems associated with nationally imposed caveats have been addressed at several NATO summits but, due to domestic political considerations, the challenges are likely to remain in the future. As Per Marius Frost-Nielsen argues, "many governments have found themselves between a rock and a hard place – between external pressure for supporting allies and domestic skepticism about what the external pressure demands and exactly how to respond to it."[22] In order to mitigate this challenge, the Supported-Supporting Relationship Concept may stimulate commanders and their planners to find practical solutions to those caveats imposed by nations prior to the employment of forces. It is also worth mentioning that without the ability to impose national caveats, some allies would be unable or reluctant to participate in NATO operations due to domestic policies or political sensitivities.[23]

Challenges and Vulnerabilities

There are some challenges and vulnerabilities associated with the concept. Since the relationship does not define the C2 structure, it may become elusive, hollow, and used to avoid sensitive and challenging discussions. It may become an easy way for the Alliance to avoid deciding on difficult matters related to C2, especially when it comes to multinational and service-specific questions. When offering forces to NATO operations, formal authority questions may represent a sensitive domestic political subject that is not easy to resolve. Relying on the Supported-Supporting Relationship Concept to mitigate this issue may be

wishful thinking and leave the Joint Force Commander with a false sense of capabilities available.

A supporting force may be deployed with separate national missions, objectives, and agendas, in addition to those specified in the allied operations plans and orders. Usually, available resources and capabilities are limited and, for a Supporting Commander, it may be regarded as contradictory to offer wholehearted support to a Supported Commander with other missions, objectives, and priorities. In the case where commanders are both simultaneously supported and supporting, there is the very real risk that these functions could turn into a counterproductive competition. Everyone desires support, but some may be reluctant, or entirely unable, to return substantial support at the same time. Furthermore, it may become challenging to plan, synchronize, and prioritize all the activities across the joint force in time and space with limited forces available. To avoid unnecessary friction, simplicity is considered a fundamental principle of war. "The more complex the plan, the more there is to go wrong, but simplicity is not an excuse for plans that lack the coordinating detail necessary to make them work. Clear direction and a thorough understanding of the Commander's intent simplify planning and conduct of operations."[24] Usually, Higher Command will try to visualize Supported-Supporting Relationships in a matrix displaying how different commanders are both supported and supporting in specific areas. For example, if a Joint Force Air Component Command is the Supported Commander for offensive air operations while simultaneously supporting a wide range of other supporting missions, prioritization may become a challenge and increase the risk to the overall mission. If everything is prioritized, nothing is prioritized.

Al Udeid - HQs for US CENTCOM and USAFCC in Qatar. Courtesy of U.S. CENTCOM.

A sufficient level of interoperability is often a prerequisite for employing the Supported-Supporting Relationship Concept, especially if the concept is applied at the tactical level. Tactical "plug and play" is paramount to efficient cooperation and coordination. Aspects such as standard procedures, training, doctrine, and equipment may decide how efficient a Supported-Supporting Relationship may become. Usually, the Joint Force Air Component Commander will be designated as the Supported Commander for strategic attack, air interdiction, personnel recovery, and airborne intelligence, surveillance, and reconnaissance.[25] In these rather complex joint air operations, it is essential that designated Supporting Commanders have a sufficient level of interoperability to effectively conduct close coordination, prevent friendly fire incidents, and de-conflict airspace activities.

It could be argued that the concept's effectiveness relies too much on goodwill efforts and personal relations between the Supported and Supporting Commanders. As personalities come into play, it could become tempting to find reasons to delay support if a positive working relationship with the Supported Commander was absent. In some ways, the concept relies on a proverbial gentleman's agreement between nations and services. The U.S. Marine General Anthony C. Zinni, known as the "Warrior Diplomat," experienced this firsthand in 1991 as the Multinational Force Commander during Operation Provide Comfort in Northern Iraq. Challenged with nationally imposed caveats, he introduced something he called Hand-Shake Con: "Some guy comes in; is a senior commander; is a national commander; he brings with him his forces. His forces are passed to you to use in a way that he agrees upon. We sit down quietly and engage in a little discussion as how we might use those forces, what kinds of missions, tasks, positions on the ground we can give them. And through a consultative, handshake process they agree to do it."[26] This informal, personal, commander to commander approach is always valuable. However, General Zinni's pragmatic method may become unmanageable and unpredictable in time, especially when a Supporting Commander is limited by domestic policies.

Conclusion

The Supported-Supporting Relationship Concept was established to meet new challenges experienced during NATO-led operations after the Cold War and to mitigate

the somewhat rigid C2 structures and terminology. The concept creates flexibility and enables combined joint cooperation across the chain of command. It promotes decentralized decision-making and is a valuable tool for Higher Command when applying Mission Command across the force. It could also be a means to clarify roles and find optimal solutions to nationally imposed caveats.

However, there are several challenges and vulnerabilities with the concept. Since it is not a command relationship, it may become elusive and unpredictable. For several reasons, Supporting Commanders may be reluctant to provide the support required or it may be overly dependent on personal relationships between commanders. The concept is also dependent on a sufficient level of interoperability within the joint force. It may also become too complex if there are Commanders simultaneously designated as both Supported and Supporting. Nevertheless, it is possible to mitigate these challenges and vulnerabilities by applying the concept transparently and plainly. In addition, establishing good working relations and mutual trust are key. Overall, the Supported-Supporting Relationship Concept has enhanced NATO's ability to plan and conduct multinational coalition operations and has proven a valuable complement to NATO's C2 doctrine and terminology.

1 Sharpy, Thomas J, Deputy Chief of Staff, Capability Development NATO SACT, "Multi-Domain Operations: The Future of Warfare", 16. Jul. 2020, p. 3.
2 NATO AJP-1 describes Joint Functions as a framework that provides the commander and staff a means to visualize the activities of the force and to ensure all aspects of the operation are addressed. They are a point of reference, as well as a description of the capabilities of the force. The joint functions are maneuver, fires, command and control, intelligence, information activities, sustainment, force protection, and civil-military cooperation.
3 NATO Command, Control, and Consultation Board (NC3B), AAP-31(Edition 3), NATO Glossary of Communication and Information Systems Terms and Definitions, 2005.
4 The NATO Command terminology and definitions are described in NATO, AJP-3, "Allied Joint Doctrine for the Conduct of Operations," Edition C Version 1, Feb. 2019, Fundamentals p. 1.78.
5 NATO, "The NATO Command Structure," Feb. 2018, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-Factsheet-NATO-Command-Structure_en.pdf, retrieved from internet 7. Jan. 2022.
6 NATO has three tiers of command: two strategic commands with Allied Command Transformation in Norfolk and Allied Command Operations in Mons, three operational commands with Joint Forces Command Naples, Brunssum and Norfolk, and three tactical level commands Allied Air Command in Germany; Allied Land Command in Turkey and Allied Maritime Command in the United Kingdom. Other commands include Naval Striking and Support Forces NATO in Portugal; NATO Communication and Information System Group in Belgium, and the Joint Support and Enabling Command in Germany.
7 NATO describes Unity of Command in AJP 1, para. 5.8: "A fundamental tenet of C2 is unity of command, which provides the necessary cohesion for planning and executing operations. Command relationships, by which commanders achieve this authority, will be determined when a joint force is established."
8 U.S. DoD Command and Control Research Program, "Lessons from Kosovo: The KFOR Experience," Jul. 2002, p. 402.
9 Auerswald, David P. and Stephen M. Saideman, "NATO in Afghanistan: Fighting Together, Fighting Alone," Princeton, NJ: Princeton University Press, 2014.
10 NATO describes Chain of Command in AJP 1:"The C2 structure is hierarchical and should be defined and understood by all levels of command. A clear chain of command strengthens integration between components".
11 Unity of effort is described in NATO AJP 1, para 1.34: "Unity of effort emphasizes the requirement to ensure all means are directed to a common goal. Military forces achieve this principally through unity of command."
12 NATO's tactical support terminology is described more thoroughly in AJP 3.1, AJP 3.2, and AJP 3.3 (NATO Restricted) for respectively Maritime Operations, Land Operations, and Air & Space Operations.
13 NATO, AJP-3, "Allied Joint Doctrine for the Conduct of Operations," Edition C Version 1, Feb. 2019, para. 1.80.
14 NATO, AJP-4, "Allied Joint Doctrine for Logistics", Edition B Version 1, Dec. 2018.
15 U.S. JP 3.0, "Joint Operations," 17. Jan. 2017, Incorporating Change 1, 22. Oct. 2018, p. III-5.
16 Ibid, p. III-6.
17 NATO describes Mission Command in AJP 1: "Mission command gives subordinate commanders' freedom of action to execute operations according to the commander's intent. It encourages initiative and decentralized decisionmaking."
18 NATO, AJP-3, "Allied Joint Doctrine for the Conduct of Operations," Edition C Version 1, Feb. 2019, para. 1.73
19 Kingsley, Regeena, "Fighting against allies : an examination of "national caveats" within the NATO-led International Security Assistance Force (ISAF) campaign in Afghanistan & their impact on ISAF operational effectiveness, 2002-2012,"2014, https://mro.massey.ac.nz/handle/10179/6984, retrieved from internet 11. Feb. 2022.
20 Erlanger, Steven, "Libya's Dark Lesson for NATO," Atlantic Council, 5. Sep 2011, https://www.atlanticcouncil.org/blogs/natosource/libya-s-dark-lesson-for-nato/, retrieved from internet 11. Feb. 2022.
21 Saltasuk, Johnathon, "NATO and the Afghanistan Mission: Lessons for the Alliance," master's Thesis submitted to the graduate faculty at the University of Manitoba, 2012, p. 49.
22 Frost-Nielsen, Per Marius, "Conditional commitments: Why states use caveats to reserve their efforts in military coalition operations," Contemporary Security Policy, 38:3, 2017, p. 371-397.
23 Ibid.
24 NATO, AJP-3, "Allied Joint Doctrine for the Conduct of Operations," Edition C Version 1, Feb. 2019, para. 1.21 k
25 U.S. Joint Publication 3.0, Joint Operations, p. III-8, 17 January 2017, Incorporating Change 1, 22 October.
26 Zinni, Anthony C., USMC General, "Non-Traditional Military Missions: Their Nature, and the Need for Cultural Awareness and Flexible Thinking," Perspectives on Warfighting. No. 6- 1998, Quantico, VA: Marine Corps University, 1998, p. 265-266.

RESOURCE SCARCITY AND CLIMATE CHANGE

CDR (ESP-N) CARLOS CARBALLEIRA

"Global warming is making the world more dangerous. It has a serious impact on our security" – NATO Secretary General Jens Stoltenberg

Resource scarcity and conflict are issues embedded in our social behaviour. Although some scholars argue and defend that the scarcity of resources can be an enhancer for cooperation and technological development, the experiences accumulated over centuries is that scarcity of resources predominantly results in conflict.[1]

According to data from the United Nations, the world population has grown from 2.5 billion in 1950 to almost 8 billion in 2020; current forecasts estimate that, in 2050, the population could reach 10 billion. As a corollary to the population increase, the demand for more energy, goods, water, and food has increased significantly in developed and developing nations.[2] The emergence of new economies such as China implies a higher standard of living for a much greater number of citizens and, therefore, a greater need for these resources.[3]

As the standard of living increases in various countries, so too does the pressure on governments to guarantee necessary resources to populations. This demand adds to the challenges of climate change that stems from increasingly industrialized societies with expanding carbon dioxide emissions.

There are any number of aspects to consider when discussing resource scarcity and climate change; however, this article will focus on two elements that arguably account for the greatest impact globally. First, it will look at the dependency on fossil fuels and will discuss the implications of the apparent need to adopt new technologies for alternative energy sources. Second, it will consider the impact of decreasing water resources in some key areas of the world as a consequence of global warming.

Future Challenges for Natural Resources and New Energy Models

With an emphasis on climate change and natural resources, the 2015 Paris Agreement was a milestone at the global level. It promised to fight against climate change, specifically by reducing harmful emissions.[4] As a result, a significant number of countries, especially developed countries, have increased and accelerated their plans to adopt new energy models independent of fossil fuels. These efforts are not without obstacles and, in some cases, even a sense of irony in their endeavours to make the world a better place. The use of new forms of energy that respect the environment such as wind power, solar photovoltaic, green nitrogen, nuclear power plants, storage technologies, etc., have driven a substantial increase in the demand for certain minerals. The construction of solar panels, wind generators or batteries for electronic vehicles requires greater mineral consumption when compared to their equivalents that produce the same energy power using technology based on fossil fuels. The production of an electric vehicle requires four times more minerals than its conventional equivalent. Onshore wind plants require nine times more mineral resources than similarly sized gas-fired power plants. With significant weight concerns when creating these products, some minerals, such as aluminum or copper, will be increasingly mined and processed as essential elements in energy production and transport systems.[5] In addition to aluminum and copper, minerals such as lead, lithium, manganese, nickel, silver, steel and zinc are also achieving greater importance in the world market.[6]

Beyond simply the minerals that are gaining prominence in new production models, energy storage and transport, the additional necessity of "rare earth metals" presents new factors to consider. These rare earth elements, all metallic, have excellent conductivity, heat resistance and magnetic properties that make them the most suitable for civil and military electronic components.[7] Although the name "rare earth metals" may give the impression that these are rare elements in nature, they are not as scarce as gold or other precious metals. However, the extraction, processing and refining processes of rare earth metals often have high costs and negative environmental impacts. These costs and environmental issues are why many countries with significant deposits have opted to import instead of exploit locally. Thus, China has positioned itself as the largest global producer,

accounting for roughly 90% of these metals. China's production and relative lack of concern on the impact to its citizens has put it in a privileged position, resulting in Beijing enjoying significantly greater influence worldwide.[8]

Although renewable energies have driven a reduction in coal consumption in the EU, USA and Canada, an unfortunate increase in natural gas consumption accounts for a portion of the decrease in coal use as well. Air and maritime transportation will continue to depend on oil to meet their energy needs until another feasible non-fossil source emerges. Biofuels, hydrogen, ammonia and synthetic carbon-based fuels are some of the options that are being considered as possible alternatives to contribute to the fight against climate change.[9] However, even the most optimistic studies predict that the weight of fossil fuels in energy generation and transportation will continue to play a significant role in the economies of developed and developing countries for at least the next two decades.[10]

Still, finite reserves of fossil fuels are driving the alternative fuel race beyond environmental impact concerns. According to a recent study conducted by BP, today's level of extraction and production rates would exhaust current and estimated proved reserves as follows: coal - year 2169; natural gas - year 2068; and crude oil - year 2066. However, it is worth pointing out that the impact of climate change in the Arctic and the possibility of discovering new reserves would affect these estimates.

The Artic: New Opportunities Or New Fault Line?

Although the Arctic has always been a changing region in terms of its physical environment, climate change is affecting it more significantly than other parts of the globe.[11] As a result of the latest research carried out, the United States Geological Survey estimates that over 87% of the Arctic's oil and natural gas resources (about 360 billion barrels of oil equivalent) are located in the Arctic basin. In addition to oil and gas, the region contains other abundant mineral resources like coal, iron, ferroalloy minerals, several non-ferrous minerals, industrial minerals and rare earth materials. Currently, many known reserves are not accessible, and others are yet to be discovered.

The Arctic's abundance of resources represents an enormous potential economic value to Arctic states and therefore has attracted the interest of powerful countries outside the region. In January 2018, China published its first strategy on the Arctic, called "China's Arctic Policy." In this document, China proclaims itself a 'Near Arctic State', stating, "the Arctic is gaining global significance for its rising strategic, economic values and those relating to scientific research, environmental protection, sea passages, and natural resources." The document also describes China's key objectives in the Arctic: establishing the use of new shipping routes and obtaining physical resources. Both of these objectives are linked to the 'One Belt, One Road' initiative. With the so-called 'Polar Silk Road', China is planning a range of Arctic infrastructure activities to include ports, undersea cables, and airports.[12] Obviously, this poses a challenge and is a potential source of conflict between states that have more legitimate claims to the region and those who would wish to exploit it.

Smoke stacks emitting carbon pollution into the sky causing climate change. Courtesy of Shutterstock.

Regardless of the efforts of China, currently the most significant factor regarding the Arctic, from a NATO perspective, are Russia's economic interests. According to recent studies, Russia bases its economy on exploiting and exporting mineral resources and hydrocarbons. Specifically, 25% of its GNP comes from exploiting natural gas and oil. Moreover, Russia obtains 90% of its gas production and 10% of its oil from the Arctic and sub-Arctic regions.[13] Russian investments in this area have been progressively increasing in recent years, indicating that this trend will continue in the short and medium term. In early 2020, Russia signed two documents that clearly reflect the importance of the Arctic from both an economic and security perspective: the "Strategy of Development of the Arctic Zone of the Russian Federation and the Provision of National Security for the Period to 2035," and the "Arctic Strategy". This essential dependence of the Russian economy on fossil resources is in apparent conflict with the urgent environmental policies adopted recently by many countries, especially those who are most developed. Independence from fossil fuels would significantly affect the always precarious world energy balance and subsequently severely impact Russia's economic interests.

From both an economic and a security perspective, it is notable that five NATO members (Canada, Denmark, Iceland, Norway, and the United States) and two closely allied nations (Finland and Sweden) all have Arctic territory that shares borders with Russia. And now with the increasing involvement of China in the region, the Alliance has become more focused on the Arctic. However, there is currently no specific Arctic policy in the Alliance that would cooperatively address the new challenges in this geostrategic space.

North Africa and Water Scarcity

The impact of climate change on the availability of essential primary resources for the development and subsistence of certain societies takes on special significance when we talk about water. As reflected in the 2020 UN report 'Water and Climate Change', the increase in the frequency and intensity of adverse phenomena will have significant consequences for water resources. Heatwaves, heavy rainfalls, thunderstorms, droughts and storm surges are all examples of climate phenomena that will have a negative impact on water resources. As a result, water-scarce regions will see their current situations aggravated and water-abundant areas will begin to suffer from progressive scarcity.[14]

Resources have always been subject to tensions between competing regions. Water has the potential to play a pivotal role in these tensions as an essential element for civilization including domestic consumption, agriculture and industrial processes. According to data published by the UN in 2021, worldwide agriculture consumes 72% of all water withdrawals, municipalities for households and services consume 16%, and industries consume 12%.[15] According to the same report, North Africa and the regions of West Asia are currently the areas of the planet where there is a greater scarcity of this essential resource. Given their proximity to southern Europe and the Strait of Gibraltar, North Africa (specifically Morocco, Algeria, and Tunisia) represents a significant area of interest for the Alliance, especially when we consider the effects on people and the potential for forced migration. According to the UN study, water scarcity stress levels in Morocco and Tunisia are assessed as medium-high, while Algeria is considered critical. These statistics are examples of why global warming due to climate change will significantly influence regions.

Although there is no outright consensus that the lack of water is the direct cause of internal or transnational population migration, it is clear that the scarcity of water is a contributing factor.[16] Beyond the migration of people, water scarcity could significantly destabilize the delicate social, economic, and political balance of these countries, especially Algeria and Tunisia. The possibility that actors such as China and Russia could take advantage of this circumstance to increase their presence and influence in this region can also not be ruled out.

Harmful emissions causing global warming. Courtesy of Shutterstock.

Conclusion

Climate change constitutes an element of significant concern in the complex and sometimes disputed struggle to obtain the necessary resources for development and prosperity. As the top leaders of the Alliance have unanimously stated in their last summit in June 2021, climate change is a 'threat multiplier'. Although it is difficult to predict or define the potential consequences for the collective and individual security of its member states, it is agreed that there will be diplomatic, security, economic and social impacts.[17] And although members have taken actions in recent years aimed at reducing the carbon footprint of their military operations, this alone is not enough to win the fight against climate change. As a clear threat to the security interests of allied nations, climate change must be considered an essential element in all government decision and planning processes. In particular, the impact on resource availability is a fundamental consideration.

The steady increase in populations and their living standards will demand greater availability and volume of natural resources to support ever-increasing energy demands and minerals for industrial processes. Climate change has driven the need to reduce emissions. New, less polluting, or zero contaminating energy systems are still in development and will require time and investment before they are widely available. Fossil fuels, particularly natural gas, will continue to be one of the primary energy resources in the short and medium-term. It will continue to represent a key element in the world energy market and, therefore, in the power struggle for its exploitation and export. Likewise, the dependence on rare earth materials makes new technologies vulnerable to supply chain uncertainties. In particular, China's commanding share of the global supply of rare earth metals represents a significant risk to the future supply of new technology for NATO nations. The Alliance should carry out a thorough analysis of the vulnerabilities and possible mitigation measures to reduce this critical dependency.

The Arctic is perhaps one of the areas of the planet where the effects of climate change are becoming most evident. Host to a vast quantity of untapped natural resources, it is a region ripe for exploitation and possibly conflict. Further complicating tensions, melting polar ice has opened new navigation routes accessible by non-

Arctic nations with interests in the region. It represents a space of vital importance to Russia from an economic and security perspective. One can expect Russia's position and military presence in this region will be increasingly firm in order to continue to exploit Arctic resources to support its economy. However, as many European countries seek new technologies to reduce reliance on fossil fuels, Russia risks losing its economic advantage, potentially causing greater strife amongst its people. China's significant interests in the Arctic, both in obtaining resources and the use of new shipping routes are also of concern. It is expected that China's desire for a more significant presence and influence in this region will only increase in the coming years, undoubtedly resulting in further complexities to assuring peace and security in the north. The lack of a unified political position within the Alliance and, specifically, the absence of an agreed-upon strategy for the Arctic, places it at a disadvantage compared to Russia and China, which already have their own strategies. This lack of a synchronized and consistent plan represents a limitation for NATO. It must face the challenges that this new geostrategic space will demand in the coming years.

On NATO's southern flank, Morocco, Algeria, and Tunisia will experience significant impacts from climate change. As dependence on agricultural exports to Europe decline, new economic models could evolve based on an increase in Chinese and Russian influence in the region. Additionally, progressive desertification due to climate change could exacerbate the current migratory movements towards Europe, which have been increasing steadily in recent years.

Recommendations

Noting that there seems to be political consensus in the Alliance to include climate change as an essential element in decision and planning processes, three areas should be addressed as a matter of priority.

First, the Alliance should take the necessary measures to eliminate or reduce China's current near monopoly on those minerals most needed for new technology development. New energy models and electronic components essential to collective security rely on minerals currently obtained from China. To ensure future supply chain resilience, nations must promote extraction and processing by member states with abundant mineral resources of this kind.

Second, NATO must develop a robust Arctic strategy. Russia and China already have Arctic strategies in place and NATO must adopt a cohesive plan in order to compete in this harsh and highly complex environment.

Finally, NATO must strengthen diplomatic relations and civil-military collaborations with countries in North Africa where water scarcity is likely to attract the opportunistic influence of Russia and China. Likewise, NATO should commission an in-depth study and assessment of the possible options to mitigate increased migratory flows from this region to Europe. In order to avert conflict in the medium term, the Alliance must take the time now to address recognized future problems, like resource scarcity and climate change.

Spanish Navy ship 'Hesperides' sailing near Antarctica. Courtesy of Spanish Navy.

1 Marcelle C. Dawson, Christopher Rosin and Navé Wald, JUL 19. Global Resource Scarcity Catalyst for Conflict or Cooperation?, Routledge, NY, USA. Downloaded SEP 21. https://www.routledge.com/Global-Resource-Scarcity-Catalyst-for-Conflict-or-Cooperation/Dawson-Rosin-Wald/p/book/9780367376925/

2 In 2019 United Nations published in its Global Resources Outlook that, from 1970 to 2017, the annual global extraction of materials grew from 27.1 billion tons to 92.1 billion tons (average annual growth of 2.6 percent). The global average of material demand per capita grew from 7.4 tons in 1970 to 12.2 tons per capita in 2017.

3 Worldbank. OCT 2021. The World Bank in China, Washington, USA. Downloaded SEP 21. https://www.worldbank.org/en/country/china/overview#1/

4 https://www.un.org/en/climatechange/paris-agreement

5 IEA (2021). The Role of Critical Minerals in Clean Energy Transitions. World Energy Outlook Special Report, Paris, France. Downloaded SEP 21. https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions/

6 https://www.worldbank.org/en/news/press-release/2017/07/18/clean-energy-transition-will-increase-demand-for-minerals-says-new-world-bank-report

7 https://www.britannica.com/science/rare-earth-element. Downloaded SEP 21

8 Russell Parman, U.S. Army Aviation and Missile Command (2019). An elemental issue U.S. Army. Download OCT 21. https://www.army.mil/article/227715/an_elemental_issue/

9 Englert, Dominik; Losos, Andrew; Raucci, Carlo; Smith, Tristan (2021). Volume 1: The Potential of Zero-Carbon Bunker Fuels in Developing Countries. World Bank, Washington. USA. Downloaded SEP 21. https://openknowledge.worldbank.org/handle/10986/35435/

10 Scott Foster and David Elzinga (2021). The Role of Fossil Fuels in a Sustainable Energy System, UN Chronicle. Downloaded SEP 21. https://www.un.org/en/chronicle/article/role-fossil-fuels-sustainable-energy-system/

11 U.S. DoD (2019). Artic Strategy. Washington, U.S.. Downloaded OCT 21 https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF/

12 U.S. DoD (2019). Report to Congress Department of Defense Arctic Strategy, Washington, USA. Downloaded OCT 21. https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF/

13 https://www.thearcticinstitute.org/countries/russia/. Downloaded FEB 22.

14 UN-Water (2020). United Nations World Water Development Report 2020: Water and Climate Change, Paris, France. Downloaded OCT 21. https://www.unwater.org/publication_categories/world-water-development-report/

15 UN-Water (2021). Summary Progress Update 2021 – SDG 6 – water and sanitation for all. Version: July 2021. Geneva, Switzerland. Downloaded OCT 21. https://www.unwater.org/publications/summary-progress-update-2021-sdg-6-water-and-sanitation-for-all/

16 Edoardo Borgomeo, Anders Jägerskog, Esha Zaveri, Jason Russ, Amjad Khan, and Richard Damania (2021). Ebb and Flow. Volume 2. Water in the Shadow of Conflict in the Middle East and North Africa. World Bank, Washington, USA. Downloaded OCT 21. https://openknowledge.worldbank.org/handle/10986/36090/

17 https://www.nato.int/cps/en/natohq/news_185000.htm. Downloaded OCT 21.

NATO´S MARINE FORCES: OPPORTUNITIES FOR BETTER INTEGRATION

CDR (POR-N) ANTONIO CARLOS ESQUETIM MARQUES

Land the Landing Force!

Traditional signal that marks the commence of the assault phase of an amphibious operation.

Amphibious forces will always be part of military response options to the world's most complex threats to global security, despite the occasional discussion concerning the utility of these operations in high-intensity scenarios and contested environments. Allies employ amphibious forces in times of peace, crisis, or conflict. From Baseline Activities and Current Operations to vigilance activities to conflicts characterized as Major Joint Operation Plus (MJO+), the flexibility and effect these forces provide has consistently proven their worth. They can be employed in nearly every operational scenario: warfighting, combat, crisis response, security, peacetime military engagement, and peace support.

In the Amphibious Leaders Expeditionary Symposium (ALES)[1] events, NATO senior amphibious leaders recognized that NATO faces challenges in the planning and conduct of combined amphibious operations and the integration and interoperability of amphibious forces. In its ALES final report, the RAND Corporation concluded that "ALES exercises highlighted the operational necessity of scalable interoperability[2] among allied amphibious capabilities". However, ALES "participants noted that many of their forces lacked recent exercise or operational experience demonstrating the anticipated degree of integration, with some exceptions for existing habitual bilateral relationships."[3] It was with this issue in mind that the Combined Joint Operations from the Sea - Centre of Excellence (CJOS COE) included in its Programme of Work 21 (PoW) a project to provoke a debate about the benefits of integrating national marine forces[4] in NATO-sponsored combined and multinational amphibious operations. The initial approach was an article published in the 2020 edition of the Cutting the Bow Wave, which later became the handbook, "NATO´s Marine Forces: Opportunities for Better Integration." This article provides an overview of that handbook, including the conceptual framework, potential force components, alliance structures, critical factors for integration in multinational operations, and some recommendations.

The Conceptual Framework

CJOS COE's handbook points out that integration is the biggest challenge facing multinational military forces seeking to operate as one interoperable force. Ideally, a multinational force is capable of achieving unity of effort without the need for fully compatible weapons or communications systems. Unity of effort is achievable for multinational forces despite differences in DOTMLPF (doctrine, organization, training, materiel, leadership and education, personnel, and facilities) among the contributing nations if there exists a sufficient level of interoperability. Interoperability can vary across multinational forces based on a variety of factors; however, NATO's dimensions of interoperability essentially include technical, procedural, and human. Further broken down, considerations such as hardware, equipment, doctrine, procedures, human nature, and training are all critical factors that must be addressed for a force to be effectively interoperable.

Amphibious Warfare

Although an amphibious force's primary purpose is to conduct amphibious operations, their unique characteristics and capabilities make them well suited for a wide range of missions and tasks in the maritime domain, including Warfare & Combat, Maritime Security, and Security Cooperation. Effective amphibious operations are based on the close integration of naval and landing forces across all domains. In addition, organic and support forces

must be trained, organized, and equipped for different combat functions. To form a multinational amphibious force, it is important to understand the current state of participating national landing forces and the extent of integration within those forces.[5] With this understanding, stakeholders are able to define strategies to promote the most efficient employment of amphibious forces.

Although generally aligned, there are varying definitions of Amphibious Force (AF) and Amphibious Task Force (ATF) among NATO countries. Building on NATO agreed definitions, the handbook defines an Amphibious Force as a "naval force and landing force, together with supporting forces that are trained, organized and equipped for amphibious operations" (AAP-06). Delving further, a Landing Force (LF) is the task organization of ground units, aviation, and surface units assigned to a Commander Landing Force (CLF) to conduct an amphibious operation. Usually, the LF centers around Marine units, but it can also include units from the Navy, Army (e.g. Artillery or Engineers), or Air Force (e.g. an Air Element). A LF may consist of the following elements:

- **Command Element:** responsible for the command and control (C2), direction, planning, and coordination of all assigned forces.
- **Ground Combat Element:** provides the combat power during land operations and consists of those elements that engage the enemy directly.
- **Combat Support Element:** provides fire support and operational assistance to the Ground Combat Element through operational C2 and fire support relationships.
- **Combat Service Support Element:** aims to sustain the force with the necessary materiel resources and logistics support.
- **Aviation Combat Element:** conducts air operations, projects combat power, and contributes to battlespace dominance in support of the LF.

