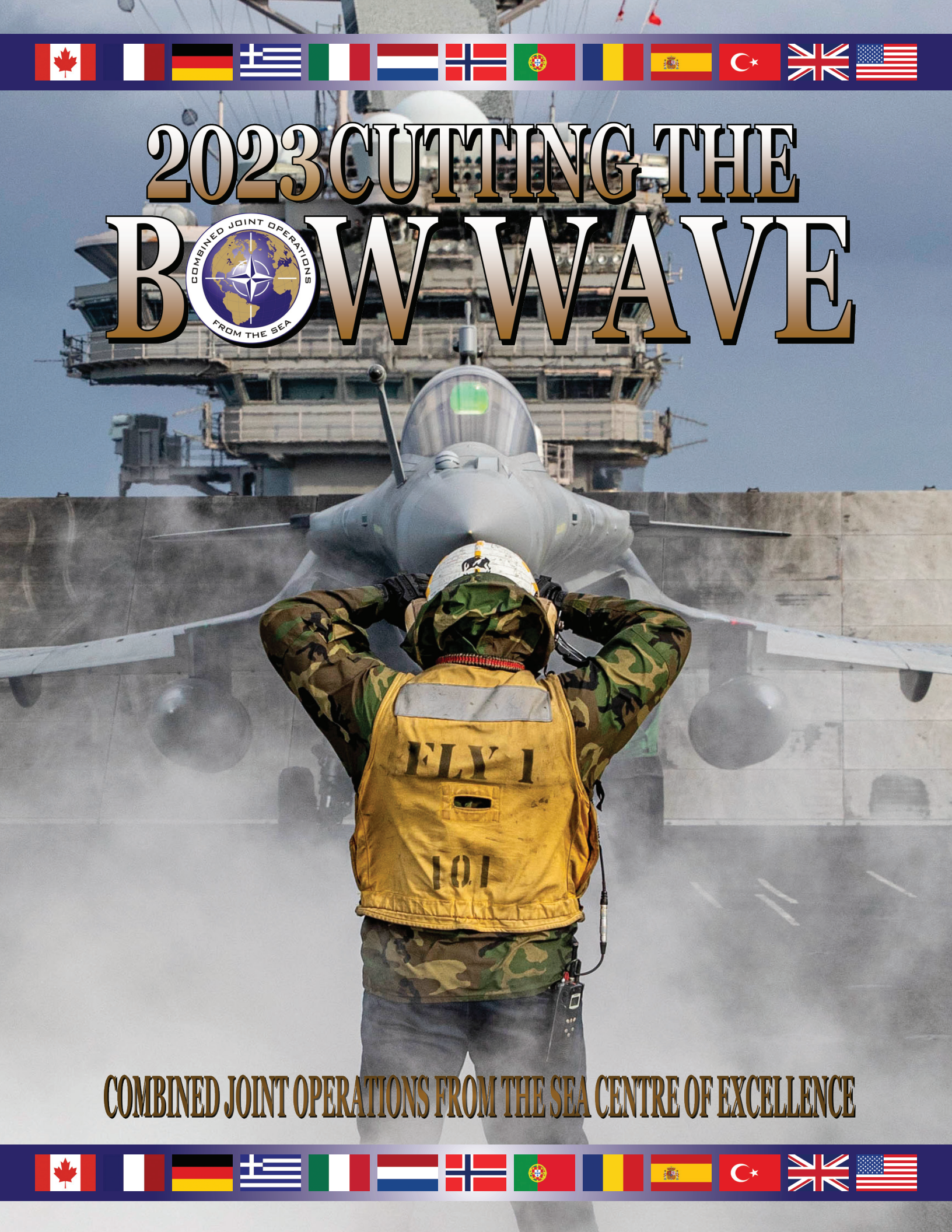

2023 CUTTING THE
BOW WAVE
COMBINED JOINT OPERATIONS FROM THE SEA
FLY I
101
COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE

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: French Navy Rafale fighter jet on the aircraft carrier USS George H.W. Bush (CVN 77) with the French Navy's Charles de Gaulle CSG, and the Italian Navy Cavour CSG, Nov. 22. Courtesy of US Navy.
Back Cover: Two unmanned surface vessels, a Saildrone Explorer and Devil Ray T-38 operate in the Gulf of Aqaba, during exercise Digital Shield, Sept. 21. Courtesy of US Navy.

Publisher's Note

Cutting the Bow Wave is an annual publication by Combined Joint Operations from the Sea Centre of Excellence, 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 Philip Nash, RN

Managing Editor:
CAPT Rory Mclay, RCN

Senior Staff Editor:
CDR Than Hathaway, USN

A Canadian CH-148 helicopter conducts a hoist exercise with a Royal Norwegian Navy Submarine during Exercise Dynamic Mongoose 21. Courtesy of US Navy.

2023 Cutting the Bow Wave – Director's Introduction

Perhaps more than any other time in recent history, the past year has underscored both the critical importance and unwavering strength of the NATO Alliance. Russia's unjustifiable invasion of Ukraine on the 24th of February 2022 has now entered its second year and, contrary to Russian notions of a limited operation and quick victory, Ukraine remains resolute in defiance. Ukraine and its people also continue to be backed by the steadfast support of a unified Alliance.

In light of this Russian aggression, the 2022 NATO Strategic Concept adopted at the Madrid Summit noted that we face a reality in which the "Euro-Atlantic area is not at peace." At the same time, the People's Republic of China continues to present a strategic challenge as it expands its reach and presence, seeking to link China to Europe through its "Polar Silk Road." Set against this backdrop, Russia's illegal acts, reckless threats and attempts at division have only served to reinvigorate and unify the Alliance, with ever stronger commitment to its mission of deterrence and defense.

As a multinational organization supporting NATO and partner nations, and in support of that mission of deterrence and defense, CJOS COE is helping drive forward the Alliance's warfighting development to meet such threats. Situated alongside Allied Command Transformation, U.S. Second Fleet and Joint Force Command Norfolk, CJOS is a key enabler in the drive for improved interoperability, enhanced multi-domain integration, a better understanding of the maritime operating context, and the development of innovative capabilities and concepts. Our work here at CJOS is multi-faceted and wide ranging – 'Cutting the Bow Wave' will provide you with a window into that world of work. I hope it will also encourage discourse between Alliance warfare professionals, not least because I strongly believe we must work, think and problem solve together if we are to overcome the challenges in front of us.

Consequently, as the Director of CJOS COE, and with thanks to the CJOS team for their diligent research, I am privileged to be able to present this year's publication. I hope you enjoy this 2023 issue of "Cutting the Bow Wave."

USS Gerald R. Ford (CVN 78) transits the Atlantic Ocean. Courtesy of US 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.

NATO ally special operations forces conduct a visit, board, search, and seizure exercise aboard the USS Leyte Gulf (CG 55) in the Adriatic Sea. Courtesy of US Navy.

2023 Cutting the Bow Wave – Deputy Director's Foreword:

In this, my first Cutting the Bow Wave, I'm honoured to continue the CJOS tradition of stimulating discussion, challenging conventional thinking, and highlighting ways to meet emerging threats. Much has been said already about the security challenges we face today and will face tomorrow – the rapid pace of change, the impact of emergent and disruptive technologies, the complexity of threats across domain and boundaries, the list goes on. Countering these challenges also prompts discussion, with a variety of fascinating and novel technological, doctrinal and conceptual solutions offered as the answer to our concerns. But beyond the eye-catching headlines there is much to do to realise the benefits of these new technologies, bridging the gap between concept and implementation. Equally, adapting and re-focusing current capabilities to ensure they remain relevant and battle winning requires a 'spiral development' mindset. And, as we all know from experience, being able to integrate and interoperate across service and national boundaries does not come for free – instead, like our own physical fitness, this requires constant discipline and deliberate effort.

Here at CJOS we are privileged to be able to help with that deliberate effort, developing and driving forward the grass roots concepts, capabilities and integration efforts that are required to achieve decisive advantage. In this edition of Cutting the Bow Wave you will see a number of articles focused on a few of these key issues. How should we think about harnessing AI and bringing it to the frontline now? How do we go about communications planning in the data age? Beyond the hype, where do hypersonic weapons really fit into the battlefield? I hope you find these articles thought provoking as they provide a shop window for the more detailed, comprehensive, and tailored work that CJOS carries out on behalf of its Sponsoring Nations and NATO customers on a daily basis. We look forward to hearing from anyone that has further interest in our programme of work, and our aim of helping turn 'Allied maritime potential into reality.'

A Lynx Mark 8 helicopter maneuvers to land. Courtesy of US Navy.

Philip Nash joined the Royal Navy as a Fleet Air Arm Observer, qualifying for front-line service on the Lynx maritime attack helicopter in 1997. His early career was dominated by operations at sea in Royal Navy destroyers as a member of a ship's flight team, deploying with NATO, coalition and UN forces in the Mediterranean and Adriatic, in the Arabian Gulf, the Indian Ocean and in the Far East.

After subsequently qualifying as a Principle Warfare Officer ('SWO') in 2003 he saw further deployed service, predominantly in the Indian Ocean and Arabian Gulf regions, as a Type 23 frigate operations officer. His most recent operational experience has been in the introduction to service of the Royal Navy's Type 45 destroyers; he was the second in command of the first of these (HMS Daring), and commanded the fifth (HMS Defender). During his three years in command he oversaw Defender's emergence from build in Glasgow, Scotland, through sea trials and training, to operations, whether at high readiness escorting Russian warships through UK waters, or as a fully integrated member of the George H W Bush and Carl Vinson Carrier Strike Groups in the Arabian Gulf in 2014.

In addition to operational appointments he has served twice on the staff of the Royal Navy Command HQ in Portsmouth, UK in capability and force generation posts, and twice in the UK Ministry of Defence in London, most recently leading on both longer term strategy formulation and shorter term defence review activity. He has also served on the staff of the Portsmouth Flotilla where he was responsible for the force generation, safety and long-term care of two thirds of the Navy's frigates, destroyers, and their people. A graduate of the University of Bristol, King's College London, the UK Advanced Command and Staff Course, the Royal College of Defence Studies, and the Capstone course, Nash served as the Naval Attaché with the British Defense Staff in Washington, DC immediately prior to taking up duties as the Deputy Director, CJOS COE in July 2022.

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 29 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 Request 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 2024 PoW should ideally be submitted by 15 August 2023. If the requests are approved by the Steering Committee, they will be included in the 2024 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 helping drive forward the Alliance's warfighting development.

An unmanned aerial system flies near a US guided missile destroyer during exercise Black Dart. Courtesy of US Navy.

Countering the Evolving Threat of Small Unmanned Aerial Systems in the Maritime Domain

LCDR (USN) Chris Ames

On July 15, 2019, while operating in international waters off the coast of San Diego, three U.S. Navy ships witnessed multiple unidentified small, unmanned aircraft[1] (sUA) maneuvering in close proximity to their position.[2] The crews of the USN ships called away their Ship Nautical Or Otherwise Photographic Interpretation and Exploitation teams, or "SNOOPIE teams." It quickly became clear to the crews that their ships were being surrounded by a swarm of small quadcopter-like sUA. What was not immediately clear to the crews were the intentions of the unidentified sUA. Who was in control of them? Where did they come from? And, most importantly, were they a threat to their ship and crew?

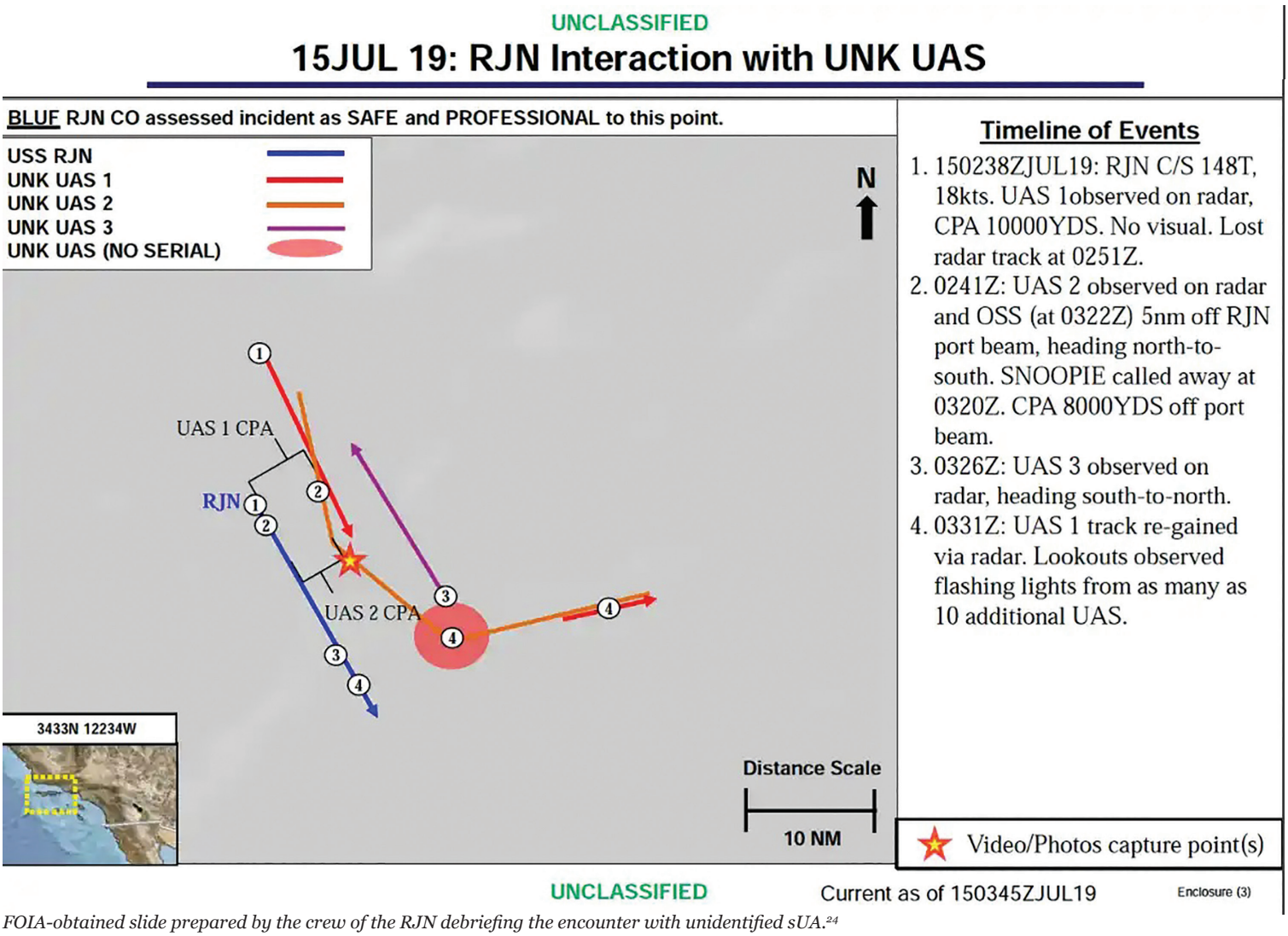
Records of the encounters on July 15 between the multiple unidentified sUA and the Ticonderoga-class guided missile cruiser USS BUNKER HILL and the two Arleigh Burke-class destroyers, the USS PAUL HAMILTON and the USS RALPH JOHNSON, present a cautionary example of the potential non-wartime use of small Unmanned Aerial Systems[3] (sUAS) against the Allied maritime fleet. As one example of a continuing trend of sUAS incursion on USN ships, this incident provides a case study for NATO to examine the threat posed by sUAS, understand the capabilities and technology of counter-sUAS (C-sUAS), and to seek a way forward to best defend the Alliance's maritime forces against this threat.

Too Close for Comfort?