Possible Components of Landing Forces (Brigade and Battalion levels)

Actual LF capabilities are highly dependent on the contributions of NATO member nations. The general description of a LF gives planners enough flexibility to build an optimal force considering each nation's individual assets and limitations. Planners must also accommodate various national interests, organizations, personnel, and doctrine. Fortunately, the NATO Defence Planning Process (NDPP) aims to provide a framework within which allies can coordinate national and Alliance defense planning activities. The NDPP creates an efficient means by which allies can provide the required forces and capabilities, and "it should facilitate the timely identification, development, and delivery of the necessary range of forces that are interoperable and adequately prepared, equipped, trained and supported, to undertake the Alliance's full spectrum of missions."[6] The NDPP specifies Capability Codes and Capability Statements, giving planners a common language for assessing capabilities. It consists of the commonly applied descriptions for Amphibious Infantry Brigade-Heavy, Amphibious Infantry Brigade-Light, Amphibious Infantry Battalion-Heavy, and Amphibious Infantry Battalion-Light. The following diagrams illustrate potential baselines of building blocks for Brigades and Battalions (excluding Aviation Combat Elements) that a multinational ATF can use for its landing force structure:

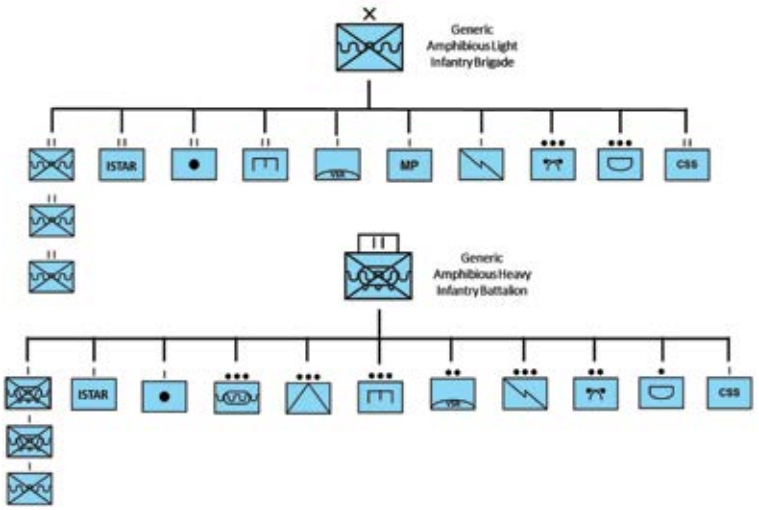


Figure 1 – Generic Amphibious Light Infantry Brigade and Amphibious Heavy Infantry Battalion baseline structure (CJOS COE. NATO's Marine Forces, 2021)

Landing Forces within NATO Countries

Several NATO member states have dedicated landing forces for the conduct of amphibious operations. Some countries can execute brigade-level operations, while others are limited by the type and number of amphibious ships. In other cases, countries are limited by the size and composition of the landing force available. Ongoing domestic challenges will always

dictate what a country has to offer when it decides to employ military forces. That being said, even lower tactical echelons, such as multinational battalions, are capable of creating meaningful synergies.

NATO´s Countries with Marines / Dedicated Landing Forces			
9th Marine Infantry Brigade 6th Light Armour Brigade "9e Brigade d'Infanterie de Marine" "6e Brigade Légère Blindée"		Sea Battalion "Seebataillon"	
32nd Marine Brigade 32 TAX PN - 32 Taxiarhia Pezonavton "Moravas"		San Marco Brigade Brigata Marina "San Marco" "Pozzuolo del Friuli" Brigade Brigata di Cavalleria "Pozzuolo del Friuli"	
Netherlands Marine Corps "Korps Mariniers"		Portuguese Marine Corps "Corpo de Fuzileiros"	
307th Naval Infantry Regiment "Regimentul 307 Infanterie Marină"		Spanish Marine Corps "Fuerza de Infantería de Marina"	
Amphibious Marine Brigade "Amfibi Deniz Piyade Tugayı Komutanlığı"		Royal Marines 3 Commando Brigade	
		United States Marine Corps (East Coast) 2nd Marine Expeditionary Force / Brigade	

Figure 2 - NATO´s countries with dedicated forces to conduct Amphibious Operations (CJOS COE. NATO's Marine Forces, 2021)

Understandably, the magnitude and strength of forces available from each contributing nation varies depending on practical influences affecting each state at a given time. National forces are normally structured for both national requirements (e.g. homeland defense and security), and commitments to other multi-national organizations such as the UN. As such, contributions from some sending states could end up being only a battalion, company, or less. The image below shows notional estimated amphibious landing forces that countries could commit for the build-up of battalion, brigade or multi-brigade forces (isolated or combined

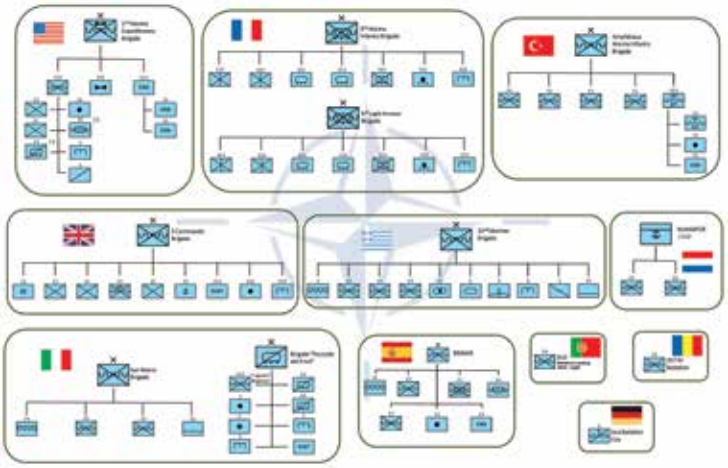


Figure 3 – Pool of Marine / Landing Operative Forces available for NATO (CJOS COE. NATO's Marine Forces, 2021)

Integration of Marine Forces – Existing structures and way ahead

Within the NATO Force Structure, there are six national Amphibious Task Groups (ATG) that form the core of a NATO multinational Amphibious Task Force. The United Kingdom, the Netherlands, Spain, Italy, France, and the United States are all capable of providing an ATG. Turkey will soon be capable of forming an ATG now that its latest amphibious ship (TCG Anadolu) is entering into service. Other countries with marine forces (Germany, Portugal, Romania, and Greece) have minimal naval assets which are not suitable for the generation of an ATG, but their forces are still capable of contributing to amphibious operations as part of a greater effort.

NATO must consider that even the more capable nations could be challenged in maintaining an independent, national, balanced, amphibious capability that is capable of fulfilling all national and international requirements. Some nations have decided to enhance combined efforts in the face of competing requirements, acting at the combined ATG level. These enhancing initiatives have given birth to the United Kingdom-Netherlands Amphibious Force (UK/NL AF) and the Spanish-Italian Amphibious Force / Landing Force (SIAF/SILF). There are also some ad-hoc forces, such as the European Amphibious Battle Group (EUABG)[7] and other bi- or multi-lateral arrangements. The United Kingdom's Joint Expeditionary Force and the cooperation between the German Sea Battalion and the Netherlands Marine Corps are also two examples of this type of force arrangement.

Possible Alliance Structures

Unlike the existing NATO maritime forces, the current NATO Force Structure does not include any permanent force to conduct amphibious operations or other operations primarily suitable for amphibious forces. Standing NATO Maritime Groups One & Two and the Standing NATO Mine Countermeasures Groups are NATO's rotational forces in the maritime domain, but a NATO Amphibious Operations Group doesn't yet fit into any of these organizations. Therefore, based on the NALES studies, the next step toward a permanent NATO amphibious capability would be to create a Standing NATO Amphibious Task Group (SNATG). One way to accomplish this would be to employ the

existing integrated forces and expand the multinational contribution for the NATO landing force.

Starting with a brigade-level composition (with different notices to move within the force), the existing landing forces in NATO countries could contribute five or more brigades and rotate regularly. The SNATG would also create a rapid-standup, multi-brigade formation to provide assurance, deterrence, and collective defense for the Alliance.

The SNATG concept is feasible, as the resources within the Alliance already exist. The advantages of forming a SNATG outweigh the costs and risks of not having one, especially when one considers that a SNATG would provide unique amphibious capabilities capable of achieving strategic and operational effects not possible with currently available forces.

Critical Factors for Integration in Multinational Operations

NATO's multinational forces have a great degree of diversity and it is imperative to understand the critical factors that affect the integration of those forces. The complexity and risk inherent in amphibious operations demand the maximum degree of integration. These marine forces would be required to maximize potential synergies, since only a few nations are capable of conducting full-spectrum operations by themselves. Noting that every contributing nation has specific capability shortfalls and skills, the goal must be to identify and best utilize all allied capabilities and in order to build up the most efficient and effective fighting force. Drawing upon the description of the integrated amphibious forces above, it is possible to identify some common factors affecting force integration. Figure 4 shows the common factors that will contribute decisively to the achievement of interoperability and full integration if addressed at the outset of force planning.

The alignment of these factors determines the level of force integration and are often interconnected themselves. Neglecting any of these factors could result in significant unexpected barriers towards achieving the desired level of integration, thus undermining the force's cohesion, effectiveness, and adaptability.

Conclusions and Recommendations

The complexity of amphibious operations in a multinational framework requires a high degree of integration across various national forces in order to

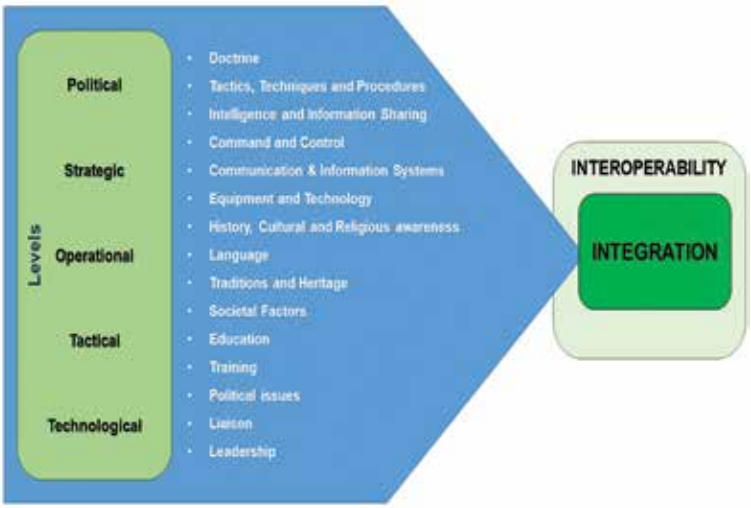


Figure 4 – Critical Factors for Integration (CJOS COE. NATO's Marine Forces, 2021)

be operationally successful. Some NATO countries already have a credible and capable amphibious landing capability but they do not train, exercise, and operate together as frequently as desired for a multinational task force. In addition, there are not enough coordinating mechanisms established to facilitate interaction and integration amongst NATO's amphibious community. Coordination mechanisms should include force agreements, memoranda of understanding, exchange officers, liaison officers, integrated staffing, information sharing, exercises, and open interoperable communication channels. CJOS COE's handbook, "NATO´s Marine Forces: Opportunities for Better Integration," provides the following recommendations in order to best achieve NATO goals in this realm:

- Establishment of a network across the NATO´s countries with marine forces for the exchange of information
- Creation of a NALES subgroup focused on the marine forces/landing forces
- Creation of a database of observations and lessons identified regarding marine forces integration process
- Development and standardization of force structures for battalion and brigade to facilitate force integration according to statements of requirements and national capabilities
-Alignment and integration into the (future) NATO Amphibious concept of the landing forces requirements in terms of force generation and force employment.

Final Thoughts

In CJOS COE's handbook, the final thoughts are a call to action for the amphibious community. There is a clear need to reduce the inefficiencies of repetitive force integration and operational buildup by establishing permanent marine forces within NATO. Establishing a SNATG would provide the ideal structure and opportunity to achieve NATO's defense planning targets for landing forces, ultimately in the form of Amphibious Infantry Brigades.

The first step toward an actual NATO amphibious capability should be to continue exploring individual nations' capabilities. Next, there must be an examination of current integration examples, engaging all stakeholders, incorporating lessons learned, and focusing on the development of landing forces as synergistic force multipliers with unique characteristics. Lastly, the unique capabilities of amphibious forces cannot be over-emphasized when discussing their potential use at all levels. The strategic, political, and military flexibility of amphibious forces allows them to respond to multiple threat axes, while creating effects at all levels of operation. Their unique capabilities enable them to respond to a multitude of operational situations, from peacetime crisis response to much more dangerous large-scale forcible entry operations. Therefore, the ultimate goal for NATO´s marine forces should be high readiness, responsiveness, adaptability, and interoperability, slowly collapsing any differences in doctrine, TTPs, training, structures, culture, or even common language. The handbook is available on the CJOS website, the ACT TRANSNET, or by request.

1 In 2016 Commander, Marine Forces Europe and Africa (COMMARFOREUR/AF) initiated ALES to generate a NATO forum to explore opportunities for improved interoperability and the aggregation and employment of amphibious forces within NATO. Since 2018 this forum is conducted under NATO's umbrella, led by Allied Maritime Command (MARCOM), and changed its designation to NATO Amphibious Leaders (NALES).
2 NATO defines Interoperability as "the ability of the forces of two or more nations to train, exercise, and operate effectively together in the execution of assigned missions and tasks".
3 NATO's Amphibious Forces – Command and Control of a Multibrigade Alliance Task Force.
4 The terms "Marine" and "Marine Forces" are used to designate the units and forces of the countries oriented to constitute themselves as the landing force of an amphibious force. These terms are general expressions and not the formal English translation for how the language of their sending states references those forces.
5 Within the Alliance, some nations have taken a more significant step towards effective integration by achieving a high standard of interoperability, as described.
6 NATO Defence Planning Process (https://www.nato.int/cps/en/natohq/topics_49202.htm)
7 In the framework of the European BattleGroups of the European Union.

ARTIFICIAL INTELLIGENCE (AI) – MARITIME ISR IMPLICATIONS

CDR (USN) FREDIRICK CONNER

"A computer would deserve to be called intelligent if it could deceive a human into believing that it was human" - Alan Turing

The Matrix and Terminator Prediction

Whether it's Arnold Schwarzenegger's terminator or a futuristic matrix, science fiction tends to portray technological advances as a one-way trip to the post-apocalyptic future. In reality, a partnership between automation, artificial intelligence (AI), and quantum computing will undoubtedly transform the world in incredibly useful ways. The maritime domain will be no exception.

AI is here today. Advances in computing are far-reaching and, from a military standpoint, have current and future implications for offensive and defensive operational plans. Future maritime Intelligence Surveillance and Reconnaissance (ISR) plans and operations could experience significant positive and negative effects based on the availability and use of AI technology. The addition of quantum computing, coupled with AI, will further change the maritime battlespace as well as all other domains.

This article is intended to be an unclassified precursor to a pending Combined Joint Operations from the Sea (CJOS) research paper. It serves to provide an overview of AI and how its use can change maritime operations, and it opens the discussion as to how the addition of quantum computing will further impact the battlespace and conduct of warfare from the sea.

What is Artificial Intelligence?

Many academic sources will explain that the term "AI" was first used in the 1950's.[1] Still today, there is no commonly agreed upon single definition of AI. The National Institute of Standards and Technology (NIST) defines AI as "systems and technology using software and/or hardware to solve complex problems, make predictions or undertake tasks that require human-like sensing, perception, cognition, planning, learning, communication, or physical action."[2] Therefore, AI is essentially a machine displaying human-like behavior to take specific actions. The ultimate goal, of course, is to use AI to perform human-like behavior in a safe, more efficient, and expeditious manner.

How Does AI Work?

In order to answer the question of how it all works, one must have a basic understanding of the technology and consider current and future categorizations of AI. The three categories of AI are artificial narrow intelligence (here today), artificial general intelligence (near future), and artificial super intelligence (the theoretical future/the singularity).[3]

Narrow AI or Artificial Narrow Intelligence (ANI) are systems designed to perform narrowly defined sets of tasks. Think about your everyday applications such as email spam filtering, financial lending decisions, voice assistance, internet search engines, or facial recognition. Self-driving vehicles, while achieving some automation, are still in this narrow AI category. While these systems have proven very useful, they are limited and are not capable of the next intellectual step to AGI.

In the near future, it's expected that AI will evolve to produce Artificial General Intelligence (AGI). AGI is meant to be equipped with a problem-solving capacity that will make it possible for the machine to self-learn various tasks in multiple areas. As a result, the general AI will have the core abilities to give it human-level intelligence. Imagine, for instance, that you are able to program or text your vehicle to pick you up at a certain time. To accomplish this, your vehicle would need to safely navigate from its current location to yours while stopping to recharge or refuel, if necessary. That need to recharge may be determined by the vehicle's independent decision-making capability. Technology today is very close to reaching AGI, but there are presently no working examples.

Artificial super intelligence (ASI) is considered as the next very futuristic AI category. This is the stage in which AI surpasses human intelligence. Sometimes referred to as the singularity, this theoretical stage of AI technology has far-reaching technical and existential implications that go well beyond the scope of daily use, let alone into the realm of maritime ISR.

All levels of AI require the necessary software and hardware for essential computer functions; however, what it requires most is data, and a substantial amount of it. Data sets that continue to grow to larger and more complex, exceeding traditional processing software abilities, are called big data. Advanced algorithms require new and varied data to make accurate predictions to resolve situations, contrary to the original programming, for any situation in the AGI or ASI category. Even the most basic level ANI requires data.

Big data, machine learning, and autonomy are part of what makes AI systems work. In the most simplistic terms, data is analyzed and used by the machine learning levels of AI in order to autonomously decide actions. AI then applies machine learning, deep learning, and other techniques to solve actual problems.[4] An example of machine learning would be a user playing the same type of music on an AI device, which then prompts that device to automatically select related music to play. Deep learning is a computer utilizing complex algorithms to mimic the human brain. The self-driving car discussed earlier that makes several unplanned human-like decisions is an example of deep learning. Storing this data and having rapid access is a key factor in the success of AI. Civilian and military sectors who conduct AI research and development do so with the above-described basic understanding of AI. Now, imagine an AI machine using advanced computing power that is much faster and more capable than any computer used today. That is quantum computing, and it could be considered as the next advancement in computer technology that further accelerates AI development.

Quantum computing will change the operation of every computerized process, essentially bringing a giant leap in computer processing speed. With this increased speed, a computer or AI system could process numerous tasks in a fraction of the time of previous computer systems. Although difficult to compare, Professor Catherine McGeoch, of Amherst College, stated that quantum computing is about one thousand times faster than a conventional computer.[5] The speed of quantum processing will enable AI systems to perform more complicated tasks and possibly reach the next artificial intelligence level.

The tremendous processing speed of quantum computing promises to solve many complex problems, but it will also present new challenges. Digital security or encryption constructed by non-quantum computers will become obsolete due to the new speed and capability brought forth by quantum computing technology. As discussed above, quantum computers will be able to solve complex security algorithms in a fraction of the time that it would take older computers. So, while quantum computing will aid AI progression, it will also bring significant security risks to non-quantum devices for both civilian and government entities. For example, in 2018 Ann Dunkin, CIO at the U.S. Department of Energy (DoE), stated that quantum encryption is an area of great concern to the U.S. Federal Government.[6] This issue could easily translate to a problem for NATO and maritime operations security. "Given the potential implications of quantum technologies for defense and security, NATO has identified quantum as one of its key emerging and disruptive technologies."[7]

AI in the Maritime Environment

AI is still currently operating in the 'narrow' category, which means current technology could allow several at-sea tasks to be automated or made more efficient. As of 2021, the commercial shipping sector consists of more than 1,000 maritime autonomous surface ships operated by more than 53 organizations worldwide.[8] The Flemish Smart Shipping program, for example, uses narrow AI, machine learning, and automation through a smart waterborne communications infrastructure network. Commercial organizations are making strides in several ways to develop and utilize AI technology, and militaries are finding uses for it as well.

Military AI applications in maritime operations include intelligence, surveillance, and reconnaissance (ISR), cyberspace, information operations, command and control, semiautonomous/autonomous vehicles, and lethal autonomous weapons systems. It's worthwhile to explore a few of the most common uses of AI in the maritime environment.

Maritime ISR operations currently use AI enabled aerial drones, operating in semiautonomous and autonomous modes. Depending on the situation, operators can elect to exert more (semiautonomous) or less (autonomous) control of the platform(s). The information collected is relayed as data to be potentially analyzed by other AI applications. For example, AI can drastically enhance the efficiency of imagery analysis, rapidly searching for the tiniest differences in historical analyses or identifying anomalous pixels that would otherwise be imperceptible to the human eye.[9] AI improves ISR operations and is in use today for both offensive and defensive operations.

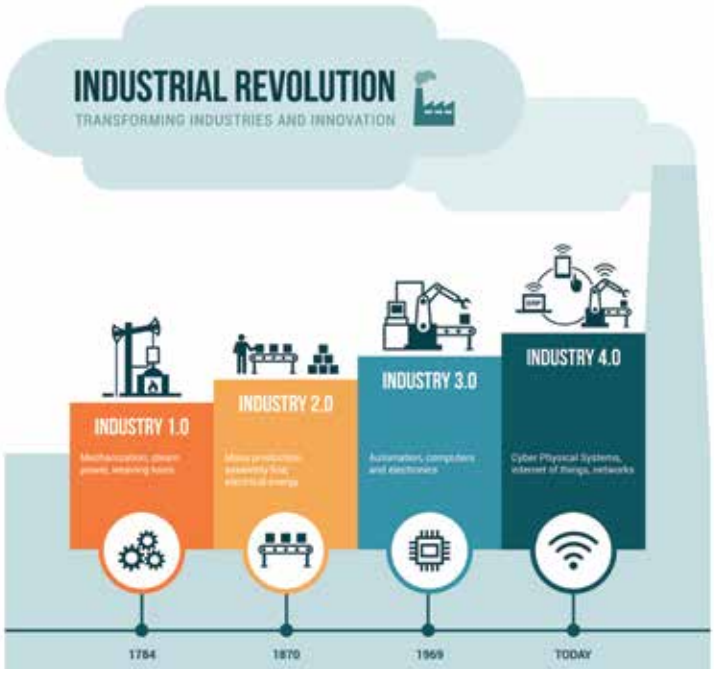
AI can positively contribute to warfare in the Cyberspace domain as well. A large part of what contributes to Cyberspace is all the equipment used to transfer data from one digital location to another. "AI and machine learning are now becoming essential to information security within cyberspace, as these technologies are capable of swiftly analyzing millions of data sets and tracking down a wide variety of cyber threats - from malware menaces to shady behavior that might result in a phishing attack".[10] AI and machine learning can predict the next system vulnerability and take action to secure the vulnerability before a malicious actor steps in. AI can increase the security of cyberspace by detecting new threats, battling cyber bots, predicting intrusion risk, and better protecting endpoints. The maritime domain makes significant use of cyberspace and increased AI implementation will support and secure its use.

AI will also support Information Operations. Information Operations are an essential mission in irregular warfare; specifically, it is the acquisition and accumulation of information about a combatant that is used to defend a military and country.[11] AI can be used to increase the efficiency of generating and disseminating information that could sway an adversary's will to enter or remain in combat. "The Alliance needs a broadly effective strategy to counter the evolving threat of disinformation. AI tools can help to identify and to slow the spread of false and harmful content while upholding the values of pluralistic and open societies."[12] Information Operations supremacy in the maritime domain can be used to change a battle before it starts.

AI can also improve Command and Control by speeding up the decision-making and tasking responsibilities of commanding officers. Many warfare commanders operate on a loop that observes, orients, decides, and acts. AI can essentially reduce the time and space at each decision point. Much like ISR, observation requires the review of large amounts of data for a specific item. AI will shorten this review time by expeditiously scanning and locating specified items. Next, AI can take large amounts of data and orient (speculate) more efficiently than human operators, thus shortening this stage. In the decide phase, AI can quickly offer courses of action based on data presented. With the support provided in the previous phases, commanders are now able to act quickly, sometimes with AI pre-determined response options as the appropriate course of action. National Defense, a popular defense periodical, states that an AI system can ingest, process, and synthesize vastly more information at superhuman speed. This empowers decision-makers with a fuller view of the "ground truth" when they need it.[13]

Semiautonomous and autonomous vehicles take advantage of AI technology. The application of mine hunting and oceanographic mapping are just two areas that AI could save lives and time. Consider an unmanned mine-hunting or mine-laying vessel that is not restricted by the consideration of human life; critical mine danger areas could be surveyed without risk. Sending an unmanned vehicle, with or without a mother ship, to map oceanographic features could reduce the need to request and plan support for an uncharted area. Of course, there are some international laws to be considered; however, NATO is committed to ensuring AI applications will be developed and used with national and international law consideration.

The military use of semiautonomous and autonomous vehicles at sea quickly leads to the topic of AI and weapons systems. Lethal autonomous weapons systems and AI are heavily debated topics and capabilities. Article 36 (Additional Protocol I) of the Geneva Convention requires nation states conduct a legal review to ensure new weapons comply with international law.[14] Non-compliance with this additional protocol means that an AI weapon system would be prohibited by international law. The bottom line is that while this technology can reduce human response time, AI systems will need to be able to distinguish between military and civilian targets. The United Nations Convention on Certain Conventional Weapons continues to discuss the legality of lethal autonomous weapons. No decision or agreement has been made between nations, which means that some nations continue to produce varying levels of autonomous weapons to potentially be used in a maritime environment.[15]



Courtesy of Shutterstock.

Implications for AI Enabled ISR

With the continued refinement and advances of AI, the implication for future maritime operations, including ISR, is significant. It's been established that AI technology will gather more data and be able to analyze it more efficiently than humans. It can usher in the capability of taking the human out of the loop for time critical decision points; the implication for maritime ISR is huge in this respect. Imagine the time-savings in the AI enabled analysis phase of ISR, where a system provides the commander of an operation a "GO-GREEN Light" to conduct a time sensitive mission. Previously, several analysts (in-the-loop) would spend hours reviewing and deciding on an action. This quick action could be a positive addition to an AI enabled ISR.

AI in a denied communications environment is worth consideration when looking at potential vulnerabilities in the technology. AI must have access to huge amounts of data or possess the code to perform in an artificial general intelligence manner to make decisions in the absence of human input. AGI must perform based on a programmed set of actions. Therefore, operating procedures must consider appropriate responses if the AI has a loss of communication as increasingly complex algorithms will be required to ensure consistent and correct use of the systems. As it stands, a loss of communication could be more of an issue for narrow AI system than actual humans. There is a high degree of uncertainty to the mission if an AI system loses communication to the human in the loop or, even more so, to the necessary data.

Conclusion – What Should NATO Do?

AI is considered as the fourth revolution and impacts all domains.[16] Similar to previous industrial revolutions, this fourth revolution will alter the course of the future. It is here today and, with continued research and development, will continue to evolve at a rapid rate. As it pertains to military maritime use, future ISR plans, and operations could experience significant positive and potentially negative impacts. NATO's AI Strategy, adopted in October 2021[17], must be a living document ready for change based on advancements in technology. This strategy drives to accelerate AI adoption by ensuring allies create policy to enhance AI enablers. Based on this strategy, NATO must perform two key tasks. First, it must continue to invest in AI and drive alliance members to match or better their investments into this technology. And second, it must ensure resilient communications that can support AI; these systems are best when necessary communications to both data and the human-in-the loop are accessible.

Courtesy of Shutterstock.

AI will continue to impact both commercial and military maritime operations for the foreseeable future. NATO must continue to benefit by the development and use of AI and automation, including the exploitation of quantum computing. While movies and science fiction novels predict AI as human-like robots that take over the world, the current evolution of this technology is worth acknowledgment, policy formulation, and careful planning on its best use for offensive and defensive military efforts. The future battlespace demands it.

1 1 Rockwell Anyoha, "The History of Artificial Intelligence," Blog, Special Edition Artificial Intelligence, August 28, 2017, https://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/#:~:text=It's%20considered%20by%20many%20to,and%20Marvin%20Minsky%20in%201956.&text=Despite%20this%2C%20everyone%20whole%2Dheartedly,sentiment%20that%20AI%20was%20achievable.
2 National Institute of Standards and Technology, U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools, August 9, 2019, pp. 7-8.
3 https://www.techtarget.com/searchenterpriseai/definition/artificial-superintelligence-ASI
4 https://www.sas.com/en_us/insights/articles/big-data/artificial-intelligence-machine-learning-deep-learning-and-beyond.html#:~:text=While%20machine%20learning%20is%20based,techniques%20to%20solve%20actual%20problems.
5 https://www.amherst.edu/news/archives/faculty/node/466477
6 https://www.meritalk.com/articles/reps-khanna-mace-developing-quantum-computing-bill-to-secure-fed-data/
7 https://www.nato.int/docu/review/articles/2021/06/03/quantum-technologies-in-defence-security/index.html
8 https://www.maritime-executive.com/editorials/autonomous-vessels-are-becoming-a-commercial-reality
9 https://www.clarifai.com/use-cases/isr-edge-ai
10 https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity
11 https://www.idb.org/what-role-does-information-operations-play-in-the-military/
12 https://www.nato.int/docu/review/articles/2021/08/12/countering-disinformation-improving-the-alliances-digital-resilience/index.html
13 https://www.nationaldefensemagazine.org/articles/2020/11/13/ais-power-to-transform-command-and-control#:~:text=There%20are%20more%20examples%20of,and%20more%20accurate%20decision%2Dmaking.&text=AI%20shortens%20and%20sharpens%20this%20decision%20loop%20at%20every%20step.
14 https://www.orfonline.org/research/42497-a-i-in-naval-operations-exploring-possibilities-debating-ethics/
15 https://international-review.icrc.org/articles/stepping-back-from-brink-regulation-of-autonomous-weapons-systems-913
16 https://www.ubs.com/microsites/artificial-intelligence/en/new-dawn.html
17 Zoe Stanley-Lockman, Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO" https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html

ARRIVAL OF 5G NETWORKS IN THE MARITIME DOMAIN

CDR (ROU-N) NECULAI GRIGORE,
CDR (USN) SHAWN NEWMAN

Failure to plan towards implementing 5G and its supporting infrastructure will leave the Alliance vulnerable to both large and small adversaries.

As warfare, and the role technology plays within it, evolves, Combatant Commanders must rapidly come to grips with Future Warfighting Concepts. Several abstract ideas dictate how we must plan and execute warfare in ways never before imagined. These ideas may be implemented alone or in conjunction with other systems, but they require a vastly improved degree of networking and augmented intelligence to succeed. This largely maritime-focused article looks at significantly advanced information and communications architecture based on 5G (or Fifth Generation Integrated Mobile Telecommunications) capabilities designed to link land, air, and maritime platforms together in a dramatically reimagined future battlespace.

The complex and rapidly changing warfighting environment will require a faster and more comprehensive decision-making process conducted at lower tactical levels than previously seen. Furthermore, anti-access / area denial (A2AD) tactics such as electronic warfare, cyber weapons, long-range hypersonic missiles, long-range air defense capabilities, and other dynamic threats will push warfighters to make decisions at the speed of relevance to counter strikes against naval and shore-based combat forces. Additionally, emerging tactics from new and traditional adversaries will dramatically shorten the timeframes for observation, assessment, response, and reassessment. Timely reactions, or on-the-loop decision-making, will be supported by artificial intelligence-based systems to enable rapid and effective decision-making for combatant commanders. This new process will require seamless information sharing and interoperability between battle systems on separate NATO platforms and across all domains, as unpredictable responses from the enemy test a commander's focus.

Presently, the range of environments and situations at the theater level limit a commander's ability to employ automation, slowing decision-making to the speed of his or her planning staffs' capabilities. Furthermore, cyber-attacks, or the destruction of critical satellites, can significantly impact operations in a contested environment due to delays in information transmission, exchange, and processing. Currently, the delegation of authority to the company, aircraft, or ship level must be considered in order to take full advantage of mission command against an adversary, but that comes with its own risks depending on the mission. In order to enable, rather than constrain, our current and future information-sharing requirements, architectural changes in Command, Control, Communications, Computers, and Intelligence (C4I) systems are required to allow alternate routing of long-range communications. Additionally, technological advances coupled with wide-ranging changes to doctrine, organizational structure, personnel training, equipment, facilities, interoperability, etc., require an acceptance throughout the Alliance's leadership. An advanced 5G system is a critical component of future warfare; however, it cannot singularly address the concerns of tomorrow's combatant commander. Developing technology in concert with the infrastructure and human elements of warfighting to maximize its effectiveness is critically important on the modern battlefield.

Current and future adversaries can quickly meet or exceed the last several decades of Alliance modernization efforts through innovations to their warfighting equipment and capabilities. They are able to leverage new technologies, including long-range precision weapons, sensors, complex electronic warfare capabilities, and cyberwarfare. To remain competitive, NATO must rethink force design and command and control (C2) to maintain its competitive edge. Previously an advantage, force packages based on large naval formations like Carrier Strike Groups with their multi-mission monolithic platforms will be vulnerable to the near-future capabilities of adversaries employing asymmetric warfare across multiple domains. Size and aggregation, a hallmark and strength of modern fleets envisioned by Alfred Mahan, are disadvantaged in detectability and the potential of engagement by determined, nontraditional combatants.[1]

5G Enabled Concepts

Future generation tactics and technologies demand that we adapt new warfighting concepts. One of these,

the Multi-Domain Operations (MDO) framework, is "an evolution of joint operations" employing strategies to frustrate and overwhelm an adversary by creating dynamic challenges across multiple domains in the tactical support, close, and deep maneuver areas. NATO must modernize doctrine and rules of engagement, C2, and weapons systems' interoperability for future air, land, and maritime conflicts where a complex observe, orient, decide, act (OODA) loop will demand an array of near-instantaneous decisions. These decisions must consider the complexity of sensory inputs, decision-making, targeting, commitment, and actions through total integration of the common operating environment across all domains. The MDO concept requires a timely, seamless, and uninterrupted exchange of information – challenging during peacetime operations, but essential during wartime.[2] [3]

Conceptually, Joint All-Domain Command and Control (JADC2) modernizes the C4I concept by enhancing the speed and integration of sensory collection, processing, decision-making, and response. It uses artificial intelligence algorithms that enhance each commander's range of options to optimally allocate and employ weapons against a wide range of enemy targets throughout the contested space. JADC2 is meant to provide decision-makers continuous access to geographically dispersed, cross-domain information in support of integrating capabilities across all domains. The result is a commander able to react incredibly fast with a potential variety of options, overwhelming the enemy physically and psychologically and gaining advantages in the operational environment [4] [5]

Distributed Maritime Operations (DMO), another important Future Warfighting Concept, works to gain and maintain sea-control through combat power spread over vast distances, between multiple domains, and amongst a wide array of platforms.[6] DMO pushes past our current force employment concept of deployed massive capital ship groups. Instead, it prefers to utilize distributed fleet assets of varying capabilities as a single, united weapons system capable of providing both collective defense and offensive strikes or fleet engagements across theaters.[7] Collectively leveraging military units' sensors and weapons systems, disparate combat power is brought together as an assembly of capabilities, not just a closely proximate squadron or strike group. These diverse force packages can be coordinated to neutralize and counter threats across multiple domains.[8]

Courtesy of Shutterstock.

Mosaic warfare is the conceptual evolution of the MDO, JADC2, and DMO frameworks in an even more flexible and adaptable warfighting approach. It presumes that decision-centric warfare will provide a superior advantage over a traditional means of defeating an opponent through attrition. The Mosaic framework leverages the capability of highly disaggregated military forces under human command and machine control in order to compose and recompose so that the enemy is enveloped by complexity, making them uncertain of how to respond. Mosaic warfare requires implementing artificial intelligence (AI) and uninterruptable communications to tie systems together, even limiting some human decision-making capabilities. The ideal Mosaic structure allows subordinate commanders to assume mission command and pursue tasks aligned with forces they can directly communicate with while having smart-machine-enabled responses.[9] Based on inputs regarding the size and effectiveness of opposing forces, the AI-enabled machine control system identifies connected units that could be tasked, thereby enabling actions based on instantly updated data related to ship, aircraft, and systems capabilities. Essentially, commanders can use machine control systems to automatically determine and employ the appropriate forces to achieve objectives or missions.

DOTMLPFI Implementation

These new force designs, C2 processes, and warfighting concepts require interconnecting information among manned and unmanned platforms across all domains. The employment of any capability in the maritime domain is a complex process. To extensively detail all doctrine, organization, training, material, leadership, personnel, facilities, and interoperability (DOTMLPFI) aspects requires a significant effort from the various distinctive teams in these areas of the maritime environment. Moreover, 5G technology is an emerging technology and, therefore, a framework under development. The main challenges for each aspect that planners should consider when implementing 5G capabilities in the maritime domain are outlined below.

Doctrine. The implementation of 5G in the maritime domain may require new doctrine. Any modifications to the fundamental principles by which commanders guide their forces in support of objectives will be dictated by new and increasingly complex challenges of the operational environment. However, 5G technology will support the implementation of new, successful warfighting concepts. These new concepts can be used to support a mission command approach for increased distribution of smaller and lighter manned and unmanned forces that require reliable, broadband, real-time exchange of information.

Organization. Presently, 5G technology is not mature enough for commanders to adequately determine its effects on an organizational structure. Its implementation process is likely to generate specific tasks and responsibilities that ensure 5G capabilities can be sustained and supported. The main advantage of 5G is its ability to support the development of new force design and command and control processes.[10] As referred to earlier, instead of fielding multi-mission warships operated by relatively large crews, the future maritime force may consist of distributed and diverse, manned and unmanned, fleet assets. We can expect the delegated C2 responsibilities and authorities of subordinate commanders to increase significantly in order to accomplish complex missions using limited personnel, but with support from AI decision systems. The leaders of today can prepare for the future through increased understanding of mission command and practicing the delegation of authority to subordinate commanders, both of which will become easier with added experience and enabling technologies in the future.

Training. Proper implementation and operation of this capability will require at least two different types of training: technical and operational. As a new technology, 5G requires training and analysis across all areas, not only on materiel aspects, but also on the processes and policies that will change. The NATO Communications and Information (NCI) Academy is the recommended organization to host complex, specialized training in various areas such as the operation, management, administration, and security of 5G systems.[11] The NATO School Oberammergau (NSO) could develop an appropriate operational training process for all commanders who require in-depth knowledge of their new roles in determining and employing force packages, guided by warfighting concepts and supported by 5G technologies.

Materiel. There is currently no plan to deliver any 5G technologies to the fleet level, as this new capability is still in the research stage. However, existing networking, processing, and storage solutions could facilitate the complete integration of the many revolutionary 5G advances.[12] [13] Developers should consider integrating 5G technology into edge and core networks during the development of new capabilities such as Federated Mission Networks and C2 systems for the maritime domain. The new radio and edge technologies (e.g., Mobile Edge Computing) bring the most advantages for naval operations; operations that involve highly deployable forces, operating in small manned and unmanned action groups, and which are dependent upon instantaneous broadband information exchange.[14] [15] Additionally, designers should plan to install massive multi-input / multi-output antennas onboard ships and other naval platforms to increase electromagnetic compatibility with systems operating in the same frequency bands.


Courtesy of Shutterstock.

Leadership. The implementation of 5G technology will follow the existing well-defined process within NATO; therefore, no additional structures are required to manage 5G employment as existing organizations can assume these responsibilities. However, two leadership aspects should be considered: the governance of 5G implementation into allied nations, and the operational C2 of future maritime forces. Regardless of which 5G solution a member nation chooses to implement, the end goal should enable disaggregated forces to compose and recompose seamlessly, creating complexity and uncertainty for the enemy. Furthermore, the critical capabilities of 5G technology could change C2 processes through the increased importance and responsibility of subordinate commanders, who must take mission command, executing tasks while utilizing a greater number of forces with whom they can communicate.

Personnel. Implementing this new capability could reduce the required number of personnel as a result of greater automation. The complexity of these systems requires more setup time; however, once they are ready, it is possible that only limited maintenance will be necessary. Moreover, the automatic and low latency platform-to-platform communications supporting unmanned maritime vehicles may also lower demands on personnel afloat who were previously required to control them.

Facilities. The flexibility and adaptability of the current IT systems in use for allied communications could satisfy all integration and management requirements for 5G networking.[16] However, installing 5G radio technologies onboard maritime platforms will require a comprehensive study to avoid interference with existing systems and ensure proper integration into ship superstructures. That being said, once these efforts have begun, assessing resiliency will improve mitigations and build more sustainable communications channels for operational efficiency.

Interoperability. The Alliance operates together in many areas of interest, which necessitates seamless interoperability and common technical and operating standards. The development of 5G technology is an ongoing process where different nations have taken multiple approaches to capture the 5G market by building individual standards, devices, and equipment; as a result, not all equipment will work on all networks or in all countries.[17]

Moreover, the frequency spectrum used for 5G by one country may not support devices from another. As a matter of urgency NATO should agree on an international standard to develop 5G infrastructure to avoid these technical limitations, related mainly to spectrum allocation and the security of systems, networks, and data. The 3rd Generation Partnership Project and the United Nations International Telecommunications Union are the key organizations for the standardization of 5G technologies; their global standard should be considered for further 5G implementation into the allied environment.[18] [19]

Conclusion

Alliance partners must embrace Future Warfighting Concepts to maintain advantages previously guaranteed with overwhelming maritime presence. Scholars and planners have developed concepts that provide a way forward for success in future wars against adversaries acting in nontraditional ways. MDO (effective Command and Control through all contested domains), JADC2 (comprehensive decision making and A2AD), DMO (distributed lethality over a wide geographical area), and Mosaic (decision-centric) Warfare must be tied together through a vastly improved system of networking, supported by AI.

An advanced information and communications architecture based on 5G (and supporting technologies) will be necessary for all domains in the near-future environment. From a maritime perspective, it will link platforms together in dramatically new ways. For example, it will alter the composition and organization of naval aviation assets through updates to computing, networking, and systems, accomplished by piecing together some of the critical technology components. The use of Federated Mission Networking (sharing data in an agile and prearranged way), Edge Computing (processing data manipulation and interpretation close to the source before sharing/transmitting), mmWave Communications (high spectrum band use), and MIMO (increasing network density and reducing high propagation loss) are key to these linkages.

As NATO advances into the future, the strategic goal of procurement, maintenance, and training processes should be a robust and seamless information-sharing platform, supporting battle systems on separate NATO systems across multiple domains. Failure to plan towards implementing 5G and its supporting infrastructure will leave the Alliance vulnerable to both large and small adversaries. These technological advances must also be coupled with wide-ranging changes to doctrine, organizational structures, personnel training, equipment, facilities, interoperability, and, especially, how the Alliance leadership thinks. An advanced 5G system is a critical component to future warfare and NATO and its extended allies must embrace, promote, and develop this technology as a key component to success on the battlefield in all domains.


Courtesy of Shutterstock.

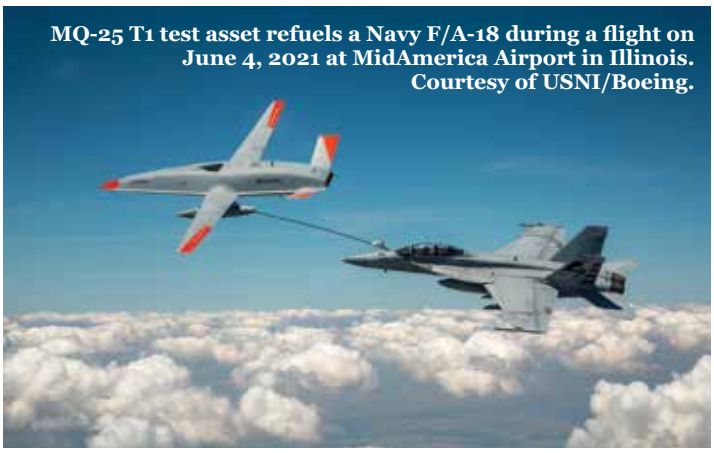
1 Philip A. Crowl, "Alfred Thayer Mahan: The Naval Historian," in Paret, Peter, Gordon A. Craig, and Felix Gilbert, eds. Makers of Modern Strategy from Machiavelli to the Nuclear Age (1986), ch. 16.
2 Lieutenant Colonel Heiner Grest and Lieutenant Colonel Henry Heren, What is a Multi-Domain Operation?, Shaping NATO for Multi-Domain Operations of the Future, Joint Air Power Competence Centre, October 2019, pg. 3
3 Bruce Hargrave, Shaping NATO for Multi-Domain Operations of the Future, Joint Air Power Competence Centre, October 2019, pg. vi
4 John R. Hoehn, Joint All-Domain Command and Control: Background and Issues for Congress, pg. 6
5 John R. Hoehn, Joint All-Domain Command and Control(JADC2), Congressional Research Service March 18, 2021, pg. 2, https://crsreports.congress.gov/product/pdf/IF/IF11493
6 Christopher H. Popa et all, Distributed maritime operations and unmanned systems tactical employment, Naval Postgraduate School Monterey, June 2018, pg. 7
7 Christopher H. Popa et all, Distributed maritime operations and unmanned systems tactical employment, pg. 7
8 Christopher H. Popa et all, Distributed maritime operations and unmanned systems tactical employment, Naval Postgraduate School Monterey, June 2018, pg. 8
9 Bryan Clark, Dan Patt, Harrison Schramm, Mosaic Warfare exploiting artificial intelligence and autonomous systems to implement decision-centric operations, Center for Strategic and Budgetary Assessments, 2020, pg. 39
10 North Atlantic Treaty Organization News, "Changing Lives and the Security Landscape – How NATO and Partner Countries are Cooperating on Advanced Technologies." 15 Jun 2021, https://www.nato.int/cps/en/natohq/news_184899.htm?selectedLocale=en
11 NATO Communications and Information Agency, "About the NCI Academy." https://www.ncia.nato.int/what-we-do/nci-academy/about-the-nci-academy.html
12 U.S. Department of Defense, "Department of Defense Successfully Demonstrates a 5G Network for Smart Warehouses." 8 Jun 2021, https://www.defense.gov/News/Releases/Release/Article/2650242/department-of-defense-successfully-demonstrates-a-5g-network-for-smart-warehous/
13 U.S. Department of Defense, "DoD Kicks Off 5G Dynamic Spectrum Sharing Experimentation at Hill AFB." 2 Dec 2021, https://www.defense.gov/News/Releases/Release/Article/2859222/dod-kicks-off-5g-dynamic-spectrum-sharing-experimentation-at-hill-afb/
14 ETSI ISG MEC (2015) Mobile edge computing: A key technology towards 5G, White paper, issue 11, September 2015.
15 Madhusanka Liyanage et all, A Comprehensive Guide to 5G Security, John Wiley & Sons Ltd, 2018, pg. 43
16 Linda Hardesty, "5G Base Stations Use a Lot more Energy than 4G Base Stations: MTN." Fierce Wireless, 3 Apr 2020, https://www.fiercewireless.com/tech/5g-base-stations-use-a-lot-more-energy-than-4g-base-stations-says-mtn
17 Jill C. Gallagher and Michael E. DeVine, Fifth-Generation (5G) Telecommunications Technologies: Issues for Congress, January 30, 2019, pg. 12
18 Chaim Gartenberg. "The First Real 5G Specification Has Officially Been Completed: A Huge Step Forward Towards Actual 5G Networks." The Verge,
19 International Telecommunications Union (ITU) - Radiotelecommunications Sector (ITU-R). "Minimum Requirements Related to Technical Performance for IMT-2020 Radio Inteface(s)." Nov 2017, https://www.itu.int/dms_pub/itu-r/opb/rep/R-REP-M.2410-2017-PDF-E.pdf

MANNED-UNMANNED TEAMING IN JOINT OPERATIONS

LTCOL (ITA-AF) ROBERTO PATTI

"Unmanned platforms – that's the future, right? And so, a hybrid fleet is where we're going, make no mistake about it" - Adm. Mike Gilday, USN

In today's increasingly complex geopolitical situation, NATO faces the most challenging security environment since the end of the Cold War, with Russia's behaviour remaining assertive and destabilising, and terrorism continuing to represent a global security threat. Adding to this, the Alliance is recognising the role of China in shifting the global balance of power, including the deep implications for the member nations' security, values, and way of life. Global uncertainty is on the rise, with cyber and hybrid threats more sophisticated and disruptive than ever. Over the last few decades, adversaries have invested heavily in advanced Anti-Access/Area Denial (A2/AD) capabilities as a means of countering traditional allied military advantages and altering the balance of power. This has made it clear to senior military leaders that in future confrontations the traditional joint approach will not suffice and has thus paved the way for a new methodology which will require Allies to use the element of surprise, rapidly integrating capabilities across all domains of operations in order to achieve the operational advantage. There is no doubt that unmanned systems will play a key role in this respect, as the United States' Chief of Naval Operations (CNO) clearly remarked. NATO's largest navy is deeply engaged in developing unmanned technologies and integration "from seabed to space." All domains are seeing expanding varieties of experimentation, including, for example, semi-autonomous, high-performance UAVs designed to carry out the strategic role of airborne tankers for their fighter fleet (the MQ-25 Stingray). We need to explore how to team up with our unmanned systems if we are to realize the full potential of the future fight.



MQ-25 T1 test asset refuels a Navy F/A-18 during a flight on June 4, 2021 at MidAmerica Airport in Illinois. Courtesy of USNI/Boeing.

Unmanned Systems vs Manned-Unmanned Teaming: The Added Value

Historically, unmanned systems have been regarded as means to replace manned assets for missions deemed too "dull, dirty or dangerous"[1] for human crews, or they were a way to offload prime assets for budget considerations. Alternatively, unmanned systems would be deployed to *augment* manned platforms, providing added capacity to the force. This construct still considers unmanned systems as single platforms (or small groups thereof) operating in isolation for specific tasks. Manned-Unmanned Teaming represents a key step in a new direction where unmanned systems will be deployed as autonomous or semi-autonomous[2] extensions of manned platforms, operating as true force multipliers. Ultimately, unmanned technology will surely add to the *capacity* of the force, but the real added value lies in its unique ability to deploy in areas or tasks where manned platforms would be facing an unacceptable risk. Deploying added sensors and weapons to previously unreachable areas will allow for a true *capability* leap, producing effects far greater than the

sum of individual contributions, reducing risk to human crews, and eliminating redundancies. In the maritime domain, the efforts to develop, and subsequent benefits of, unmanned technologies are a necessity given the growth in size and quality of our adversaries. The resurgence and growth of respective Russian and Chinese navies have put an end to the days of relatively uncontested western superiority. Allied navies have had to face a growing demand for new capabilities despite increasing budgetary constraints, inevitably leading to an increased reliance on a relatively small number of high-value assets. By virtue of their increased strategic significance, high-value assets face a proportionally higher risk levels against credible threats. The vulnerability of these assets represents a risk to the Alliance; Manned-Unmanned Teaming promises to be part of the solution to this conundrum.

What is Manned-Unmanned Teaming?

Despite some semantic ambiguity, and the lack of a generally agreed-upon definition, Manned-Unmanned Teaming can be defined as "the synchronized employment of Soldiers, manned and unmanned air and ground vehicles, robotics, and sensors to achieve enhanced situational understanding, greater lethality, and improved survivability."[3] Also referred to as "Human-Machine collaboration", "Man-Machine teaming," or "Manned-Unmanned pairing," the underlying concept is to leverage the combined strengths of manned and unmanned platforms to achieve operational advantage. The idea of combining manned and unmanned assets to pursue common mission objectives as an integrated team is not a new one. First attempts date back to July-October 1944, when the U.S. Navy operated the TDR-1 "Assault Drone" aircraft from airstrips based in the Russell Islands. This first experiment used a remarkably simple design consisting of a steel-tube frame covered with a molded wood skin, minimizing the use of strategic materials from production of higher priority aircraft. A modified Grumman TBM-1C Avenger torpedo bomber served as the mothership, taking off first and circling over the airfield while a ground crew would launch the drone and hand control over to the bomber crew. The airman in the TBM's rear cockpit would receive visual signals from the TDR's nose-mounted camera and guide it via a joystick for the duration of the mission. Despite the rudimentary design, the TDR-1 proved successful against Japanese vessels, demonstrating remote control capability up to

TDR-1 "Edna III" being readied for a bombing mission on the following day against a Japanese freighter beached at Guadalcanal, 29 July 1944. Courtesy of Wikipedia Commons.

seven nautical miles and the ability to accurately strike targets with zero loss to manned mothership crews.[4]

What substantially distinguishes modern iterations of Manned-Unmanned Teaming from previous ones is their dependence on autonomy and its various degrees of implementation. Autonomy represents a key driver for unmanned systems to perform more articulate, complex mission objectives while at the same time maintaining a reasonably steep increase in joint operational tempo. Research in the field of Artificial Intelligence, Machine Learning, and Deep Learning is giving way to new unmanned systems developed for an even larger variety of tasks. For example, unmanned systems may operate independently or as an extension of a manned mothership, or they may to interconnect amongst themselves (swarms), or they may even integrate with manned weapons systems.[5] New and improved Human-Machine Interfaces (HMI),[6] which rely heavily on autonomy, will be instrumental in shifting the role of the human element from operator to mission manager. This will mean evolving from controlling one single drone at a time to overseeing multiple autonomy-enabled platforms. Subsequently, new HMIs will be capable of handling a larger number of unmanned vehicles in swarms or as reliable teammates, fully integrated with land, maritime and air forces. The advantage to military operations goes far beyond combat missions that require larger advances in technology and longer development timelines. In the near future, with adequate protocols in place, manned and unmanned platforms will be able to cooperate across domains, dramatically increasing situational awareness and effectiveness in missions like Maritime Patrol, Anti-Submarine Warfare (ASW), or Search and Rescue (SAR).

A Look Ahead

The development of the next generation of weapons systems is being driven by future operational scenarios that include the employment of integrated air defences, hypersonic weapons, and low observability technologies in highly contested, communications-degraded environments.[7] Using the air domain as an indicator of future warfare trends, the aerospace industry is well invested in developing the "next generation" of fighter aircraft, which, albeit being a vague descriptor for yet unspecified platforms, is presumed to mean stealthier, faster, more "*connected*", and generally more capable than their predecessors.[8] This marks a departure from the customary "performance bump" of previous generations of weapons systems, indicating instead that the future will trend more towards connectivity and the ability to receive, process, and disseminate data. One recurrent idea is that future weapons systems will operate connected to a "combat cloud" of sorts that is able to pair any platform capable of sharing Intelligence, Surveillance and Reconnaissance data (ISR) with any weapons system, regardless of the specific domain. In this vision, any platform can *see* and *shoot* well beyond its physical limitations, and the large mass of data involved is processed at computer speed through Artificial Intelligence and Machine Learning. The result is the ability to identify targets and make optimal weapon-shooter pairing recommendations to tactical decision makers.[9]

Implementation of this vision of a network of collaborative, integrated platforms across all operational domains has already started, although it is heavily dependent on technological advances and concept development. The United States Navy (USN), for example, is currently experimenting with the Distributed Maritime Operations (DMO) concept,[10] which envisions a better interconnected, global-reach fleet enabled by Unmanned Surface Vehicles (USV). Such USVs will be substantially less expensive than multi-mission manned vessels and will form the foundation of the vision of a hybrid fleet capable of delivering synchronized lethal and nonlethal effects across all domains. The smaller, relatively inexpensive unmanned vessels could be used as forward-deployed sensors, decoys, or weapons dispensers, working alongside manned ships. They would exponentially increase the USN's overall capacity at a fraction of the cost of building new larger ships and training new personnel to crew them. Also, their presence will constitute a twofold buffer for the crewed ships, given the additional surveillance range and complications posed to an adversary's targeting calculus. Such is the importance of manned-unmanned systems integration that the USN's CNO declared it the one of the highest developmental priorities in the service.[11]

The Challenges

There are several caveats and obstacles to the vision of Manned-Unmanned Teaming coming to fruition, besides the obvious capacity problem. For one, the importance of defining the right composition of the new "hybrid" force (intended here as the combination of manned and unmanned weapon systems) is not to be underestimated. Achieving the right balance of unmanned platforms serving as intelligence gatherers, ballistic missile launchers or aerial refuelers will be just as critical in terms of capacity and capability as fielding the largest force possible. Subsequently, one issue to be reconciled is the limited interoperability between new (and expected) future-poised weapons systems and legacy systems still in operation. All NATO nations are dealing with budget pressures and ageing inventory, while striving to develop and operationalise new, more capable systems as replacements. As a consequence, one major challenge for Manned-Unmanned Teaming is the very coexistence of legacy and next-generation weapons systems. Unfortunately, no nation can afford to retire its entire inventory of legacy systems simply because they are less than ideal to partner with the newer generation of unmanned systems. Although bound to be mitigated over time as older systems are retired, the assertiveness of our competitors and adversaries leaves no space for inaction.

Another major impediment is the fact that current Command and Control (C2) systems are generally not optimized for the complexity and speed required by the envisioned scenarios. Moreover, adequate C2 structures either do not exist or require maturation. Analysts agree that future operations requiring a high level of coordination (as is the case for Manned-Unmanned Teaming) could prove vulnerable as a direct consequence of the steady increase in data consumption and reliance on long-range communications (satellite or undersea cable) for planning, execution, or assessment.[12] This is especially true when combined with the understanding

that future operations will likely happen in heavily contested, communications-degraded environments. While obstacles to real multi-domain planning are becoming apparent, there is a requirement to explore concepts to achieve the most effective outcomes.[13] Allies must define priorities, carefully explore the benefits and disadvantages of options, and consider which changes are most necessary and most urgent to current C2 constructs. Once that analysis is complete, nations can be assured that their investments of effort and resources do not go to waste when committing to rebuilding any C2 architecture.

Conclusion

The geopolitical picture in which NATO operates has dramatically changed in recent years, driving a paradigm shift from the post-Cold War anti-terrorism posture back to great power competition with peer or near-peer adversaries. Future allied operations will see the extensive, integrated exploitation of all five domains, with joint enablers like unmanned systems playing a key role in determining the success or failure of conflicts.[14] Manned-Unmanned Teaming will allow for a future force where the unmanned component constitutes a true *multiplier*, not just a substitute or an addition to the manned aspects of warfare. Emerging concepts point to a future where autonomy-enabled unmanned systems will be deployed both alongside and beyond manned platforms. These systems can act as additional carriers of sensors and weapons with the unique ability to conduct tasks in areas unreachable by a manned crew, either physically or from a risk-analysis point of view. These abilities will provide for a substantial capability leap with effects far greater than the sum of single contributions, while at the same time reducing unnecessary redundancies and risk. It is safe to assume that the implementation of unmanned systems goes hand in hand with the development of multi-domain concepts of operations. In this context, the importance of a robust C2 architecture linking together all domain actors, sensors, and shooters cannot be overstated. While the relevance of this dilemma has become apparent, its solution has not yet been identified. Greater effort is required to develop C2 systems capable of overcoming current complexity and speed limitations, to support the next era of multi-domain operations. Success in the future fight requires ingenuity, technological advantage, and the ability to expand and control the area of operations. In order to win that fight, NATO nations must now understand and embrace the concepts of, and commence investment in, Manned-Unmanned Teaming.

1 "Dull" as in repetitive tasks bound to lead to operational fatigue for manned crews (which also can best be addressed with automation) or high-endurance operations; "dirty" is used to describe those missions or tasks involving a high potential for loss of life or severe injury, including operations in potentially CBRN-contaminated areas.
2 I.e. with humans overseeing the course of decisions taken autonomously by the unmanned systems
3 Definition by the U.S. Army Aviation Center of Excellence (USAACE) - U.S. Army Aviation Digest, Vol.2/Issue 3, July-September 2014
4 What sealed the fate for the TDR and the first experiment of manned-unmanned teaming, despite its success in battle, were technical difficulties in developing the drone, a continued low priority given to the project, and the unrivalled U.S. air superiority in the Pacific. As the determination was made that more conventional weaponry would suffice in defeating Japan, the project was retired.
5 Joint Operations with Unmanned Aircraft Systems (UAS) and their Future Development, CJOS COE, 2020
6 Ibid
7 Manned-Unmanned Teaming in Joint Operations, CJOS COE, 2021
8 Ibid
9 Ibid
10 First appearing in December 2018, in "A Design for Maintaining Maritime Superiority, Version 2.0." https://cimsec.org/operationalizing-distributed-maritime-operations/
11 Memo announcing the launch of Project Overmatch, the USN's ambitious effort to build the future Naval Operational Architecture, the fundamental tool to support the Distributed Maritime Operations concept which in turn represents the service's effort to implement the U.S. DoD's Joint All-Domain Command and Control (JADC2) concept. https://news.usni.org/2020/10/27/navy-focused-on- strengthening-networks-to-support-unmanned-operations
12 Manned-Unmanned Teaming in Joint Operations, CJOS COE, 2021
13 Multiple Dilemmas for the Joint Force. Joint All-Domain Command and Control, RAND, 2020
14 Manned-Unmanned Teaming in Joint Operations, CJOS COE, 2021

COMMAND & CONTROL OF MULTINATIONAL MARITIME FORCES: CHALLENGES WITH CONDUCTING OPERATIONS IN THE HIGH NORTH

CDR (USN) SHAWN NEWMAN

Allies are advised to invest in technologies in two ways: maritime units should be capable of tapping into multiple C2 inputs in the north, and governmental support to dedicated and secure communications systems should remain a priority.

NATO must maintain modern, credible, rapid response joint forces who are able to sustain a battle winning edge in the most demanding operational circumstances. The maritime component, in particular, may find itself securing sea control, delivering interoperable maritime and amphibious strike actions, providing a base of operations at sea, and even exercising coherent Command and Control (C2) while interoperating with non-NATO navies and civilian organizations. In essence, it must be able to deliver decisive effect on, under, and above the sea.

The emerging security conditions for the early 21st century have placed new demands on NATO. The need to protect its broader security interests and contribute to international stability by expanding its influence and presence on the international stage remains extant. With ever advancing threats from near-peer adversaries like China and Russia, members of the Alliance have been forced to not only prepare for potential armed action against these highly capable militaries, but are also recognizing the need to pay particular attention to portions of the globe that may have been given little consideration until relatively recently.

One region that is garnering increased attention is north of the Arctic Circle. Although NATO has been increasingly focused on the Arctic over the last number of years as Russia has continued to militarize the region, recent events add a new impetus to the need for the Alliance to be able to operate effectively in the High North. The melting of the polar icecaps, close proximity of the eight Arctic coastal nations[1] (which includes Russia), and sea routes that are opening for longer periods each year, have made it even easier for potential adversaries to get close to Allies.[2] As our collective armed forces focus more closely on the Arctic, the unique challenges as to how commanders will exercise C2 of assigned units becomes more apparent.

There are a number of changes to standard processes when it comes to C2 in the north; for example, the combined force must resolve which mediums are compatible for high bandwidth communications as most standard Geosynchronous Satellite networks have limited, or no, availability in the Arctic. Furthermore, unconventional systems will have unique communications capabilities and limitations when used by the remote commander. Intermittent communication due to weather effects, such as the impact of precipitation on Ka Band, is one obvious limitation. The following has been asked on multiple occasions, "is C2 of combined multinational maritime forces achievable in the High North?"[3] For NATO, however, there must be no question as to 'if' C2 can be achieved; rather, the question that must be answered is how can the C2 of combined maritime forces in the High North best be achieved? This article serves to inform NATO by exploring C2 structures, technologies, and communications capabilities for Arctic operations.