As a result of multiple Freedom of Information Act (FOIA) requests made to the USN by the blog "The War Zone" (TWZ) for reporting on the topic, there exists detailed firsthand unclassified accounts of the July 15 encounter. These primary source accounts, from multiple USN ships, all on the same night, provide insight into what an encounter between NATO vessels and unidentified sUA could look like in a non-wartime environment. Despite occurring over three years ago, the following unclassified accounts raise the issue of potential threats and vulnerabilities that are persistent today:

USS RALPH JOHNSON

At 1938 local time, the Arleigh Burke-class destroyer, USS RALPH JOHNSON (RJN) observed a sUA on radar while operating in international waters off the coast of Southern California.[4] After losing radar track of the initial sUA, the crew of the RJN established radar track and visual sighting of a second sUA at 2020 local time. The second sUA came as close as 8000 yards (~7300 meters) to the RJN's port beam. Minutes later, the RJN observed a third sUA on radar, traveling parallel to the course of the ship in the opposite direction. With the incident lasting a little over an hour, lookouts for the RJN claimed to have observed flashing lights from as many as 10 additional sUA (~13 sUA total). Ultimately, the RJN characterized the interaction with the unidentified sUA as "safe and professional" and "in accordance with the COLREGs 'Rules of the Road' and internationally recognized maritime customs." An email from the RJN's Commanding Officer to the U.S. THIRD Fleet's Battle Watch Captain stated that, "No C-sUAS action was taken for this event."[5] The email went on to state that,



FOIA-obtained slide prepared by the crew of the RJN debriefing the encounter with unidentified sUA.[24]

"RJN is not equipped with DRAKE or other C-sUAS equipment."[6] DRAKE is Northrop Grumman's man-portable "Drone Restricted Access Using Known EW" C-sUAS system that uses radio-frequency (RF) jamming to deliver a non-kinetic, selective electronic attack to sUAS.[7]

USS BUNKER HILL and USS PAUL HAMILTON

At 2120 local time, less than an hour after the unidentified sUAS incident with the RJN concluded, the Ticonderoga-class guided missile cruiser, USS BUNKER HILL (BKH) observed multiple sUA off its port bow.[8] The BKH was conducting routine operations along with the Arleigh Burke-class destroyer, USS PAUL HAMILTON (PHM), in international waters off the coast of Southern California. In addition to multiple sUA, BKH identified the BASS STRAIT, a Hong Kong flagged bulk carrier, in the vicinity of the BKH and PHM. At 2150 local time, BKH determined the closest point of approach for the BASS STRAIT to be three nautical miles and altered its course to open that distance.[9] Approaching from the south of both the BKH and the BASS STRAIT, PHM gained visual detection of the BASS STRAIT at 2211 local time and the three vessels paralleled each other's course for the next 5 hours.[10] During this time, both the BKH and PHM observed up to 11 unidentified sUA in close vicinity to their vessels. BKH unsuccessfully attempted radio communication with the BASS STRAIT over bridge-to-bridge circuits to determine if the sUA originated from the vessel and to warn them of their use in close proximity to the USN vessels. According to the BKH's CO's assessment of the event, "several Quadcopter style UAS" had "operated in and around the BKH position." The assessment from the PHM was that they "observed M/V BASS STRAIT likely using UA to conduct surveillance."[11]

Defining the Threat

The encounters of July 15 are just two examples out of nine incidents involving unidentified sUA and USN ships in the waters off Southern California in 2019 (according to the information released by the USN through TWZ's FOIA requests). Given the proliferation of cheap, commercially available sUAS, the encounters of July 15 are indicative of a universal and ongoing concern to the ships of the NATO Alliance.

In 2021, former U.S. Central Command Combatant Commander General (Retired) Kenneth F. McKenzie stated in a speech to the Middle East Institute that sUAS, "is the most concerning tactical development

since the rise of the improvised explosive device in Iraq. [They] are inexpensive, easy to modify and weaponize, and easy to proliferate. Right now, we're on the wrong side of the cost and position curve because this technology favors the attacker, not the defender."[12]

General McKenzie's words detail the unique threats sUAS pose, and although he was speaking from the position of a former CENTCOM Commander, they are as relevant to the maritime domain as they are to troops on the ground. Specifically, the threats posed by sUAS to the vessels of the NATO Alliance are as follows:

Proliferation. In the U.S. alone, there are over 850,000 unmanned aircraft registered with the FAA.[13] Although it is difficult to accurately determine worldwide commercial off the shelf (COTS) sUAS' sold, the global sales of UAS in 2021 was estimated at $16.7B USD. Of that enormous figure, 38% of sales were from North America, 21% from the Asia Pacific, and 27% from Europe.[14] The largest global retailer of sUAS is SZ DJI Technology Co. (DJI), a Chinese technology company that owned 54% of the global market share in commercial sUAS in 2021.[15] DJI and its ties to the Chinese military have been scrutinized by the U.S. Department of Defense (DoD) and, in October of 2022, DJI was placed on its list of "Chinese military companies" in an effort to remove it from U.S. supply chains and make the U.S. defense-industrial base more secure.[16] DJI offers sUAS to customers around the world with offerings starting at $759 USD.

DJI Mavic 3 modified by Ukrainian fighters to carry two M433 40mm grenades.[17]

Modifiable/weaponizable. The modification of COTS sUAS has been well documented in fighting around the world. Most recently, Ukrainian fighters have weaponized COTS sUAS, including DJI sUAS, to drop air delivered improvised munitions on Russian troops. Much like the development of IEDs, the simple engineering and open-source nature of sUAS has lent itself to an iterative process of creative modifications and weaponization.

Plausible deniability. One of the great benefits of sUAS, especially COTS sUAS, is the plausible deniability afforded to enemy users due to the many commercial and hobbyist uses of sUAS. For example, of the nine disclosed incidents of unidentified sUA incursions on USN ships in the waters off Southern California in 2019, two incidents were attributed to the possibility of local fishermen using personal sUAS, and in a third incident the unidentified sUAS was attributed to a pleasure vessel that was operating in the vicinity. Having occurred in international waters, and without visual evidence of recovery or launch in any of these incidents, there was no recourse taken to these suspected vessels. Despite their seemingly benign attribution, these incidents were an incursion on USN vessels and, at the very least, posed a threat to flight operations aboard these ships. Of these three incidents, two involved a swarm of sUAS (4x and 5x unidentified sUAS respectively) and in one of the incidents a USN ship was directly overflown multiple times.[18]

Swarming. The small footprint, inexpensive cost, and ease of operation lend sUAS to being operated as a swarm. Swarm tactics, coupled with the small size of sUA, can make them difficult to track and counter with non-dedicated C-sUAS systems (like the existing radars and air defense systems on most NATO ships). Although effective C-sUAS systems exist that would have been effective against encounters such as those on the night of July 15, they are not universally deployed on Alliance warships.

Countering the Threat

Given the proliferation of sUAS and the threat that they pose to NATO vessels, it is important to understand what is known as the C-sUAS processing chain, and the current technology capable of countering the threat in the maritime domain. The C-sUAS processing chain can vary depending on the mission; however, a good framework is Detect, Track, Identify, and Defeat. Like other more traditional counter-threat systems, the C-sUAS processing chain can include the human user in the loop or can be an autonomous process capable of detection through defeat.

C-UAS Processing Chain[19]

Detect: Detection is the first and most important step to countering the sUAS threat. The earlier a sUAS can be detected, the more time and distance is available to complete the remainder of the C-sUAS processing chain. In the maritime environment there are three traditional methods of detection utilized by C-sUAS: 1) passive radio frequency (RF) detection, 2) electro-optical/infrared (EO/IR) detection, and 3) radar detection. The pros, cons and examples of each detection method is outlined in Table 1. Optimally, a C-sUAS system uses all three methods of detection in a layered approach to offset the "blind spots" of each method. Importantly, without a dedicated C-sUAS system, a crewmember visually spotting a sUAS may be the only method of detection.

Passive RF Detection	**Pros**: Allows for long range, omni-directional, non-line of site detection. Extremely effective at detecting and classifying COTS sUAS for which frequencies are known and cataloged. RF detect systems are generally the most inexpensive.	**Cons**: Requires that the sUAS utilizes RF signals for command and control (C2). If a sUAS utilizes a preprogrammed route or passively homes in on signals transmitted by its target, detection is not possible.	**Examples**: DRAKE (Northrop Grumman), NINJA (AFRL), CORIAN (CACI)
EO/IR Detection	**Pros**: EO/IR search and track can provide passive detection of sUAS even when it is not utilizing RF for command and control or telemetry.	**Cons**: Compared to other methods of detection, EO/IR can be limited at the range in which it can detect sUAS. EO/IR requires line of sight (LOS) and is susceptible to background visual clutter.	**Examples**: WISP (Anduril), HELIOS (Lockheed Martin)
Radar Detection	**Pros**: Phased array radars can provide accurate location and elevation which also make for an effective means of tracking sUAS for defeat. Radar can detect and track sUAS that doesn't transmit RF.	**Cons**: Radar systems tend to have bad angular detection, with many systems having a ~30-degree elevation limit, meaning they are unable to detect or track sUAS that are at a high angle relative to the C-sUAS platform.[1] Also, radar detect requires LOS to sUAS.	**Examples**: E-LRST-42/82* (Anduril), MADIS* (NSWC-Crane), Medusa* (SAIC), FS-LIDS* (SRC, Inc.) *Examples all utilize a combination of RF, EO/IR, and radar

Comparing Methods of Detection in C-sUAS (Table 1)

Track: Upon detection of a sUA, the C-sUAS will begin tracking its location. For C-sUAS systems with a kinetic defeat capability, the tracking phase will also seek to provide a firing solution. For C-sUAS that do not have the automatic track function, it will be the responsibility of the crew to visually track the sUA.

Identify: Identification is made either by the C-sUAS or by the operator visually. As able, the C-sUAS will attempt to identify UAS type, group, manufacturer and/or specific communication protocol. Some C-sUAS technology is capable of determining the make and model of the sUAS through interception of the sUAS' RF telemetry data while other systems can identify type and group based off an EO/IR or radar signature.

Defeat: Defeat is the final and optional step in the processing chain. It is used to describe the method used to remove or reduce the threat posed by sUAS. Depending on the C-sUAS system in use, defeat can range from RF jamming, spoofing, to kinetic defeat. Defeat may not always be the appropriate conclusion to the C-sUAS processing chain; however, it is an important capability for a commander at sea to have in the defense of personnel and equipment.

Jamming is dependent on sUAS utilizing RF for their C2 or navigation. In the process of C2 jamming, the C-sUAS transmits RF energy (noise) in the frequency band of the sUAS at a greater power level than that of the sUAS. This noise is designed to prevent the C2 signal from being received and prompting the sUA's preprogrammed "lost link" procedure. During "lost link," a sUAS will typically execute a procedure designed to aid it in re-establishing RF communications with its controller, the most common being returning to its launch location. C2 jamming creates a standoff that is dependent on the power and propagation of the RF energy being transmitted from the C-sUAS. In addition to C2 jamming, the Global Navigation Satellite System (GNSS) used by the sUAS for navigation and positioning can be jammed, denying the sUAS the ability to properly position or navigate.

Spoofing is a capability that allows the C-sUAS to intercept data being transmitted between the sUA and its ground control station through an exploitation of its communication protocols. This "man-in-the-middle" spoofing can allow the C-sUAS to collect information on the sUAS and even send it C2 inputs, effectively taking control of the device.

Kinetic defeat is the physical destruction of the sUA and can be accomplished through directed energy (DE) weapons like lasers and microwaves (HELIOS, Lockheed Martin), ballistic weapons (LPWS, Raytheon), or even other sUA platforms that use physical nets or kinetic energy to fly into the threat (Anvil, Anduril).

Rapid Innovation in Countering the sUAS Threat

It has been over three years since unidentified sUAS swarmed three USN ships on the night of July 15, 2019. Since then, the US DoD has further committed to the development of technology and training to better counter the threat. Notably, in February 2020, the Joint C-sUAS Office (JCO) was established to direct and synchronize defence activities across the branches of the DoD. Creation of the JCO was an important step to focus C-sUAS development and acquisition and create a holistic DoD-wide strategy for countering the constantly evolving hazards and threats posed by sUAS.[20]

In January 2021, the DoD published its C-sUAS strategy which emphasizes a new approach to C-sUAS that is focused on rapid innovation, synchronization of materiel and non-materiel solutions, and relationships with allies and partners. Most recently, US CENTCOM has begun the development of the Red Sands

Integrated Experimentation Center, Saudi Arabia. Set for completion in 2023, Red Sands will develop and demonstrate C-sUAS solutions to address shared concerns with U.S. partners across CENTCOM.

In-line with the DoD's re-focused efforts on countering the threat of sUAS, the USN has continued to develop and test C-sUAS systems capable of both jamming and kinetic defeat. Since 2019, the USN has expanded its fielding of the DRAKE man-portable C-sUAS within its fleet.[21] A relatively low cost, small footprint (backpack sized), and easy to operate system, DRAKE provides a baseline of C-sUAS with the ability to detect, identify, and RF jam. The USN has also invested in the development of DE weapons to help combat sUAS. In May 2020, the USN successfully destroyed a sUA target while testing the Laser Weapon System Demonstrator (LWSD) on board the USS PORTLAND, a LPD. The LWSD program is scheduled to close out by 2024 but has given way to two additional C-sUAS DE weapons on the USN's 2023 budget: the Optical Dazzling Interceptor, Navy (ODIN), and High-Energy Laser with Integrated Optical-dazzler and Surveillance (HELIOS).[22] ODIN provides a shipboard counter-ISR capability that is designed to dazzle UAS sensors in an effort to prevent intelligence gathering, thereby offering a non-kinetic response to sUAS used for surveillance. HELIOS is a dual-purpose, high-powered laser capable of either destroying sUAS or dazzling enemy optical sensors. HELIOS was installed on the Arleigh Burke-class destroyer, the USS PREBLE, in 2022 and will begin at-sea testing in 2023. Designed with an EO/IR sensor for detection and tracking, the HELIOS could eventually be integrated into the Aegis Combat system.[23]

Defending the Alliance from sUAS

The threat to the NATO fleet from sUAS, whether it be a wayward hobbyist or a swarm attack with improvised explosives, is real and expanding with the continued proliferation of these devices. Just as the USN has bolstered its employment of C-sUAS systems and invested in their future development, navies of the Alliance also need to ensure their fleets have adequate systems and training to counter this growing threat. The sUAS incursion on USN ships on the night of July 15, 2019, within close proximity to the U.S. coastline, demonstrates that they pose an equal threat to vessels both in blue water and close to shore in the littorals. C-sUAS systems that are portable, easy to operate, and are capable of RF jamming against the most common sUAS threats should be the baseline of protection for our ships. No ship would choose to go to war without the means to defend itself and defeat the enemy. Navies of the Alliance must recognize the potential of "going to war" against sUAS anywhere and at any time, and must be ready to defend themselves to win the fight.

Endnotes

1 sUA is used to refer to the aircraft itself, while sUAS refers to the entirety of the system and includes aircraft, payload, ground control station, antennas, and operator.

2 The War Zone, "Drone Swarms That Harassed Navy Ships Off California Demystified In New Documents", JUN 10, 2019. Available at https://www.thedrive.com/the-war-zone/drone-swarms-that-harassed-navy-ships-demystified-in-new-documents.

3 The term sUAS is used to refer to any Group 1 or Group 2 unmanned aircraft (any UA weighing less than 55lbs).

4 United States Navy, 15JUL19: RJN Interaction with UNK UAS, July 15, 2019

5 The War Zone, "Drone Swarms That Harassed Navy Ships Off California Demystified In New Documents"

6 Ibid.

7 Northrop Grumann Newsroom, "Company's mobile acoustic sensing and electronic attack innovations detect and defeat emerging threats in complex scenarios", October 4, 2016. Available at https://news.northropgrumman.com/news/releases/northrop-grumman-demonstrates-counter-uas-technologies-at-black-dart-exercise

8 United States Navy, 15JUL19: BKH Interaction with Multiple U/I UAS, July 15, 2019

9 United States Navy, 15JUL19: BKH Interaction with Multiple U/I UAS

10 United States Navy, 15JUL19: MV BASS STRAIT, July 15, 2019

11 Redacted, Commanding Officer RJN. '(U) USS PAUL HAMILTON/VIR/CHINA/MV BASS STRIT/150511ZJUL19'. Email, 2019.

12 McKenzie, Gen. Kenneth F., interview by Paul Salem. 2021. Keynote Address: The Middle East Institute

13 FAA. 2022. FAA.gov. FEB 7. https://www.faa.gov/uas.

14 Precedence Research, "Commercial Drone Market", Precedence Research. July, 2022. Available at https://www.precedenceresearch.com/commercial-drone-market.

15 Reuters, "DJI is a more elusive U.S. target than Huawei", December 16, 2021. Available at https://www.reuters.com/markets/asia/dji-is -more elusive-us-target-than-huawei-2021-12-17

18 Defense News, "More can be done to ban US government use of Chinese drones", January 12, 2023. Available at https://www.defensenews.com/opinion/commentary/2023/01/12/more-can-be-done-to-ban-us-government-use-of-chinese-drones

17 OSINTtechnical, "Ukrainian DJI Mavic 3 modified to carry two M433 40mm grenades", July 27, 2022. Available at https://twitter.com/Osinttechnical/status/1552436339572080640

18 The War Zone, "Drone Swarms That Harassed Navy Ships Off California Demystified In New Documents"

19 Homeland Security Science and Technology, "Counter-Unmanned Aircraft Systems", September, 2019. Available at https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf

20 U.S. Department of Defense, "Counter-Small Unmanned Aircraft Systems Strategy", January 7, 2021. Available at https://media.defense.gov/2021/Jan/07/2002561080/-1/-1/1/DEPARTMENT-OF-DEFENSE-COUNTER-SMALL-UNMANNED-AIRCRAFT-SYSTEMS-STRATEGY.PDF

21 USNI News, "Navy Arming Surface Ships with Drone Repellent System", September 7, 2021. Available at https://news.usni.org/2021/09/07/navy-arming-surface-ships-with-drone-repellent-system

22 Congressional Research Service, "DoD Directed Energy Weapons: Background and Issues for Congress", September 13, 2022. Available at https://crsreports.congress.gov/product/pdf/R/R46925

23 Congressional Research Service, "DoD Directed Energy Weapons: Background and Issues for Congress"

24 United States Navy, 15JUL19: RJN Interaction with UNK UAS

Swedish Visby Class Corvettes Copyright Saab AB,
Foto: Peter Liander

Finnish and Swedish Naval Capabilities Will Strengthen NATO in the Baltic Sea Region

CDR (RNoN) Per Christian Gundersen

Increased tension in a congested area

In October 1981, Sweden found a grounded Soviet Navy Whiskey-class submarine on the doorsteps of their major naval base Karlskrona, in the south of the country. The Swedish Navy discovered the beleaguered submarine while testing new equipment during a large-scale exercise. The incident became embarrassing to both countries. For the Swedes, the submarine had managed to get uncomfortably close without being detected before running aground, and the Russians were caught with their pants down, even if they tried to blame it on navigation errors. The submarine was stuck for nearly ten days before being hauled off the rocks by Swedish tugs, escorted to international waters, and handed over to the Russian Baltic Fleet. The incident was quickly named "Whiskey on the Rocks."[1] It was arguably the most extraordinary naval incident with the Soviets in the Baltic Sea region during the Cold War, but far from the only one. Being a somewhat congested area, the Baltic States experienced numerous Russian territorial intrusions throughout the Cold War era.

Once again, tension is running high in the Baltic Sea Region, especially after the illegal Russian annexation of Crimea in 2014 and an increasingly more assertive and aggressive Russia, especially towards the Baltic states. The situation became even more worrisome after the overt Russian attack and war of aggression on Ukraine in February 2022, eventually prompting Finland and Sweden to reassess their security situations and submit formal applications in May 2022 to join NATO. The deteriorating relationship between the Western World and Russia has made the congested Baltic Sea Region an arena for increased arms race and competition. This has been firmly demonstrated during the last few years by increased Russian military activity, presence and provocative posture around some of the sensitive Baltic areas, including the strategically located islands of Finland's Åland, Sweden's Gotland, and Denmark's Bornholm.[2]

This article aims to provide insight into some fundamental maritime security aspects of the Baltic Sea Region and argues that Finnish and Swedish membership in NATO will profoundly and positively impact the military dynamics in the Baltic Sea Region in favour of the Alliance. In terms of naval capabilities, Russia will face an even more coherent potential adversary, and at the same time, NATO will grow more flexible and resilient in these confined waters. Even if the Finnish and Swedish Navy are primarily tailored for national defense, they will narrow and close some Alliance capability gaps, increase NATO's ability to deter Russian aggression, and ultimately strengthen the defence of Allied territory in the region when required.

Geography matters

The Baltic Sea is a confined sea area enclosed by (clockwise) Denmark, Sweden, Finland, Russia,

> **Even if the Finnish and Swedish navies are primarily tailored for national defense… they will increase NATO's ability to deter Russian aggression.**

Estonia, Latvia, Lithuania, Kaliningrad (Russia), Poland, and Germany, with one main entrance from the North Sea through the narrow Danish strait.[3] Being the largest brackish water system in the world, the Baltic is shallow, with an average depth of around 50 meters.[4] It generally has low salinity, but at the same time, "salt pockets" are common. Both conditions cause problems for sensors, navigational, and surveillance equipment.[5] In addition, the low salinity levels create widespread surface ice during wintertime, on average covering 40% of the total area.[6] In general, the coastal areas are rather treacherous, containing archipelagos, rocks, straits, fjords, scattered islands, and jagged shorelines. These characteristics make the region relatively easy to defend with small and low signature platforms, but also create challenges when executing Sea Control and Sea Denial Operations. An examination of the geography quickly reveals that Russia only controls a small share of the Baltic Sea coastline and is enclosed by NATO countries, Finland and Sweden. The Russian Baltic Fleet primarily deploys from the major naval base in Baltiysk in Kaliningrad Oblast and secondly from Kronstadt outside Saint Petersburg in the Gulf of Finland (mainly submarines and some MCM vessels). Both naval bases and their approaches are vulnerable. Baltiysk Naval Base is not only within artillery distance from NATO territories, but also lacks a land connection to the Russian mainland, being sandwiched between Lithuania and Poland. In addition, Russian naval vessels heading to the Baltic Sea must transit the two-kilometer-long Strait of Baltiysk, which cuts through the Vistula Spit. Comparably, the Kronstadt Naval Base is a bit easier to defend. However, any vessel deploying to the Baltic Sea proper must transit the entire, relatively shallow 400 km Gulf of Finland.[7]

Considered one of the busiest shipping routes in the world, around 2,000 ships are usually at sea at any given time in the Baltic Sea, including large oil tankers, ships carrying dangerous and potentially polluting cargoes, and a substantial number of passenger ferries.[8] In addition to the shipping component of the economy, the Baltic region also accounted for more than 40 percent of all Russian energy exports prior to the Ukraine war.[9] Intended to provide continuous energy from Russia to continental Europe, the Nord Stream seabed pipelines run across the Gulf of Finland, through the Baltic Sea, and ultimately come ashore in

Map of the Baltic Sea region. Courtesy of Shutterstock.

Germany. These pipelines were intended to provide continuous low-cost energy for continental Europe for decades to come. However, Russia's annexation of Ukrainian territory drove European capitals to seek alternative energy sources after recognizing that reliance on Russian gas had made them vulnerable. Currently, the pipelines are considered non-operational after several explosions in late September 2022, that were confirmed as sabotage. The pipelines were cut at four locations, two in Denmark's exclusive economic zone and two in Sweden's exclusive economic zone. Though Russia has been widely blamed for this incident, no clear evidence has been provided to support a firm assessment.

The Russian Baltic Fleet

Since most of the air, land, and naval forces in Kaliningrad are organized within the Baltic Fleet, it is better understood as a joint command rather than a single service naval force.[10] The Russian Baltic Naval Fleet is mainly equipped for coastal operations, consisting primarily of smaller combat units. Despite the ongoing Russian naval modernization programs, the Baltic Fleet is mainly composed of Cold War-era ships. The larger combatant vessels in the Fleet have become somewhat outdated, with the destroyer Nastoychivyy of the Sovremenny-Class and two frigates of the Neustrashimyy-class, all developed during the 1980's. Significantly more potent for littoral warfare are the three different corvette-class combat vessels recently developed. To date they have built four blue

water capable Steregushchiy-class multi-purpose corvettes equipped with modern anti-surface and anti-air missiles, three of the Buyan-M corvettes, and three of the Karakurt corvettes, mainly equipped with anti-ship cruise missiles. Several more of these smaller combat vessels are under construction. The Fleet also contains various older coastal combatant vessels, such as the Parchim, Nanuchka, and Tarantul class corvettes, one Kilo-class conventional submarine (primarily used for commercial training), and more importantly, a dozen mine warfare and mine-countermeasure vessels. Russia is known to maintain the largest sea mine stockpile in the world, estimated to be approximately 250,000 munitions.[11] A fair amount of these mines are likely essential to the Russian A2/AD concept in the Baltic Sea region.

Russian Baltic-based air forces, ground-based air and missile defenses, and naval infantry forces, with four amphibious tank landing ships and numerous smaller amphibious landing crafts constitute important additions to the Baltic Fleet. Of note, is the 152nd Guard Missile Brigade in Kaliningrad, equipped with Iskander-M missiles[12] and the 25th Coastal Missile Brigade, equipped with Bastion and Bal anti-ship missiles. These weapon systems provide a flexible and powerful ground-based surface missile threat, covering the entire southern part of the Baltic Sea Region. Furthermore, Kaliningrad is well equipped with air defense weapons. The 44th Air Defense Division has regiments with S-400 and S-300V4 missiles, and the 22nd Guards Air Defense Regiment has short-range Tor-M2 systems. There are also potent deployed artillery systems in Kaliningrad, such as the Uragan multiple rocket launcher system (MLRS), as well as the Msta.[13] Even if the Russian air forces in Kaliningrad may fluctuate in numbers due to the level of tension and activity, it typically consists of fighter squadrons with upgraded Su-27 and advanced Su-35 fighter jets. In addition, there have been reports of MiG-31 fighters with Kinzhal hypersonic missiles deploying to the Naval Air Base in Chkalovsk.[14] The major ground forces in the Baltic Fleet Coastal Troop Command are the newly formed 11th Army Corps, the 25th Coastal Missile Regiment, and the 336th Guards Naval Infantry Brigade. Over the last few years, the latter has been modernized with new armored vehicles and other equipment. Parts of these ground units have also been involved in warfighting in Syria and Ukraine.

The Baltic Naval Fleet serves several purposes. Broadly, the main tasks in peacetime and during low-level tension are maritime presence and deterrence operations. The Fleet contributes to the Russian presence in the Baltic Sea, ensuring territorial integrity, surveillance, and monitoring of NATO activities. In addition, it contributes to Russia's ambition internationally. On several occasions, the Baltic Naval Fleet has deployed its modern combat vessels to the Atlantic, Mediterranean, and even the Red Sea. In crisis and armed conflict, it is meant to play a crucial role in denying NATO access to the Baltic Sea Region by conducting Sea Denial Operations within a layered Anti Access/Area Denial (A2/AD) concept. Even if most of Russia's A2/AD capability in the Baltic Sea is concentrated around its ground and air forces, one should not overlook the Fleet, especially its mine and anti-ship cruise missile capabilities.[15] One may

Russian warships on the Neva River, St. Petersburg, 28 July 2022. Courtesy of Shutterstock.

argue that despite a decrease in the actual number of platforms, there has been an increase in combat power during the last years, mainly due to Russia's strategic emphasis on developing new guided-missile systems such as the Kalibr missile family. With an operational range of up to 2500 km, these cruise missiles may target surface vessels, submarines, and land objectives.

Bilateral cooperation and the approach to NATO

Sharing a long and intertwined history as close neighbours, Finland and Sweden have developed strong military ties during the last decade. They have signed several defense cooperation agreements, including a memorandum of understanding on defense cooperation and host nation support for military activities.[16] Becoming gradually more concerned about the security situation in the Baltic Sea Region given an increasingly revisionist and aggressive Russia, both countries have steadily ramped up their defense spending and have sought closer bilateral cooperation. Some recent major initiatives have been the shared use of naval bases, mutual support and partial integration of their respective air forces, and the development of a combined Finnish-Swedish Brigade Framework that includes force integration and interoperability. However, with the blatant Russian attack on Ukraine in February 2022, it became evident to both countries that they needed to reassess their somewhat similar long-term national security policies. It culminated in May 2022, with both countries determining to submit applications for NATO membership. These decisions were not taken lightly, nor without a thorough political and public discussion. Even with both countries being close NATO partners since 1994[17] and establishing even closer ties with the U.S. during the last decades, applying for NATO membership was obviously a game-changing strategic decision not just for each country, but also for the entire region. Finland and Sweden have historically maintained a pragmatic, defensive, and non-provocative profile towards Russia. At the same time, both countries have evolved in recent years to become two of NATO's most active partners. They have prioritized a permanent presence in NATO's command structure and organizations and providing a long-standing engagement in the NATO Response Force. They have also proved to be invaluable contributors to NATO-led exercises in the North, as well reliable partners in operations in the Balkans, Afghanistan, and Iraq.

Finnish and Swedish naval capabilities

Contrary to the "peace-dividend" posture adopted by most European countries, Finland has maintained a strong national defense force since the end of the Cold War. Based on conscription, the Finns have Europe's largest and arguably one of the most well-trained Reserve Forces. This long-lasting defense strategy has remained unchanged mainly due to geographical and historical reasons, given the 1340 km common border with its Eastern neighbour and having experienced three wars with the Russians in the 20th century.[18] The Finnish Navy is a relatively small service compared to its Army for obvious geographical reasons. Based on this geographical driver, the Navy is primarily configured for littoral operations, with essential capabilities for surface warfare, mine warfare, anti-submarine warfare, and coastal unit mobility and fire support. It employs approximately 1400 people, and about 3200 conscripts are trained annually.[19] Its major tasks are to defend Finland and its territorial waters and protect sea lines of communication, bearing in mind that about 90% of Finnish imports and exports are transported by sea.[20] Noteworthy to more traditional maritime capabilities, Finland is a major designer of the world's icebreakers and operates a fleet of nine state-owned icebreaking vessels. Arguably, being world-leading in that regard will become valuable for NATO in the future. Currently, NATO members only have a handful of icebreakers at their disposal. In contrast, Russia has approximately 40 icebreakers.[21]

Sweden chose a different path after the Cold War. As the threat from Russia was perceived to fade away, the Armed Forces were dramatically reduced in the 1990's. Priorities were realigned from a territorial defense posture to include more "Out of Area Operations" and peacekeeping missions worldwide. In 2000, the Swedish Coastal Defense Forces were downsized and reorganized, and in 2010, conscription was abandoned. Consequently, the Swedish Navy became a purely professional force with no Reserve Forces. However, this was reversed in 2014 when defense spending was boosted, and conscription was reintroduced. Currently, the Swedish Navy has about 1300 personnel and 900 dedicated amphibious forces. The Swedish Navy's major combat assets are five non-nuclear submarines (SSK), five highly advanced stealth corvettes, four patrol craft with guided missiles and torpedoes, seven mine warfare ships, and 129 fast patrol boats. Major tasks are similar to the Finnish Navy, including defensive coastal operations and protecting Sea Lines of Communication.

Even if the Finnish and Swedish naval forces are primarily designed for homeland defense, there are arguably capabilities within both countries' navies that will close gaps and significantly enhance NATO's ability to defend, deter and counter any Russian aggression within the Baltic Sea Region. A way of assessing what the Finns and Swedes would bring to the "maritime table" in the Alliance could be by assessing their current capabilities, using some of NATO's Joint Functions as a point of reference.[22]

Maneuver and fires

The Finnish Coastal Fleet Command operates from Pansio Naval Base in the southwest archipelago and from the Upinniemi Naval Base, which is part of Coastal Brigade base further to the east. It comprises all combat

vessels, including eight fast missile attack craft of the Rauma and Hamina class, both of which have recently undergone mid-life updates. The main armament on the Rauma class is the Swedish-developed RBS-15 long-range fire-and-forget missile, primary for anti-surface warfare but also land attack capable. The main weapon system on the Hamina class is the PTO2020 Gabriel, a surface-to-surface missile with a range of more than 200 km. Both missile systems enable the attack crafts to cover the entire Gulf of Finland from covert inshore positions, making it challenging for any Russian naval assets to deploy in or out of the naval base in Kronstadt. The missiles can also neutralize fixed and mobile sensors, C2-nodes, weapon systems, and installations onshore in the littorals. It is also worth mentioning that the Finnish fast missile attack crafts have some anti-submarine warfare capabilities, mainly used to ensure the protection of sea lines of communication. Bearing in mind that the narrow, shallow straits and myriad islets along the Finnish coastline are highly suitable for minelaying, most naval vessels also have this capability.[23] In addition, the Finnish Navy has several up-to-date inshore mine countermeasure platforms and minelaying vessels, which would be a much-appreciated capability within the Alliance. Surely, both Finland and Sweden would be requested to participate regularly in the Standing NATO Mine Countermeasures Groups (SNMCMG) and even in the NATO Standing Maritime Groups (SNMG) in the future. For NATO, Finnish sea denial capabilities are likely to play a vital role in denying the Russian Navy's freedom of maneuver in the Baltic Sea region, protecting NATO territory with potent anti-surface warfare and minelaying capabilities. The Finnish Navy also includes two marine-type formations, the Coastal and Nyland Brigade. Both brigades specialize in naval reconnaissance and warfighting in the littorals, operating mainly in the southern part of the country in the Gulf of Finland. Being highly mobile and accustomed to operating in the region throughout the year, these forces could also play an essential role in supporting the NATO defense of the Baltic countries.

In 2015, the Finns officially launched its Squadron 2020 project, which focuses on the future development of the Finnish Navy. A vital part of this project is the building of four multi-role Pohjanmaa class corvettes, which would be the country's largest surface combatants since the 1930s. With an ice-strengthened hull, the 115m long corvettes will include anti-surface, anti-air, anti-submarine, and minelaying capabilities. In addition, they will be able to operate a medium-sized helicopter and unmanned maritime systems.[24] Latest estimates suggest the first ship will be operational around 2030. These multi-role combatant vessels, which could be considered small frigates, promise to further enhance NATO's ability to deter and defend against any Russian aggression in the Baltic Sea Region, including degrading any potential Russian A2/AD.

The Swedish Navy operates mainly out of Karlskrona Naval Base, strategically located in the south, already chosen by the Swedish King Charles XI in 1679. The base has favorable ice conditions during the winter, enabling the Navy to have a permanent presence at the southern entrance into the Baltic Sea. Its warfighting capabilities are mainly organized and suited to conduct defensive littoral operations. The Navy uses a combination of stealthy coastal anti-ship missile vessels, small submarines, mine warfare vessels, and mobile amphibious forces. The small, fast in-shore attack crafts can maneuver and discreetly deploy anti-ship missile defenses within the ragged coastline. For NATO, the Swedish Navy would likely provide support in protecting Allied forces entering the Baltic Sea by employing anti-surface, anti-air, anti-submarine, and mine warfare capabilities. Simultaneously, Sweden may deny Russian naval and air forces operating forward in the western part of these confined waters by supporting the defense of the strategically important Danish Island of Bornholm.