Command and Control

Answering these questions will require two parts; first, an understanding of what is implied with the intent of C2 of multinational forces as this has a different meaning to some nations compared to others. For example, one nation may endorse the idea of mission command, where others may approach operations with centralized control and decentralized execution.[4] The second part will examine some of the communications capabilities currently available with a basic understanding of how these may be leveraged to achieve a reasonable approach to C2 in the High North. C2 is generally considered to be a combination of "organizational and technical processes, employed by personnel through physical and information systems, in order to solve problems and accomplish tasks in support of a larger mission; the expression is often in reference to military structures and procedures."[5] However, the definition for C2 is not universal and has various changes depending on the source; for example, a NATO definition

for C2 is the "exercise of authority and direction by a properly designated individual over assigned resources in the accomplishment of a common goal."[6] Similarly, an Australian Defence Force definition, akin to NATO's, highlights that C2 is the system of "empowering designated personnel to exercise lawful authority and direction over assigned forces for the accomplishment of missions and tasks."[7] Regardless of how C2 is defined, there are a few underlying commonalities amongst the various definitions. Primarily, there is the designation of authority, the assignment of resources (personnel, equipment, supplies, etc.), and the accomplishment of a mission and/or task. While this may be seemingly simple, how the Alliance or an individual nation approaches C2 can be very different. These differences can lead to complexities or incompatibilities in areas of limited use; for example, potentially high-bandwidth operations such as those north of the Arctic Circle. A group commander operating in the High North who is provided with mission command may easily exercise C2 over assigned units during periods of limited connectivity to a remotely located fleet commander. Conversely, a group commander operating in the Arctic who is provided regular direction from a remote centralized fleet commander may find exercising control over assigned units and tasks difficult if communications with fleet staff are limited. Therefore, the communications systems available, the capabilities and limitations of those systems, and the individual command elements willingness to delegate authority may determine the success or failure of a multinational maritime taskforce operating north of the Arctic Circle.

The Technology and Capabilities

When it comes to C2 in nearly any context, the topic cannot be discussed without understanding how communications will be achieved, especially as today's military is increasingly reliant on network-connected platforms and weapons systems. In modern operations, where common operating pictures and data sharing have become staples necessary to keep unit, group, fleet, and theater commanders all on the same page, the extensive use of data links and high-bandwidth communications is required. Furthermore, while many militaries may practice operations in a denied, degraded, intermittent, and limited (DDIL) bandwidth environment, there is no denying that effective and consistent communications provide a tactical and strategic advantage to warfighters.[8] This data traffic primarily requires the use of satellite communications, especially in the context of the maritime domain and mobile units; the satellites typically providing communications services are in a fixed Geosynchronous Earth Orbit above the equator. Their stationary placement creates a limitation on use by units operating at a latitude of N 70° or further north as communications from these satellites degrades due to a low look-angle to the satellite above the horizon.

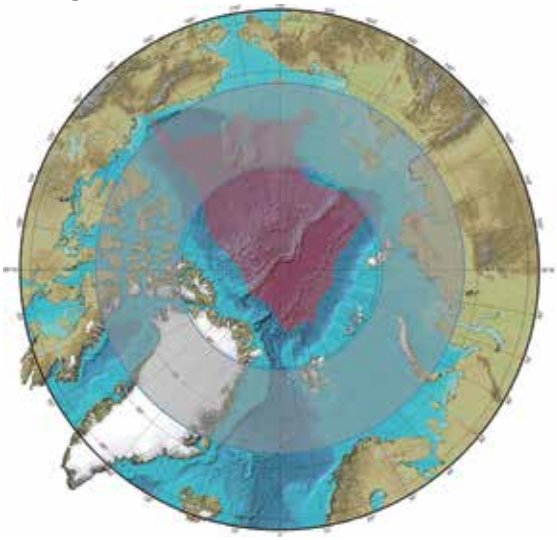


Figure 1: A view of the North Pole from above. The shaded area from N 72°-79° shows where geosynchronous satellite broadband coverage diminishes towards zero. The rate of loss with latitude depends on the weather, size of the antenna, height of the antenna above the surface, and the horizon.[9]

The loss of geosynchronous satellite coverage for high-bandwidth communications creates the need for unique communications capabilities in order to operate in the High North while keeping fleet or regional commanders informed. One relatively new signal processing capability has enabled data connections of over 150Kbps through the use of an overlapping band between the Medium Frequency (MF) and High Frequency (HF) bands, operating between 1.5-30MHz. While somewhat constrained, this communications medium has supported limited internet protocol (IP) services like chat, email, and small file transfers. Unfortunately, despite the HF band's advantage of long-range communications due to radio waves being able to be reflected by the ionosphere, it is still prone to rapidly changing transmission conditions that naturally occur in the Arctic like skip zones, latency, and electromagnetic interference (EMI). Therefore, realistic data rates and effective ranges of communication are significantly lower.[10] Some of these disadvantages have been mitigated with the development of cognitive Software Defined Radio (SDR) waveforms. The result is a reduced link connection from minutes to seconds, improved overall link quality, reduced latency, and reduced impacts from EMI.

An alternative communications platform, often used during times of limited connectivity, is the Iridium satellite constellation. With more than seventy satellites in low-earth orbit (LEO), the Iridium system

has achieved global earth coverage and can be used while operating in the Arctic.[11] Historically, Iridium was a voice-only net until 2017 when the company began launching a second-generation constellation, called Iridium-NEXT, that became operational in 2018 and incorporates features such as data transmission that were not in the original design.[12] [13] [14] [15] With the Iridium satellites operating in a low-earth orbit (an altitude of approximately 780km compared to nearly 36,000km for GEO), they provide better signal strength and lower latency (due to a shorter transmission path) while simultaneously utilizing a smaller antenna and having a lower power demand when compared to traditional satellite communications.[16] Additionally, Iridium operates in the Ultra-High Frequency (UHF) L-Band (1-2GHz) which is able to penetrate clouds, fog, rain, and storms making the system more resilient to weather effects when compared to most traditional GEO communications systems.[17] However, the system is also not without fault as there are recorded cases of interruptions to the service lasting several minutes which could have significant impacts during combat depending on the C2 structure.[18]

Similar to Iridium, private companies like SpaceX and OneWeb have also developed and launched hundreds of LEO satellites as a means to provide broadband coverage to users around the world.[19] SpaceX has named its satellite constellation Starlink and has garnered particular attention by the U.S. military as it looks for ways to solve the communications gaps in the Arctic.[20]

Another dedicated high-bandwidth service for operations in the High North is the Enhanced Polar System (EPS). The EPS provides continuous coverage in the Arctic that is jam-resistant and offers tactical and strategic communications in support of operations. Additionally, the system provides an update to Extremely High Frequency (EHF) and Advanced EHF satellite communications in the High North and serves as another next-generation satellite communications system, replacing the still in-service low-bandwidth Interim Polar System (IPS).[21] While EPS is a dedicated communications medium for operations in this region, the satellites do have some disadvantages. One drawback is that the satellites operate in a Highly Elliptical Orbit (HEO) which supports a long dwell time (approximately 12hrs) over the earth's pole at an altitude similar to satellites in a GEO orbit when at their peak distance from the earth. Similar to communications using GEO satellites, this high altitude results in added latency and signal degradation due to distance which is partially mitigated using the EHF spectrum, but does come at a cost of weather susceptibility due to the extremely short wavelength of the transmission being affected by rain, fog, clouds, or other forms of precipitation. Finally, EPS only has three satellites in orbit (two in service to allow for 24-hr coverage and one in-flight spare) which allows for potentially limited availability and vulnerability should they be targeted by an enemy.

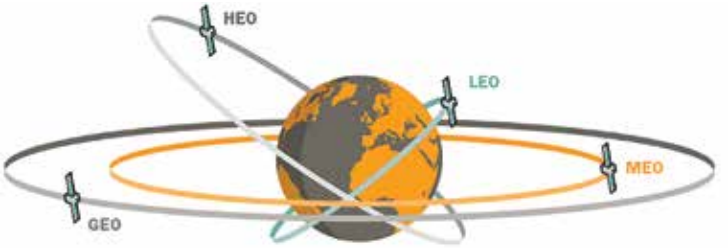


Figure 2: Visual representation of the four main types of orbits; Highly Elliptical Orbit (HEO), Geosynchronous Earth Orbit (GEO), Medium Earth Orbit (MEO) and Low Earth Orbit (LEO).[22]

Lastly, a commercial terrestrial telecommunications medium is another potential option when it comes to mobile C2 networking. While not preferred as it can be considerably expensive to use as a commercial service, it does present an advantage as seven of the eight Arctic nations are either members of NATO or NATO-friendly and have invested considerable resources for their residents living in the High North. With variations in population densities across the Arctic, Finland, Iceland, Norway, and Sweden often have a broad availability of telecommunications infrastructure and services in the region.[23] They are among the NATO membership or Partnership for Peace nations that are more populated in the far north compared to Canada, Greenland, and the United States (Russia is the eighth Arctic nation and it has areas of both sparse and dense populations). Norway, for example, was one of the first countries to commercially deploy fourth generation (4G) Long Term Evolution broadband cellular technology in 2009 and has built up the infrastructure within the country, offering considerable coverage for residents north of the Arctic Circle.

Figure 3: Cellular coverage map of Norway's largest cellular provider, Telenor.[24]

Some additional good news for those in the north is that a 4G wireless cellular standard was defined by

the International Telecommunication Union (ITU) and specified the key characteristics of 4G communications, including transmission technology and data speeds.[25] [26] As cellular technology has developed, each generation of the equipment has introduced increased bandwidth speeds and network capacity; as such, 4G systems are capable of speeds up to 100 Mbps; and, depending on transmission power and antenna size, a typical cellphone has enough power to reach ranges of 45 statue-miles away.[27] Some shipboard applications conducted by the U.S. Navy have demonstrated 4G communications at ranges of 20 nautical miles; although, ships are somewhat limited due to the close proximity to other communications antennas and limited shipboard space for installation.[28] [29] With additional development, 4G technology could be integrated into shipboard systems and use existing antennae and RF paths. The practical applications of this technology and the application of these standards bode well for NATO countries. Norway, for example, could have a continuous connection whilst transiting through the fjords where, in the past, satellite communications have proven particularly difficult when in transit due to the high sided mountainous geography blocking the satellite signal.

Conclusion – C2 in the North

When it comes to operating mobile platforms in the High North, there is no 'one size fits all solution'. Can C2 for units operating north of the Arctic Circle be effective? Yes; however, it will depend greatly on the structure and delegation of authorities as well as the communications capabilities available. At a minimum, C2 structures will require some degree of delegated authority in order to enable local commanders to effectively manage assigned forces and accomplish prescribed missions. One thing is for certain, there will be impacts to communications, so commanders will need to think differently. Arctic weather and magnetic pole effects are unpredictable and satellite service capabilities supporting the Arctic region are varied, but each come with limitations. Therefore, NATO would be best advised to take a hybrid approach to accomplishing C2 for units operating in the Arctic. Being able to quickly and seamlessly use various, and potentially unfamiliar, communications mediums in order to conduct C2 and keep remote commanders informed will provide the tactical advantage. Allies are advised to invest in technologies in two ways: maritime units should be capable of tapping into multiple C2 inputs in the north; and governmental support to dedicated and secure communications systems should remain a priority. The protection and freedom of movement in the northern flank depends on it both on, under, and above the sea.

1 The nations include Canada, Greenland, Iceland, Norway, Sweden, Finland, Russia, and the United States

2 Bill Eidson (Jul 2019). "Navigating the Arctic's Communications Challenges." Mitre: https://www.mitre.org/publications/project-stories/navigating-the-arctics-communications-challenges

3 Arctic Council. https://arctic-council.org/

4 Ross Pigeau; Carol McCann (Spring 2002). "Re-conceptualizing Command and Control." Canadian Military Journal. 3 (1): pp. 53–63.

5 Vassiliou, Marius, David S. Alberts, and Jonathan R. Agre (2015). "C2 Re-Envisioned: the Future of the Enterprise." CRC Press; New York; p. 1

6 Neville Stanton; Christopher Baber; Don Harris (1 January 2008). "Modelling Command and Control: Event Analysis of Systemic Teamwork." Ashgate Publishing, Ltd. 17 May 2016.

7 "ADDP 00.1 Command and Control." Commonwealth of Australia. 27 May 2009. pp. 1–2.

8 Schradin, Ryan (12 Jun 2020). "Connectivity in the Cold – SATCOM for Arctic Circle Operations." The Government Satellite Report. https://ses-gs.com/govsat/defense-intel/connectivity-in-the-cold-satcom-for-arctic-circle-operations/

9 Arctic Council Task Force on Telecommunications Infrastructure in the Arctic (2017). "Telecommunications Infrastructure in the Arctic: A Circumpolar Assessment." Arctic Council Secretariat: p. 42.

10 Ibid: p. 46.

11 Iridium Museum. https://www.iridiummuseum.com/

12 Peter B. de Selding (29 Apr 2016). "First Batch of Iridium Next Satellites good to go for July SpaceX Launch." Space News: https://spacenews.com/iridium-says-2nd-generation-constellation-ready-to-launch-with-spacex-starting-in-july/

13 GPS World Staff (17 Jan 2017). "SpaceX Launches First Batch of Iridium NEXT Satellites." GPS World: https://www.gpsworld.com/spacex-launches-first-batch-of-iridium-next-satellites/

14 Jeff Foust (25 Jun 2017). "SpaceX Launches Second Batch of Iridium Satellites." Space News: https://spacenews.com/spacex-launches-second-batch-of-iridium-satellites/

15 Caleb Henry (9 Oct 2017). "SpaceX launches Third set of Iridium Next Satellites." Space News: https://spacenews.com/spacex-launches-third-set-of-iridium-next-satellites/

16 Iridium Network. https://www.iridium.com/network/

17 Ibid.

18 "Arctic Poses Communications Challenges." The European Space Agency: https://www.esa.int/Enabling_Support/Preparing_for_the_Future/Space_for_Earth/Arctic/Arctic_poses_communications_challenges

19 Nathan Strout (12 May 2020). "SpaceX Could Fill the U.S. Military's Arctic Communications Gap by the End of this Year." Defense News: https://www.defensenews.com/smr/frozen-pathways/2020/05/11/spacex-could-fill-the-us-militarys-arctic-communications-gap-by-the-end-of-this-year/

20 Ibid.

21 Enhanced Polar System. Northrop Grumman. https://www.northropgrumman.com/space/enhanced-polar-system/

22 Everything RF Editorial Team. "What is a Highly Elliptically Orbit?" Everything RF: https://www.everythingrf.com/community/what-is-a-highly-elliptically-orbit

23 Arctic Council Task Force on Telecommunications Infrastructure in the Arctic (2017). "Telecommunications Infrastructure in the Arctic: A Circumpolar Assessment." Arctic Council Secretariat: p. 429

24 "Network Coverage: Cellular Data Networks in Norway." nPerf: https://www.nperf.com/en/map/NO/-/164116.Telenor-Mobile/signal/?ll=64.66151739623564&lg=15.4687500000000002&zoom=4

25 "Requirements Related to Technical Performance for IMT-Advanced Radio Interface(s)." ITU-R: http://www.itu.int/pub/R-REP-M.2134-2008/en

26 "ITU World Radiocommunication Seminar Highlights Future Communication Technologies." International Telecommunication Union: https://www.itu.int/net/pressoffice/press_releases/2010/48.aspx

27 Bert Markgraf. "How Far Can a Cell Tower Be for a Cellphone to Pick Up the Signal." Chron: https://smallbusiness.chron.com/far-can-cell-tower-cellphone-pick-up-signal-32124.html

28 Adam Stone (12 Feb 2016). "Navy Rethinks How to Bring 4G LTE to sea." C4ISRNet: https://www.c4isrnet.com/show-reporter/afcea-west/2016/02/12/navy-rethinks-how-to-bring-4g-lte-to-sea/

29 John Konrad (4 Jun 2012). "U.S. Navy Ships to Get 4G LTE Broadband – Will..." gCaptain: https://gcaptain.com/navy-ships-4g-lte/

INFORMATION SHARING IN THE MARITIME ENVIRONMENT AND DEVELOPING A 'NEED TO SHARE' CULTURE

WO1 STEPHEN SCOTT, RM

NATO must assume the responsibility to ensure that the information exchanged between allies is respected and protected.

Sharing Information at Sea

The advancements in maritime information sharing parallel the course of nautical history and development itself. Until the discovery of radio waves, maritime communications were limited to visual and audio mediums only. Early examples of visual communications were simple channel markers to guide ships into port. Eventually, the advent of lighthouses extended the visual range beyond a vessel's 7-10 miles limit of view. One of the most famous examples of this advancement was the third century BC lighthouse in Alexandria, which was the tallest structure in the world for many centuries. Believed to be visible up to 28 miles out to sea, this ancient wonder's sole purpose was to guide trade safely into the city.

Fig 1. Artist depiction of the Lighthouse in Alexandria[1]

Innovations such as markers and the ability to navigate more effectively fueled maritime exploration. In turn, globalization expanded and the information necessary to coordinate naval traffic increased. One of the first methods used to exchange information at sea from a distance was the signal flag. Flags became the primary means to share information between vessels causing a necessary codification of their use. In 1855, the first international code system for flags was drafted[2]. Although still a method of communication between ships today, signal flags paved the way for more advanced technology. Eventually we learned to exploit radio waves, progressing from Morse code to voice and data capabilities over the air to navigation though satellite global positioning. Many capabilities that were developed over the years remain in force for safety reasons. For example, the Global Maritime Distress and Safety System (GMDSS) is a globally recognised standard under the SOLAS Convention of 1974[3] and is mandatory for ships at sea. However, when it comes to sharing information on military networks with allies on the oceans, the levels of cooperation are a different matter.

Despite centuries of multinational partnerships and technological developments, there are still obstacles to achieving modern day interoperability.

Why Don't We Share?

The primary reason nations don't share is because of Operational and National security. Combined operations offer clear mutual advantages to the nations involved but, for many nations, the majority of operations and exercises are conducted unilaterally. For example, a ship's deployment may include a joint exercise, but will not necessarily sail with another nation as a matter of course. This is particularly the case in larger nations with a heavier global footprint that have interests and obligations in other smaller nations. During these national exercises and operations, it is important to protect the tactics, techniques, and procedures that are being trained, because interception and exploitation of secure transmissions by our enemies during real-world operations could be the difference between victory and defeat.

Information security is often a high priority during the design phase of communication systems, meaning that technical interoperability considerations often take a back seat. As a result, the technical process for releasing information is often cumbersome and time consuming, even after overcoming the administrative hurdles to authorize the release of information. Compounding these obstacles, there is a tendency to take a conservative approach to classification of data. Users of classified information often feel that it is better to over protect rather than unwittingly release sensitive information.

This approach is motivated by a fear of career-ending punishments for violation of strict information sharing rules. In addition, improper application of the 'NOFORN' label has become normalized due to lack of knowledge and training on accurately classifying information for dissemination between allies. This was highlighted by Lt Gen. Ben Hodges, Commanding General of U.S. Army Europe, who stated, "A good portion of the information classified as Secret NOFORN or Secret doesn't need that classification. It makes it very difficult to operate collaboratively in a multinational environment. Unless you're at Fort Irwin, a training facility for Army electronic warfare forces, you're never going to be by yourself; you're always going to be with *allies.*"[4]

So, What Has Changed?

There was always a number of combined operations with a requirement for some form of interoperability; however, on September 11, 2001, everything changed. After the terrorist attacks in New York, the U.S. and its allies declared a global war on terror and much of the effort was centred around Afghanistan. With over 50 nations involved, and a multinational force numbering over 132,000 troops at its peak in 2011[5], the 'need to know' gave way to the 'need to share'. In the early days, interoperability was greatly limited. Much of the information that needed to be moved between systems could only be done by physically copying to a physical disk and importing. This practice became known as 'Sneaker Netting', as you had to walk the information from one computer to another. Moving data in this way was inefficient, time consuming and begged for a better solution. In January, 2010, the Commander of the International Security and Assistance Force (COM ISAF) directed that all coalition networks within ISAF be federated into a single network access. This concept became the Afghan Mission Network (AMN).

"Coalition forces within Afghanistan cannot communicate effectively and share theatre related operational Commander's guidance, information and intelligence. These communication gaps increase risks to life, resources, and efficiency." - GEN Stanley A McChrystal, [then] COMISAF

Providing security alongside Afghan National Army in Nuristan province, 2010. Courtesy of U.S. Army.

The maritime environment has also seen the introduction of multinational interoperability efforts. A good example of the "need to share culture" in the maritime domain is Task Force (TF) 150, which was tasked to undertake counter terrorist operations at sea in the wake of 9/11. TF 150 participation has included Australia, Canada, Denmark, France, Germany, Italy, Netherlands, New Zealand, Pakistan, Spain, Saudi Arabia, the United Kingdom and the United States.[6] Since the drawdown of Afghan operations, a rise in aggression from other world powers has led nations to closely consider the necessity to operate more cohesively. In March 2021, the Dwight D. Eisenhower Carrier Strike Group conducted an interoperability exercise in the Mediterranean Sea with the Hellenic Armed Forces utilizing NATO operations and tactical procedures. Rear Adm. Scott Robertson, Commander, Carrier Strike Group TWO stated, "We are stronger when we work alongside our allies and operations like this, integrating our maritime forces help to ensure free and open conditions at sea."[7]

We Still Operate, So What's the Problem?

Lack of sharing, particularly in a hostile environment, can have devastating and fatal consequences. Combined operations often rely heavily on information from each participating nation to enhance overall situational awareness and gain a clearer understanding of the operating environment. When information sharing is restricted, allied forces may be unable to see threats and friendly troop positions, greatly increasing the risk of enemy engagement or friendly fire. Furthermore, a lack of sharing and the technical ability to share, make a combined joint operation slow and inefficient. Technical inefficiencies include the need to 'airgap', or manually move information between systems, which creates a cumbersome and time-consuming process that could also limit the type of information that can be shared. For example, much of the coordination in the modern battlespace is conducted using chat service, a function that would not be possible without an authorized information sharing solution. One could imagine the peril and inefficiency if a force was tasked to conduct risky reconnaissance missions to gather intelligence that is already available.

Sharing: The Technical Solution

As previously mentioned, the war in Afghanistan set a new standard for interoperability. It provided commanders with an unprecedented amount of tactical intelligence; changing the perception of the quantity of information that a commander requires to plan and operate on the frontlines. After combat operations in Afghanistan drew to a close, planners struggled with how to deliver an equivalent level of granularity over restricted bandwidth. Furthermore, planners became accustomed

to the 'need to share' culture of operations in Afghanistan, leading them to pursue equivalent levels of interoperability in other areas of operation around the world. Fortunately, there are a number of systems already in place that could offer a solution.

Combined Enterprise Regional Information Exchange System (CENTRIXS) is a U.S. capability created in 1999 and quickly developed after the 9/11 attacks as a coalition data sharing network. CENTRIXS consists of a combination of multilateral and bilateral virtually separate networks, which support multinational theatre-specific operations. CENTRIXS' advantages are its separate networks, referred to as enclaves, which are built to the same architectural design, yet not interconnected. This type of design makes the system a more cost effective and secure option but does require a relatively significant level of planning and permissions to operate. As a result, CENTRIXS is often utilized as an information sharing system for more ad-hoc use.

Another notable current solution is the NATO Secret Wide Area Network (NSWAN). NSWAN is a single network that offers all the capability that most forces require. However, as a NATO-owned system, NSWAN is limited to only NATO countries with a Memorandum of Understanding in place. NSWAN is also relatively expensive to operate and maintain.

The Battlefield Information and Collection Exploitation System (BICES) offers the advantage that it can extend beyond NATO to other partnering nations and allies. Primarily developed for the U.S. Air Force, BICES has yet to be as widely recognized and adopted as other similar capabilities.

Finally, following on from the success of the AMN Concept, NATO ACT is developing the Federated Mission Networking (FMN) system. FMN is a similar principle to AMN in so much as it links disparate systems together, using mission configurable open architecture and multinational agreement of using common technical standards to support C4ISR[8].

Fig 2. Conceptual diagram of the AMN. Courtesy of NATO.

Developing The 'Need To Share' Culture

Nations can spend as much money and time on developing the most innovative and ingenious methods for technical information sharing that science will allow, but if the information owner chooses not to release the information, they may as well not be connected. As a result of years of needing to protect networks from any foreign intrusion, there is a cultural mindset that needs to be addressed. Flag Officers have said that excluding allied nations from information needs to be the exception rather than the default. Unfortunately, this has yet to be engrained into the psyche of information owners who continue to maintain a more cautious approach to releasing information to partner nations. An overly cautious approach is equally as damaging to the advancement of collaborative work as not having a technical solution in place. Nations can only improve by looking at the ways in which they protectively mark information and introduce a new method of education and processes.

The Way Forward

The technical aspects of information sharing are becoming better understood every day, moving ever closer towards seamless information exchanges. At present, capabilities exist that allow military vessels to share information with their allies, securely and instantly, anywhere in the world. Unfortunately, not all allies are able to take advantage of these capabilities. Military effects at all levels are greatly diminished without the ability to operate in a fundamentally collaborative space. Engendering a "need to share" culture is the first step toward allied interoperability in any military operation. Through working together, 'NOFORN' markings will continue to be scrutinized, ensuring that it will no longer be the default setting. The alliance should continue investment in federated systems, increasing its understanding of how to use them and the benefits they bring.

Technical, procedural, and cultural aspects of interoperability and collective C2 should be treated as vital components of every exercise and operation. NATO, in particular, must assume the responsibility to ensure that the information exchanged between allies is respected and protected. By sharing best practices and using mutually agreed upon standards, NATO can continue to improve trust and assurance in our combined joint warfighting forces and seize the advantage on the battlefield.

1 The-lighthouse-of-Alexandria (yesofcorsa.com)
2 Finally published in 1857. Brief history of the International Code of Signals. (navalmarinearchive.com)
3 Safety of Life at Sea - Global Maritime Distress and Safety System (GMDSS) | Federal Communications Commission (fcc.gov)
4 Info-sharing hurdles hinder alliance partnerships (c4isrnet.com)
5 Afghanistan troop numbers data: how many does each country send to the Nato mission there? | News | theguardian.com
6 CTF 150: Maritime Security – Combined Maritime Forces (CMF)
7 USS Dwight D. Eisenhower Conducts Interoperability Exercise with Hellenic Armed Forces > U.S. Naval Forces Europe-Africa / U.S. 6th Fleet > News Display (navy.mil)
8 Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance

BURST THE A2/AD BUBBLE: FOSTER ALLIED STAND-IN FORCES

CDR (USN RET.) JOSH HEIVLY

Cooperative development partnerships should be formed to further the establishment of full-capability stand-in forces.

The United States relies on freedom of maneuver on the seas to create deterrence and respond to crises. Anti-Access/Area Denial (A2/AD) systems were developed by competitors to forestall timely responses to short term military adventures aimed at delivering a fait accompli outcome. Recent years have seen the rise of operational concepts designed to enable U.S. forces to operate in the face of these threats. Called stand-in forces, they propose to use a dispersed force connected by a robust C2 network, sharing sensors and massing fires to deny the seas to potential adversaries and hold their forces at risk.

The USMC and U.S. Army are in the process of delivering forces purpose-built for this task, but for these to be relevant they must either be forward based or speedily deployed. For deterrence by denial to be effective, Allied stand-in forces, similarly equipped, trained and organized, are required. NATO nations are especially well-positioned to take full advantage of these approaches and refine them accordingly.

Current U.S. Efforts

Since the 2010 release of the Joint Operational Access and AirSea Battle concepts, the U.S. Department of Defense has wrestled with ways to counter A2/AD threats. This work culminated in the 2018 National Defense Strategy, which made explicit an emerging deterrence by denial strategy,[1] which seeks to convince prospective opponents that their goals are unattainable or unlikely to succeed.[2] In the past few years, each of the services have developed concepts designed to operationalize this approach. Two of these, the Marine Corps' Expeditionary Advanced Base Operations (EABO) and the Army's Multi-Domain Operations (MDO), both propose to use forward-deployed land forces to contest sea spaces within competitor Weapons Engagement Zones (WEZs).

Although advanced base operations have been a part of the Marine Corps' repertoire since the turn of the last century, [3] these ideas received renewed emphasis in the middle of the last decade when the implications of Chinese and Russian A2/AD capabilities became apparent. Early work done in 2013-14 at the Marine Corps' Advanced Studies Program[4] influenced the progression of the concepts arriving in the following years. All were designed to be complementary to the developing Distributed Maritime Operations concept,[5] in keeping with a vision in which the Marines would support the Navy by occupying key maritime terrain and executing various mission sets, including ASW, strike, logistics and more. It was with the release of the 2019 Commandant's Planning Guidance that the Marine Corps began in earnest to re-structure and re-calibrate in accordance with these concepts. The current vision defines EABO as

> ...the employment of mobile, low-signature, persistent, and relatively easy to maintain and sustain naval expeditionary forces from a series of austere, temporary locations ashore or inshore within a contested or potentially contested maritime area in order to conduct sea denial, support sea control, or enable fleet sustainment.[6]

In 2020 the Marine Corps began adapting the 3rd Marine Regiment in Hawaii in a multi-year project that will transform it into a Marine Littoral Regiment (MLR) by early FY 2022.[7] Two additional MLRs may follow later in the decade and will also be based in the Pacific. With an end-strength of around 2,000,[8] each will notionally comprise a headquarters, a Littoral Combat Team built around a Marine infantry battalion, a Littoral Logistics Battalion and a Littoral Antiair Battalion (air defense plus air C2 and FARPs).[9] Fires units will be attached to the MLR in the form of HIMARS batteries, eventually to be replaced by Remotely Operated Ground Unit Expeditionary (ROGUE) vehicles (based on the JLTV) armed with the Kongsberg/Raytheon Naval Strike Missile (NSM)

and later possibly also the Tomahawk-based Ground Launched Cruise Missile.[10] Each MLR may also employ a company of Long Range Unmanned Surface Vehicles[11] operating 11-meter autonomous boats in swarms, firing loitering munitions.[12]

Similarly, the Army began to explore the idea of a Pacific sea denial role in the middle of the last decade. The central idea of MDO is for Army forces, as part of a larger Joint force, to solve the problem of layered standoff (i.e., A2/AD) through the continuous integration of all domains of warfare in support of deterrence and competition, transitioning when required to conduct operations to

> ...penetrate and dis-integrate enemy anti-access and area denial systems; exploit the resulting freedom of maneuver to defeat enemy systems, formations and objectives and to achieve our own strategic objectives; and consolidate gains to force a return to competition on terms more favorable to the U.S., our allies and partners.[13]

This is achieved in MDO through the combination of a calibrated force posture (forward positioning and strategic maneuver), multi-domain forces able to operate in contested spaces against a near-peer adversary, and the continuous convergence (integration) of effects in all domains to achieve overmatch.[14] Interestingly, unlike EABO, in which the need for interoperability and integration with Allied and partner nations is acknowledged, MDO seeks to position the Army as the primary vehicle for security cooperation with Allied and partner nations in forward areas.[15]

The first Multi-Domain Task Force (MDTF) was established at Joint Base Lewis-McChord, Washington, in February 2021,[16] to be followed by up four more MDTFs stationed in the Indo-Pacific, Europe, and the Arctic, and one positioned for global deployment.[17] The proposed design for the MDTF includes:

- a Strategic Fires Battalion;
- an Intelligence, Information, Cyber, Electronic Warfare, & Space (I2CEWS) Battalion;
- an Air Defense Battalion; and
- a Brigade Support Battalion.[18]

The Strategic Fires Battalion will deliver the MDTF's striking power in the form of a HIMARS Battery, a Mid-Range Capability Battery and a Long-Range Hypersonic Weapon Battery. Weapons for all three are currently in development. The Army intends to equip its HIMARS Batteries with the Precision Strike Missile, while the Mid-Range Battery will employ Tomahawk and SM-6 variants. The Long-Range Battery will fire the joint Army-Navy hypersonic missile. All of these are due to enter service in 2023.[19] Army watercraft will be used to rapidly deploy the MDTF across the theatre "...to support regional alliances and reinforce the existing security architecture," as demonstrated during exercise Valiant Shield in late 2020.[20]

Analysis

While similar in several respects (e.g., air defense and support battalions, long-range fires), the proposed designs for the MLR and MDTF differ significantly. In the MLR we find a battalion-sized Littoral Combat Team that will operate various types of expeditionary advanced bases, while the MDTF's I2CEWS battalion offers considerable multi-domain capability. The MLR's use of drones will enable considerable savings in manning, while the MDTF looks to be manpower intensive, which will reduce its ability to frustrate targeting through dispersal. The MLR is oriented specifically around supporting naval operations, while the MDTF is packaged as an equal contributor to the joint force.