The Muskö Naval Base, with its large underground facility on the Stockholm archipelago's east coast, has recently been reactivated. This base could enhance the Navy's flexibility and resilience, providing shorter deployment distances eastwards into the Baltic Sea and to the strategically important island of Gotland, set in the middle of the Baltic Sea. Gotland lies just 300 km from the major Baltic Fleet Naval Base in Baltiysk in Kaliningrad,[25] and has recently been re-militarized. Arguably, the island could be considered a possible future base for NATO air defence assets, enabling it to cover most of the Baltic Sea in a crisis and armed conflict. As described by Rutger Banholtz, former head of the Swedish Home Guard, Gotland may be considered an aircraft carrier controlling most of the Baltic Sea."[26]

A future Swedish naval program worth mentioning is the development of two new submarines of the Blekinge class (A26). Although their delivery is somewhat delayed, they will replace the submarines of the Södermanland class by 2028. In parallel, the three Gotland class submarines are undergoing a mid-life upgrade. These small but highly capable Swedish diesel-powered submarines have already impressed the international naval community. During an exercise in 2005 with the U.S. Navy, HSwMS Gotland conducted several simulated torpedo attacks on the USS Ronald Reagan without being detected by the carrier or its anti-submarine escorts. The U.S. Navy later leased the submarine and its crew for two years to conduct anti-submarine exercises.[27] There are also future naval development plans to acquire four new surface combatants to supplement the five existing Visby-class corvettes from 2030. The Visby-class corvettes will also undergo a mid-life upgrade which, among other things,

A Swedish Combat boat 90 and a Finnish Jehu-class landing craft brake together during BALTOPS 22, Foto: Finnish Navy.

will add new anti-submarine warfare and medium-range surface-to-air missile systems.[28]

Intelligence and C2

There is no doubt that geography plays an essential part when it comes to developing and maintaining situational awareness of a potential adversary. As a case in point, Finland never stopped monitoring Russian military activities, even during the years immediately after the Cold War. This long-term commitment is key to maintaining a deep and up-to-date understanding of Russian intent, capabilities, and modus operandi. It will only serve to benefit NATO's intelligence community in the Baltic Sea Region. Both Finland and Sweden have mobile platforms and fixed installations with sensors to assess Russian military activities in the region. In addition, it is worth mentioning that the Swedish intelligence-gathering vessel HSwMS Orion, which was rammed by a Soviet Nanuchka-class corvette in 1985 after she got too close to a Soviet naval exercise in the Bay of Gdansk,[29] is soon to be replaced by a new SIGINT ship, the HSwMS Artemis.[30] Since both Finland and Sweden are tracking Russian military activity daily and in general, have a deep understanding of Russian operations in the Baltic Sea, a more formalized information sharing regime within the NATO Intelligence community will surely create synergies for the entire Alliance. It will improve situational awareness and understanding within the Alliance and enhance the ability to detect changes in Russian posture, presence, and profile, especially in times of increased tension, cases of crisis, and armed conflict.

NATO Command, Control, Communications, Computer, and Cyber Information Systems (C4IS) may also take advantage of Finnish and Swedish territories being adjacent to Russia and Russian military activities. Having the opportunity to maintain a permanent NATO C4IS presence in these countries creates resilience and enhances the ability for early indications and warnings of Russian activity and hostile intent. At the same time, when firmly integrated into NATO, both countries may offer their own C2 capabilities, such as headquarters facilities for NATO operations.

Sustainment and Force Protection

Finland and Sweden have naval bases primarily fitted for national-level operations. However, the Swedish Navy has recently introduced two new naval logistics formations established at the Karlskrona and Haninge garrisons, operational from autumn 2023.[31] Arguably, both Finland and Sweden will in the future be able to sustain NATO naval forces. Indeed, it could evolve into a key component of maintaining a permanent NATO naval presence in the region, enhancing flexibility and resilience. In times of crisis, Finnish and Swedish bases would also increase the replenishment options for Allied forces in the region, critical to force survival. Noteworthy is the port of Gothenburg, strategically located on the west coast of Sweden, and with more than 11,000 visits

annually, already a major logistical hub for the entire Scandinavian peninsula.[32] If required, the port could become a key strategic entry point for reinforcing NATO forces into the region.

As already mentioned, Russian A2/AD in the Baltic Sea Region may become challenging for NATO naval forces to penetrate. With Finnish and Swedish operational forces already in place, the odds of success for Allied in the area increase. They may conduct shaping operations and support overall force protection, enhancing the freedom of operations for NATO follow-on forces to the Scandinavian Peninsula and into the Baltic Sea.

Closing remarks

Once again, the Baltic Sea Region has become a contested arena for increased competition and influence. Finland and Sweden joining NATO will definitely be game-changing for both countries, and even so for Russia and the Alliance. Although relatively small, tailored, and highly specialized for national operations, the Finnish and Swedish Navy will solidify the Alliance's ability to deter and defend NATO territory. Both navies have capabilities that enhance NATO's ability to challenge Russian A2/AD in the region, especially in shaping operations, sea denial operations, and warfighting in the littorals. Being close partners to NATO for almost two decades, they already have intimate knowledge about Alliance doctrine, planning, and execution of naval operations, even if it will take some time to be fully integrated and interoperable. With modern platforms, sensors, and weapon systems in the maritime domain, the two countries will undoubtedly strengthen the northeastern NATO flank in the future, making the Alliance more resilient and capable of facing the security challenges of the 21st century.

Endnotes

1 Nieuwint, Joris, "Whiskey on the Rocks – When Sweden woke up to find a Russian Submarine stuck on a rock," August 5, 2015. https://www.warhistoryonline.com/war-articles/whiskey-on-the-rocks-when-sweden-woke-up-to-find-a-russian-submarine-stuck-on-a-rock.html?chrome=1&A1c=1.

2 Kuczyński, Grzegorz, "Russia Violates Baltic Airspace and Waters, Sending Warning to Sweden, Finland," Warsaw Institute, June 20, 2022. https://warsawinstitute.org/russia-violates-baltic-airspace-waters-sending-warning-sweden-finland/.

3 The Öresund and the Kiel Canal are supplementing entrance alternatives for smaller vessels and merchant shipping.

4 Helsinki Commission. August 26, 2022. http://archive.iwlearn.net/helcom.fi/environment2/nature/en_GB/facts/index.html.

5 Thomas, Matthew, "Maritime Security Issues in the Baltic Sea Region," July 22, 2020. https://www.fpri.org/article/2020/07/maritime-security-issues-in-the-baltic-sea-region/.

6 Finnish Metrological Institute. August 26, 2022. https://en.ilmatieteenlaitos.fi/ice-season-in-the-baltic-sea.

7 Corporal Frisk. October 12, 2019. https://corporalfrisk.com/2019/10/12/the-true-face-of-the-baltic-fleet/.

8 Baltic Marine Environmental Protection Commission. September 9, 2022. http://archive.iwlearn.net/helcom.fi/environment2/nature/en_GB/facts/index.html.

9 International Energy Agency. "Fact Sheet: Why does Russian oil and gas matter?". March 21,2022. https://www.iea.org/articles/energy-fact-sheet-why-does-russian-oil-and-gas-matter.

10 Nielsen, Anders Puck, "A look at the Baltic Fleet and the defense of Kaliningrad," ROMEO SQUARED: DEFENSE WITH A BALTIC EDGE. April 6, 2020.

11 Freedberg Sidney J., "Minefields at Sea: From the Tsars to Putin." March 23, 2015.

12 The Iskander-M is a road-mobile short-range ballistic missile (SRBM) with a range of up to 500 km, both nuclear and conventional capable, targeting hostile fire weapons, air and anti-missile defenses, command posts and communications nodes and troops in concentration areas.

13 Navy Recognition. "Russian Baltic Fleet trains with Grad and Uragan MLRS in Kaliningrad." September 30, 2022.

14 Al Jazeera. "Russia says it moved hypersonic Missiles to Kaliningrad Region." August 18, 2022. https://www.aljazeera.com/news/2022/8/18/russia-says-it-moved-hypersonic-missiles-to-kaliningrad-region.

15 Chang, Felix K., "Crowded pond: NATO and Russian Maritime Power in the Baltic Sea," Foreign Policy Research Institute. December 14, 2021. https://www.fpri.org/article/2021/12/crowded-pond-nato-and-russian-maritime-power-in-the-baltic-sea/.

16 Forsberg, Robin, Aku Kähkönen & Janna Öberg, "Implications of a Finnish and Swedish NATO Membership for Security in the Baltic Sea Region," Wilson Center. June 29, 2022. https://www.wilsoncenter.org/article/implications-finnish-and-swedish-nato-membership-security-baltic-sea-region.

17 NATO established the Partnership for Peace programme (PfP) in 1994 to strengthen mechanisms allowing non-NATO countries to cooperate with the Alliance to reform still-evolving democratic and military institutions and to relive their strategic isolation. Finland and Sweden were the first to join the same year.

18 Germanovich, Gene, James Black, Linda Slapakova, Stephen J. Flanagan, and Theodora Ogden, "Enhancing US-Finnish and regional defence cooperation: An exploratory analysis." Santa Monica, CA: RAND Corporation. 2021. https://www.rand.org/pubs/research_reports/RRA1424-1.html.

19 Finnish Navy, "Brigade Level Units." Last modified August 31, 2022. https://merivoimat.fi/en/navy-units.

20 Finnish Navy, "Finnish Navy." Last modified August 31, 2022 , retrieved from internet 31. August 2022.https://merivoimat.fi/en/about-us.

21 Forsberg, Robin, Aku-M. Kähkönen & Jason C. Moyer, "Finland's Contributions to NATO: Strengthening the Alliance's Nordic and Arctic Fronts," Wilson Center. November 8, 2022. https://www.wilsoncenter.org/article/finlands-contributions-nato-strengthening-alliances-nordic-and-arctic-fronts.

22 In the current AJP 3 – Allied Joint Doctrine for the Conduct of Operations, Joint Functions are a point of reference, as well as a description of the capabilities of the force. The Joint Functions, Manoeuvre, Fires, Information, and Civilian-Military-Cooperation focus on affecting adversaries through combined joint actions, underpinned by the joint functions C2 and Intelligence (including surveillance and reconnaissance), and furthermore, supported by the joint functions Sustainment and Force protection.

23 Toremans, Guy, "The Finnish Navy – 'Leaner and Meaner'," European Security & Defence. February 14, 2020. https://euro-sd.com/2020/02/articles/16171/the-finnish-navy-leaner-and-meaner/.

24 Ibid.

25 O'connor, Philip and Ilze Filks, "Sweden's Gotland at crossroads of history as NATO decision looms," Reuters. May 10, 2022. https://www.reuters.com/world/europe/swedens-gotland-crossroads-history-nato-decision-looms-2022-05-10/.

26 Ibid

27 Roblin, Sebastian, "How a cheap Swedish submarine 'ran rings' around a US aircraft carrier and its sub-hunting escorts," Insider. September 8, 2022. https://www.businessinsider.com/how-swedish-sub-ran-rings-around-us-aircraft-carrier-escorts-2021-7.

28 Pittaway, Nigel, "Swedish Navy chief prepares for growth,"Australian Defense Magazine. June 9, 2022. https://www.australiandefence.com.au/defence/sea/swedish-navy-chief-prepares-for-growth.

29 Aid, Matthew M., Cees Wiebes , «Secrets of Signals, Intelligence during the Cold War and beyond," Taylor & Francis. September 1, 2001.

30 Pittaway, Nigel, "Swedish Navy chief prepares for growth," Australian Defense Magazine. June 9, 2022. https://www.australiandefence.com.au/defence/sea/swedish-navy-chief-prepares-for-growth.

31 Swedish Armed forces, March 20, 2023, https://www.forsvarsmakten.se/sv/aktuellt/2022/11/marina-basbataljoner-ger-stark-tillvaxt-inom-marinen/

32 Port of Gothenburg, "The Port of Gothenburg." January 19, 2023. https://www.portofgothenburg.com/about-the-port/the-port-of-gothenburg/.

Seabed Warfare: Who Is Driving this Thing?

CDR (RNN) Bernd Roelink

Old tanks left underwater. Via Reddit.

Although the perpetrators' identities and the motives behind this intentional sabotage remains debated, the explosions on Nord Stream 1 and Nord Stream 2 natural gas pipelines rescheduled the agendas of many prominent civil and military servants, putting Seabed Warfare at the top of the security agenda.

Effective and operational civilian national infrastructure is key to Western economies, but the incident above demonstrated a critical vulnerability that cannot be countered by one country alone. Efforts to protect such a large and extensive infrastructure need a collaborated, persistent, and dedicated approach. It needs research, training, planning, and coordination. But if Seabed Warfare is like the train that has already left the station, who is driving this thing?

The history of submarine cables began between 1854 and 1858 when the first Atlantic Telegraph cable was constructed. The first official telegram to pass between two continents was a letter of congratulations from Queen Victoria of the United Kingdom to President James Buchanan of the United States on August 16, 1858. The second cable was laid in 1865. It allowed a message and a response within 24 hours.

Fast forwarding to the present day, submarine cables carry about 99% of transoceanic digital communications (e.g., voice, data, internet), including trillions of daily international financial transactions, and serve as the backbone for the global internet. There are about 486 undersea cables worldwide, stretching over one million kilometers and connecting every continent except Antarctica.[1]

Cables and Pipelines

Underwater infrastructure continues to develop across the world's oceans, driven by a number of factors. Northern countries are racing to build undersea communications cables through the waters of the Arctic as shrinking ice coverage opens the region to new business opportunities and heightens geopolitical rivalries between Russia and the West.[2] Because the geographical distance between continents is less at the Arctic than further south, a cable through the region would promise faster communications.

Russia has unveiled its plan to build the Polar Express subsea cable, a 12,650 km subsea cable along Russia's entire Arctic coastline from Murmansk to Vladivostok. The entire Polar Express subsea cable project is expected to be completed in 2026.[3]

Historically, cables are owned by groups of private companies, mostly telecom providers. However, during the last decade, this has changed. 2016 saw the start of a massive submarine cable boom, but this time the buyers are content providers: corporations like Facebook, Google, and Amazon.[4]

Underwater infrastructure is not solely about communicating. According to the Global Energy Monitor, there were at least 2,381 operational oil and gas pipelines distributed across 162 countries as of December 2020. The combined length of these pipelines is more 730,000 miles – enough to circle the Earth 30 times.[5]

The recent boom in pipeline usage is conservative compared to the recently achieved developments in offshore wind and solar energy. A spokesperson for Wind Europe explained that the current capacities of Europe's

first few floating wind farms (113 Megawatt) is expected to triple in just two years. Wind Europe predicts that there will be 10-Gigawatt offshore energy installations around the European continent by 2030, a 100x multiple of the current capacity and enough to provide energy to approximately ten million homes.[6]

Vulnerability

Although submarine infrastructure is generally situated on the seabed deep under water, it is far from safe. The most common threat today, responsible for roughly 150 to 200 subsea cable faults every year, is accidental physical damage from commercial fishing and shipping, or even from underwater earthquakes.[7] Fixing damaged cables is an inevitable cost of operations, but the impact on economies can be enormous. Sabotage, cyberattacks, interference, tapping, and terrorism have become more persistent threats in the last decade. Damaging submarine cables or pipelines, especially in areas with shallow waters, does not require a high level of technical expertise. Deliberate State and Non-State attacks have the ability to strike at the most inopportune times, ensuring high impact and dire consequences with relatively low cost and risk.

Locations of submarine cables and pipelines, including landing sites, are publicly known or easy to track down, further allowing interference by adversaries. Cables located deep underwater are difficult to access, but areas with high cable concentrations in shallow waters, like chokepoints and landing sites, represent a key vulnerability to data transmission security.

Ambiguous and Deniable Actions

Why would a nation, who would normally be inferior to its competitors, risk losing tons of hardware and manpower in large scale warfare when it can create devastating effects through ambiguous and deniable actions? Actions to monitor, hamper, or disrupt an opponent's military might be far more rewarding if those actions are challenging to attribute, hard to counter, and arguably conducted below the threshold of armed conflict.

At a meeting of NATO defense ministers in 2020, the Alliance produced a report underscoring the vulnerabilities related to undersea cables and the importance of protecting undersea infrastructure. NATO Secretary General Jens Stoltenberg addressed the issue directly by saying, "It is important to understand that most of these cables are privately owned and it's publicly known where they are and that makes them potentially vulnerable."[17]

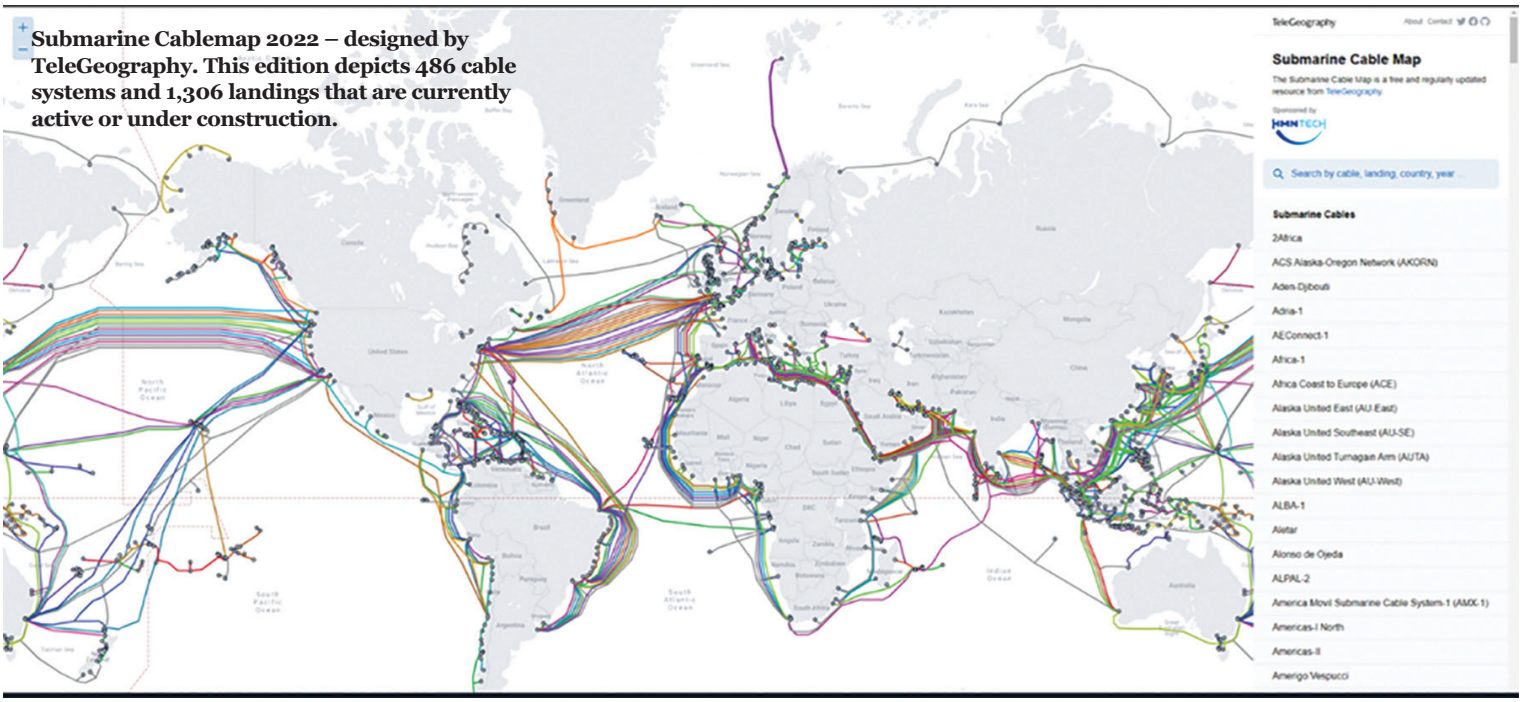
In the years since that meeting, there have been several incidents that illustrate this point:

- In November 2021, a unique underwater observatory in the strategic waters off the coast of northern Norway was knocked out of service when more than 4.3 kilometers of its specially designed offshore fiber-optic and electric cables were cut and removed. That type of damage was no accident.[8]
- In September 2022, explosions crippled the Nord Stream pipelines in the Baltic Sea. Analysis showed traces of explosives on several of the foreign objects that were found at the site.[9]
- In October 2022, an act of vandalism disrupted land-based internet cables that connect Marseille, France's second largest city, to other French cities and much of Europe. The damage in Marseille resembled suspected acts of sabotage to other cables in the country earlier in the year.[10]

These events clearly demonstrate the vulnerability of undersea infrastructure and the difficulty in attributing these types of incidents.

Seabed Warfare: Protecting Underwater Infrastructure and Countering the Threats

Seabed Warfare has many different objectives:



Submarine Cablemap 2022 – designed by TeleGeography. This edition depicts 486 cable systems and 1,306 landings that are currently active or under construction.

controlling, monitoring, surveilling, patrolling, searching, locating, identifying, countering hybrid/cyber, assessing, neutralizing, attacking, and probably more. So, in order to make the protection of seabed infrastructure manageable and feasible, it is critical to set the right priorities. Seabed Warfare planners need to identify and prioritize Critical National Infrastructure and Mission Vital Infrastructure, and assess associated vulnerabilities like weak spots, chokepoints, and landing sites.

Knowing one's own key infrastructure and vulnerabilities is just as important as knowing our potential enemies' capabilities. Leaving other potential adversaries like China aside, Russia is one of the most capable nations to conduct seabed operations today. According to Andrew Salerno-Garthwaite, "Russia has a specific directorate for deep sea operations, known as GUGI, operating through the Russian Army and manned by Spetsnaz Special Forces. The Russian fleet includes a variety of subsurface boats as well as highly capable oceanographic survey vessels."[11]

> **It is not satellites in the sky, but pipes on the ocean floor that form the backbone of the world's economy.**
> ***- Admiral Stavridis US Navy (Ret)***

Do We Lack a Sense of Urgency?

Certainly, the intentional sabotage of the Nord Stream pipelines changed the sense of urgency amongst Allied nations but, as long as the seabed remains unprotected under international law, a widespread lack of ownership persists. Under the Law of the Sea, the national mandate for prevention, detection, protection and response in the face of security risks and threats is limited beyond the 12 nautical mile boundary. The Hague Centre of Strategic Studies poses the question, "How and by whom is the integrity of the – increasingly critical and vulnerable – processes and associated infrastructure in the North Sea guaranteed?"[12] Current policy documents barely address this crucial question.

The only legal effort made so far by the international community is the 1884 International Treaty for the Protection of Submarine Telegraph Cables. Some considerations were incorporated into the 1982 United Nations Convention on the Law of the Sea (UNCLOS), but consensus on 'right to inspect' or 'obligations to protect' the infrastructure on the ocean's floor shines in absence.

On top of that at the national level is the question of whether the protection of underwater infrastructure is a responsibility for Homeland Security, Defense, Home Department, Justice, or all of the above? Is there a role for the private companies or content providers that own the cables or pipelines?

Nevertheless, despite these ambiguities several allied nations are already involved in Seabed Warfare. For example, France recently unveiled its new Seabed Warfare Strategy, and the UK recently updated its fleet with the first of two Multi-Role Ocean Surveillance (MROS) ships, capable of monitoring and protecting seabed communications.[13] Also, the United States is making progress in Full Spectrum Undersea Warfare, which aims to address the protection of undersea infrastructure. These efforts reflect the desire at state level to combat seabed threats despite inherent challenges, as noted by H.I. Sutton, an independent naval researcher and author of Covert Shores."[14] Protecting underwater infrastructure is primarily a national responsibility, but unfortunately Seabed warfare is extremely difficult to defend against and no country on earth is well-equipped or prepared to do the defending."

NATO exercises like Robotic Experimentation and Prototyping using Maritime Unmanned Systems (REPMUS) and Dynamic Messenger bring stakeholders together for testing and learning. The Alliance is also taking some steps in the right direction with technological development programs such as the Maritime Unmanned System Initiative (MUSI). Unfortunately, apart from these exercises and a couple multilateral agreements, nations seem to be struggling to pool their forces. NATO must increase its efforts to combat this problem and its members need to both provide and request support – without nations supporting these endeavours, NATO can drive all it wants – the train car will be empty.

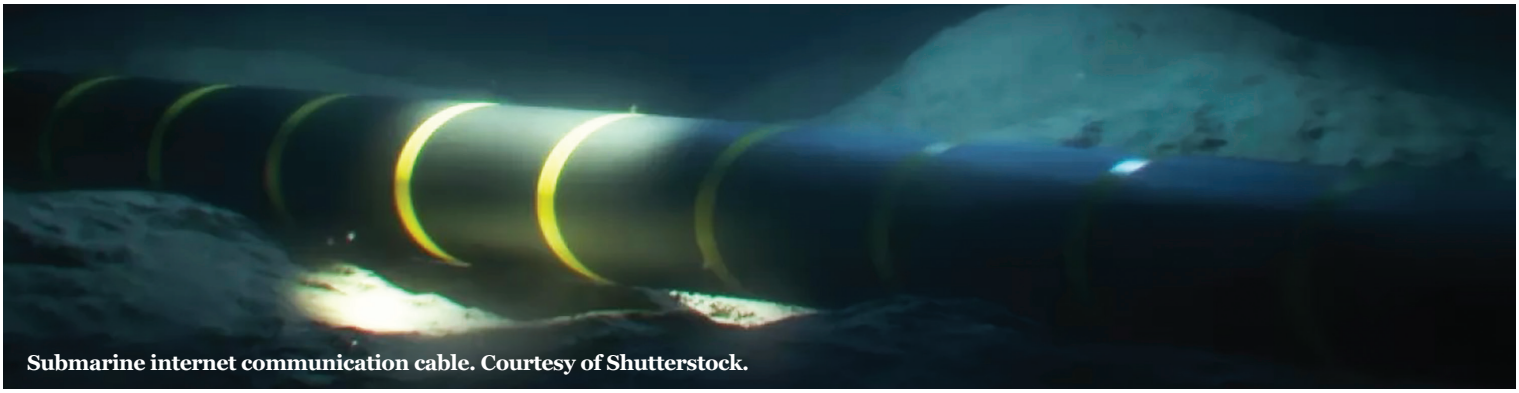
Shared Interests Feed Unity

Following the acts of sabotage on the Nord Stream pipelines, NATO Secretary General Jens Stoltenberg said that a deliberate attack against Allies' infrastructure would be met with a determined response.[15] The Alliance's coherence and deterrence was clearly demonstrated when Standing NATO Maritime Group 1 was deployed to the North Sea immediately after the Nord Stream sabotage.

Recently the leaders of Germany and Norway jointly asked NATO to coordinate the protection of Europe's subsea infrastructure in light of the suspected attacks on the Nord Stream gas pipeline network.[16] Countering hybrid warfare is not new to NATO.

It has deployed its Counter Hybrid Support Teams twice in recent years: first in 2019 to help Montenegro counter Russian election interference, and then again in 2021 to help Lithuania deal with a migration crisis manufactured by Belarus and Russia.

Seabed Warfare provides NATO with a good opportunity (we are stronger together!) to prove its strategic concept: ensuring the Alliance remains fit and resourced for the future.



Submarine internet communication cable. Courtesy of Shutterstock.

Because NATO has the authority, the structure and the network to protect Allies' critical underwater structure and to oppose the threat, it is the most likely pick to drive this proverbial train. Whether NATO has the capacity is a matter of approach, degree of delegation, and priorities.

Guidance, the standardization of processes, and coordination benefit the Alliance and help combat the lack of time, capacity, and need for national level money-consuming research programs. NATO must encourage nations and civil stakeholders to share intelligence on our potential adversaries. It will also be important for stakeholders to share information on critical seabed infrastructure and data collection capacity. By leveraging shared best practices and lessons learned from NATO-led Seabed Warfare training, Allies could benefit from future protection plans and a specific concept of operations for Seabed Warfare scenarios.

Final thoughts

Whether natural or deliberate damage occurs on the seabed, Allies need to be prepared when things go wrong. Self-sustainability and a high degree of resilience are critical ingredients to potentially saving the day. Nations must combine both civil preparedness and military capacity in order to be able to resist, or at least be resilient enough to recover from a major shock such as a natural disaster, failure of critical infrastructure, or a hybrid attack. In worst case scenarios, Allies need to have their continuity of government assured. They need to have back up plans for energy supplies and food and water resources. They should also have robust civil communication and transportation systems to handle mass casualties and disruptive health crises.

NATO provides a valuable forum for its members to share best practices and national experiences, including counter-hybrid support teams designed to assess, advise, and improve Allies' resilience in the face of hybrid threats. Although Seabed Warfare is a relatively new concept, it is already well underway – like a train that has left the station. As the Allies on the train look around the train car, it makes sense that NATO should be the one to take the wheel.

Endnotes

1 Congressional Research Service, "Undersea Telecommunication Cables: Technology Overview and Issues for Congress", September 13, 2022. Available at https://crsreports.congress.gov/product/pdf/R/R47237

2 The Wall Street Journal, "A Warming Arctic Emerges as a Route for Subsea Cables", June 15 2022. Available at https://www.wsj.com/articles/a-warming-arctic-emerges-as-a-route-for-subsea-cables-11655323903

3 Submarine Cable Networks, "Russia builds Polar Express subsea cable along Arctic coastline", August 13, 2021. Available at https://www.google.com/search

4 Broadband Now, "Google Owns 63,605 Miles and 8.5% of Submarine Cables Worldwide", September 12, 2018. Available at Available at https://www.google.com/search?q=Google+Owns+63%2C605+Miles+and+8.5%25+of+Submarine+Cables+Worldwide+(broadbandnow.com

5 Global Energy Monitor, December 16 2021. Available at https://globalenergymonitor.org/projects/global-fossil-infrastructure-tracker

6 Wind Europe, "Europe can expect to have 10 GW of floating wind by 2030", June 2, 2022. Available at https://www.google.com/search?q=Europe+can+-expect+to+have+10+GW+of+floating+wind+by+2030+%7C+WindEurope

7 Center For Strategic & International Studies. June 11, 2022. Available at https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-trans-atlantic-security

8 TheBarentsObserver, "Human activity behind Svalbard cable disruption", January 09 2022. Available at https://www.google.com/search?q=%27Human+activity%27+behind+Svalbard+cable+disruption+%7C+The+Independent+Barents+Observer+(thebarentsobserver.com)

9 New York Post, "Sweden finds explosives traces near damaged Nord Stream pipeline", November 18 2022. Available at https://www.google.com/search?q=Sweden+finds+explosives+traces+near+damaged+Nord+Stream+pipeline+(nypost.com)

10 Associated Press, ABC News, "French police probe multiple cuts of major internet cables", October 21 2022. Available at https://www.google.com/search?q=French+police+probe+multiple+cuts+of+major+internet+cables+-+ABC+News+(go.com

11 Naval Technology, "Seabed Warfare is a real and present threat", December 20 2022. Available at https://www.google.com/search?q=Seabed+warfare+is+a+%E2%80%98real+and+present+threat%E2%80%99+-+Naval+Technology+(naval-technology.com)

12 The Hague Centre for Strategic Studies (HCSS), The High Value of the seas, pg. 4. Available at https://www.google.com/search?q=The+High+Value+of+The+North+Sea+-+HCSS

13 Naval Technology, "Seabed Warfare is a real and present threat", December 20 2022. Available at https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/

14 Naval Technology, "Seabed Warfare is a real and present threat", December 20 2022. Available at https://www.naval-technology.com/features/seabed-warfare-is-a-real-and-present-threat/

15 Reuters, " Attacks against NATO allies critical infrastructure to be met with determined response", September 29 2022. Available at https://www.google.com/search?q=Attacks+against+NATO+allies+critical+infrastructure+to+be+met+with+determined+response+-+NATO+chief+%7C+Reuters

16 Reuters, "Germany and Norway want NATO to protect subsea infrastructure after Nord Stream attacks", November 30 2022. Available at https://www.google.com/search?q=Germany+and+Norway+want+NATO+to+protect+subsea+infrastructure+after+Nord+Stream+attacks+%7C+Reuters

17 Online press conference by NATO Secretary General Jens Stoltenberg following the first day of the meetings of NATO Defence Ministers. October 22, 2020. Available at https://www.nato.int/cps/en/natohq/opinions_178946.htm?selectedLocale=en

Standing NATO Mine Countermeasures Group 1 sail in formation in Geiranger Fjord, Norway, during Exercise Cold Response, March 9, 2022. Courtesy of US Navy.

Arctic Perspectives

Olga R. Chiriac, PhD

February 2022 marked the end of the post-Cold War era in world affairs and the official return to great power politics. In an Op-ed article from August last year, NATO Secretary General Jens Stoltenberg designated the events in Ukraine "a game-changer for global security."[1] From a Russian standpoint, said changes had already been taking place for years, including in the Arctic. The Alliance is present in the Arctic by means of its member states, including the United States (US), but the region has thus far been an atypical geopolitical space, where the great powers have managed to balance cooperation and strategic competition. Given the rapid developments due to both geopolitical and climate change realities, the key question for the North Atlantic Treaty Organization (NATO) going forward will undoubtedly be how can the Alliance design strategies that will produce positive outcomes for the international community and, certainly not least, for the environment. Moreover, the time has arrived to have a more in-depth discussion about unconventional maritime warfare. NATO planners and stakeholders will ideally start from correct assumptions, which add one more level of complexity given the tensions between the West, Russia, and the myriad of frozen cooperation mechanisms, including the Arctic Council. At the very least, the discussion must start from an objective, clinical evaluation of Russia's view of the Arctic.

Even before the events of February 2022, Russia had started to perceive itself as a great power in a hybrid war with the collective West.[2] The image of a hostile West looking to contain Russia and deplete its natural resources spilled over into the maritime domain and remains today. An underexplored aspect of this discussion is the way Russia employs unconventional warfare means in the Arctic. This article discusses said aspect and underscores how an operationally challenging environment like the Arctic requires more region specific, socio-culturally comprehensive approaches.