Unfortunately, both concepts share a common, underlying weakness that cannot be addressed by the services themselves: lack of assured access, basing and overflight. A credible forward defense is required if deterrence by denial is to be established,[21] but this hinges upon the consent of Allied nations to host these forces on their soil, which is by no means guaranteed. "Past research has shown that partner decisions to allow access will likely be contingent on the scenario and the broader political relationship between the United States and each host country."[22] The presence of American stand-in forces in contested areas will almost certainly elicit hostile responses from Russia and China towards their neighbors, many of whom will be loath to provoke them unnecessarily.[23] As noted by retired Lieutenant General Thomas Spoehr, "Today, there is probably not

USS Harry S. Truman. Courtesy of U.S. Navy.

one of our regional partners in the first island chain that would be willing to base Army — or any other service — long range strike missiles in their country."[24] NATO nations may be more amenable due to the long-standing nature of the Alliance and ongoing Enhanced Forward Presence rotations, although EABO and MDO are primarily focused on the Western Pacific and China.

The MDTF's planned basing scheme may offer at least a partial solution, but they will still be restricted to U.S. territory or terrain owned by our closest Allies, possibly hundreds or even thousands of miles away (e.g., Guam or Hawai'i) from contested spaces like the First Island Chain. This problem may be further exacerbated by the now well-established U.S. preference for rotational (vice forward based) forces in which only a fraction of each unit is maintained in-theater at any given time.

Without significant forces operating forward, there may be a limited window to rapidly deploy in time to head off a conflict or contribute to its resolution. The mere existence of U.S. stand-in forces may prompt adversaries to shorten their operational timelines and attempt to achieve objectives before they can be introduced. Without a persistent, credible presence, stand-in forces may pose a potential threat once deployed but their ability to achieve desired assurance and deterrence effects, or arrive in time, may be in doubt. The lighter MLR may ultimately have a comparative advantage in terms of response time, but it may not matter.

The Allied Contribution is Critical

Allied nations along the frontiers of potential adversaries represent the equity of forward engagement, already living and operating in the shadow of A2/AD. They enjoy an inherent "home court" advantage, with all of the advantages that U.S. stand-in forces lack. No matter how well trained or lavishly equipped, the most appropriate inside force, the one best-suited to disperse and operate in any country, is the one created by and operated by the nations themselves.

Missile launch from USS Sterett. Courtesy of U.S. Navy.

To deter and defend against potential aggression, Allies should consider moving away from current maritime structures in which resources are focused on a few blue water units and instead look toward a force designed to "[d]istribute offensive capability geographically."[25] This can be done by reapplying resources to develop an agile, resilient maritime defense with nodes across all domains. A heavily armed, hard-to-find, hard-to-kill networked fires complex would challenge the underlying calculus for any attempt to prevent intervention via A2/AD capabilities; it would "...open battlespace and enable concealment and deception in order to inject uncertainty and complexity into an adversary's targeting."[26] Such a force would be ideally designed and positioned to integrate with and be reinforced by U.S. and Allied expeditionary units.[27]

NATO's forward points of contact with Russia offer the most fertile ground for capitalizing on this approach. For example, the three Baltic nations, deep within Russian WEZs, could use their limited resources to each field a battalion centered upon a fires company of trucks and boats armed with NSMs, supported by ISR and logistics companies designed to distribute these capabilities across each nation's territory. This would pose a persistent, difficult-to-counter threat to any surface ships in the Baltic Sea. If equipped with a dual-purpose missile like the currently in development Joint Strike Missile,[28] they would be able to strike both land and maritime targets, multiplying their deterrence value accordingly. Similar forces could be developed by Allied and partner nations in the High North and Black Sea regions, to great effect.

While several Western European nations use amphibious landing forces, only a few maintain units dedicated to fighting in the littorals. Italy's Lagunari Brigade, Norway's Coastal Ranger Commando and Romania's 307th Marine Regiment are all nominally marines due to their amphibious capabilities but in actuality are designed to primarily operate in the littorals, not from ships. NATO partners Sweden and Finland operate similar units. Only a few of these employ missile systems, all short-ranged. While some nations maintain limited Coastal Defense Cruise Missile (CDCM) capabilities, these are generally operated as batteries, with a full complement of launch, C2, radar and support vehicles, in a way that is not doctrinally compatible with tactical and operational dispersal.

The foremost concern in the formation of stand-in forces must be the development and delivery of effective, mobile missile systems designed to be employed from a wide variety of platforms. The U.S. has already purchased the Norwegian Naval Strike Missile (NSM) to equip the Littoral Combat Ship and Marine Littoral Regiments. Other possibilities exist, such as the French Exocet MM40 Block 3[29] or the Israeli Delilah cruise missile,[30] among others. Whatever missiles are used, they should be small enough to be mounted on platforms as small as light trucks, combat boats and helicopters, in addition to MPRA, strike aircraft and naval combatants. For example, the NSM is already carried by ships and fixed-wing aircraft;[31] India is considering putting NSMs on its MH-60R helicopters,[32] and Kongsberg has already produced CDCM batteries built around this system for Poland.[33]

Existing littoral forces could be adapted, re-structured as small, dispersed units armed with stand-off weapons, operating directly inside adversary weapons arcs. Complex multi-mission missile systems may be outside the defense budgets of small nations, even with U.S. assistance, but the groundwork for a distributed defense can still be laid. ISR and logistics teams, supply caches, and the active preparation of necessary EMCON and C2 architecture[34] are all both feasible and easily scaled. Local forces prepared and trained to operate in tandem with stand-in forces deployed from other nations would accelerate responsiveness and enhance the effectiveness of the deterrence by denial strategy.

Recommendations

The U.S. can immediately take action to strengthen deterrence by denial by fostering the creation and integration of Allied stand-in forces. Because it is so early in the development of these capabilities there is a golden opportunity to bring Allies in "at the ground floor" to discuss the creation of complementary structures and explore partnerships in development of the necessary technologies. Allies already squarely within adversary A2/AD bubbles, like those in Central and Eastern Europe, are struggling with military modernization[35] and should be designated as prime candidates for military assistance with the express purpose of developing and equipping their own stand-in forces.

Within the NATO context, local forces could be re-oriented to integrate with and support deployed stand-in forces. Cooperative development partnerships should be formed to further the establishment of full-capability stand-in forces. Additional options include:

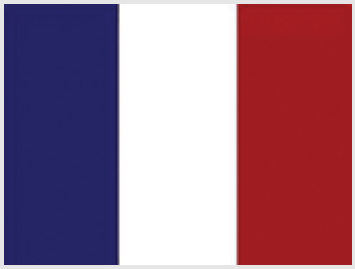
1. Direct the Centre for Maritime Research and Experimentation to develop and experiment with integrated approaches to Allied stand-in forces;
2. Engage the NATO Support and Procurement Agency to coordinate acquisition partnerships in support of collective procurement of the necessary systems;
3. Use the NATO Security and Investment Program (NSIP) to build the necessary infrastructure support dispersed logistics and networked C2 systems in forward areas;
4. Incorporate multi-national stand-in capabilities into ongoing NATO concept development and planning efforts; and
5. Integrate these forces into exercises as a demonstration of Allied resilience and capability.

In the Pacific, similar approaches could be utilized to create stand-in capabilities in the First and Second Island Chains.

Final Thoughts

As the world returns to Great Power competition, the U.S. should encourage its allies and partners to re-evaluate their force structures and attenuate strategies to maximize littoral defenses, where they enjoy distinct home field advantages. In Europe and the Pacific, the U.S. and its Allies can cooperatively create stand-in forces to deliver deterrence by denial effects where they are needed most. Restructured to increase resilience, firepower and the ability to mitigate threats in peace and in war, a more distributed force would be able to"....change the adversary's cost calculus and buy time for flexible deterrent options and assembling a joint task force."[36] As long as allies maintain control of their coastlines and vital airports, they will be able to hamper and hold at risk adversary military operations, providing opportunities to disrupt, flank and strike key facilities and assets. There is a golden opportunity here to collectively re-orient around a multi-domain force that emphasizes weapons rather than platforms by using units designed to integrate in deep, resilient defensive networks able to resist enemy advances from the outset.

1 Montgomery, Mark and Sayers, Eric. Make China the Explicit Priority in the Next NDS. 27 Juil 2020. Accessed: 5 Apr 2021: https://www.cnas.org/publications/commentary/make-china-the-explicit-priority-in-the-next-nds
2 Borghard, Erica et al. Elevating 'deterrence by denial' in U.S. defense strategy. 4 Feb 21. Accessed 5 Apr 2021: https://www.atlanticcouncil.org/content-series/seizing-the-advantage/elevating-deterrence-by-denial-in-us-defense-strategy/
3 Winnefeld, James. The 20th-Century Roots of EABO. Proceedings. Feb 2019. Annapolis: U.S. Naval Institute. Accessed 5 Apr 2021: https://www.usni.org/magazines/proceedings/2021/february/20th-century-roots-eabo
4 Jensen, Benjamin. "Distributed Maritime Operations: Back to the Future?" 9 Apr 2015. Accessed 6 Mar 2020: https://warontherocks.com/2015/04/distributed-maritime-operations-an-emerging-paradigm/
5 Lundquist, Edward. DMO is Navy's Operational Approach to Winning the High-End Fight at Sea. 2 Feb 2021. Accessed 5 Apr 2021: https://seapowermagazine.org/dmo-is-navys-operational-approach-to-winning-the-high-end-fight-at-sea/
6 Headquarters USMC. Tentative Manual for Expeditionary Advanced Base Operations. Feb 2021. 1-4.
7 Shelbourne, Mallory. Marine Corps to Stand Up First Marine Littoral Regiment in FY 2022. 20 Jan 2021. Accessed 1 Apr 2021: https://news.usni.org/2021/01/20/marine-corps-to-stand-up-first-marine-littoral-regiment-in-fy-2022
8 South, Todd. Marine Corps looks at building 3 new Pacific regiments to counter China. 3 Feb 2021. Accessed 1 Apr 2021: https://www.marinecorpstimes.com/news/your-marine-corps/2021/02/04/marine-corps-looks-at-building-3-new-pacific-regiments-to-counter-china/
9 Headquarters USMC. Tentative Manual for Expeditionary Advanced Base Operations. Feb 2021. A-1.
10 Eckstein, Megan. Marines Will Field Portfolio of JLTV-Mounted Anti-Ship Weapons in the Pacific. 11 Mar 2020. Accessed 1 Apr 2021: https://news.usni.org/2020/03/11/marines-will-field-portfolio-of-jltv-mounted-anti-ship-weapons-in-the-pacific#more-74293
11 Headquarters USMC. Tentative Manual for Expeditionary Advanced Base Operations. Feb 2021. A-11.
12 Keller, Jared. The Marine Corps is eyeing a long-range robot boat that can nail targets with kamikaze drones. 27 Jan 2021. Accessed 1 Apr 2021: https://taskandpurpose.com/news/marine-corps-long-range-unmanned-surface-vessel-contract/
13 The U.S. Army in Multi-Domain Operations 2028. TRADOC Pamphlet 525-3-1. 6 Dec 2018. iii.
14 The U.S. Army in Multi-Domain Operations 2028. TRADOC Pamphlet 525-3-1. 6 Dec 2018. vii.
15 Headquarters, Department of the Army. Army Multi-Domain Transformation. 16 Mar 2021. 16.
16 Barnett, Jackson. Army stands up first multi-domain task force in Washington state. 21 Feb 2021. Accessed 29 Mar 2021: https://www.fedscoop.com/army-multi-domain-task-force-washington-state/
17 Congressional Research Service. In Focus: The Army's Multi-Domain Task Force (MDTF). 29 Mar 2021. Accessed 5 Apr 2021: https://crsreports.congress.gov/product/pdf/IF/IF11797
18 Headquarters, Department of the Army. Army Multi-Domain Transformation. 16 Mar 2021. 12.
19 Freedberg, Sydney. Can Army Triple PrSM Missile's Range? 2 Apr 2021. Accessed 5 Apr 2021: https://breakingdefense.com/2021/04/can-army-triple-prsm-missile-range/
20 Munoz, Carlos. U.S. Army validates Multi-Domain Task Force in key Pacific exercise. 2 Oct 2020. Accessed 29 Mar 2021: https://www.janes.com/defence-news/news-detail/us-army-validates-multi-domain-task-force-in-key-pacific-exercise
21 Colby, Elbridge and Slocombe, Walter. The State of (Deterrence) by Denial. 22 Mar 2021. Accessed 6 Apr 2021: https://warontherocks.com/2021/03/the-state-of-deterrence-by-denial/
22 Priebe, Miranda et al. Distributed Operations in a Contested Environment. Santa Monica: Rand Corporation. 2019. xi-xii.
23 Freedberg, Sydney. '$64K Question': Where In Pacific Do Army Missiles Go?. Accessed: 31 Mar 2021: https://breakingdefense.com/2021/03/64k-question-where-in-pacific-do-army-missiles-go/
24 Freedberg, Sydney. '$64K Question': Where In Pacific Do Army Missiles Go?. Accessed: 31 Mar 2021: https://breakingdefense.com/2021/03/64k-question-where-in-pacific-do-army-missiles-go/
25 Rowden, Thomas. Surface Force Strategy: Return to Sea Control. Commander Naval Surface Forces. Jan 2017.11
26 Rowden, Thomas. Surface Force Strategy: Return to Sea Control. Commander Naval Surface Forces. Jan 2017. 9.
27 Jensen, Benjamin. "Distributed Maritime Operations: Back to the Future?" 9 Apr 2015. Accessed 6 Mar 2020: https://warontherocks.com/2015/04/distributed-maritime-operations-an-emerging-paradigm/
28 "Raytheon and Kongsberg to build Joint Strike Missile (JSM)." 5 Mar 2020. Accessed 13 Apr 2021: https://www.globaldefensecorp.com/2020/03/05/raytheon-and-kongsberg-to-build-joint-strike-missile-jsm/
29 Exocet Mobile Coastal. Accessed 6 Apr 2021: https://www.mbda-systems.com/product/exocet-mobile-coastal-defence-system/
30 Rogoway, Tyler. Vietnam Eyes Israel's Delilah Standoff Missile, and F-16s Could Be Next. 10 Mar 2017. Accessed 28 Jan 2021: https://www.thedrive.com/the-war-zone/8219/vietnam-eyes-israels-delilah-standoff-missile-and-f-16s-could-be-next
31 "Kongsberg Naval and Joint Strike Missiles Update Precision Strike Annual Review (PSAR-14)." Accessed 13 Mar 2020: http://docplayer.net/30928877-Kongsberg-naval-and-joint-strike-missiles-update-precision-strike-annual-review-psar-14.html
32 Dalløken, Erlien. USA punger ut for flere norske missiler: – Helt nødvendig for å øke vår kampkraft. 20 Feb 2020. Accessed 28 Feb 2020: https://www.tu.no/artikler/usa-punger-ut-for-flere-norske-missiler-helt-nodvendig-for-a-oke-var-kampkraft/485517
33 Accessed 13 Mar 2020: https://www.altair.com.pl/news/view?news_id=10814.
34 Kolb, John. "High-Density, Low-Cost C2 for Expeditionary Advanced Base Operations." Proceedings. Jan 2021. Vol 147/1/1.
35 Kallberg, Jan. Prioritize NATO integration for multidomain operations. 10 Mar 2021. Accessed 6 Apr 2021: https://www.c4isrnet.com/opinion/2021/03/10/prioritize-nato-integration-for-multidomain-operations/
36 Jensen, Benjamin. "Distributed Maritime Operations: Back to the Future?" Accessed 6 Mar 2020: https://warontherocks.com/2015/04/distributed-maritime-operations-an-emerging-paradigm/



CRUISE MISSILES - FROM STRATEGIC GAME CHANGER TO THE SWISS ARMY KNIFE

CAPT (FRA-N) MAX BLANCHARD

"We are excellent at launching Tomahawk missiles; we need to get better at launching ideas" - ADM James G. Stavridis (USN ret.)

During the last three decades, cruise missiles, embodied mainly through the American Tomahawk variant, have epitomized the technological leadership of the United States. Used as a strategic weapon as part of a military campaign or in support of U.S. diplomacy, recent developments have brought cruise missiles to the forefront of debates. Their extensive use both during and since the First Gulf War, coupled with their increasing affordability (especially compared to ballistic missiles), have increased the attention devoted to these types of missiles. The recent surge in technological improvements with the development of hypersonic capable scramjet/ramjet engines is likely to cause users of these missile systems to reassess their utility on the modern battlefield. With supersonic weapons emerging as a probable game changer in a broader proliferation context, there is a growing need to reevaluate the employment of cruise missiles to determine if they remain an effective, versatile and cost-effective weapon system.

History and Use

The employment of cruise missiles dates back to World War II and the development of the V1 rockets. With a range of 250 km and capable of speeds of 650 km/h, more than 9,000 V1s were launched against Britain with the aim of crippling the country's economy and morale, underscoring the strategic dimension of this new weapon.[1] After the war, these missiles evolved with the development of nuclear-capable cruise missiles (Regulus I), constituting the first U.S. nuclear deterrence weapons. However, the increasing momentum in the ballistic program temporarily postponed further developments of cruise missiles. The Polaris program retained center stage at the height of the Cold War until technological advances in propulsion and guidance made it possible to revisit the cruise missile in the 80s.

Designed initially as a submarine-launched anti-ship missile, the Tomahawk evolved into a nuclear variant before being developed into a land-attack conventional version in 1985. Since then, it has remained the unchallenged leader in the cruise missile category and some 2,300 missiles have been fired by the U.S. in support of military operations.[2]

The Tomahawk first saw action in combat during Operation Desert Storm in 1991. Approximately 300 missiles were fired during the first days of the campaign.[3] Their targets were command and communication networks as well as air defenses and high value assets. The Tomahawk's operational value has only been reinforced with its use in Bosnia, Serbia, Afghanistan and most recently Operation Iraqi Freedom where the U.S. launched more than 800 missiles.[4] The impact of cruise missiles during these operations shared similar characteristics: initial use at the onset of a campaign to disrupt air defense systems and command and control (C2) networks; and, later, strike missions in coordination with air strikes, using a significant number of missiles fired mainly from the sea to capitalize on the surprise effect.

The Los Angeles-class fast attack submarine USS Annapolis (SSN 760) launches a Tomahawk Land Attack Missile (TLAM). Courtesy of U.S. Navy.

In an effort to accurately portray the importance of the cruise missile, one only has to examine the 1986 Operation El Dorado Canyon. In response to repeated terrorist actions led by Libya's Col. Gaddafi, the U.S. planned a retaliatory strike against terrorist installations. Although Tomahawk missiles had just been declared operational, their employment was ruled aside. If these weapons were somehow captured, they would be handed over to the USSR and compromised. So, instead, an air raid was carried out by a combination of F-111 aircraft taking off from bases in the UK alongside attack aircraft launched from U.S. carriers. Over 100 aircraft were necessary to conduct the raids which delivered 60 tons of ordnance over seven targets. The F-111s had to fly over 13 hours back and forth to the UK; one aircraft and its crew were lost during that mission. Arguably, had that operation been conducted with the sole use of cruise missiles, although more than 100 Tomahawks would have been required to achieve the objectives, their employment would have preserved the autonomy of the U.S., increased the surprise factor and, more importantly, would have avoided the loss of an aircrew.

Overall, the employment of cruise missiles during the last three decades has been carried out during military campaigns (85% of the total) as opposed to retaliatory strikes with the bulk of them being launched from surface assets. Interestingly enough, the number of weapons fired has decreased over time with more than a thousand employed in the 90s, and only 400 in the 2010s. Although we have seen a decrease in use, as Robert Farley explains, "For the past three decades, America's signature weapon of war has been the Tomahawk Land Attack Missile, or TLAM. The TLAM has helped bust down the doors of air-defense networks from Iraq to Libya, and has become a favorite tool of political influence for several presidents."[5]

A BGM-109 Tomahawk cruise missile launched from battleship USS Iowa. Courtesy U.S. Navy.

Definition, Development and Competition

It is not easy to give a precise definition of a cruise missile, from either technical or operational standpoints. 'Classic' cruise missiles such as the Tomahawk or the Russian Kalibr, share a set of relatively common characteristics such as propulsion systems (turbofan), speed (subsonic) and payload (around the 0.5t mark), with differences in accuracy and range depending on the guidance systems. However, technological improvements have made this classification increasingly difficult with the development of multi-effect warheads, and the constant improvement of navigation and guidance technologies. On the other hand, we see a possible major game changer that is blurring the definition lines even more with the development of scramjet engines, which can increase the missiles speed six to eightfold. Furthermore, stating that cruise missiles have to meet a specific set of criteria could lead to the exclusion of certain systems and distort the doctrinal process related to these types of weapons. Negotiators of the late Intermediate-Range Nuclear Forces Treaty chose a very broad definition in order not to exclude any relevant missiles. The Treaty states that a cruise missile constitutes "an unmanned, self-propelled vehicle that sustains flight through the use of aerodynamic lift over most of its flight path."[6] Even so, some operational characteristics do set the cruise missiles apart from other weapons and therefore dictate their method of employment. As mentioned earlier, range, speed and accuracy allow the user to ensure an element of surprise and invulnerability, especially in the case of submarine launched missiles, keeping the shooter at a standoff distance from the enemy air defense systems.

Even though conventional cruise missiles would normally be categorized as tactical weapons, the capability they deliver, in the broadest sense, clearly falls under strategic or theater weapons as they are equally as political as they are military weapons. For the last 30 years, the naval cruise missile was virtually an uncontested U.S. monopoly. In the past few years however, this monopoly has faded with the

arrival of new contenders who have demonstrated their capabilities in operations as well as important improvements in missile design. Russian technology is directly linked to the proliferation of Land Attack Cruise Missiles (LACM). For a long time, Russia has been cooperating in the field of weapons' development with China and India. Unsurprisingly, these two countries have fielded LACM designs based on existing Russian systems. The Chinese YJ18 is reportedly based on the Russian Kalibr 3M54 E Club missile, and the Indian Brahmos was developed with Russia on the basis of the P-800 Oniks.[7] Russia retains its spot as one of the top three arms exporting countries in the world, selling cruise missiles and naval platforms to strategic partners globally, but even now other countries are taking advantage of technological advances on the open market. For decades, analysts have emphasized the widespread availability of cheap guidance, navigation and digital-mapping technologies throughout the world, making it easier for new countries to manufacture cruise missiles. For example, both Iran and Brazil have either developed, or are in the process of developing, indigenous cruise missiles. In recent years, as research and development have increased in multiple countries, the weapon technology attracting more interest than any other within the strategic community is the hypersonic cruise missile. The groundbreaking improvement in these systems has been the ability to control and update the weapon during its hypersonic flight to achieve a highly maneuverable and accurate trajectory.

Implications

The capability of employing cruise missiles is, however, a double-edged sword. The proliferation of this technology has increased significantly, including in regions of the world where the possession of cruise missiles is likely to increase instability and heighten the risks of escalation. This is true in the case of Europe but can also be applied to other regions of the world. Indeed, seven European NATO states have acquired LACM while Finland is also in the process of acquiring their own Joint Air-to-Surface Standoff Missile (JASSM). This may lead potential enemies to adopt a more aggressive posture in respects of their own cruise missile employment; there is a perceived benefit to striking first. Indeed, while cruise missiles

French FREMM firing MdCN cruise missile. Courtesy by L. Bernardin/Marine Nationale.

are highly effective weapons against High Value Targets, they are particularly vulnerable if stricken first (with the exception of submarine launched missiles). These considerations could set up a "use them or lose them" strategy.

Another destabilizing by-product of this proliferation is the entanglement of nuclear and non-nuclear assets. Whether it is the C2 structures or Intelligence, Surveillance, and Reconnaissance (ISR) installations, they often share their employment to some degree between nuclear and conventional weapons. Furthermore, in some cases both variants share the same missile body (Russia's Kh-55/555 or Kh-101/102, for example). It is therefore possible to provoke a nuclear escalation in a conventional crisis due to confusion between both systems. Similar dynamics are in place in Southeast Asia, where China deploys dual-capable missiles.

Lastly, the proliferation of cruise missiles has extended to non-state actors. Hezbollah in Lebanon, and more recently Ansarullah in Yemen, have used cruise missiles in their operations against Israel and Saudi Arabia, respectively.[8] Such attacks highlighted the vulnerability of strategic facilities lacking proper air defense capabilities and the reputational impact they can have if successful. If this sort of proliferation does spread to other organizations, it will become a challenge for national armed forces, which will have to allocate increased amounts of ISR and targeting assets to counteract the threat. Maintaining a robust and effective integrated missile defense will become a main concern for military planners.

In addition to the challenges of counter-proliferation, the cost-effectiveness of cruise missiles and their future employment must be considered.

Historically, the prohibitive cost of cruise missiles has long been an issue and a limitation to its employment in the planning process. Reduction in the cost of technologies, especially relative to guidance systems, has directly affected their purchase and use. In times where all major operations are likely to be conducted with the extensive use of Precision-Guided Munitions (PGMs), Tomahawks stand out as a relatively affordable option with an associated cost around $1 million USD, compared to more recent PGMs such as the Naval Strike Missile ($2.2 million USD), the SM-6 ($4 million USD)[9] or the JASSM ($1.4 million USD).[10] Furthermore, comparisons are even more favorable to the cruise missile in respects to air strikes or the use of armed drones when employed against similar objectives.

Conclusion

Today, a large stock of TLAMs is available, as only a fraction has been used in past operations. As described by Lorent Thompson, "The Navy has taken delivery of over 4,000 Block IV Tomahawks since 2004, about a tenth of which have been used in combat and testing."[11] In times of constrained defense spending, the fact that existing cruise missiles can evolve technologically without major modifications to surrounding infrastructures (e.g. C2 and launchers), is a major consideration when addressing emerging threats quickly, rather than developing entire new weapon systems.

A hallmark of U.S. post-Cold War superiority, more than 2,000 cruise missiles have been fired since the First Gulf War with outstanding results and an extremely low rate of failure. Although likely to become overtaken by hypersonic weapons as a strategic asset, with large stockpiles and a lifespan of 30 years, cruise missiles could see a drift in their employment towards more tactical missions. Such an evolution and the potential increase of cruise missiles must come with an enhanced flexibility in the joint targeting cycle which, for the time being, is partially retained at the strategic level. Arguably, "Hunter-killer SAGs [can] seize maritime-operations areas for subsequent activities (including power projection), [...], and hold adversary land targets at risk."[12]

In essence, cruise missiles can, and should, stay part of the current order of battle in NATO, just as they are becoming a mainstay for other countries. Granted, the concerns over adding an element to the pervasive arms race and the potential for increased use/aggression by our adversaries are valid, but that really only serves to underscore their utility as either a deterrent or first strike effect. They are prolific and are likely to remain so into the second and third horizon of operational use. They provide a lethality and flexibility that add to a commander's toolbox on the modern battlefield, taking full advantage of the relative stealth and safety of the maritime environment. As new ideas on how to conduct warfare present themselves year by year, the pragmatic warrior knows that the venerable precision guided cruise missile must still be considered key to a successful campaign.

A launched Tomahawk Cruise Missile. Courtesy of U.S. DoD.

1 "V-1 flying bomb". https://en.wikipedia.org/wiki/V-1_flying_bomb
2 Werrell, Kenneth P. "The Evolution of the Cruise Missile" Alabama: Library of Congress, 1985
3 Dyfed Loesche,"United States Cruise Missile Diplomacy," Statista, April 12, 2018 https://www.statista.com/chart/8907/united-states-cruise-missile-diplomacy
4 ibid
5 Robert Farley, "What could the U.S. do without the Tomahawk missile? (A lot)" The National interest December 22,2020 https://nationalinterest.org/blog/reboot/what-could-us-military-do-without-tomahawk-missile-lot-174962
6 Fabian Hoffmann, "Cruise missile proliferation: Trends, strategic implications, and counterproliferation," European Leadership Network, march 17,2021 https://www.europeanleadershipnetwork.org/report/cruis-missile-proliferation-trends-strategic-implications-and-counterproliferation/
7 "Missiles of the world" CSIS, Accessed December 15,2021 https://missilethreat.csis.org/missile
8 Joseph Trevithick," Yemen's Houthi Rebels Say They Struck Saudi Oil Facility With New Type Of Cruise Missile," The Drive, November 23,2020 https://www.thedrive.com/the-war-zone/37783/yemens-houthi-rebels-say-they-struck-saudi-oil-facility-with-new-type-of-cruise-missile
9 David Axe, " The U.S. Navy's SM-6 Missile Can Hit Almost Any Target," The National Interest, March 4,2021 The U.S. Navy's SM-6 Missile Can Hit Almost Any Target | The National Interest
10 Amanda Macias, "U.S. taxpayers paid millions of dollars for the airstrikes on Syria. Here's a breakdown of key costs," CNBC, April 16,2018 https://www.cnbc.com/2018/04/16/syria-airstrikes-cost-to-us-taxpayers.html
11 Loren Thompson, "The Navy's Tomahawk Cruise Missile Is becoming More Lethal, More Versatile," Forbes, October 23.2019 https://www.forbes.com/sites/lorenthompson/2019/10/23/the-navys-tomahawk-cruise-missile-is-becoming-more-lethal-more-versatile/?sh=6c7a227e71d7
12 Vice Admiral Thomas Rowden, et al., "Distributed Lethality," Proceedings - January 2015 Vol. 141/1/1,343

MARITIME SECURITY OPERATIONS IN CHALLENGING WATERS

CDR (RNoN) PER CHRISTIAN GUNDERSEN

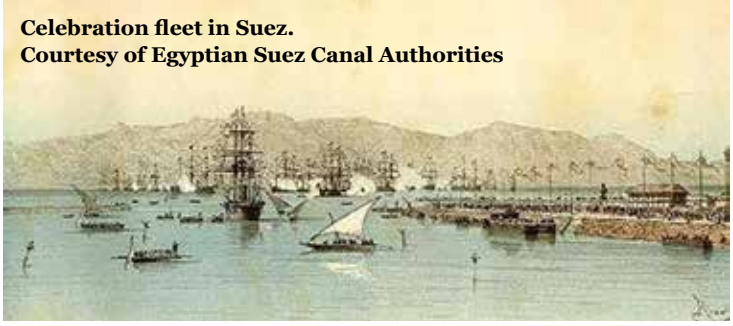
The character of the seas has changed. From an open space where freedom was the rule, they have now turned into a shared, common domain, vast but fragile, needing world-wide management and protection.

Combined Maritime Forces (CMF) is a U.S.-led naval coalition conducting Maritime Security Operations (MSO) to ensure the free movement of merchant shipping and prevent illicit activity in the waters surrounding the Arabian Peninsula. With headquarters in Bahrain, a small island state in the southeast of the Persian Gulf, CMF unquestionably has an important mission: upholding the International Rules-Based Order in some of the world's busiest and vital shipping lanes. Nonetheless, the coalition is a relatively unknown entity for those who are not explicitly engaged in international maritime security.

The aim of this article is to describe how CMF assesses and manages the maritime security challenges in this region. In addition, it aims at providing some context regarding what the future may hold for this coalition, perhaps as a model for others to follow.

A Historically Important Trade Route

Most of us are aware of international trade's dependency on maritime transportation. As of today, approximately 90% of global trade goes by sea. Unhindered and unchallenged passage of civilian shipping through international waters is of great importance for maintaining stability in the world economy. Some of the most strategically critical maritime areas are located in the waters around the Arabian Peninsula. Within this region, there are three geostrategic, narrow, and vulnerable international straits; Hormuz at the entrance to the Persian Gulf, Bab Al Mandeb at the Horn of Africa, and Suez between the Red Sea and the Mediterranean.



Celebration fleet in Suez.
Courtesy of Egyptian Suez Canal Authorities

Even before the rise of European naval powers in the 16th and 17th centuries, Hormuz was important for trade between Arab and Persian civilizations and the Indian and Indochinese subcontinent. Porcelain from China and spices from the Indochinese Peninsula were transported by sea through Hormuz to Central Asia and Europe. The local rulers, clans, and merchants quickly understood the importance of controlling the trade route through the straits. It was an essential means to sustain both political power and economic prosperity. For the same reason, the region later became an arena for growing European interest. Portugal, the Netherlands, France, and the United Kingdom have fought for influence and power in these areas over the last centuries.

The Suez Canal was completed in 1869 after ten years of construction work, initially under French control. At Bab Al Mandeb, the British Empire established its presence as early as 1799. Even the "anti-imperialist" Americans realized the importance of this region, and in 1879 the first American warship, USS Ticonderoga, sailed through the Strait of Hormuz. The region became even more strategically important after oil was discovered at the beginning of the 20th century, with extraction and production beginning about 20 years later.

Fast-forwarding to more recent history, the importance of how maritime events in this region affect the western economy was demonstrated during the build-up and initial phase of the Iran-Iraq War and the so-called Tanker War in the 1980s. Warring parties' initial targeting of oil tankers led to a 25 percent drop in commercial shipping and a sharp rise in the price of crude oil, from $14 per barrel in 1978 to $35 per barrel in 1981.[1] Later still, the Iraqi attack on Kuwait in 1990 and the response from the U.S. and the rest of the western world proved how important this area was for maintaining the free flow of trade, especially keeping oil production and unencumbered tanker shipping in this area.

However, during the last decades, hydraulic fracking technology has created several more major oil-producing participants on the market, especially in North America. The new technology has created a general oversupply of oil. Should an incident of any sort hamper the flow of oil from the Middle East, the ability for other suppliers to step in has decreased the vulnerability in the market. In addition, there is far more real-time information available today, which reduces uncertainties and rumors. To some extent, it also mitigates the risk for unnecessary global economic volatility. Still, about 50% of the global oil reserves are in the Middle East, primarily bound for markets in China, Japan, the Republic of Korea, and Singapore.[2]

Presently, around 60 large tankers and merchant ships transit daily through each of the straits of Hormuz, Bab Al Mandeb, and Suez. The threats towards these sea lines of communication are rather complex. During the last few decades, we have witnessed how both state and non-state actors, using relatively simple methods, have been able to impede the freedom of movement at sea in this region.

Today, the United States, Russia, China, the United Kingdom, France, Japan, and the Republic of Korea have a continuous maritime presence in the region, often with large surface vessels and maritime patrol aircraft. In addition, major western maritime countries such as the U.S., UK, and France, have established a permanent presence with national naval bases in the Persian Gulf, some dating as far back as the 1930s. It is also worth mentioning that China, in 2017, established a large naval base in Djibouti as part of the well-known long-term strategy, The Belt and Road Initiative. The base is still expanding and will probably serve as a sustainment hub for the People's Liberation Army Navy blue-water capital ships like the large deck amphibious warships or the newly designed aircraft carriers.[3]

Since the Cold War, Russia has had a naval base on the west coast of Syria in Tartus. As a long-standing ally of Syria, it has been evident during the last decade of civil war in the country that this base is considered very important to Russia. It provides a foothold in the Mediterranean and supports further deployments of capital ships southwards into the Red Sea and the Indian Ocean. In addition, it is interesting to note that even if the final agreement with the new regime in Sudan is pending, Russia is looking at developing a naval base in Port Sudan on the Red Sea, with the capability to keep up to four naval vessels, including those that are nuclear-powered.

U.S. Navy in the Suez Canal. Courtesy of U.S. Navy.

Combined Maritime Forces

In addition to national interests and initiatives, several maritime international coalitions and operations have been established in the region over the years. The oldest of these, which still exists, is CMF. CMF is a U.S.-led coalition of the willing that was created in the aftermath of the 2001 terrorist attacks in support of Operation ENDURING FREEDOM. However, the CMF was not to fight terrorism directly but, through MSO, prevent terrorist organizations from using the sea to obtain revenue, weapons, and ammunition. Later, both the CMF mandate and the mission were expanded. In addition, the coalition has increased from the original 12 to 34 member nations. With the U.S. as the lead nation, CMF is constantly looking to further expand membership. The latest members, Brazil and Egypt, were welcomed in 2018 and 2021, and the number is likely to grow over the next couple of years. Regional nations such as Sudan and Djibouti play essential roles in MSO within the Bab Al Mandeb and the Red Sea area. Nations like Kenya, Tanzania, Mozambique, Sri Lanka, and Indonesia may work with CMF to enable law enforcement to counter illicit activity at sea. CMF engages with all of these countries regularly, aiming at enlarging the coalition through a Pathway to Membership process, which includes regular dialog, liaising, and security arrangements.

The CMF mission is based on several United Nations Security Council Resolutions but is limited to addressing only non-state illicit activity. CMF will not take part in any conflicts involving states and, as such, has not been involved in the ongoing conflict between the U.S. and Iran. Instead, CMF is restrained to conducting MSO by safeguarding free movement by sea and preventing terrorism and other non-state criminal activities in international waters. The area of operations is the size of the European continent and covers the Persian Gulf, the Gulf of Oman, the Arabian Sea, the Gulf of Aden, the Red Sea, and parts of the Indian Ocean. CMF has three subordinate Maritime Task Forces; Combined Task Force (CTF) 150, CTF 151, and CTF 152, all with different mandates and tasks to accomplish this enduring mission.

Hunting Smugglers

CTF 150's mission is primarily to prevent the smuggling of weapons to Somalia and Yemen, and drugs from the Makran Coast (desert coast of Iran and Pakistan) to the Arabian Peninsula, the East Coast of Africa, or southeastward to markets in Southeast Asia and Oceania. The mission is challenging for several reasons. The area to

cover is enormous, compared with the limited resources available. CTF 150 has, during the last decade, experienced a steady decline in capabilities made available from member nations. Unfortunately, the naval force often consists of only one or two frigate sized vessels available for tasking. In addition, ISR operations by Maritime Air Patrols may happen only once a week, making it challenging to establish and maintain situational awareness and an operational maritime surface picture in the hotspot areas close to the Iranian and Pakistani coastline. Bluntly, it could be compared to patrolling and preventing speeding on the European continent with a couple of police cars. Furthermore, and equally important, CMF has so far been unable to persuade a state agree to establish a legal finish regime. This could be defined as a system where suspects of illicit activity in international waters are taken into custody, given a fair trial, and, if found guilty, sentenced by competent legal authorities in the region. Instead, CTF 150 forces can seize contraband, but due to restraints from operating in international waters and within international regulations, they are somewhat powerless when it comes to detaining and prosecuting the actors involved. There is also no appetite from the member countries providing naval assets to CTF 150 to take on national responsibilities for establishing a legal finish regime. Creating a proper national judicial system to confront illicit activity in international waters is assessed by the participating member nations to be rather difficult and costly. In addition, there exists a multitude of practical challenges including the requirements for establishing temporary custody premises onboard, transportation, and guaranteeing the chain of evidence remains unbroken for the trial process. The smugglers may lose a drug load now and then to CMF, but the profits undoubtedly outweigh the losses over time.

That is not to say there have not been successes. It was, of course, applauded when the Canadian frigate HMCS Calgary, operating within the CTF 150 mission, conducted 17 successful counter-narcotics interdictions during an eight-week period throughout the summer of 2021.[4] Nevertheless, the magnitude of the loads demonstrated the enormity of the challenge at hand. CMF assesses that it is able to stop about 5-10% of the seaborne drug smuggling through the area of operations, although it literally becomes a drop in the ocean (pun intended since CMF usually dumps the drugs overboard after they have been documented). On average, CTF 150 has, during the last decade, confiscated between 3-6 tons of heroin and more than 50 tons of hashish annually. Lately, there is a concern about the increasing smuggling of methamphetamine, with almost 5 tons seized last year. In total, CMF seized illegal drugs worth more than $193 million during counter-narcotics operations at sea in 2021, which is more than CMF has interdicted in the previous four years combined.[5] With more vessels, surveillance aircraft, and closer cooperation with Pakistan, Kenya, and Tanzania, among others, narcotics smuggling could undoubtedly be reduced considerably. For East African countries, drug addiction has become a major societal problem. At the same time, they are being smuggled further into the European and Asian markets and have become an ever-increasing global problem.

Boarding team from HMCS Calgary, Courtesy of CMF.

When it comes to weapons smuggling, CTF 150 has seized only a handful of weapons and ammunition en route to Somalia and Yemen over the past eight years. However, it should be mentioned that some member nations carry out similar MSO under national flags. Over the past years, both U.S. and Australian vessels have boarded and seized weapons in smaller civilian cargo vessels, most likely on their way from Iran to Yemen.

Hunting Pirates And Countering Attacks

CTF 151 is the second maritime force subordinate to CMF, established after the sharp rise in pirate attacks experienced in 2009 in the Gulf of Aden. This force works closely with the EU Naval Forces (EUNAVFOR) and their named Operation ATALANTA which, in principle, has the same mandate and mission. CTF 151 primarily patrols the internationally established transit corridor through the Gulf of Aden, Bab Al Mandeb, into the Red Sea and along the east coast of Somalia to ensure freedom of navigation and protect transiting merchant shipping. The operation has been very successful. In 2011, more than 200 attacks and 28 successful hijackings were carried out in the Gulf of Aden and off the coast of Somalia. Today, thanks to significant civilian and military efforts, the situation is different and the current risk for pirate attacks in the area has been reduced substantially. The last successful pirate attack was carried out in April 2017 against a smaller Indian cargo vessel. The last confirmed attempt was carried out two years later against two fishing vessels from the Republic of Korea and Taiwan off the coast of Mogadishu. That being said, it is not unusual for motor vessels (MV) to report suspicious approaches by skiffs as possible pirate attempts. Most of the time, assessments later reveal the reports to be angry fishermen unhappy with MVs transiting through their fishing grounds and possibly damaging fishing nets.

On any given day, 3-4 surface vessels and 1-2 maritime patrol aircraft from CTF 151 and EUNAVFOR operate outside Somali waters. In addition, a number of independent naval vessels from China, Russia, and India operate in the Gulf of Aden to support their own national merchant shipping. In total, up to 10 warships are continuously patrolling off the coast of Somalia. The sheer number of naval vessels present at all times is undoubtedly deterring potential pirates. For them, a large, gray-painted warship, often with an organic helicopter onboard, constitutes a viable threat, no matter what flag it carries. Nevertheless, Somalia is still a country in a deep crisis with far from resolved challenges. It is assessed as highly likely that piracy activities will resume if the naval presence in this area disappears.

At the same time, terrorist organizations such as Al-Shabaab in Somalia, Al Qaeda in Yemen, and the Yemeni rebel movement Houthi have both the will and the ability to carry out seaborne attacks in the Gulf of Aden and in the maritime areas around Bab Al Mandeb. In March 2020, three small boats east of the Gulf of Aden attacked a Saudi-registered merchant vessel in the International Recognized Transit Corridor. Two of these boats were remotely controlled with explosives on board. The attack was unsuccessful, and the merchant vessel continued the transit unharmed; it is still unclear who was behind the attack. In September 2021, a skiff with outboard motors and nine persons onboard approached a bulk carrier close to Bab Al Mandeb. Ladders and drums were observed onboard. However, the skiff diverted course and moved away towards the Yemeni coast after the privately contracted armed security personnel onboard the bulk carrier deterred the potential attackers by showing their weapons.

Capacity Building

The third subordinate force under CMF is CTF 152. It was established in 2004 and made up of naval units from the Gulf countries including Kuwait, Saudi Arabia, Bahrain, Oman, and the United Arab Emirates. CTF 152 is heavily supported by the U.S. Navy, U.S. Coast Guard, and the UK's Royal Navy. The activities in CTF 152 are focused on maritime security in general, but it is primarily about capacity building. The goal is to strengthen cooperation and interoperability between the Gulf countries in the maritime domain. This is accomplished by units operating in the same waters, being visible and present, and conducting integrated basic maritime operations, training and exercises together. It is obvious that this part of the CMF mission has a high priority for the U.S. as the lead nation as CTF 152 receives the most attention and support in the form of vessels and other military resources compared with the two other subordinate forces, especially these days with the increased tensions with Iran. The long-term goal is to enhance the naval capabilities, interoperability, and bolster cooperation in the region, creating a foundation for greater Arab independence in executing MSO. From U.S. and British perspectives, maintaining close relations with the Gulf countries is essential, and supporting CTF 152 will ostensibly have the follow-on effect of creating highly competent allies in the region.

The Case Of Iran

Since the U.S. withdrew from the nuclear deal with Iran in 2018 and then implemented further economic sanctions against the country, the threat against maritime trade has increased in the area. During the summer of 2019, tensions intensified due to several provocations from the Iranian side, including multiple attacks on oil tankers in the Persian Gulf and the Strait of Hormuz. As a result, the U.S. established the International Maritime Security Construct (IMSC) and Operation SENTINEL to secure the maritime trade routes through the Persian Gulf, Hormuz, the Gulf of Oman, and Bab Al Mandeb. In addition to the U.S., the members of the IMSC are Albania, Bahrain, Estonia, Lithuania, Saudi Arabia, the United Arab Emirates, and the United Kingdom.[6] Currently, only the U.S., UK, and Bahrain (only with base facilities) provide naval forces and support to this construct. However, since both the U.S. Navy 5th Fleet and UK Maritime Component Commander are collocated with IMSC HQ in Bahrain, this maritime mission can, at short notice, increase in size and capability to include approximately ten capital warships, a U.S. Carrier Strike Group, and amphibious forces.

Capacity Building. Courtesy of CMF.

In parallel with the U.S. initiative, France established the European-led Maritime Awareness Mission in the Strait of Hormuz (EMASOH). This initiative is supported by Belgium, Denmark, France, Germany, Greece, Italy, the Netherlands, Portugal and, recently, Norway. The mission is similar to the IMSC but not directly related to the U.S. Maximum Pressure strategy against Iran. So far, France, the Netherlands, Greece, Italy, and Denmark have provided forces to EMASOH's military component, Operation AGENOR. The headquarters is located in the UAE at the French Naval Base in Abu Dhabi.

Although EMASOH and IMSC provide different political-strategic guidelines, and have somewhat different

mandates, the two coalitions cooperate effectively, especially at the tactical level. There is, for instance, a routine exchange of information between the vessels of these two forces, somewhat solidifying the allied response to Iranian aggression.

The Way Forward

In addition to the leading western nations' individual national interests and missions, CMF, IMSC, and EMASOH compete for the same maritime resources in this region. The U.S. assassination of the leader of the Iranian Revolutionary Guard, Quasem Soleimani, and the subsequent Iranian attacks on U.S. bases in Iraq in early January 2020, clearly highlighted the priorities of the leading CMF member nations. Understandably, the U.S., UK, and France prioritize forces to IMSC and EMASOH rather than CMF. In particular, CMF's mission to stop smuggling has been downplayed over the past few years.

Recognizing that member countries' interests and participation have been declining in recent years, CMF conducted an internal Comprehensive Strategic Review of the entire mission in the first half of 2020. In July of that year, the way forward for CMF was presented and discussed with member nations during the Maritime Security Conference, which was conducted virtually due to COVID-19 restrictions. The CMF vision was to create a somewhat broader portfolio of assignments to ensure its relevance and legitimacy in the region and, in the long term, limit the negative effects of continued low turnout of naval forces from the member nations. Specifically, three fundamental changes to the mission were proposed and approved by the member nations: strengthen CMF's ability to conduct capacity building, establish closer cooperation with national and international entities, and streamline the organization to focus main efforts and enable synergies. More than a year and a half later, CMF has come a long way in implementing the approved proposals even with the ongoing pandemic that has somewhat affected the overall progress of the mission.

During the last year, capacity building has become a significant line of effort, focusing mainly on three areas: the Persian Gulf, the Red Sea, and Africa's Southeastern coast. CMF has stood up a specific Capacity Building Branch whose primary purpose is to assess the member and partner nations' specific maritime capacity-building needs. Equally as important, the coalition encourages member nations to participate in this long-term and essential part of the overall mission. Generally, the trend is positive, and CMF is currently conducting capacity building by utilizing organic staff, subordinate units, or tailored Mobile Training Teams. In addition, CMF supports international organizations such as the UN Office on Drugs and Crime (UNODC) with training teams. The overall aim is to support both member states and partner countries in their efforts to develop abilities to ensure maritime safety, sovereign rights, and territorial integrity in their respective Exclusive Economic Zones and Territorial Waters.

CMF has acknowledged that, with the limited resources available, the coalition cannot solve all mandated challenges in the area of operations in splendid isolation. There is unquestionably a requirement to encourage a comprehensive approach where civilian and military instruments of power and resources pull together in the same direction. CMF can, in many ways, be compared to a potent police force at sea, albeit with a somewhat limited enforcement mandate. Significantly, though, the increased cooperation with the UNODC and their Global Maritime Crime Program has been rewarding. CMF has established a working relationship with UNODC's training facilities in Sri Lanka and The Seychelles, sending teams to support the UN training efforts to counter illicit activities at sea in this region. At these facilities, various maritime courses are conducted for the coastal nations' navy, coast guard, maritime police, and customs officials, focusing on seamanship and maritime law enforcement. There have also been recent talks with Kenya about closer naval cooperation, especially concerning information sharing on drug smuggling-related activity.

A tangible result of the comprehensive strategic review has been the streamlining of the CMF structure. The establishment of a combined watch floor for the CTFs has resulted in more efficient use of the entire staff available. Instead of a doubling or a tripling of positions at the CTF level, the workforce and responsibilities have been moved from the CTFs to CMF HQ. This has made force generation easier as member nations are not required to man large CTF-staffs anymore. In addition, Plans, Key Leader Engagement, and the Capacity Building Branches are now arranged within the same directorate at CMF HQ. Both changes have created synergy in the form of presence, information sharing, and support to most effectively use all available assets to uphold the rules-based order at sea.

In order to increase presence and situational awareness within the Red Sea and its surrounding areas,

The French frigate Chevalier Paul conducting Maritime Security Operations. Courtesy of French Navy.

CMF is planning to generate a new task force in early 2022, designated CTF 153. In essence, CMF is splitting up CTF 150 and its mandate. While CTF 150 will continue to operate in the Gulf of Oman and Northern part of the Arabian Sea, CTF 153 will focus on the Red Sea, Bab Al Mandeb and into the Gulf of Aden. Nevertheless, both CTFs will continue focusing on countering smuggling activities including narcotics, weapons, and even charcoal, to disrupt maritime activities that support terrorism.

One aspect that has not received enough attention is illegal, unreported, and unregulated fishing in the region. Researchers estimate that one in five fish is caught illegally in the Indian Ocean and that over 70% of fish stocks are either fully exploited or overexploited. Large predatory fish such as swordfish, marlin, and tuna have been reduced by 90% from pre-industrial levels. This situation represents a major revenue loss for several nations and harms coastal populations significantly. Fish provide food for hundreds of millions of people in the region and are a crucial source of income. If the trend continues, researchers estimate that fish stocks in the Indian Ocean will collapse by 2050. Many coastal nations lack sufficient infrastructure, organizations, patrol vessels, and maritime patrol aircraft to maintain control of sovereign rights in their Exclusive Economic Zones. The result has been countries like China, Taiwan, South Korea, and even some European states sending trawlers and exploiting the area over decades. However, CMF does not have the mandate or the ambition to intervene and enforce fishing regulations directly. Still, there is the potential for CMF to proactively support coastal nations with the resources at hand. Closer cooperation in training and exercises is undoubtedly welcome, and information sharing about suspicious foreign trawlers in the area will definitely be appreciated. Indirectly supporting coastal nations' fights against illegal, unreported and unregulated fishing would strengthen the coalition's trust and cooperation within the region, especially on the eastern coast of Africa. The second and third order effects of garnering trust and support from multiple nations to the CMF missions would undoubtedly be felt.

Conclusion

It is obvious for all actors in the region that expanded, structured, and continuous information-sharing and cooperation provides better maritime security for all. However, the challenge is, as is often the case, that everybody wants to coordinate, but not everybody enjoys being coordinated. That said, as a coordinating body, CMF is well-suited for this purpose. The coalition has members from all continents and is not involved in any state-to-state disputes. In addition, it has a structure that makes it relatively easy to initiate and maintain a dialog with most maritime entities related to maritime security, be it the Kenyan Coast Guard, the National Maritime Operations, and Emergency Response Center in Madagascar, the UK Maritime Trade Operations, or even the UNODC. Everyone is basically concerned about the same maritime security challenges in the region. It would be naïve to believe that deterring and defeating all illicit activity at sea in this region is possible. However, it is possible to mitigate the threats, primarily by providing a functional coordinating structure, getting the most out of scarce resources, and creating a sustainable situation to uphold the enduring Rules-Based Order at sea in this important part of the world, including the sometimes-overlooked resource management. Looking at the geopolitical characteristics of the region, the CMF profile and posture have been essential to its relative success. By demonstrating flexibility, engaging partners and developing their skills and participation, and consistently seeking out ways to more efficiently accomplish the various missions, it must be seen as a template for MSO worldwide.

1 Robert Strauss Center for International Security and Law, "Tanker War", https://www.strausscenter.org/strait-of-hormuz-tanker-war/, retrieved from internet 16. Nov 2021
2 Richter, Felix, Statista, "Venezuela Sits Atop the World's Largest Oil Reserves", 16. Sep. 2019, https://www.statista.com/chart/16830/countries-with-the-largest-proven-crude-oil-reserves/, retrieved from internet 16. Nov. 2021
3 LaGrone, Sam, USNI News, "AFRICOM: Chinese Naval Base in Africa Set to Support Aircraft Carriers", 20. Apr.2021, https://news.usni.org/2021/04/20/africom-chinese-naval-base-in-africa-set-to-support-aircraft-carriers, retrieved from internet 17. Nov. 2021
4 Combined Maritime Forces, "HMCS Calgary redeploys with CMF record for most interdictions by a single ship", 14. Jun. 2021, https://combinedmaritimeforces.com/2021/06/14/hmcs-calgary-redeploys-with-cmf-record-for-most-interdictions-by-a-single-ship/, retrieved from internet 18. Nov. 2021
5 U.S. NAVCENT Public Affairs, "Record Seizures in 2021 after NAVCENT and CMF Increase Patrols", 18. Jan 2022, https://www.dvidshub.net/news/412985/record-seizures-2021-after-navcent-and-cmf-increase-patrols, retrieved from internet 19. Jan. 2022
6 International Maritime Security Construct, "An International Approach", https://www.imscsentinel.com/, retrieved from internet 18. Nov. 2021

THE NEW CHALLENGE FOR THE OLD RIVAL – RUSSIAN MARITIME PRIORITIES

CDR (TUR-N) EMIR ARICAN

Even if it is not impossible for NATO, countering increasing Russian influence will require more capacity and resources.

The dissolution of the Soviet Union from 1988 to 1991 led to a severe decline in the Russian Navy. Defense expenditures were severely reduced, many ships were scrapped or laid up at naval bases, and shipbuilding programs were essentially stopped. Between 1990 and 1995 the number of Russian Navy personnel declined by 50 percent.[1] "In addition, the lack of funding meant that the remaining operational ships and submarines rarely deployed in the period from 1994 to 2005."[2]

After struggling for a number of years, the strength and quality of the Russian Navy finally began to improve in the 2010s. In 2012, as part of an ambitious rebuilding effort, President Vladimir Putin announced a plan to construct 51 modern ships and 24 submarines by 2020.[3] Putin's timeline to execute his rebuilding plan has now past and, although short of his target, his plans can be considered moderately successful; he has added several new assets to the Russian arsenal including 17 new submarines, 5 frigates, 18 Corvettes, 2 landing ships and several other small ships.[4]

The modernization process for the Navy is still ongoing. Four officially published documents on the Russian Federation's maritime strategy describe the future plans and the waypoints required to achieve success. New Russian strategy documents were expected in 2021, though they were not forthcoming. By utilizing U.S. Naval War College translations[5] of these documents, the aim of this article is to describe the main aspects of the key Russian maritime strategies, analyze them for common themes, and offer recommendations to NATO nations on how to appropriately react.

2015 Maritime Doctrine

The 2015 Doctrine is an essential document in Russia's ambition to maintain military relevance and exert global influence. Its primary intent is to underline Russian sovereignty inside its territorial waters, exclusive economic zone, and continental shelf while underscoring the importance of the Russian Navy to accomplish this goal.[6]

The doctrine emphasizes the necessity of modernizing the naval fleets, having high-tech shipyards, and being the world leader for the production of nuclear icebreakers. The modernization of the fleets is ongoing, including the development of new Gorshkov class frigates[7] and the continued production of world-class nuclear icebreakers.[8] Russia currently has more than 40 icebreakers[9] and three more are planned for the future.[10]

One of the goals to be achieved in the doctrine is developing and producing advanced systems and models of weapons and special equipment. On this subject, Russia's work and research on new missile systems is ongoing. The best example of this effort has been the development of the Kalibr (NATO: SS-N-30A)[11] missile system; it has been in service since 2015, with Russia already using these missiles in combat scenarios in Syria[12]. Russia is also working on hypersonic missile technology and has already conducted some tests[13].

The doctrine also highlights the role of the Federal Security Service (FSB), the successor to the KGB. The FSB, along with its subordinate, the Russian Coast Guard[14], is responsible for establishing and protecting the state borders of the Russian Federation. As a result, the Coast Guard is also increasing in number, with more than 50 new ships added to its inventory since 2013.[15]

Although it addresses vital points on regaining influence in the maritime environment, some parts of the doctrine describe future ambitions like developing the illegally-annexed Crimean Ports as tourist destinations. Considering the current conflict between Russia and Ukraine, along with tension with NATO and the international community, this desire seems to remain unfulfilled and unlikely, at least for the foreseeable future.

Fundamentals of the State Policy for Naval Operations Until 2030

Fundamentals of the State Policy of the Russian Federation in the Field of Naval Operations for the Period Until 2030 is a part of the central core of Russian maritime priorities.

The Fundamentals states that naval operations are a high priority and an integral part of the state's military activities carried out on the high seas to deter aggression against the Russian Federation and fulfill its national interests.

The Navy, as one of the key elements charged with defending Russia, is essential for confronting any potential threat to the homeland and its territorial waters. It doesn't do it alone; for example, one of the Navy's vital objectives in Russian policy and doctrine is to demonstrate Anti-Access / Area Denial (A2AD) within a complex joint force structure including both the Russian Air Force and Army. It is safe to say that mainly in the Baltic Sea and the Black Sea, with the help of geography, Russia is following this strategy.[16] It is also part of Russia's complex layered "Active Defense" policy[17], which aims to use both offence and defence as a complex deterrence strategy.

"Russia's Chief of General Staff has described Russian military strategy as one of "active defense," most prominently in a 2019 speech to the Russian Academy of Military Sciences. Active defense conceptualizes what the Russian military should do to deter a war before it begins and describes the general tenets for how it would fight a war against a militarily superior opponent. The strategy is characterized by plans to take anticipatory actions during a threatened period (period of military threat) or crisis. This is not necessarily a preemptive strike, but can be inclusive of direct use of force against a massing opponent."[18]

The Fundamentals predicts unstable military and political situations until 2030 and points out existing and emerging risks and threats to the national security of the Russian Federation on the World Ocean. It declares that the United States and its allies, which is the definition of NATO for the Russians, are dominating the World Ocean. More specifically, the document identifies the threats for the Russian Federation as follows: the increase in the number of states that have powerful combat-capable navies; the proliferation of weapons of mass destruction; new missile technologies and the spread of international terrorism; piracy; and, the smuggling of arms, narcotics, chemicals, and radioactive materials. It's a fair assumption that when mentioning the increase in the numbers of combat-capable navies (with the emphasis on "capability" as opposed to numbers of platforms), Russia is addressing NATO and its global partners. The other threats mentioned in the documents (terrorism, piracy, smuggling, etc.) can be classified as more universal concerns amongst all states, possibly opening the door to share efforts to address them should a fundamental shift in Russia's current global policies and actions occur.

Murmansk, Russia - May 25, 2010: Heavy aircraft-carrying cruiser "Admiral Kuznetsov" at the wall of the Murmansk port. Courtesy of Shutterstock.

The Fundamentals highlights the requirement for a naval presence in what the state sees as strategically important areas of the world ocean. Of course, the presence of Russian Naval Forces could be seen as a destabilizing force amongst areas where existing and emerging interstate conflicts exist. The document also mentions increased aspirations of owning hydrocarbon energy resources in the Near East, the Arctic, and the Caspian Sea basin.

It also addresses improving capabilities of the Black Sea Fleet by expanding the concentration of joint capabilities on the territory of the Crimean Peninsula, and securing the permanent naval presence of the Russian Federation in the Mediterranean Sea. Russia aims to be close to energy and transportation corridors to build more influence, as exemplified by its new naval base in Tartus[19], Syria, and its plans to construct another new base on the Red Sea coast of Sudan.

Accessing the Mediterranean is a major point in Russian policies and, even though it has the most substantial fleet, it is still effectively land-locked in the Black Sea by the Turkish Straits in the region. According to the Montreux Convention[20], in peacetime, Black Sea littoral countries have the right to transit their warships through the Turkish Straits without any tonnage restriction if they notify Türkiye eight days before the proposed transit. However, they may not transit warships designed solely for the transport of aircraft and may only transit submarines on their maiden voyage to their homeport in the Black Sea after construction.

Under the convention, non-Black Sea countries may not transit aircraft carriers or submarines into the sea at all. They may, however, transit warships under the following conditions: a ship's aggregate displacement does not exceed 45,000 tons; no more than nine ships may be in the Black Sea simultaneously; and, a ship may not remain longer than 21 days. Non-Black Sea countries are required to provide 15 days' notification before the passage.