The Russian Arctic – "The Beginning of Russia"

"We are here forever," declared Admiral Nikolai Yevmenov, Commander-in-Chief of the Russian Navy, in December 2022, as he was delivering remarks on the development of the Arctic at "The Arctic: Present and Future" forum. "The Arctic," Yevmenov continued, "is not a bears' corner of the empire, but the beginning of Russia."[3] Notably, the Admiral referred to the Russian Federation as an empire, a modern great power. This declaration coming from the very top of the Russian Navy eloquently summarizes how Russia conceptualizes the high north and what role the region plays in the overarching strategy of the country. If we were to look at history and geography, the prioritization of the Arctic, especially in the context of accelerated climate change, makes a lot of sense. For more than two centuries,

The Russian Navy's missile cruiser Marshal Ustinov.
Courtesy of Shutterstock.

both Imperial Russia and the Soviet Union have been exploring and developing the Arctic. The USSR made great strides in the scientific northern exploration. Joseph Stalin first dispatched a team of researchers in 1937[4] at the height of the Great Terror and years before the Cold War. Accessing resources for a large population and defending those resources have been strategic constants in Russian political thinking. At present, the Russian portion of the Arctic represents more than half of the Arctic Ocean coastline. Moreover, according to the Arctic Council, the Russian population in the region accounts for half of the grand total (approximately two and a half million of Russia's inhabitants live in Arctic territory). In the Arctic, all Russian activities are primarily linked to the "interests of the country's military security."[5] The Arctic is, and always was, a strategically significant area for Moscow; an integral, geopolitical and geo-economic pivot of Russian grand strategy.

In modern Russia, even before the first post-Cold War Russian Maritime Doctrine was published in 2001, Moscow was slowly regrouping in order to regain control of its Arctic area of influence. Under President Boris Yeltsin, a Decree of the President of Russia from August 1994 created the "Arctic Group of Border Troops."[6] The declared aim of this law was to strengthen the protection of the state border in the Arctic sector of the Russian Federation. Follow-on leaders continued these efforts, morphing this military group into the "Arctic Regional Border Directorate of the FSB of Russia" (in 2003), and, since October 2004, the "Border Directorate of the FSB of Russia for the Murmansk Region."[7] Some of the tasks include, but are not limited to, ensuring effective protection of the state border and protecting the economic and other legitimate interests of the Russian Federation. The Directorate is also tasked with preventing and/or countering threats that are global in nature, namely international terrorism and drug trafficking, theft of natural resources, and illegal migration. Nevertheless, the concept behind these efforts was to build a force with special, Arctic specific skills, rather than focusing on conventional forces.

A 15-year Russian Arctic strategy is laid out in the Foundations of the Russian Federation State Policy in the Arctic for the Period up to 2035[8] and it was approved by decree of the President on March 5, 2020. This document underscores the centrality of the Northern Sea Route (NSR) in Russian strategy; it gives Moscow a lot of potential control and, inherently, leverage. Running parallel to its Arctic coastline, the NSR is a strategic anchor of Russia's geopolitical and economic future as it is vital to maritime shipping, resource extraction, and scientific research. Unsurprisingly, the NSR, and the overall Arctic region, was added to the list of national interests in the 2022 released Maritime Doctrine. For the Arctic State Policy, Mr. Alexander Kozlov, then serving as Minister of the Russian Federation for the Development of the Far East and the Arctic, explained the novelty and inherent value Russia claimed this strategic document brought forth: "For the first time in a document of this level, the main goal of the development of the Arctic zone is to improve the

quality of life of the people living there and, accordingly, a number of decisions are formulated that are aimed at the social development of the region."[9] The Minister noted this "strategy has a special regional section that defines the priority areas for the socio-economic development of each territory in the Arctic zone."[10] The marked emphasis on socio-economic development and improvement of living conditions reappeared in the updated Maritime Doctrine[11].

The release in July 2022 of the Maritime Doctrine of the Russian Federation announced that the development of the Arctic Zone of the Russian Federation and the NSR were upgraded to national interests. Despite strict sanctions being imposed on Russia, officials seem confident the development of the region will go on according to plan. Furthermore, in August 2022, Mikhail Mishustin approved the plan for the development of the NSR until 2035. Order No. 2115-r dated August 1, 2022, prioritizes the consolidation and expansion of the infrastructure of the NSR as "the most important transport corridor of national and global importance."[12] An integrated plan for the development of the NSR until 2035 was sent to the Russian government for consideration. According to official sources, the proposal includes development of infrastructure and the construction of new icebreakers, the launch of space satellites, the improvement of security systems and the renewal of meteorological technologies.[13] It is in Russia's national interest to develop the Arctic: a statement released in December 2022 by the Communications Department of Rosatom State Corporation announced the target of 32 million tons of cargo traffic, specified in the federal project, "Development of the NSR," was reached ahead of schedule.[14] Finalized plans for the development of the NSR were submitted to the decision makers back in 2019.[15]

> ***The time has arrived to have a more in-depth discussion about unconventional maritime warfare.***

Aspects of Russian Conventional Force Structure in the Arctic

Russian force structure in the Arctic is extensive and serves to confirm that Moscow regards the region as both a primary security concern and an opportunity for economic growth through hydrocarbon and mineral resource exploration as well as controlling the sea lines of communication. In fact, the forces have been in a state of consistent buildup since the now infamous flag planting on the Arctic Seabed in 2007.[16] In the overarching Russian strategic picture, this appropriately mirrors the foreign policy recalibration marked by the equally infamous 2007 Munich Security Conference Speech. Russia has systematically expanded and strengthened its Arctic military presence "through a combination of bases, airfields, and large-scale radar installations, as well as defensive and offensive weapons systems."[17] The area is also home to a large part of the nuclear element.

Russia's military presence in the Arctic is designed to prioritize limiting external access to the NSR and to maintain strategic strike potential via its submarines and long-range aircraft carriers (ex. second strike capabilities off Kola Island). The anti-aircraft, anti-missile and anti-submarine posturing is meant to address perceived threats from NATO's Northern Flank. The 2022 Russian Maritime Doctrine clearly designates NATO and especially the US as a threat. Prior to this clear declaration, the narrative was consistently present in Russian political discourse.

The current force structure also includes several airfields/airbases "capable of receiving not only MiG-31 fighter-interceptors, but also heavy transport aircraft" and 50 military facilities (a mixture of former Soviet and newly constructed infrastructure).[18] The newly established bases are Nagurskoye Air Base on Alexandra Land, Rogachevo Air Base on Novaya Zemlya and Temp Air Base on Kotelny Island. Also, an additional S-400 Air Defense System has been deployed in Rogachevo. According to Russian Arctic experts, in total 10 Russian radars cover the Arctic. Sopka-2 radar systems are located on Wrangel Island and Cape Schmidt in close proximity to Alaska.[19] The radars are considered a protective dome, not an offensive position.

The Russian Military Industrial Complex is also closely supporting developments in the region. The Krylov State Research Center and Rosatom's machine-building division, Atomenergomash, held a conference on the development of a project for a domestic Arctic gas tanker. Presented in June 2022, Project 10070 is the result of the work of Atomenergomash and Saint Petersburg State Marine Technical University.[20] There will be transshipments of cargo to ice-class vessels that can operate on the NSR routes. "Work on the creation of the logistics complex is planned to be completed by 2026,"[21] the report says. On February 15, 2023, the Ministry of Digital Development, Telecommunications and Mass Media of the Russian Federation announced how, in the framework of said project, Rosatom is developing a gas tanker for year-round operation on the NSR.[22] Russian posture in the Arctic has always been about security and economic development.

Looking Forward: Unconventional Warfare in the Arctic?

So, what does all this mean for NATO? While the answers may offer limitless options, there are a few aspects which stand out immediately after reading the 2022 Maritime Doctrine and framing it correctly, from a Russian vantage point.

First, Russian ambitions in the Arctic must be filtered through history and a correct read of its political culture. Both indicate Russia is existentially dependent on the Arctic. Research and development of the region started in 1648[23] and continued regardless of who was leading the nation. The vast amounts of hydrocarbons and mineral resources present in the Arctic as well as control over the NSR, a potential game changer in global maritime transport, rate very significantly in Moscow's strategic calculus. The more assertive tone and comprehensive content of the newly released Maritime Doctrine reflect both urgency and steadfast commitment to maintaining dominance in the Arctic. Russian political elites consider this aggressive tone, especially towards the US and NATO, not only appropriate but necessary for the "establishment of concrete and systematic 'red lines' at the level of strategic planning documents."[24] If Moscow's leadership declares that it considers the country in a hybrid war with the collective West, it makes no strategic sense to contradict that, and it is better to understand what that means in a Russian mindset. The Arctic presents us with very niche challenges but also ample opportunities for guarded cooperation. Looking at the history of Russian Special Forces in the Arctic or conceptualizing Russian Force Structure (conventional, special and nuclear forces holistically) can help NATO and allied stakeholders in designing efficient strategies and operational approaches.

Second, Russia has operated in the Arctic for centuries. NATO's Arctic nations, despite some being relatively new to the region and, at times, having divergent national interests, must understand the operational environment in all its socio-cultural specificities. Capabilities required to "survive, thrive, and operate in harsh Arctic conditions"[25] are not matched anywhere else on the planet. The Norwegians and Danes have long operated in the region, providing opportunities for Allies to learn beyond limited missions and exercises. Meanwhile, the Northern Fleet (around sixty percent of the Russian Navy) was built for Arctic operations. Russian Special Forces in Alexandra Land and Kotelny might not match the overwhelming mass of conventional forces of NATO, but they do bring impressive skills. It is for this very reason the Arctic Group of Border Troops was established in 1994 and it is for this very reason Russia favours operators versus conventional forces. It would also not be strategically wise to count out the quality of the Russian Arctic naval forces. It's the same Navy, but a much different Fleet than the southern forces who performed underwhelmingly in the Black Sea in 2022.

Finally, there are asymmetric means Russia can use to harass NATO. The Svalbard Treaty,[26] for example, recognizes the sovereignty of Norway over

A Marine scans for simulated targets during an exercise in Setermoen, Norway, March 7, 2022, as part of Cold Response, a readiness and defense exercise. Courtesy of US DOD.

the archipelago of Svalbard; however, it is subject to certain stipulations, including letting Russia engage in commercial activities and ensuring the demilitarization of the archipelago. The United Nations Convention on the Law of the Sea and maritime international law are also significant in the region and warrant their own an entirely separate in-depth assessment. Potential problems for the Alliance could stem from a non-discrimination clause in the Treaty. Russia has diligently ensured that ethnic Russians populate the area; a fact that raises concerns considering the apparent policy of Moscow to intervene to protect its ethnic "citizens" anywhere it deems necessary.

There are, of course, many more aspects of the Arctic region that provide challenges and opportunities for both Russia and NATO. Both sides will continue to assert their interests; however, there is room for cooperation in the future. The overarching umbrella issue of climate change provides a unique opportunity, ostensibly following a "favourable to the West" outcome of the Ukraine war. Preserving the climate, just like strategic stability engagements, is of interest to all parties, and presents serious prospects for great power dialogue, and ultimately hope for the future.

Dr. Olga R. Chiriac is the Project Europe Head of Engagement, Irregular Warfare Initiative, Associated Researcher, Joint Special Operations University.

Endnotes

1 Stoltenberg, Jens. "NATO Is Stepping Up In The High North To Keep Our People Safe." NATO, August 25, 2022. https://www.nato.int/cps/en/natohq/opinions_206894.htm.

2 Chiriac, Olga R. "The 2022 Maritime Doctrine Of The Russian Federation: Mobilization, Maritime Law, And Socio-Economic Warfare." Center for International Maritime Security CIMSEC, November 28, 2022. https://cimsec.org/the-2022-maritime-doctrine-of-the-russian-federation-mobilization-maritime-law-and-socio-economic-warfare/.

3 Фомичева, Екатерина. "Главком ВМФ: 'Арктика - Это Не Медвежий Угол Империи, а Начало России.'" (Commander-in-Chief of the Navy: "The Arctic is not a bears' corner of the empire, but the beginning of Russia"), New Prospect, December 9, 2022. https://newprospect.ru/news/aktualno-segodnya/glavkom-vmf-arktika-eto-ne-medvezhiy-ugol-imperii-a-nachalo-rossii/?sphrase_id=24061.

4 Vladimir Zenzinov."The Soviet Arctic."The Russian Review 3, no. 2 (1944): 65–73.https://doi.org/10.2307/125409.

5 "Военная Доктрина Российской Федерации (Military Doctrine of the Russian Federation)." Approved by the President of the Russian Federation on December 25, 2014, No. Pr-2976. Security Council of the Russian Federation, December 2014. http://www.scrf.gov.ru/security/military/document129/.

6 Илья, Оришин. "Современное Присутствие Военных Стуктур в Арктике." ("Current Presence of Military Structures in the Arctic") Арктик-фонд. Accessed February 13, 2023. https://arctic.narfu.ru/ru/infologia-arktiki/gosudarstvennaya-politika-v-arktike/qqq.

Studies Institute, Russia Maritime; Davis, Anna; and Vest, Ryan, "Foundations of the Russian Federation State Policy in the Arctic for the Period up to 2035" (2020). RMSI Research. 5.
https://digital-commons.usnwc.edu/rmsi_research/5

7 Ibid.

8 Studies Institute, Russia Maritime; Davis, Anna; and Vest, Ryan, "Foundations of the Russian Federation State Policy in the Arctic for the Period up to 2035" (2020). RMSI Research. 5. https://digital-commons.usnwc.edu/rmsi_research/5.

9 Принята Стратегия Развития Арктической Зоны России До 2035 Года." МЕЖДУНАРОДНЫЙ АРКТИЧЕСКИЙ ФОРУМ 2022. Accessed February 14, 2023. https://forumarctica.ru/news/prinyata-strategiya-razvitiya-arktich-eskoy-zony-rossii-do-2035-goda/.

10 Ibid.

11 Ibid.

12 ""Михаил Мишустин Утвердил План Развития Северного Морского Пути До 2035 Года (Mikhail Mishustin Approved the Plan for the Development of the Northern Sea Route until 2035)." Правительство России, August 2022. http://government.ru/news/46171/.

13 ""Михаил Мишустин Утвердил План Развития Северного Морского Пути До 2035 Года (Mikhail Mishustin Approved the Plan for the Development of the Northern Sea Route until 2035)." Правительство России, August 2022. http://government.ru/news/46171/.

14 Communications Department of Rosatom State Corporation. "The 2022 Target of The Federal Project Development of the Northern Sea Route- 32 Million Tons-Was Achieved Ahead of Schedule, Rosatom State Nuclear Energy Corporation, December 14, 2022, https://rosatom.ru/journalist/news/tselevoy-pokazatel-2022-goda-federalnogo-proekta-razvitie-severnogo-morskogo-puti-32-mln-tonn-dostig/.
"Объем Перевозок По Северному Морскому Пути Превысил 32 Млн Тонн." Портньюс, December 15, 2022.
https://portnews.ru/news/340243/.

15 Berezina, Elena, and Evgeny Gaiva. "План Развития Северного Морского Пути Внесен в Правительство (Plan for the Development of the Northern Sea Route Submitted to the Government)." Российская газета, November 25, 2019. https://rg.ru/2019/11/25/plan-razvitiia-severnogo-morskogo-puti-vnesen-v-pravitelstvo.html.

16 Chivers, C. J. "Russians Plant Flag on the Arctic Seabed." Russians Plant Flag on the Arctic Seabed. The New York Times, August 3, 2007. https://www.nytimes.com/2007/08/03/world/europe/03arctic.html.

17 Humpert, Malte. "From Ukraine to the Arctic: Russia's Capabilities in the Region and the War's Impact on the North." From Ukraine to the Arctic: Russia's Capabilities in the Region and the War's Impact on the North. High North News, September 28, 2022. https://www.highnorthnews.com/en/ukraine-arctic-russias-capabilities-region-and-wars-impact-north.

18 "Авиация в Арктике: Эпоха Возрождения." Arctic Russia, October 22, 2020. https://arctic-russia.ru/article/aviatsiya-v-arktike-epokha-vozrozhdeniya/#:~:text.

19 Ibid. Also: Air-Route Radar Complex "sopka-2". Accessed February 14, 2023. https://lemz.ru/en/sopka-2/.

20 "В Росатоме Разрабатывают Танкер-Газовоз Для Круглогодичной Работы н... (Rosatom Is Developing a Gas Tanker for Year-Round Operation on the Northern Sea Route)." Новостной портал о ТЭК России и Мира Neftegaz.RU. Neftegaz.ru, February 15, 2023. https://neftegaz.ru/news/Suda-i-sudostroenie/770459-v-rosatome-razrabatyvayut-tanker-gazovoz-dlya-kruglogodichnoy-raboty-na-sevmorputi/.