In wartime, or if Türkiye, a NATO ally for 70 years, considers itself to be threatened with imminent danger of war, the passage of warships is at Türkiye's discretion. According to some critics, the situation for peacetime may seem to favour Russia; however, in reality, every nation in the Black Sea has equal rights to the free passage of their warships. Of course, Russia is keenly aware that a possible

conflict or war may prevent its access to the Mediterranean. Regarding the use of Turkish Straits, another study done by the Combined Joint Operations from the Sea Centre of Excellence observed:

"Despite some critics who see the Montreux Convention as an impediment to a robust NATO presence in the region, it represents a valuable legal tool allowing Türkiye to regulate and constrain transit through the Turkish Straits should the need arise. Russian decision-makers are well aware that, in the event of open conflict with a NATO country, their ability to project in the Mediterranean would be minimal due to their geographical position and the Montreux Convention. In such an open conflict, Russian supply lines into the Mediterranean and Russia's only overseas base, Tartus, which supports Russia's freedom of action operations in the Mediterranean and political interests in Syria, would be easily cut off."[21]

Russia desires to have the second most combat-capable Navy globally, although that goal seems unlikely. Currently, China has 335 ships while the U.S. has around 293.[22] The Chinese Navy is mostly comprised of frigates, destroyers, submarines, and two aircraft carriers, while the U.S. Navy has 11 nuclear-powered aircraft carriers.[23] The modernization program of the Russian Navy will expand its capabilities but, with the Chinese Navy rising in numbers and the U.S. Navy at least maintaining its force, it seems unlikely for Russia to find itself in the top two.[24]

It can also be assumed that having another aircraft carrier would cause some extra difficulties for the Russian Navy.[25] The only aircraft carrier of the Russian Navy, Adm. Kuznetsov, has had an extended period of maintenance, commencing in 2018; it is still in the yards today.[26] According to Business Insider, "the biggest problems with the carrier are its outdated propulsion system and its arresting cables."[27] Having another aircraft carrier is a force multiplier but, with the remaining maintenance problems[28] and new technology requirements, it can bring more complexity and will undoubtedly require a bigger maintenance budget at a cost that may negate any true advantages. Nevertheless, Russia has been developing plans and designs for new carriers for the last several years.

Strategy for the Development of Maritime Activities Until 2030

The Strategy for the Development of Maritime Activities until 2030 mainly focuses on how to strengthen the economy through a maritime vision. It is designed to secure the national interests of the Russian Federation in the World Ocean, including developing and implementing an effective socio-economic policy of the state in its maritime activities.[29] The Navy, in particular, is tasked to guard the state's commercial ships and maintain open routes for its vessels.

The Strategy identifies several primary challenges as follows: the aging fleet of nuclear-technology support ships; the deterioration of the FSB fleet and bases; the insufficient level of modern naval ships and onboard equipment; and, the lack of qualified experts in training personnel for maritime activities and state governance.

That being said, recently Russia's modernization programme has resulted in an increased production schedule. For example, as mentioned earlier, the Coast Guard (FSB Fleet) has enacted its own modernization programme and has built more than 50 ships in the last 10 years.[30] With the new ships introduced to the fleet, Russia has been able to improve its capabilities along its coastline.

Finally, Russia's Strategy provides a somewhat "whole of government" approach to operations in the maritime environment, assigning duties to several state institutions and ministries beyond the Navy and Coast Guard. It mentions goals like the freedom of transportation and movement, fishing and the use of marine resources, navigation, pollution of sea areas, and search and rescue activities, all of which touch multiple departments and agencies.

Strategy for the Development in the Arctic up to 2035

The Strategy for the Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035 shapes the desired achievements in the Arctic by describing national interests. This interests of the Russian Federation in the Arctic are as follows: ensuring sovereignty and territorial integrity; increasing the quality of life and well-being of the population; and, developing the Arctic zone as a strategic base to accelerate economic growth.[31] It also addresses the importance of developing the Northern Sea Route as the Russian Federation's competitive national transportation passage in the world market while still preserving the Arctic as a region for (allegedly) peaceful activities, stability, and mutually beneficial partnerships. According to the Arctic Institute, "the Russian economy is dominated by the extraction of natural resources, primarily oil and natural gas. The country is the world's third-largest producer of hydrocarbon resources, and more than 50 percent of Russia's federal budget depends on revenue derived from oil and gas production."[32] Russia is not underestimating the

Arnavutkoy, Istanbul / Türkiye - September 8 2019: Russian battleship passing Istanbul Strait on a sunny day. Courtesy of Shutterstock.

economy and the homogeneous economic development of the region. The Arctic holds a significant potential of oil and gas resources worthy of exploitation despite the harsh climate conditions.

The Strategy points out that the primary challenges to Russian national security in the Arctic are the attempts by several foreign states to revise the introductory provisions of international treaties and the unsettled international legal delimitation of northern maritime areas. It also emphasizes the actions by foreign states and (or) international organizations to obstruct the Russian Federation's so-called legitimate economic activities in the Arctic.

Members of "The Arctic Council," which, in addition to Russia, includes Canada, Denmark, Finland, Iceland, Norway, Sweden, and the U.S., are the country's main competitors in the region. It is somewhat of a balancing act for Russia between trying to assert itself and acting as a legitimate stakeholder in the region. The Arctic Council still holds significant importance for activities such as preventing military conflicts, protecting the ecological balance of the environment, and acting as a mediator between the various actors and interested parties.

Russia controls a vast part of the Arctic, much of it more austere than its other coasts, but it is determined to focus efforts on several regional projects. Notably, the population density is low in the north due to both climate difficulties and terrain conditions. It is far from being a center of attention in its current state, causing Russia to focus efforts to encourage immigration to the area. In particular, Russia is providing incentives to populate, building new facilities, and producing projects to renew existing infrastructure in the region. By improving living standards, Russia is trying to make its northern flank attractive to its citizens in order to better achieve its strategic goals.

Analysis

Upon reviewing each of the above Russian strategic documents, a few themes can be identified that may give a clearer picture of its overall maritime priorities.

First, the strategies discuss a desire to strengthen the Russian economy from the maritime perspective. The 2015 Maritime Doctrine focuses on guarding the Russian EEZ and building new nuclear icebreakers which will assure the freedom of passage in the economically essential Northern Route. The State Policy document highlights the importance of being close to energy corridors and strategic areas on the world ocean, assuring access to rich resources and the commerce they provide. The State Policy also discusses increased aspirations for owning highly valuable hydrocarbon resources in regions like the Arctic and the Caspian Sea Basin. The Maritime Activities Strategy describes how the Navy will be used to guard the Russian commerce that feeds the national economy. It also outlines objectives for modernizing the fishing and transportation fleets, which carry essential revenue streams back to the homeland. The Russian Arctic Strategy provides a high-level blueprint to address the challenges to improve infrastructure capabilities to enhance the region's population and economic capacity. One might go so far to say that the Arctic Strategy depicts the Arctic region as Russia's investment in future resource security.

Second, the modernization of Russian Naval capabilities appears consistently throughout current Russian strategy. The 2015 Maritime Doctrine addresses the strategic importance of modernizing the Russian Navy and FSB's Coast Guard. The doctrine also places importance on developing and producing advanced weapons and special equipment. The State Policy defines Russia's modern Navy as a critical element for its defense through "Active Defense" and A2AD strategies such as those found in the Baltic region. It also states the goal of Russia becoming the second most powerful Navy in the world, based in part on the development of a new aircraft carrier. The Maritime Activities Strategy mainly discusses the modernization program for the Coast Guard, but still goes further to detail the way ahead and which aspects of the maritime environment it wishes to control. The Arctic Strategy points out how improvements to infrastructure, including ports, will achieve strategic deterrence in the region.

Lastly, according to each of the strategy documents, it is obvious that Russia wants to expand its influence beyond its geographic national boundaries and EEZ. The 2015 Maritime Doctrine clearly states Russia's ambition to expand the illegally annexed Crimean Ports for use as tourist destinations. The State Policy highlights emerging risks and threats to Russian national interests, which leads to its desire for an increased presence in international maritime areas. The Maritime Activities Strategy mainly addresses the modernization program for the Fishing and Transportation Fleets in order for Russia to have a more considerable portion of the world's commerce. The Arctic Strategy points out that the economy's strength can ease future challenges for Russia, including expansion of influence.

By illuminating some of the most substantial themes running through Russian strategy documents, it is possible to identify key areas where NATO must apply focus in order to maintain its advantage over Russia.

Conclusions & Recommendations

As NATO planners continue to refine strategic guidance each year, they should pay particular attention to those areas that are most important to their chief adversary,

Russia. By focusing mitigation strategies on the three specific areas listed above, NATO will be able to effectively prioritize resources as it competes with Russia.

In terms of economic competition, NATO must act to ensure lawful access to energy rich areas such as the Arctic. Russian efforts to claim ownership of regions beyond their territorial waters should be contested openly in the appropriate forum, including the Arctic Council. As Russian claims expand, recent activities have shown that NATO must be prepared to aggressively react either diplomatically, economically, or, in the case of military options, defend freedom of navigation in the Arctic in accordance with UNCLOS. By upholding the rules based order in the Arctic, the Alliance can ensure the free flow of commerce in international waters and restrain unlawful Russian economic and military aggression.

NATO member nations should continue to modernize military and infrastructure projects to meet the requirements of the modern era in order to maintain the competitive edge over Russia. Investments in emerging technologies are key, especially in areas such as interoperability, unmanned systems, and artificial intelligence. Emerging disruptive technologies can create an arms race of technology and NATO nations must be prepared to keep pace.

As Russia seeks to expand its sphere of influence, the Alliance must continue to maintain strong relationships. A nation's strategic strength comes from the close relationships amongst its allies; NATO must not lose sight of the importance of cultivating its external relationships, outside the normal Alliance borders. Following an assymetric approach, Russia will likely pursue influence in those geopolitical regions where there is the least amount of NATO presence. To mitigate this action, NATO must be prepared to apply diplomacy where needed to minimize Russian influence and ensure access in contested regions. Indeed, the modernization of its Navy's capabilities and its efforts to increase its sphere of influence may bring current conflicts to new levels in favour of Russia. Even if it is not impossible for NATO, countering increasing Russian influence will require more capacity and resources.

Russia may be considered an old rival, but it is certainly presenting new challenges as evidenced in its recent actions in Ukraine and through its strategic planning documents. However, NATO is a long-standing Alliance and military planners provide state leaders with consistent assessments and options for timely reactions to our adversary. Russia's application of extensive military assets in Ukraine may impact its ability to follow through with its strategic plans, particularly if the conflict in Eastern Europe severely depletes Russian national resources. NATO must continue to maintain its advantage by paying close attention to, and strategically countering, Russia's plans before they become actions against our collective interests.

1 DECKER, Erin. 2010. " The State of the Russian Navy: History and Prospectives " https://geohistory.today/russian_navy/ Accessed 10 January 2022
2 GORENBURG, Dmitry. 2015. "NO, THE RUSSIAN NAVY ISN'T GOING TO COLLAPSE" https://warontherocks.com/2015/02/no-the-russian-navy-isnt-going-to-collapse/ Accessed 10 January 2022
3 https://jamestown.org/program/putin-pledges-billions-to-build-a-blue-water-navy/ Accessed 25 November 2021
4 http://russianships.info/eng/today/Accessed 24 February 2022
5 https://usnwc.edu/Research-and-Wargaming/Research-Centers/Russia-Maritime-Studies-Institute
6 DAVIS, Anna. 2015. "The 2015 Maritime Doctrine of the Russian Federation" The United States Naval War College. Newport, Rhode Island.
7 VAVASSEUR, Xavier.2020. "Project 22350 Gorshkov-Class Frigates To Join Russia's Black Sea Fleet" https://www.navalnews.com/naval-news/2020/04/project-22350-gorshkov-class-frigates-to-join-russias-black-sea-fleet/Accessed 10 January 2022
8 DASGUPTA, Soumyajit. 2022. "Top 10 Biggest Ice Breaker Ships in the World in 2022" www.marineinsight.com Accessed 24 February 2022
9 DI PANE, James. 2021 "U.S. Needs Icebreakers to Keep Up With China and Russia in Arctic" The Heritage Foundation. Washington DC.
10 NILSEN, Thomas. 2021. "Second giant nuclear icebreaker handed over to Rosatomflot" https://thebarentsobserver.com/en/arctic/2021/12/second-giant-nuclear-icebreaker-handed-over-rosatomflot Accessed 10 January 2022
11 https://missilethreat.csis.org/missile/ss-n-30a/ Accessed 25 November 2021
12 "Russia hits targets in Syria from Mediterranean submarine" https://www.bbc.com/news/world-middle-east-35041656 Accessed 25 November 2021
13 https://www.reuters.com/business/aerospace-defense/russia-test-fires-new-hypersonic-tsirkon-missiles-frigate-submarine-2021-12-31/ Accessed 24 February 2022
14 http://www.hazegray.org/worldnav/russia/bord_grd.htm Accessed 25 November 2021
15 http://russianships.info/eng/coastguard/ Accessed 10 January 2022
16 BRAUSS, Heinrich and Dr. RACZ, Andras. "Russia's Strategic Interests and Actions in the Baltic Region" German Council on Foreign Relations. Berlin
17 https://warontherocks.com/2019/09/anticipating-a-new-russian-military-doctrine-in-2020-what-it-might-contain-and-why-it-matters/ Accessed 10 January 2022
18 KOFFMAN,Michael, FINK, Anna, GORENBURG, Dmitry, CHESTNUT, Mary, EDMONDS, Jeffrey and WALLER, Julian. 2021. "Russian Military Strategy: Core Tenets and Operational Concepts" CNA. Arlington, Virginia.
19 DAVIS, Anna and MOSS, Richard. 2017 "Russian-Syrian Naval and Air Basing Agreements, 2015-2020" United States Naval War College. Newport, Rhode Island.
20 http://www.mfa.gov.tr/implementation-of-the-montreux-convention.en.mfa Accessed 24 February 2022
21 GOMENGIL, Hatice. 2020 "Conflict 2020 And Beyond: Russian Black Sea Priorities And Capabilities" CJOS COE. Norfolk, Virginia.
22 HARPER, John. 2020. "Eagle vs Dragon: How the U.S. and Chinese Navies Stack Up", National Defense Magazine, Arlington, Virginia.
23 https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2169795/aircraft-carriers-cvn/ Accessed 17 February 2022
24 https://news.usni.org/2021/11/03/china-has-worlds-largest-navy-with-355-ships-and-counting-says-pentagon Accessed 17 February 2022
25 https://nationalinterest.org/blog/reboot/russia-has-major-aircraft-carrier-issues-195352 Accessed 10 January 2022
26 https://www.navalnews.com/naval-news/2021/11/russias-aircraft-carrier-admiral-kuznetsov-to-resume-repairs-in-june-2022/ Accessed 10 January 2022
27 https://www.businessinsider.com/russia-aircraft-carrier-admiral-kuznetsov-outdated-problems-2018-4 Accessed 10 January 2022
28 https://www.navalnews.com/naval-news/2021/11/russias-aircraft-carrier-admiral-kuznetsov-to-resume-repairs-in-june-2022/ Accessed 23 December 2021
29 Davis, Anna and Vest, Ryan. 2019."Strategy for the Development of Maritime Activities of the Russian Federation until 2030" The United States Naval War College. Newport, Rhode Island.
30 http://russianships.info/eng/coastguard/ Accessed 10 January 2022
31 Davis, Anna and Holland, Emily. 2020 "Strategy for Development of the Arctic Zone of the Russian Federation and Provision of National Security for the Period up to 2035" United States Naval War College. Newport, Rhode Island.
32 https://www.thearcticinstitute.org/countries/russia/ Accessed 24 February 2022

TERRORISM IN THE MARITIME DOMAIN

CDR (RNoN) PER CHRISTIAN GUNDERSEN

"The ships that sail to and fro must have secure ports to which to return, and must, as far as possible, be followed by the protection of their country throughout the voyage." - A.T. Mahan

Frightening Scenarios

Imagine a supertanker, almost 400 meters long and more than 60 meters wide, transiting north through the Suez. The canal is narrow at this location, only 200 meters wide and 24 meters deep. Loaded with 2 million barrels of crude oil from Mina al Ahmadi in Kuwait, the tanker is destined for Hamburg. Suddenly, an explosion occurs on the bridge. It is being hit by a remotely controlled, weaponized drone. The explosion rips through the bridge and destroys control systems, making the ship drift starboard and onto the ground. Due to the wind, with the bow stuck in sand and mud, the tanker's stern slowly moves outwards, stopping only when the ship is blocking the entire canal. The fire spreads quickly on board as the other ships, which are transiting through the canal, frantically man their emergency positions with armed security teams and prepare to anchor up.

Imagine a large containership with more than 15,000 containers onboard loaded in Shanghai, entering the narrow inlet of the Rotterdam harbour area. Suddenly, an explosion caused by an improvised mine rips a hole in the hull just below the sea line. In just minutes, the giant ship begins to heel over, and containers are sliding off the ship into the water as the harbour authorities scramble all available means to manage the incident.

Imagine a busy Monday morning at the New York and New Jersey Port authorities, when suddenly the power to the entire vessel traffic management system crashes due to a major cyber-attack caused by malware. Even with backup systems, the severity of the attack slows down the ability to manage the communication and computer systems. For weeks, both arrivals and departures of ships, including delays in loading and offloading, have a considerable impact on the flow of commerce in the U.S., Europe, and Asia.

Arguably, the hypothetical scenarios above are not farfetched. The risk of a major maritime terror attack could be defined as a function of probability and severity. Risk can be hard to spot, prepare for, and manage. Even if the current probability of a major maritime terror attack is assessed to be unlikely by most experts,[1] the impact, if it was to occur, would have severe and wide-ranging consequences on markets and economies in allied countries. In that regard, there are several timely questions to be asked. What are the specific threats for terror attacks in the maritime domain, and are we able to prevent such attacks from occurring? Equally important, are we well prepared and resilient and do we have the required readiness, plans, and contingencies to mitigate the consequences if it occurs? This article aims to describe current and future threats of terror in the maritime domain and, furthermore, to display some major efforts NATO and the international community are taking to mitigate these threats.

Suez Canal Traffic. Courtesy of Egyptian Suez Canal Authorities.

Maritime Vulnerabilities

As most of us are aware, around 90% of traded goods globally are carried by sea.[2] Any major maritime terror attack would most likely have serious economic consequences, not only to the western economy but also on the global economy. The examples above illustrate this point. The Suez Canal observes more than 40 daily transits,[3] mainly of container ships and tankers, Rotterdam Port has around 30,000 sea-going vessel arrivals every year,[4] and The Port of New York and New Jersey is the gateway to one of the most concentrated consumer markets in North America and the largest port on the U.S. East Coast.[5] The

easy access and proximity to land make merchant shipping vulnerable when transiting through straits and canals connecting the high seas. The same goes for maritime infrastructure facilities like ports and harbours. With relatively limited efforts and resources, it is possible to reduce the flow of commerce and, in some instances, block it all together at these chokepoints.

Even if there are international regulations such as The United Nations Convention on the Law of the Sea (UNCLOS), the high seas could be considered somewhat anarchic, being ungoverned and unregulated outside most countries' territorial waters. This creates opportunities for those who want to undermine the current Rules-Based International Order and harm western and global trade without necessarily entering the NATO realm. During the last decades, weak and failing states have allowed terrorist organizations to establish safe havens and operating areas close to allied countries' borders, leading NATO to identify terrorism as one of the most immediate asymmetric threats to the Alliance and its member nations.[6]

Assessing future consequences, including second or third-order effects of major terror attacks in the maritime domain, is rather challenging. However, looking at a recent real-life maritime incident may provide some insight. When the container ship Ever Given was stuck in Suez for six days in March 2020, the insurance company Allianz estimated the cost to the shipping industry to be about a billion dollars a day.[7] It is reasonable to assume that the economic consequences would accelerate if the canal was blocked for weeks or even months. In addition, the Ever Given incident was not deliberate. If it had been a terror attack, the threat of new attacks would have created frantic security discussions in the international community and within the shipping industry.

Defining Maritime Terrorism

Creating fear is considered a key aspect of terrorism.[8] Arguably, terrorism in the maritime domain is less about creating fear and more about targeting maritime trade to harm the western world economy in a rather direct manner. Al-Qaeda's "bleed to bankruptcy strategy,"[9] is still assessed to be a guiding philosophy to destabilize western economies that rely on vulnerable resources. Some state actors have also seen the advantages with a similar approach. With these aspects in mind, maritime terrorism could be defined as the unlawful use or threatened use of force or violence against maritime trade onshore or at sea in an attempt to harm the economy of governments, to achieve political, religious, or ideological objectives.

The Nexus between Maritime Terrorism and Maritime Crime

There are some fundamental differences between maritime terrorism and illicit activity at sea such as piracy or smuggling. In general, terrorism is ideologically motivated, while illicit activity is driven by money. However, there are some grey areas and a nexus between the two varieties of illegitimate activities. When the ends justify the means, illicit activity such as the smuggling of weapons and drugs by sea may directly or indirectly support terrorism. On several occasions, the terror group Al Shabaab in Somalia has utilized piracy and smuggling to generate revenue[10] and during the last decades, Iran has allegedly been caught smuggling weapons by sea in support of terrorist groups. In late December 2021, off the northern reaches of the Arabian Sea, the U.S. Navy seized 1400 Kalashnikov-style assault rifles and 226.600 rounds of ammunition being smuggled by an Iranian fishing ship, most likely en route Yemen and the Houthis.[11] Furthermore, Israel has claimed to have intercepted Iranian merchant ships with advanced weapons bound for Gaza and Hamas on several occasions.[12] Smuggling may be the primary business for some illicit crime syndicates, but maritime terrorism also relies on illegal shipping, just for very different reasons.

The Hybrid Warfare Threat in the Maritime Domain

Too often terrorism is solely linked to the Middle East Region and Jihadism; however, as the Director of the NATO Shipping Centre Captain (N) Niels Markussen correctly points out, "…State-sponsored terrorism is often overlooked, and currently that is the biggest threat in the maritime domain… Furthermore, terrorism is a natural part of hybrid warfare."[13] According to a recent NATO review, hybrid warfare is the combination of conventional as well as unconventional instruments of power, blended in a synchronized manner to exploit the vulnerabilities of an adversary, achieving synergistic effects.[14] Looking at specific hybrid threats, NATO defines those as the combination of "military and non-military as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, deployment of irregular armed groups and use

U.S. Navy seized weapons in the North Arabian Sea 6 May 2021. Courtesy of U.S. Navy.

of regular forces."[15] Currently, NATO's adversaries are employing different methods of hybrid warfare by putting pressure on governments and decision-makers, including attempting to drive wedges between the allied members. In addition, hybrid warfare is often characterized by actions that are difficult to attribute, concealing a state's involvement, delaying allied consensus and stifling unified response efforts. Russia has employed different methods of hybrid warfare in Ukraine and, in Yemen, the Houthis take responsibility for maritime attacks that are clearly directed by Iran.[16] When thinking about the potential effects of hybrid warfare on allied nations, if U.S.-Iran tensions escalated and a staged maritime accident closed the Suez-canal for weeks, a U.S. Strike Group in the Mediterranean Sea bound for the Indian Ocean would be delayed for approximately a month, forced to circumnavigate Africa. As part of a hybrid warfare strategy, maritime terrorism may be a perfect tool for operating in the grey areas below the threshold of war, creating uncertainty and blurred lines between motives and the actors involved.

Threats from Unmanned Technology

Recent technological development in unmanned systems have provided terrorist groups with several new low-cost and easily accessed means to conduct maritime terror attacks. Remotely controlled, weaponized drones and water-borne improvised explosive devices, like unmanned fast crafts filled with explosives, are examples that have recently been employed by different state-backed and non-state terrorist groups. On the 29th and 30th of July, 2021, the Israeli Motor Tanker (M/T) Mercer Street was attacked by three unmanned aerial vehicles (UAVs) while transiting international waters off the coast of Oman. While the first two attacks were unsuccessful, the last UAV, loaded with a military-grade explosive, hit the pilothouse's topside. The explosion created a 6-foot diameter hole, killing two crew members and badly damaging the interior.[17] Based on the investigation, U.S. experts have concluded that the UAV was produced in Iran; however, no official attribution for the attack has been made public.

During the last couple of years, there have been several reports where remotely controlled small boats carrying explosives have been used to attack merchant shipping. In March 2020, three small boats east of the Gulf of Aden attacked a Saudi-registered merchant vessel in the International Recognized Transit Corridor. Two of these boats were remotely controlled with explosives on board. The attack was unsuccessful, and the merchant vessel was able to continue the transit unharmed: it is still unclear who was behind the attack.[18] In addition, several similar attacks have been reported by Saudi Arabia during recent years amid the regional conflict with Iran.[19]

Cyber Threats

The maritime industry is increasingly digitalizing, and in some cases automating its operations. This development has streamlined and simplified shipping. However, the dependency on computer systems to manage day-to-day operations onboard ships and in ports has also created opportunities that can be exploited by adversaries.[20] Modern merchant ships rely on highly technical computer systems to communicate internally and externally, to navigate, and to manage the ship. Sophisticated data systems have simplified and streamlined the daily command and control functions but have also created more vulnerabilities. Even with redundancy systems onboard, hacking or jamming of a ship's control, communication, or navigation systems, may create dangerous accidents.[21]

Several maritime stakeholders, including ports, carriers, and logistics providers, have been victims of significant and costly cyber-attacks during the last decade. The increased dependency on information and operational technology has made commercial supply hubs vulnerable. Cyber-attacks on any of these systems may not only negatively affect the specific company or port, but will most likely have severe consequences for trade, economies, and security in general. In June 2017, A.P Moller-Maersk, the world's largest container ship operator and among the five largest port terminal operators, was attacked by a piece of the wiper malware called NotPetya. The malware affected Maersk operations in 17 major port terminals and spread through critical IT systems. In the end, the company had to reinstall its entire IT infrastructure, and it is estimated that the total financial loss was up to 300 million USD.[22]

Currently, it is unlikely that terrorist groups are able to utilize the cyber domain for launching significant attacks, but there are state actors who are certainly

Drone attack on MT Mercer Street July 2021. Courtesy of U.S. CENTCOM.

phishing, distributed denial-of-service attacks, destructive malware, and cyberattacks intended to cause physical consequences.[23] Arguably, cyber-attacks are the perfect tool in a hybrid warfare strategy, since they are often below the threshold of war and difficult to attribute.

Physical Threats to Maritime Infrastructure

Ports, harbours, and ship terminals are often located in areas where large numbers of people live and work. Even with strict security measures in place, these essential components of the global supply chain represent some of the most challenging infrastructure to protect due to the complexity of all the moving parts. Giant merchant ships, millions of containers, thousands of trucks, rails, and people all come together in confined areas, keeping the global economy moving forward 24 hours a day. Rotterdam, for example, is the largest port in Europe, extending more than 40 km in length, processing more than 23,000 freight containers daily, and employing a workforce of around 180,000 people.[24] Unfortunately, the port of Rotterdam is also infamous as the major cocaine smuggling gateway into Europe. Last year, almost 500 people working at the port were arrested for participating in this illicit activity.[25] Although drug smuggling is not directly related to terrorism, it does demonstrate how dedicated terrorists could potentially smuggle weapons or a dirty bomb onto a ship bound for a western port. In addition, the availability and speed of maritime shipping itself could be used by terrorists to move operatives or weapons, if desired. According to Lloyd, there are about 3000 registered ports and more than 4000 harbours globally,[26] which are all connected by the maritime domain. This global interconnectedness of the shipping industry represents nearly worldwide reach for terrorists seeking to utilize containers as their delivery platform of choice. A single container could be handled on various means of transportation and visit several ports before arriving at the final destination, allowing it to be used in a wide range of illicit means. Internationally, only 2% of all containers are physically inspected by customs authorities, allowing terrorists to hide materiel in plain sight. Even with different scanning technologies, it is widely believed that the only viable way to control containerized cargo is through information-based risk analysis.[27] The vulnerability of shipping terminals, combined with the economic importance and dependency on the shipping industry, make port infrastructure and operations attractive targets for terrorist attacks or exploitation.[28] In that regard, maritime infrastructure is a relatively risk-free and cost-effective means for terrorism to have a global reach.

Countering Maritime Terrorism

In the aftermath of 9/11, several counter-terrorism initiatives were launched by NATO. Especially of note in the maritime domain was the establishment of Operation Active Endeavour, with the mission to deter, defend, disrupt, and protect shipping against terrorist activity in the Straits of Gibraltar and the Mediterranean. In October 2016, it was superseded by the still ongoing Operation Sea Guardian. Both missions have been highly effective, successfully deterring and preventing terror attacks in the Mediterranean since 2001.[29]

Port of Rotterdam. Courtesy of Shutterstock.

In 2004, NATO established a Defense Against Terrorism Programme of Work (DAT POW) with the aim to "strengthen the Alliance's contribution to combating terrorism by enhancing capability development, supporting operations and fostering partnerships."[30] Currently, the programme has projects covering a wide range of areas in the maritime domain, including protection of harbours and ports. Under the leadership of France, various technologies have been explored, included sensor nets, electro-optical detectors, rapid-reaction capabilities, underwater magnetic barriers, and unmanned underwater vehicles.[31] Furthermore, under the leadership of the NATO Centre for Maritime Research and Experimentation (CMRE) located in La Spezia, Italy, there is ongoing research assessing the use of autonomous underwater systems to detect maritime IEDs and virtual reality for situational awareness.

In 2012, NATO agreed on Policy Guidelines for Counterterrorism, which provided strategic direction for allied activities. The Policy Guidelines identify critical areas where the Alliance could implement initiatives to enhance the prevention of, and resilience to, acts of terrorism. Linking counter-terrorism efforts closer to NATO's core tasks of Collective Defense, Crisis Management and Cooperative Security, the new policy focuses on NATO's strengths such as intelligence sharing, capacity-building, special operations forces, training, and technology and capabilities.[32] "In doing so, the guidelines inaugurate a new phase of NATO's engagement in countering terrorism,

predicated around the three principles of compliance with international law, NATO support to allies, and non-duplication and complementarity in addition to focusing on the three key areas of awareness, capabilities, and engagement."[33] At the same time, SHAPE established the Comprehensive Crisis and Operations Management Centre (CCOMC). As SHAPE's new horizon scanning entity, the CCOMC was seen as a step in the right direction, enhancing information and intelligence sharing across the Alliance. NATO has embraced a comprehensive approach, acknowledging that allies must cooperate and coordinate plans, activities, and operations with civilian entities, governmental and commercial, to counter terrorist threats.

To keep a required readiness and enhance competence across the Alliance, NATO and member nations conduct training and exercises in which counterterrorism is part of the scenario. In addition, NATO conducts more specific counterterrorism exercises like Northern Challenge. This annual NATO exercise, hosted by the Icelandic Coast Guard, focuses on countering IEDs. The main purpose of this exercise is to realistically practice how to neutralize IEDs at a variety of critical infrastructure locations, including airports, shipping ports, onboard ships, and at piers. In the 2021 exercise, operators from 15 countries participated, aiming at enhancing member nations' capabilities and verifying NATO Tactics, Techniques, and Procedures.[34]

The United Nations and other international organizations have also been proactive in preventing terror attacks in the maritime domain. In 2004, the International Maritime Organization (IMO) established a new set of mandatory security regulations, The International Ship and Port Facility Security (ISPS) Code, which was amended as a part of the International Convention for the Safety of Life at Sea (SOLAS) 1974. The ISPS Code prescribes responsibilities to governments, shipping companies, shipboard personnel, and port facility personnel to detect security threats and take preventive measures against security incidents.[35] The general view is that the implementation of the ISPS Code and other security measures have been successful, especially in countries that have the knowledge, government structures, and economy to implement these regulations.[36] Currently, SOLAS has 168 contracting states, flagging about 99% of merchant ships around the world in terms of gross tonnage. Since the ISPS Code is part of SOLAS, it is mandatory for all signatories to comply with the regulations. Nevertheless, IMO does not have a policy to retain a list of non-compliant ports or flag states and there are still numerous ports and ships, especially in developing countries, that are not in compliance with the regulations.