21 Ibid.

22 Ministry of Digital Development, Telecommunications and Mass Media of the Russian Federation, В Росатоме разрабатывают танкер-газовоз для круглогодичной работы на Севморпути(Rosatom is developing a gas tanker for year-round operation on the Northern Sea Route), Published February 15, 2023, Accessed March 8, 2023 at https://digital.gov.ru/ru/events/42735/

23 Vladimir Zenzinov. "The Soviet Arctic." The Russian Review 3, no. 2 (1944): 65–73. https://doi.org/10.2307/125409.

24 Tebin, Prokhor. "The Naval Doctrine of Russia" Valdai Discussion Club, August 4, 2022. https://valdaiclub.com/a/highlights/the-new-naval-doctrine-of-russia/.

25 Meade, Julian R. "Russia's New Arctic Policy 2035: Implications for Great Power Tension Over the Northern Sea Route." National Defense University, July 21, 2020. https://ni-u.edu/wp/wp-content/uploads/2021/06/NIU-Catalog-2021-2022-Final.pdf.

26 Treaty of February 9th 1920 Relating to Spitsbergen (Svalbard), Act of 17 July 1925 Relating to Svalbard.https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19250717-011-eng.pdf

Courtesy of US Air Force.

NATO's Maritime Information Warfare Commander

CDR (USN) Fred Conner

The Information in Information Warfare

Information warfare is critical to military success. Ukraine's use of social media to gain public support for their war efforts along with Russia's manipulation of international information channels to spread disinformation serve as recent, newsworthy examples of information warfare. NATO and its allies must understand and adapt to this constantly changing warfare domain in order to maintain military superiority.

Information warfare can and should be considered one of the domains of operation in all nations' doctrines. The U.S. Navy's (USN) Information Warfare Community aims to defeat any enemy by using assured command and control, battlespace awareness, and integrated fires to achieve freedom of manoeuvre across all warfighting domains.[1] NATO defines information warfare as an operation conducted in order to gain an information advantage over the opponent. The amount of information required to achieve this mission has increased and continues to grow. Set against this background of change, NATO's maritime missions need commanders to understand, collect, manage, and disseminate vital information to senior decision makers.

Successful implementation of the Information Warfare Commander (IWC) is already outlined in NATO's Maritime Information Warfare (MIW) ATP. The IWC is an integral part of information warfare as successful MIW must be implemented to maintain maritime success.

What's out there?

It starts with an idea: information is out there! Information, as defined by Webster's dictionary, is knowledge obtained from investigation, study, or instruction.[2] One could understand that information is knowledge and, as technology futurist Daniel Burrus suggests, information can be used as power. Globally, data created and information gathered continues to grow. Statista, a leading provider of market and consumer data, reports that the total amount of data created, captured, copied, and consumed globally is forecast to increase rapidly; it reached 64.2 zettabytes in 2020 and is projected to reach over 180 zettabytes by 2025.[3] That's over 180 billion terabytes that a system or group of people must interpret and properly utilize!

Similarly, data usage within militaries has also increased. In 2017, the U.S. Department of Defense estimated that the Pentagon collects 22 terabytes of data daily.[4] The amount of information, its usage, and the complexity of systems and their equipment have continued to increase. Vice Admiral Kelly Aeschbach, Commander of Naval Information Forces, has highlighted the increasing complexity of having multiple sailors operating multiple information systems at once.[5] Simultaneously handling multiple sources of information could be a complicated puzzle when an expeditious and efficient response is necessary. Information gathered, produced, and stored supports cybersecurity, electronic warfare, information operations, cryptology, and meteorology. The synergy

and effective use of these systems and contained data are necessary for information dominance and maritime superiority. Vice Admiral Matthew Kohler (retd), a former Naval Information Warfighting Development Center Commander, stated that this domain has become so complex that its function requires full-time trained staffers to ensure that naval forces can keep up with the growing intricacies.[6] The increasing amount of information and the management complexity of interconnecting systems are the drivers for the necessity of the information warfare domain and the specialists who will be trained to harness it.

Information Warfare Domain

It is evident that information dominance can directly impact strategic and tactical decisions, the current war in Ukraine serves as an example of its importance.

A recent New York Times article described how photos and videos of the war's horrors have impacted the global opinion towards Russia and likens the use of social media to a weapon for stirring resistance.[7] The Ukrainian people, government officials and civilians alike, used the information spread on social media to change hearts and minds in support of their country's resistance to Russia. Throughout this war, Ukraine has used information strategically to provide near real-time updates to validate or invalidate wartime reports.

Russia also continues to use information warfare against NATO members. A Carnegie senior fellow, Dr. Bilyana Lilly, discussed that Russia uses information warfare to threaten democratic countries, with their tactics being used to spread election disinformation, encourage coup plots, and create a general sense of chaos across various information channels.[8] NATO nations must continue their efforts to understand this domain of warfare and be prepared to respond with appropriate operations. Information, however, is being used by more than just the two examples above. Both Russia and China use information to support their countries' missions. NATO must be prepared to respond to information warfare in all domains, including the maritime environment.

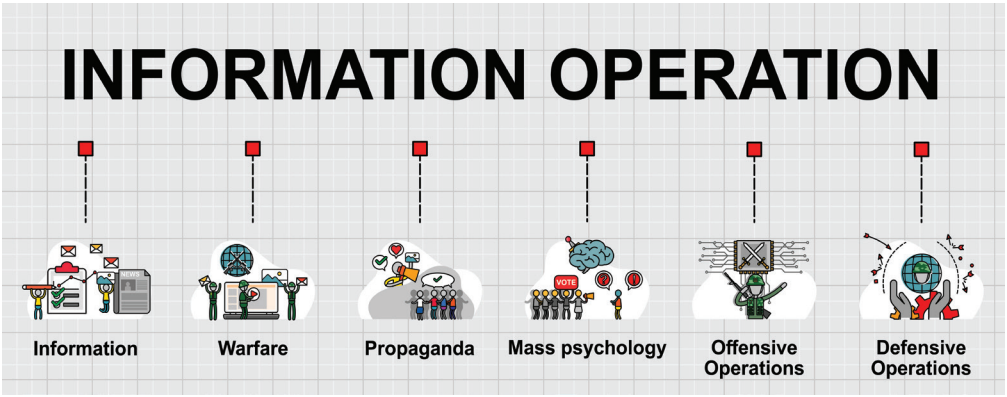
NATO's MIW

Expert collaboration when dealing with vast amounts of information is necessary for its effective conversion to military power. Achieving this operational advantage requires intelligence, information, knowledge about adversaries and their environments, as well as the ability to command and control forces. The US Joint Maritime Operations Publication (JP 3-32) describes maritime operations as any action performed by maritime forces to gain or exploit command of the sea, sea control, and sea denial, or to project power from the sea.[9] Tasked forces can only conduct efficient maritime operations by gaining warfare superiority of the information environment. The effective use of information is vital to achieving an operational advantage across the maritime battlespace.

Management of the information environment is conducted within the MIW domain and is organized around assured command and control, battlespace awareness, and integrated joint operations. It is a term aligned with MIW's pillars and includes the physical, virtual, and cognitive domains. MIW is not a process or a collection of information systems and cannot be managed by a single specialty group. Managing the information environment as part of maritime warfare requires expertise from key specialties to ensure the availability of adequate information to effectively carry out operations.

Courtesy of Shutterstock.

Managing MIW collective can be a complicated task. Specialists who are considered part of MIW include officers and enlisted members across several departments and specialties. These information specialists and their management structure add to the complexity in which a command uses this domain. The complexity is unintentionally created by an individual specialist's typical chain of command structure. An operator may have many supervisors, instead of just one, and will need to navigate several different departments to obtain all the information needed for their task at hand. As a result, a person seeking information may face challenges created by this scenario. Cases involving large staffs afloat and ashore benefit from the assignment of a single trained leader who is highly experienced in information warfare. A senior commander familiar with MIW will efficiently navigate the information domain and staff structure to create effective steps towards mission success.



The Way Forward for NATO MIW

Effective operators, systems, and apt use of information are key to warfighting superiority. The IWC initiative is the way forward for NATO maritime warfare.

Information has been used in warfare since the beginning of armed conflicts. The designation of a senior leader to understand, collect, manage, and disseminate vital information to senior decision-makers has had some recent use in the maritime domain. In 2019, the USN deployed its first IWC to a Carrier Strike Group (CSG), adding the new position to supplement the Air and Missile Defense, Strike Warfare, Surface Warfare, and Undersea Warfare Commanders under the CSG commander.[10] Vice Admiral Aeschbach, as Commander Navy Information Forces stated that the initial feedback that she received on the IWC initiative was positive and that information warfare leadership initiatives were being explored for the submarine community.

As an example of a functioning IWC structure, the USN's IWC was created to support and be part of the Composite Warfare Commander's (CWC) structure. The U.S. Chief of Naval Operations website describes that within the CWC concept, the IWC is responsible for integrating the various elements and activities of information operations, including electronic warfare, into naval and joint operations. Finally, the IWC is responsible for assessing and shaping the information environment, achieving and maintaining information superiority, and developing and executing information operations plans in support of CWC objectives while supporting other warfare commanders.[11] The U.S. model of the IWC has had successful outcomes and can be considered a reference for a NATO MIW Commander organization.

What Does IWC Look Like in MIW?

NATO's MIW commander organization can function in a similar way to the U.S.-initiated model. The notional IWC area of responsibilities (Table 1) can explain the functional relationships to the CSG missions and how the organization may function. An IWC's authority and scope of responsibilities fall within the three areas listed in the table below and should be understood to support the various information warfare staff organization requirements.

In this structure, the IWC is responsible to the CWC/Officer in Tactical Command (OTC) to create effects and operationally desirable conditions that influence

Battlespace Awareness	Assured Command and Control (C2)	Integrated Joint Operations
Intelligence Collection and Management through IPOE (Intelligence Preparation of the Operational Environment)	Communications	Electronic Manoeuvre
	Network Operations	Electronic Warfare
Oceanography	Spectrum Management	Information Operations
Meteorology	Cyberspace Operations	Space Operations
	Tactical Data Systems	Targeting

Table 1 Notional IWC Area of Responsibilities

the adversary's decision-making. These key areas of responsibility can be tailored to fit an IWC into a small, medium, or large task group.

In a small task group construct (destroyer and frigate sizes), the IWC would be led by a navy OF-2 or OF-3. In a small group, a communications division to include Cyber and Electronic Warfare with supporting personnel would report to the senior lead officer and would provide information warfare effects, limited in scope due to capacity.

In a medium group with three to six units, the IWC would be led by an OF-3 or OF-4. This staff construct would manage the same responsibilities supported in the small group plus the addition of an Intelligence, Meteorology and Oceanography Officer, spectrum manager, and additional watch stations and associated personnel. Military public affairs would also provide support in an indirect reporting structure.

In a large group, including a CSG, the senior officer should be an OF-4 or OF-5, depending on the size of the force and mission requirements. This senior officer works with and supports the other warfare commanders in the group, will be familiar with information warfare, and will be capable of effective management of the maritime information domain. The required functions of MIW tasks to meet the OTC's desired effects are defined in NATO ATPs. The staff size increases to provide capability in a high-intensity, multi-threat scenario.

The responsibilities and functions of the IWC are numerous and a Strike Group Commander would benefit from having a single officer responsible for the many associated tasks. The U.S. IWC model provides some insight into the advantages of this initiative while taking note of other considerations that would need to be addressed to ensure success. The model requires a senior leader; one with the necessary expertise may take some time to effectively progress from a junior to senior officer. This necessary development time means smaller nations may not have available personnel resources to produce officers who are fully qualified to assume the vast responsibilities associated with serving in this role. The assignment of highly capable individuals and successful IWC implementation will ensure that those do who fill this role will become deserving of the same respect as other warfare commander positions and be seen as critical members needed for military success.

Conclusion

The amount of information provided to a warfighting commander is vast, growing in demand, and comes from multiple sources at variable frequencies. Ukraine and Russia are current examples of nations using forms of information warfare to influence the battlefield and global opinion. Information warfare is not a new phenomenon, yet its modern form contains innovative elements as a result of technological development, which results in information being disseminated faster and on a larger scale.[12] The importance of integrating and incorporating the various tasks and responsibilities required to conduct successful information warfare tactics has been proven. The USN has successfully codified these duties into a warfare commander, the IWC. This model has been trialed, evaluated and verified by the U.S. as the best information warfare decision space for today's maritime commander.[13] All Allied nations can employ the model, as an IWC is scalable to fit all task groups. NATO has recognized this need, creating the roadmap to effective MIW in governing ATPs. The management and utilization of MIW can be complicated, but commanders can now rely on an IWC to provide information synthesis to increase their overall situational awareness and warfighting capabilities. The time for nations to prepare and implement these crucial assets is now.

Endnotes

1 "Information Warfare - Center for Information Warfare and Innovation - Naval Postgraduate School," n.d., https://nps.edu/web/ciwi/info-warfare.

2 "Information." In The Merriam-Webster.Com Dictionary, February 6, 2023. https://www.merriam-webster.com/dictionary/information.

3 Statista. "Amount of Data Created, Consumed, and Stored 2010-2020, with Forecasts to 2025," September 8, 2022. https://www.statista.com/statistics/871513/worldwide-data-created/.

4 Mehta, Aaron. "Space Force May Hire Companies to Service Orbiting Satellites." Defense News, August 19, 2022. https://www.defensenews.com/pentagon/2017/04/06/pentagon-tech-advisers-target-how-the-military-digests-data/.

5 Eckstein, Megan. "Navy Doesn't Want to Keep Guessing Whether Its Information Warfare Systems Work." Defense News. Defense News, August 18, 2022. https://www.defensenews.com/naval/2022/02/18/navy-doesnt-want-to-keep-guessing-whether-its-information-warfare-systems-work/.

6 Pomerleau, Mark. "Navy Creates Information Warfighting Development Center." C4ISRNet, August 19, 2022. https://www.c4isrnet.com/show-reporter/afcea-west/2019/02/15/navy-looks-to-expand-the-reach-of-its-information-warfare-teams/?contentQuery={"section":"/home","exclude":"/show-reporter/afcea-.west%22%2C%22from%22%3A285%2C%22size%22%3A10%7D&contentFeatureId=fofmoahPVC2AbfL-2-1-8

7 Specia, Megan. "How Ukrainians Are Using Social Media to Stir Resistance." The New York Times, April 5, 2022. https://www.nytimes.com/2022/03/25/world/europe/ukraine-war-social-media.html.

8 "Russian Information Warfare: A Conversation With Dr. Bilyana Lilly." Bilyana Lilly, October 17, 2022. http://www.carnegieendowment.org/2022/10/17/russian-information-warfare-conversation-with-dr.-bilyana-lilly-event-7957.

9 "Joint Publication 3-32," September 20, 2021. Accessed February 23, 2023.

10 Eckstein, Megan. "Space Force May Hire Companies to Service Orbiting Satellites." Defense News, August 19, 2022. https://www.defensenews.com/naval/2022/02/18/navy-doesnt-want-to-keep-guessing-whether-its-information-warfare-systems-work/.

11 Braswell, Bryan. "Evolving the Information Warfare Commander," September 2017. Accessed February 23, 2023. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=9422.

12 Defence Education Enhancement Programme (DEEP). "MEDIA-(DIS) INFORMATION - SECURITY INFORMATION WARFARE," n.d.

13 Shelbourne, Mallory. "Navy to Experiment with Information Warfare Commanders Operating from Maritime Operations Centers." USNI News, April 22, 2021. https://news.usni.org/2021/04/22/navy-to-experiment-with-information-warfare-commanders-operating-from-maritime-operations-centers.

A Saildrone Explorer unmanned surface vessel and the guided-missile destroyer USS Black operate in the Arabian Gulf. Courtesy of US Navy.

Manned-Unmanned Teaming in Joint Operations: A Command & Control Perspective

LtCol (ITA-AF) Roberto Patti

Introduction

Today, NATO faces the most complex security environment since the end of the Cold War. The unprovoked invasion of Ukraine by the Russian Federation has forced western nations to reconsider their understanding of the current geostrategic balance. The overtly aggressive behaviour of Russia will inevitably drive a change in NATO's posture and priorities, while the Alliance continues to address enduring challenges from cyber, hybrid, and international terrorism threats. At the same time, China is shifting the global balance of power and continues to represent a strategic conundrum that challenges western nations' ideas of security, values, and way of life.

Senior military leaders envision future operational scenarios where Allied forces operate in highly contested, communications-degraded environments with integrated air defences, hypersonic weapons, and low observability technologies. Unmanned systems will play a key role in any future confrontation, and they are "one of the service's top development priorities"[1] according to United States' Navy's (USN) Chief of Naval Operations. Future confrontations will require a much more capable and faster decision cycle than what is possible with today's Command and Control (C2) architectures.[2] The United States' Department of Defense (DOD) has made the case that, in the near future, military operations may require decisions to be made in substantially shorter timeframes than the current standard,[3] sounding the alarm that existing C2 systems may be insufficient for future multi-domain operations. Similarly, the global defence industry expects that future weapons systems will operate connected to a 'combat cloud,' capable of connecting any platform sharing Intelligence, Surveillance and Reconnaissance data (ISR) with any weapons system, regardless of domain. In this vision, any platform can 'see' or 'shoot' well beyond its own limitations. The large mass of data required would be processed at computer speed, using artificial intelligence (AI) and machine learning algorithms to identify targets, recommend the optimal response (often what weapon to use), and recommend the ideal 'shooter.' The next major trend in the evolution of weapons systems, as exemplified by the air domain, will push toward interconnection and the ability to receive, process, and disseminate data. In fact, air forces and the aerospace industry are well invested in pushing the next generation of fighter aircraft in a new direction. The 'sixth generation' of fighter aircraft is expected to be stealthier, more "connected", and generally more capable of acquiring and sharing information than its predecessors, marking a substantial departure from previous iterations of weapon systems.