It is also worth mentioning that the United States has been at the forefront of several additional moves to upgrade global maritime security over the last decades, including the Container Security Initiative[37], the Proliferation Security Initiative,[38] and the Customs-Trade Partnership against Terrorism.[39] The U.S. has also been instrumental in instituting regional maritime security initiatives and capacity building efforts in areas recognized as vital to its counter-terrorism strategy.[40]

Lastly, the maritime industry has taken significant steps to harden its operations against the threat of physical and cyber terrorist attacks on ships, ports, and other critical infrastructure. Realizing the effectiveness of proactive defensive efforts, the industry has employed armed security teams onboard ships, enhanced physical perimeter and cyber security, conducted training, developed comprehensive threat assessments and established plans to mitigate and handle maritime terrorism. While acknowledging that the risk of a terror attack never will disappear entirely, the maritime industry has established a cost-effective approach, mitigating the risk to manageable levels.

Exercise Northern Challenge. Courtesy of NATO.

Conclusion

The world is increasingly dependent on a predictable and reliable international shipping industry, and this is of course the case for NATO member nations as well. The Western economy is built on the Rules-Based International Order established after World War II with global trade becoming even more interdependent during the last few decades. With new disruptive and emerging technologies, sea lines of communication are vulnerable to new avenues of attack such as unmanned vehicles and cyber. The introduction of more state-backed terrorism and hybrid warfare strategies applied in the maritime domain needs to be taken seriously. It is possible to conduct low-cost and low-risk attacks in both ports and on the high seas, which would have severe economic consequences for NATO countries. Although there have been no major terror attacks

in the maritime domain in recent years, it is important to remember that surprise is an essential element of terrorism, making it an ever-present threat. NATO, its member nations, international organizations, and the shipping industry must continue to stay vigilant to ensure various security measures are in place and the terror threat is being consistently addressed. NATO's Operation Sea Guardian is currently deterring terrorism in the Mediterranean and the DAT POW has several ongoing counterterrorism projects in the maritime domain. In addition, the IMO's establishment of the ISPS Code and the U.S. Container Security Initiative have enhanced the level of global maritime security.
An attack may not occur today or tomorrow, but the vulnerability of the maritime sea lines of communication and the international shipping industry demands allied nations stay resilient and well prepared.

1 UKMTO, quarterly reports 2021, https://www.ukmto.org/indian-ocean/products/quarterly-reports/2021, retrieved from internet 14. Jan. 2022.
2 OECD, "Ocean shipping and shipbuilding," https://www.oecd.org/ocean/topics/ocean-shipping/, retrieved from internet 4. Feb. 2022.
3 Statista, "Average daily number of transits in the Suez Canal from January 2019 to February 2021," https://www.statista.com/statistics/1127798/average-number-of-transits-in-the-suez-canal-per-day/, retrieved from internet 4. Feb. 2022.
4 Port of Rotterdam, "Harbor Master," https://www.portofrotterdam.com/en/about-port-authority/our-organisation/harbour-master, retrieved from internet 4. Feb. 2022.
5 The Port of New York & New Jersey, "The Largest U.S. East Coast Container-port," https://www.panynj.gov/port/en/index.html, retrieved from internet 4. Feb. 2022.
6 NATO, "Countering terrorism," 14. Sep. 2021, https://www.nato.int/cps/en/natohq/topics_77646.htm, retrieved from internet 14. Jan. 2022.
7 Caesar, Ed, "The Ship that became a bomb," The New Yorker, 4. Oct. 2021, https://www.newyorker.com/magazine/2021/10/11/the-ship-that-became-a-bomb, retrieved from internet 30. Nov 2021.
8 Nato describes terrorism as "the unlawful use or threatened use of force or violence, instilling fear and terror, agains individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives.", NATO, "NATO's military concept for defence against terrorism," 19. Aug. 2016, https://www.nato.int/cps/en/natohq/topics_69482.htm, retrieved from internet 9. Nov 2021.
9 Pippard, Tim, "Oil-Qaeda': Jihadist Threats to the Energy Sector," Perspectives on Terrorism, Volum 4, Issue 3, July 2010
10 Farquhar, Samantha D., "When Overfishing Leads to Terrorism," The Journal of International Issues, Vol. 21, No. 2 (Summer (April-June) 2017), pp. 68-77.
11 Debre, Isabel, "U.S. Navy says it seizes arms from Iran likely bound for Yemen," Washington Post, 22. Dec. 2021, https://www.washingtonpost.com/world/us-navy-says-it-seizes-arms-from-iran-likely-bound-for-yemen/2021/12/22/51ac88f6-63a9-11ec-9b51-7131fa190c5e_story.html, retrieved from internet 4. Jan. 2022.
12 Kershner, Isabel, New York Times, "Israel Says It Seized Ship in Red Sea With Load of Iranian Rockets Headed to Gaza," 5. Mar. 2014, https://www.nytimes.com/2014/03/06/world/middleeast/israel-fires-on-militants-along-syrian-border.html, retrieved from internet 4. Feb. 2022.
13 Markussen, Niels, in mail correspondence, 25. Nov 2021.
14 Bilal, Arsalan, "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote," NATO Review, 30. Nov. 2021, https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html, retrieved from internet 15. Dec. 2021.
15 NATO, "NATO's response to hybrid threats," 16. Mar. 2021, https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en, retrieved from internet 15. Dec. 2021.
16 Zimmerman, Katherine and Nicholas A. Heras, Foreign Policy, "Yemen Has Become an Iranian Proxy War Against Israel," 24. Jan. 2022, https://foreignpolicy.com/2022/01/24/yemen-houthi-uae-israel-iran-abraham-accords/, retrieved from internet 4. Feb. 2022.
17 U.S. Central Command, "U.S. Central Command Statement on the Investigation into the Attack on the Motor Tanker Mercer Street," 6. Aug. 2021, https://www.centcom.mil/MEDIA/PRESS-RELEASES/Press-Release-View/Article/2722418/us-central-command-statement-on-the-investigation-into-the-attack-on-the-motor/, retrieved from internet 15. Dec. 2021.
18 Binnie, Jeremy, "Saudi Arabia identifies tanker attacked in Gulf of Aden," Janes, 25. Mar. 2020, https://www.janes.com/defence-news/news-detail/saudi-arabia-identifies-tanker-attacked-in-gulf-of-aden, retrieved from internet 16. Dec. 2021.
19 Aljazeera, "Saudi Arabia says it foiled boat attack off Yanbu port," 27. Apr. 2021, https://www.aljazeera.com/news/2021/4/27/saudi-arabia-says-it-foiled-boat-attack-off-yanbu-port, retrieved from internet 4. Feb. 2022.
20 Portase, Ovidiu, "Cyber Risk within the Maritime Domain," Cutting the Bow Wave, CJOS COE, 2017
21 Youd, Frankie, "Cyber-attacks: how hackers are targeting seafarers," Ship Technology, 22. Jun. 2021, https://www.ship-technology.com/features/cyber-attacks-how-hackers-are-targeting-seafarers/, retrieved from internet 15. Dec 2021.
22 Organization of American States, "Maritime Cybersecurity in the Western Hemisphere," 2021, https://www.oas.org/en/sms/cicte/docs/Maritime-cybersecurity-in-the-Western-Hemisphere-an-introduction-and-guidelines.pdf, retrieved from internet 17. Dec. 2021.
23 U.S. Cybersecurity & Infrastructure Security Agency, "Iran Cyber Threat Overview and Advisories," https://www.cisa.gov/uscert/iran, retrieved from internet 16. Dec. 2021.
24 Port of Rotterdam, "Working and Learning, A world full of opportunities," https://www.portofrotterdam.com/en/building-port/working-and-learning, retrieved from internet 17. Dec. 2021.
25 NL Times, "Over 450 "drug extractors" caught at Rotterdam port this year," 19. Nov. 2021, https://nltimes.nl/2021/11/19/450-drug-extractors-caught-rotterdam-port-year, retrieved from internet17. Dec. 2021.
26 Lloyd, Lloyd's List, https://directories.lloydslist.com/, retrieved from internet 17. Dec 2021.
27 The European Commission's Science and Knowledge Service, "Monitoring container traffic and analysing risk," https://ec.europa.eu/jrc/en/research-topic/monitoring-container-traffic-and-analysing-risk, retrieved from internet 17. Dec. 2021.
28 Willis, Henry H., "Ten Years After the Safe Port Act, Are America's Ports Secure?," The RandBlog, 6. Apr. 2016, https://www.rand.org/blog/2016/04/attractive-targets.html, retrieved from internet 17. Dec. 2021.
29 NATO, "Operation Sea Guardian," 17. May 2021, https://www.nato.int/cps/en/natohq/topics_136233.htm, retrieved from internet 9. Feb. 2022.
30 NATO, "Defence Against Terrorism Programme of Work (DAT POW)," 24. Mar. 2021, https://www.nato.int/cps/en/natohq/topics_50313.htm, retrieved from internet 1. Dec. 2021.
31 Ibid.
32 Santamato, Stefano, "The New NATO Policy Guidelines on Counterterrorism: Analysis, Assessments, and Actions," Strategic Perspectives 13, National Defense University Press Washington, D.C., February 2013.
33 Ibid, p.1.
34 Thompson, Desirai, "International Bomb Experts Train At Keflavík," Reykjavik Grapevine, 20. Oct. 2021, https://grapevine.is/news/2021/10/20/international-bomb-experts-train-at-keflavik/, retrieved from internet 4. Jan. 2022.
35 IMO, "What is the ISPS Code?," https://www.imo.org/en/OurWork/Security/Pages/FAQ.aspx#What_is_the_ISPS_Code, retrieved from internet 17.Dec. 2021.
36 SAFETY4SEA, "Security Measures: A brief review of ISPS Code implementation," 18. Jun. 2019, https://safety4sea.com/cm-security-measures-a-brief-review-of-isps-code-implementation/, retrieved from internet 25. Jan. 2022.
37 U.S. Customs and Border Protection, https://www.cbp.gov/border-security/ports-entry, retrieved from internet 25. Jan. 2022.
38 Ibid, https://www.cbp.gov/border-security/international-initiatives/proliferation, retrieved from internet 25. Jan. 2022.
39 Ibid, https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat, retrieved from internet 25. Jan. 2022.
40 U.S. Defense Security Cooperation Agency, Institute for Security Governance, "Building Sustainable Maritime Capacity," Version 1, Jan. 2021, https://instituteforsecuritygovernance.org/documents/113018911/125185574/MarSec.pdf/a587ac6b-9a71-8a7d-a5ba-6131df25bf03?t=1622747075389, retrieved from internet 25. Jan. 2022.

STRATEGIC LINES OF COMMUNICATION, A MODERN APPROACH TO LINES OF COMMUNICATION

MAJ (RCAF) ALEX CONSIDINE

NATO should adopt the term Strategic Lines of Communication in order to more accurately represent the multi-domain environment and the LOCs therein.

NATO has, through multiple Summits, made it clear that enablement and reinforcement from North America to Europe are fundamental to collective defence, which traditionally relies on Sea Lines of Communication (SLOC). However, does the single domain thinking on Lines of Communication (LOCs) accurately describe the intricate web of relationships that comprise today's global security environment?

The concept of LOCs, conventionally referred to as the domain-focused SLOC, Air Lines of Communication (ALOC), and Land Lines of Communication (LLOC), is not new. They largely exist in a single domain connecting home base to a theatre of operations. However, the security of these domain-centric LOCs relies heavily on contributions from all the other domains, which will be explored below. As NATO moves into a multi-domain environment, and with the political decision to designate Cyber and Space as operational domains, a term to connect the various LOCs is necessary.

This article suggests that NATO should adopt the term Strategic Lines of Communication, abbreviated StLOC. StLOC expands established thinking of single-domain focused LOC to a multi-domain approach, capturing the joint operational perspective expected of modern NATO Commands and acknowledging interrelated and multi-domain LOCs. NATO has not formally recognized the term StLOC, but it is being used with increasing regularity in allied documents. To cover all aspects of the expression, a proposed definition is offered as "a system of systems of interconnected domains from seabed to space inclusive of all Lines of Communication."

Courtesy of U.S. CENTCOM.

This article will rationalise the relevance of StLOC via an exploration of the related threats and the relationships of the maritime, land, air, space, and cyber domains. Through a common NATO understanding of a multi-domain StLOC methodology, the Alliance is better poised to shape and coordinate non-military and military instruments of power.

Long-Established Concepts

The concept of LOCs is familiar, defined by the NATO Standardization Office (NSO) as "all the land, water, and air routes that connect an operating military force with one or more bases of operations, and along which supplies and reinforcements move".[1] Specifically, SLOCs are "the primary maritime routes between ports, used for trade, logistics, and naval forces."[2] According to NATO AJP 3.1 Allied Joint Doctrine for Maritime Operations, SLOCs are conventionally secured via maritime power.[3] However, these definitions fall short of accurately describing LOCs in modern times, mainly because they focus on a single-domain and do not recognise the essential need for a comprehensive approach. With evolving technology and warfare, NATO must move beyond the stove-piped focus as allied security demands a joint, 360 degree, all domain methodology. To analyse the transition from individual LOC to StLOC, we must first consider the threat.

Modern Threat

Recent history has demonstrated that adversarial state actors are not constrained by conventional methods; instead, they operate across the entire spectrum, including asymmetric, hybrid, conventional, and nuclear activities. Hybrid warfare[4] is the existing reality and has become a tool of state and non-state actors alike.[5] The world has witnessed cyber hacking, events in Crimea and Ukraine, political interference, military exercises, and weapon advancement. It is also entirely feasible that multiple adversaries could cooperate for common strategic goals.

Recent conflicts demonstrate that the threat to NATO is not simply from state actors, as terrorist organizations may also target allies in order to create disorder that can be exploited to achieve political, religious or ideological objectives. As state and non-state actors may attempt to manipulate allied actions across all domains, adding StLOC to the LOCs lexicon is a necessary evolution.

A Multi-Domain Approach

In his December 2020 speech to the Royal United Services Institute (RUSI) conference General Sir Nick Carter, former UK Chief of Defence Staff, argued that allies cannot operate in silos and that integration is essential across the maritime, land, air, space, and cyber domains.[6] NATO is in the process of implementing a multi-domain approach to operations but, broadly, it means orchestrating military activities across multiple domains synchronized to generate effects.[7] This multi-domain approach forms the core of the StLOC. Figure 1, from the U.S. Joint Planning Publication 5-0 reinforces the intricate linkage of the various domains in the operational environment. Knowing that each domain is vulnerable to, contingent on, and generates effects in the others provides a lens through which to view the relationships that support a movement towards StLOC recognition.

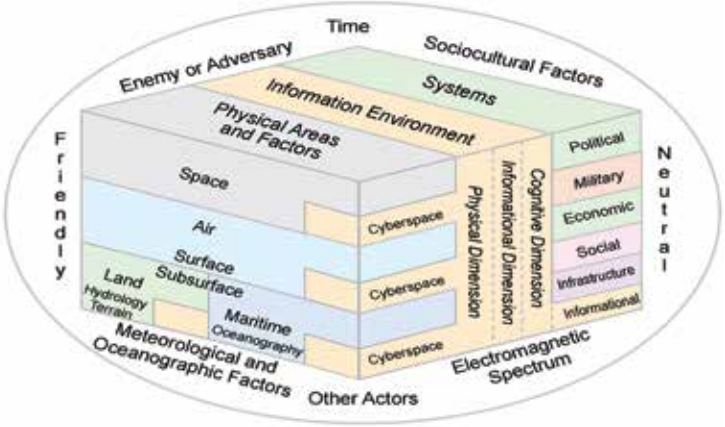


Figure 1: Holistic View of the Operational Environment. Courtesy of U.S. Joint Chiefs of Staff.

The Maritime Domain

The maritime domain is multi-dimensional, from military reinforcement and commercial shipping to the development and distribution of natural resources. It "encompasses oceans, seas and littorals, on, above and below the surface, in all directions."[8]

As a key consideration, the traditional understanding of SLOCs forms a portion of the StLOC. However, conventional definitions do not relate to the fact that merchant shipping and naval vessels operating along the SLOC, in addition to being susceptible to the traditional warfighting environments (subsurface, surface, and air), are vulnerable to threats from all the other domains including cyber and space. The use and assurance of SLOC rely on space-based communications, cyber environment connection, and command and coordination with air assets. Furthermore, there is a requirement for security of Sea Ports of Embarkation (SPOE), Sea Ports of Disembarkation (SPOD), staging areas, and onward movement of forces, equipment, and supplies traveling to the theatre of operations. The traditional view on SLOC does not take into account that maritime capabilities are able to influence other domains and LOCs, including striking land targets or contributing to their security by support to integrated air and missile defence.

The term subsurface corresponds to everything below the surface of the sea down to and including the seabed. When discussing this environment, most think initially of submarines but, taken a step further, modern submersibles have the ability to threaten land, sea, and air targets and LOCs. Today there are more than 400 active cables spanning the globe from the Mediterranean to the Arctic. Considering that an estimated 95% of international data travels via the "information super-highways" of undersea cables, their vital importance to global affairs cannot be underestimated: communications (both civilian and secret diplomatic/military), international scientific cooperation, and $10 trillion in daily financial transfers are a few examples.[9] Adversary nations possess the capability to sever these connections completely or, perhaps more surreptitiously, intercept information to steal, subvert, and exploit data. Beyond the risk to information, vulnerable undersea pipelines supply vast amounts of fuel and energy resources to allies and countries around the world. Disrupting these essential civilian LOCs or infrastructure would be catastrophic to the communication, commerce, and energy security of allied nations and beyond. Repairs, sometimes miles below the surface, are not only difficult but also costly, requiring specialized equipment owned and operated by private companies in both international and national waters. This obliges the nurturing of robust non-military instruments of power coordination.

In essence, the term StLOC captures the reality that the maritime domain spans from the seabed to surface and beyond, intertwined with all domains, reinforcing the fact that a more appropriate and comprehensive LOC term is required.

The Land Domain

NATO defines the land battlespace as "the land surface of the earth, natural and constructed features, and the underground areas below it."[10] As with other domains, the land domain relies on logistics, cyber, and space-based communications, air and sea transport, and finally positioning, navigation, and timing (PNT). Forces in the land domain also provide support by securing vital infrastructures such as seaports, airports, satellite launch sites, and undersea structure terminal points. Subsurface, surface, and air assets can transport SOF forces stealthily. Forces operating along LLOCs are vulnerable to interference and attack from actors in other domains, including naval and aerial bombardment. Evidently, the domains intermingle and mutually support each other, thus demonstrating the significance of adopting the term StLOC to represent the importance of every LOC to NATO success.

The Air Domain

The air domain extends from the surface of the earth up to space. NATO defines it as "the volume of airspace above land and maritime battlespace up to the Karman line,"[11] recognized to be at 100 kilometres (approximately 62 miles) above sea level. A significant portion of military and commercial equipment and personnel travel along ALOCs. Military aircraft contribute to NATO strike capabilities with land and sea-based aircraft, supporting both maritime and land domains. Some aircraft can travel between the air and space boundary, and nations are investing in air-launched anti-satellite weapons that could have a potential impact on every domain and LOC. The NATO Military Committee paper to the Council on Joint Air Power advocates that Joint Air Power "includes

Courtesy of Shutterstock.

elements operating in the Air, Maritime, Land and Cyber domains, supported by Space, it represents one of the strongest drivers for the integration of multi-domain operations."[12] These interrelations align themselves more accurately to the concept of StLOC.

The Space Domain

As of 2019, "Allies adopted NATO's Space Policy and recognized space as a new operational domain alongside air, land, sea and cyberspace."[13] Space-based contributions to StLOC include satellites for PNT, intelligence collection, communications, and integrated air and missile defence warning. Forces in every domain operating along the air, land, or sea LOCs rely on crucial space-based environmental data. If the PNT or SATCOM were lost, it would create a need to rely on reversionary modes, seriously inhibiting NATO's ability to counter an adversary's actions and jeopardizing international security. According to the NATO AJP-3 Allied Joint Doctrine for the Conduct of Operations, space is its own domain that "serves as an enabler for the more traditional operating environments of maritime, land and air."[14]

The Cyber Domain

The cyber domain (cyberspace) refers to the "virtual, non-physical domain formed by all information technology systems interconnected on a global scale."[15] While the cyber domain is not a physical battlespace, it is equally as important in its enhancement of the StLOC conversation. In July 2016, allies "recognized cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea."[16] Nations rely on the cyber domain for uninterrupted, secure transmission and storage of vital financial, personal, military, and political data. From a NATO and StLOC perspective, the undersea infrastructure previously discussed is a component of the cyber link. NATO Command and Control architecture relies on communication and information systems to conduct operations. Modern military equipment is reliant on robust software but can be susceptible to adversary hacking and interference. Disruption of the cyber domain has severe consequences across all of the interconnected domains and LOCs. Kristiansen and Haem's paper on Russian Cyber Strategy offers, "cyber warfare is intended to be used as part of a multi-domain effort."[17] This supports the argument that StLOC more accurately summarizes the interactions from a LOC perspective.

Conclusion

As discussed, "lines-of-communications should be globally monitored and secured over (space) cyber, land, sea and in the air."[18] The threats to NATO are conventional and unconventional, symmetric and asymmetric, persistent across all domains and LOCs. Maritime, land, air, and space domains each occupy unique physical battlespaces, whereas the cyber domain is virtual (with physical nodes). The domains form an intricate web of interdependencies wherein each influences the others, forming a 360-degree multi-domain battlespace. As Major Jerry Drew professes, "in contemporary warfare, domains are inseparable, and domain-specific theories of warfare may be misleading."[19] NATO should adopt the term Strategic Lines of Communication in order to more accurately represent the multi-domain environment and the LOCs therein. The proposed StLOC definition forms part of the alignment to an MDO reality, consistent with political ambitions for a NATO Command and Force Structure fit for purpose deep into the 21st century. Reinforcement and sustainment may be the main goal of a domain-specific LOC but ensuring freedom of manoeuvre is the business of StLOC.

Courtesy of Shutterstock.

1 Definition of lines of communication, NATO Standardization Office, https://nso.nato.int/natoterm/Web.mvc, accessed 17 Dec 2020

2 Global commerce and sea lines of communication in the Indian Ocean: A Sri Lankan perspective, (1O April 2019). Daily FT www.ft.lk/opinion/Global-commerce-and-sea-lines-of-communication-in-the-lndian-Ocean--A-Sri-Lankan-perspective/14-67. accessed 19 Nov 2020

3 NATO, AJP 3.1 Allied Joint Maritime Operations, Dec 2016, p. 1, https://nip.ac.nato.int/edms/dcosops-oc opcon/public/201612 NU AJP-3.1 Allied Joint Doctrine for Maritime Ops EDA V1 E.pdf#search=AJP%2D3%2E1%20Allied%20joint%20maritime%20operations accessed 15 Dec 2020

4 Hybrid threat -"A type of threat that combines conventional, irregular, and asymmetric activities in time and space" Definition of hybrid threat, NATO Standardization Office, https://nso.nato.inUnatoterm/Web.mvc, accessed 22 Jan 2021. Jovana Marovic, It can include cyber, interference, disinformation, and financial attacks to name a few, 'Wars of Ideas: Hybrid Warfare, Political Interference, and Interference", 28 Nov 2019, Return to the new perspective on Shared Security: NATO's Next 70 Years, Carnegie Europe, https://carnegieeurope.eu/2019/11/28/wars-of-ideas-hybrid-warfare-political-interference-and-disinformation-pub-80419 accessed 22 Jan 2021

5 Bachmann and Gunneriusson, "Hybrid Wars: the 21st- Century's New Threats to Global Peace and Security", p. 80, University of North Georgia, https://unq.edu/inslitute-leadership-strategic-studies/ uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientiamiIitaria.pdf?t=1569110400096. Accessed 22 Jan 2021.

6 General Sir Nick Carter GCB CBE DSO ADC Gen, Chief of Defence Staff's speech, (Annual RUSI Conference, 17 Dec 2020).

7 NATO Standardization Office, TTF 2019-0229 multi-domain operations – MDO, 13 Jan 2022, Accessed 14 Feb 2022.

8 NATO, "NATO's maritime activities", 17 May 2021, NATO.int, https://www.nato.int/cps/en/natohq/topics_70759.htm#:~:text=The%20maritime%20domain%20encompasses%20oceans,to%20other%20domains%20and%20areas. Accessed 14 Feb 2022.

9 Pierre Morcos and Colin Wall, 11 June 2021, "Invisible and Vital: Undersea Cables and Transatlantic Security," CSIS, accessed 03 March 2022, https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

10 NATO, AJP-3 Allied Joint Doctrine for the conduct of Operations, Edition C Vol 1, February 2019, p. C-2, accessed 20 Apr 2021.

11 NATO, AJP-3 p. C-2,

12 NATO, enclosure 1 TO SH/PLANS/J5/PLP/TV/17-316334 5000 TSC FPP 0110 ITT-161549/Ser: NU, 09 NOV 17, p. 4, https://nip.shape.nato.int/edms/shape/public/JAPS_2018-08-02_NU_Joint%20Air%20Power%20Strateqy%20inl.%20CL%20to%20MC%20MCM-0257-2017_ENG_ NU.pdf#search=cyber%20domain. accessed 27 Jan 2021

13 NATO, "NATO's Approach to Space", 23 Oct 2020, NATO.int, https://www.nato.int/cps/en/natohq/topics_175419.htm#:-:text=ln%202019%2C%20Allies%20adopted%20NATO%27s,as%20communications%2C%20naviqation%20and%20intelligence. Accessed 25 Jan 2021.

14 NATO, AJP-3, p. C-2

15 NATO, AJP-3, p. C-2

16 NATO, Cyber defence, 02 Jul 2021, https://www.nato.int/cps/en/natohq/topics_78170.htm . Accessed 14 Feb 2022.

17 Marius Kristiansen & Njaal Hoem, "Russian Cyber Strategy", 14 Feb 2021, p. 3, Small Wars Journal, https://smallwarsjournal.com/jrnl/art/russian-cyber-strategy.

18 NATO, enclosure 1 TO SH/PLANS/JS/PLP/TV/17-316334 5000 TSC FPP 0110 /TT-161549/Ser: NU, 09 NOV 17, p. 7, https://nip.shape.nato.inl/edms/shape/public/JAPS_2018-08-02_NU_Joint%20Air%20Power%20Strategy%20inl.%20CL%20to%20MC%20MCM-0257-2017_ENG_NU.pdf#search=cyber%20domain, accessed 27 Jan 2021

19 Major Jerry V. Drew, "Space Operations: Lines, Zones, Options, and Dilemmas", Joint Force Quarterly 99, 19 Nov 2020, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2420870/space-operations-lines-zones-options-and-dilemmas/

CJOS COE STAFF DIRECTORY

NAME	POSITION	TELEPHONE #
		+1 (757) 836-EXT
		DSN 836-EXT
STAFF HEADQUARTERS		
VADM Dan Dwyer, USN	Director	7551
CDRE Tom Guy, RN	Deputy Director	2452
CDR Michael Winn, USN	Fiscal Officer	2457
LCDR Christopher Ames, USN	Flag Aide	2452
CDR Diana Marron, USN	Directorate Coordinator	2611
YN1 Shannel Blake, USN	Administrative Assistant	2453
WARFARE ANALYSIS BRANCH		
CAPT Rory McLay, RCN	Branch Head	2450
CDR Per Christian Gundersen, RNON		2442
CDR Fred Conner, USN		2451
CDR Shawn Newman, USN		2463
CDR Carlos Carballeira, SPN		2462
CDR Emir Arican, TUN		2466
CDR Nathaniel Hathaway, USN		2440
WO1 Steve Scott, RM		2960
ITCS Jennifer Pate, USN		2467
DOCTRINE DEVELOPMENT BRANCH		
CAPT Giuseppe Catapano, ITN	Branch Head	2449
CAPT Max Blanchard, FRN		2446
CDR Dimosthenis Aliferis, HN		2537
CDR Esquetim Marques, PRTM		2444
LTCOL Jos Schooneman, RNLM		2443
LTCOL Roberto Patti, ITAF		4080
LCDR Courtney Mills, USN		2448

MAILING ADDRESS:

CJOS COE, 7927 Ingersol Street, Suite 150

Norfolk, VA 23551-2334, USA

USFF.CJOS.COE@NAVY.MIL

HTTPS://TWITTER.COM/CJOS_COE

CJOS activities are guided by a programme of work (PoW) approved by the sponsoring nations based upon requests received by NATO, CJOS member countries, and other entities. CJOS is open to requests for support by any organization. Requests received will be considered for inclusion in the PoW based upon alignment to CJOS interests and those of the sponsoring nations and NATO. The 2022 CJOS PoW is listed below:

CJOS COE Programme of Work - 2022

Red = New work for 2022

Doctrine Development and Standards	Concept Development and Experimentation	Lessons Learned and Analysis	Education and Training
1. Drive Interoperability, Integration, and Force Development			
• M2I2 (inc. Secretary position) • I2AG • MAROPS WG • Liaison to NWDC • Allied Interop and Integration Guide • Maritime ISR Doctrine • Coastal Defence Study Support • NATO Interop, Evaluation, and Certification	• Maritime Level of Effort • IAMD Conference • Collaboration with Romanian NDU • MEAB WG • Support to ACT's NWCC follow-on activities • Support NATO Defense Planning Process • Support JFCNF iFSA development • NATO All Dimension ASW Concept • FMN Spiral Specification Roadmap	• Lessons Learned Process and Analysis • Missile Deterrence and Defense • BALTOPS support • Support to C2F Allied Interoperability and Integration • NATO Interop, Evaluation, and Certification • Interoperability considerations on the Employment of Command and Control Systems • GRF 2022 Allied Interop Employment	• NATO Exercise Support • CJOS engagement with NDUs • BALTOPS support • Support to C2F Allied Interoperability and Integration • NATO Interop, Evaluation, and Certification • Support to Education and Training Activities • GRF 2022 Allied Interop Employment
2. Multi-Domain Integration			
	• Support JFCNF MaOC development • Artificial Intelligence (AI) and Maritime ISR implications • Support JFCNF STDE24 Planning and execution • Maritime Security Regimes Round Table (inc. WGs) • Support to JFCNF DDA Activities	• Impact of Danube Delta and Danube River • Artificial Intelligence (AI) and Maritime ISR implications	
3. Support the Alliance's Development and Integration of Amphibious Capability			
• AMPHIBOPS WG • Joint Combined Sea Basing WG	• NATO Amphibious Leaders (NALES) • NATO ATF Concept • Future NATO Surface Connectors		• Participate in CPAOT
4. Support the Alliance's Development of Innovative Technologies			
• Maritime Unmanned Systems Tactical Doctrine Development • ASW Barrier SDI	• Manned-Unmanned Teaming in Joint Operations: A C2 perspective • Cooperative ASW C2 • DYMS 22 support to unmanned systems	• DYMS 22 support to unmanned systems	
5. Deepening Our Understanding of Challenges and Competitors in the Maritime Domain			
	• Cutting the Bow Wave • StLOC Study • Support to Cold Weather Operations • NATO maritime activity in the Arctic • Long Term Military Transformation	• China's influence in the Med • Chinese Maritime Strategy • Terror Groups in the Maritime Domain	
6. Support Administrative Activities			
			• COE Support to NATO as DH • Dean of COE Directors • ACT CPD Branch Coordination

CJOS COE — *Transforming Allied Maritime Potential Into Reality*

TRANSFORMING ALLIED MARITIME POTENTIAL INTO REALITY