Today's Allied militaries are fielding unmanned systems in increasing numbers and enhancing the interconnectivity between manned and unmanned portions of the force.[4] Historically, unmanned systems have been regarded as means to replace manned assets for missions deemed too "dull, dirty or dangerous" for human crews or as a way to divest of larger, more expensive platforms. Today, unmanned systems can be deployed

to augment manned platforms, providing added capacity to the force, like the USN's MQ-25 Stingray. Manned-Unmanned Teaming (MUMT) concepts represent a key step to leveraging unmanned systems as true multipliers that enable an unprecedented capability leap for NATO.[5]

The MUMT construct will address a near future where unmanned systems will be deployed as autonomous or semi-autonomous extensions of manned platforms. In this construct, unmanned systems will provide additional sensors and weapons to areas previously unreachable by manned crews. Unmanned systems will also be capable of executing tasks which would pose unacceptable risks to manned systems. In this not-so-distant future, the combined used of manned and unmanned weapons systems will produce effects far greater than the sum of the single contributions, while reducing risks to human crews.

The case for a new C2 architecture

The Russian invasion of Ukraine has provided an unfortunate real-world manifestation of what NATO has been anticipating in recent years. While analysts sounded the alarm on the need to quickly re-shift the Alliance's focus on peer or near-peer adversaries and great power competition, NATO's adversaries worked relentlessly at devising innovative asymmetric challenges to the standing world order. By harnessing military, economic, diplomatic, and informational tools, Russia and China have challenged western democracies' abilities to ensure the stability of the global commons that has endured since the end of WWII.

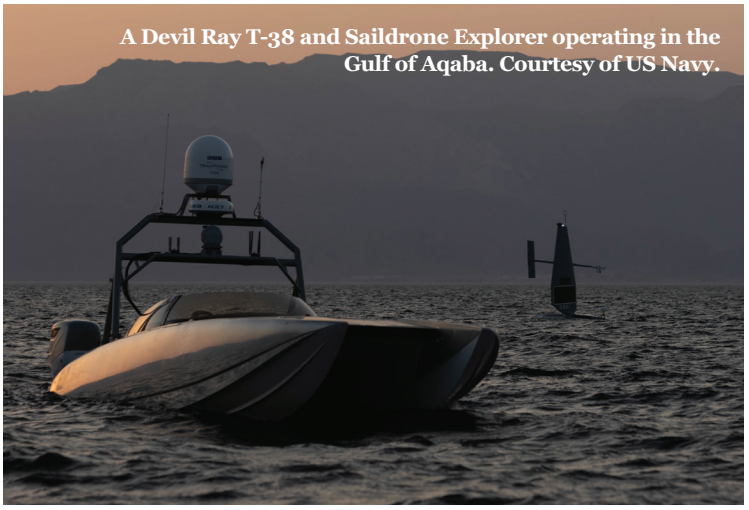
The 2018 US National Defense Strategy (NDS) Commission unequivocally stated that many of the skills necessary to counter capable adversaries "have atrophied," and the requisite C2 skills "have deteriorated."[6] The Commission's analysis suggested the need for creative responses to counter adversaries' unconventional approaches. The NDS Commission's report addressed the skills of the nation's current conventional force, which is arguably less complex than the manned and unmanned network of sensor and weapon platforms of the future military. C2 of a *"military internet of things"* for the battlespace will entirely depend on speed and the ability to handle massive data rates. The nature of this expected evolution and the pace at which it is happening raises serious questions about the suitability of existing C2 systems and processes. Analysts are starting to predict that technology and warfare evolution will render them dangerously obsolete and inadequate for the task.

> ***In the coming years, NATO forces will be shaped by… increased integration of unmanned systems into the conventionally manned force.***

Communications

In the manned-unmanned paradigm, reliance on long-range communications for planning, execution, or assessment of military operations will become an increasingly difficult challenge. Analysts predicted as early as 2008 that total demand for SATCOM bandwidth would double over the years (from 40 Gbps in 2020 to 80 Gbps in 2022), reaching almost twice as much as the projected capability available, leaving a significant supply and demand gap.[7] Moreover, new generations of autonomous unmanned systems will require short latency and secure communications in addition to increased capacity to ensure proper control.[8] The days of NATO's reliance on traditional SATCOM (both military and commercial) seem to be approaching an end as nations acknowledge its vulnerabilities. NATO's adversaries have developed and tested technologies capable of disrupting Allied satellite capabilities by electromagnetic interference, direct hit, or orbit alteration.

Traditional satellite communications rely on satellites in geosynchronous orbit roughly 36000Km above the equator. These satellites move at the speed of the earth's rotation and offer the best geographical coverage with the smallest constellation (fig. 1). Because of their stationary position relative to the earth's surface, their high altitude makes them ideal platforms for broadcasting. However, geosynchronous satellites have limitations in support of military operations. In addition to being vulnerable to direct attack, they can suffer damage from periodic geomagnetic storms. Their signals can degrade due to obstacle interference, and they are not reliable outside of a 65° latitude window across the equator. This means, for example, that a sizeable portion of Norway is practically outside SATCOM coverage[9] because of latitude and/or terrain.



A Devil Ray T-38 and Saildrone Explorer operating in the Gulf of Aqaba. Courtesy of US Navy.

Possibly the greatest disadvantage of the current SATCOM architecture for manned-unmanned teaming is latency. All variables being equal, the time a signal takes to travel to and from a higher satellite (such as a geostationary satellite) is necessarily longer than it takes to reach a lower satellite, which means a time delay that threatens to be incompatible with the next generation of highly automated/autonomous unmanned systems.[10]

In recent years, Low Earth Orbit (LEO) satellite constellations have promised to improve latency and throughput, sparking a "commercial space race" that has the potential to rival or possibly exceed the fastest ground-based networks. In 2019, a London-based company backed by Richard Branson, OneWeb, recorded an average latency of 32ms on transmissions to space from South Korea. Elon Musk's Space Exploration Technologies Corporation is aiming for a latency of 20ms and plans to eventually reduce latency to just 10ms. When compared to the median latency related to high-orbit satellites (~600ms[11]), it becomes immediately clear how this could represent the next technological breakthrough in this field.

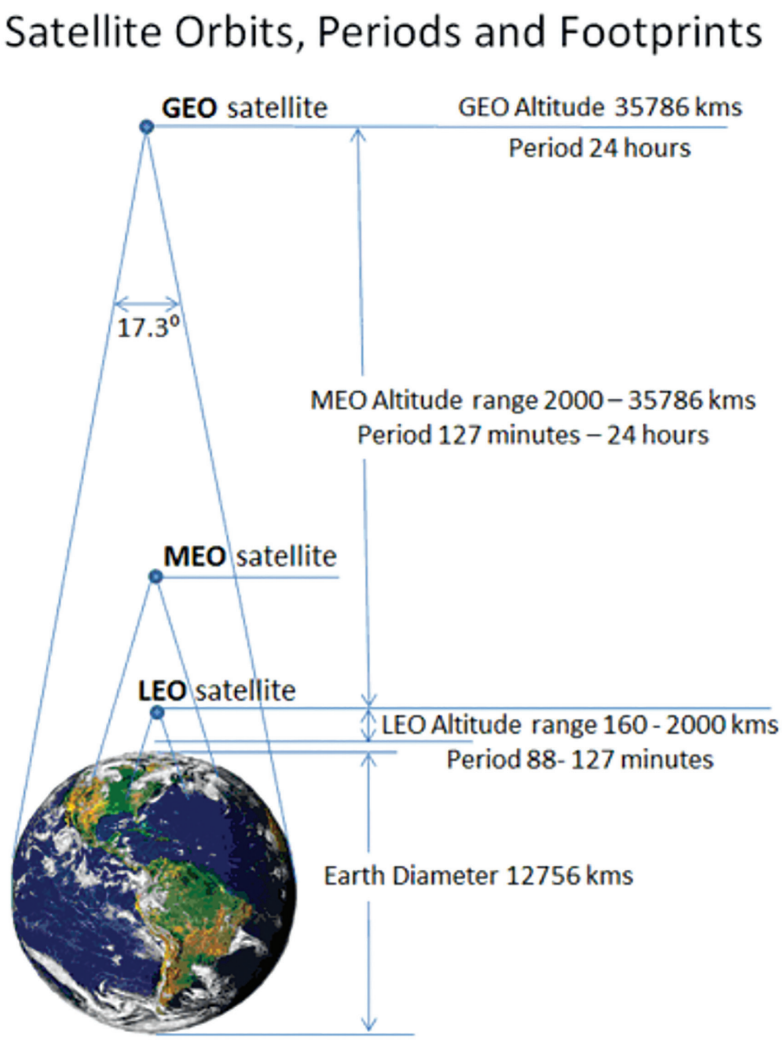


Figure 1 - Satellite orbits, periods and footprints (Electropaedia)

There are, however, still many challenges to overcome before these technological breakthroughs become a reality. For one, LEO satellites are in contact with ground transmitters only for a relatively brief period of time, which requires a large number of satellites in orbit in order to maintain constant communications. More satellites also mean more ground equipment required for support.[12] In terms of military operations, more satellites and more ground stations simply means increased vulnerability,[13] but it also means a higher probability of collisions between objects. Satellite collisions are especially dangerous because of the cascading likelihood of further collisions, a phenomenon known as the *Kessler syndrome*.[14]

Autonomy in C2

Although frequently used interchangeably, autonomy and automation are not synonymous, each describing very different behaviours to which machines are bound. In a growing level of sophistication, machines (either robots or computers) can have automatic, automated, or autonomous behaviours, depending on the relative intelligence of their internal cognitive processes.[15] Where automated systems are governed by a set of prescriptive rules and algorithms from which they cannot deviate, autonomous systems are meant to understand and interpret their operating environment, ultimately deciding on the best course of action based on the actual situation. This results in a more fluid, less predictable behaviour relative to a given baseline. Researchers often refer to autonomous systems as being "goal-oriented"[16] (fig. 2).

'Autonomous' generally applies to a broad spectrum of machines powered by artificial intelligence, from computers to ships to airplanes. Future military C2 of autonomous systems will depend on AI, machine learning, and deep learning.[17] NATO is facing a future where new technologies and hypersonic weapons will impose a much higher-paced rhythm than today, possibly exceeding the limits of human cognition. Future confrontations may require decisions to be made "within hours, minutes, or potentially seconds" compared with some of the current multiday processes used to analyse the operating environment and issue commands.[18] Although human oversight remains an essential element of military operational decision making, defense ministries are facing the reality that humans are inherently slower than machines. As such, people represent a tangible constraint to the speed of the OODA loop[19] in fast-paced battle rhythms. The only way to achieve the C2 speed required for an increasingly automated force is to rely on a new

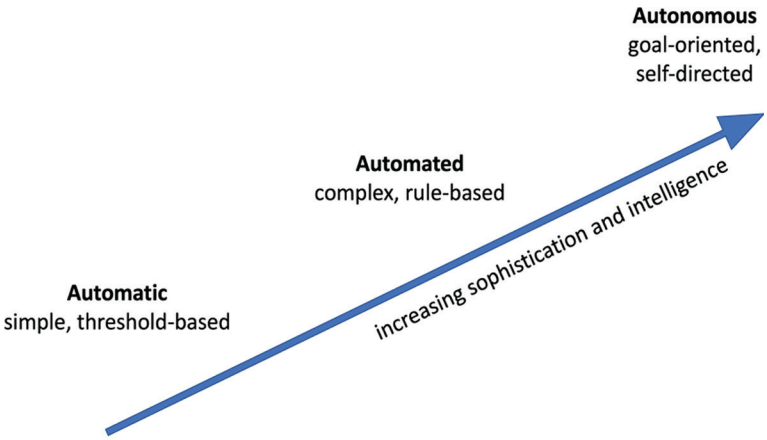


Figure 2 - Spectrum of intelligence in machines

generation of networked AI-enabled computers that can replace humans in most tasks along the decision chain.

In military operations, the development of autonomy has historically been met with scepticism. Critics are concerned about the ethical viability of choices made by a machine that is intrinsically devoid of 'judgement' and has no conscience. Automated lethal weapon systems raise the most concern, where accountability must be established and decisions must be the product of the human qualities of "originality, responsibility, and empathy."[20] Trust is the crucial element of automated decision-making and, given the current shortcomings of ethical reasoning in AI, it is generally understood that autonomous systems will continue to be used only under close human supervision ("human in-the-loop" or "on-the-loop[21]"). Due to the broad range of scenarios that militaries face in the battlespace, it will take decades before AI reaches the necessary level of maturity to substitute humans in decision-making. However, efforts are already in motion to implement autonomy wherever it can supplement the human element in the decision cycle.

Conclusions

Today, unmanned systems represent a constantly growing element of the joint force. As unmanned systems are deployed in increasing numbers, the need for greater interconnection with manned systems becomes an undeniable reality. In the coming years, NATO forces will be shaped by advances in technology and increased integration of unmanned systems into the conventionally manned force. Allies need to holistically rethink their approach to C2 to maintain relevance in the fast-changing world of automated decision making. To secure the competitive edge, the development of an interoperable Joint Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) architecture will be critical to support the needs of future multi-domain, hyper-connected warfare. By furthering unmanned systems implementation and multi-domain integration, Allied militaries will capture the upper hand against any adversary.

Endnotes

1 https://news.usni.org/2020/11/11/cno-gilday-ready-to-act-on-parts-of-future-fleet-plan-as-long-as-it-doesnt-hurt-readiness

2 Joint All-Domain Command and Control (JADC2), Congressional Research Service, United States, 2020

3 "Future conflicts may require decisions to be made within hours, minutes, or potentially seconds compared with the current multiday process to analyze the operating environment and issue commands." Joint All-Domain Command and Control (JADC2), Congressional Research Service, United States, 2020

4 Manned-Unmanned Teaming in Joint Operations, CJOS COE, 2021

5 For example, the U.S. Navy's Distributed Maritime Operations (DMO) concept

6 Gary Roughead, Eric Edelman, et al., Providing for the Common Defense, National Defense Strategy Commission, The Assessment and Recommendations of the National Defense Strategy Commission, United States, 2018, pg. 24. https://www.usip.org/sites/default/files/2018-11/providing-for-the-common-defense.pdf

7 Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army, United States, 2017

8 Navy Large Unmanned Surface and Undersea Vehicles: Background and Issues for Congress, Congressional Research Service, United States, 2022

9 At this latitude, even an object 50 meters away and only 15 meters high would obstruct the satellite signal (Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army, United States, 2017)

10 Joint All-Domain Command and Control (JADC2), Congressional Research Service, United States, 2020

11 https://www.washingtonpost.com/business/why-low-earth-orbit-satellites-are-the-new-space-race/2020/07/10/51ef1ff8-c2bb-11ea-8908-68a2b9eae9e0_story.html

12 ibid. In a constellation such as OneWeb's receivers are able to get a consistent signal because a new satellite will fly into range and pre-emptively replace the signal of the satellite which is about to fly beyond the horizon about every 2 minutes.

13 for a more comprehensive threat analysis, see NATO Satcom Threat Assessment, CJOS COE, 2021.

14 ibid. The Kessler syndrome also known as the Kessler Effect is a scenario proposed by NASA Scientist Donald Kessler in 1978

15 Army of None, Paul Sharre, United States, 2018

16 ibid.

17 Machine learning and deep learning are two separate subsets of artificial intelligence: machine learning is typically associated with algorithms that, given an initial set of structured data, can change themselves and evolve without human intervention to achieve a given result; deep learning is a subset of machine learning where algorithms are created and function in a similar way, but they are built to form several overlapping layers (similar to how the human brain functions and therefore called artificial neural networks), each providing a different interpretation of the data it conveys.

18 Defense Primer: What Is Command and Control? Congressional Research Service, United States, 2021

19 The OODA loop is the cycle observe–orient–decide–act, developed by military strategist and United States Air Force Colonel John Boyd in the 1950's.

20 Joint Operations with Unmanned Aircraft Systems (UAS) and their Future Development, CJOS COE, 2020

21 When referencing Human-Machine Interface (HMI) control levels, various options can be defined according to the role assigned to the human operator: "human off-the-loop" means the machine operates autonomously, without any form of human control over it; "human in-the-loop" means the machine responds to direct inputs from a human operator for guidance or payload operation; "human on-the-loop" means the machine navigates and operates autonomously, but a human operator supervises the mission and can interact with it or intervene, if needed. (Source: US DoD's Unmanned Systems Integrated Roadmap FY2017-2042, 2017)

AI is Here: NATO's AI Arms Race

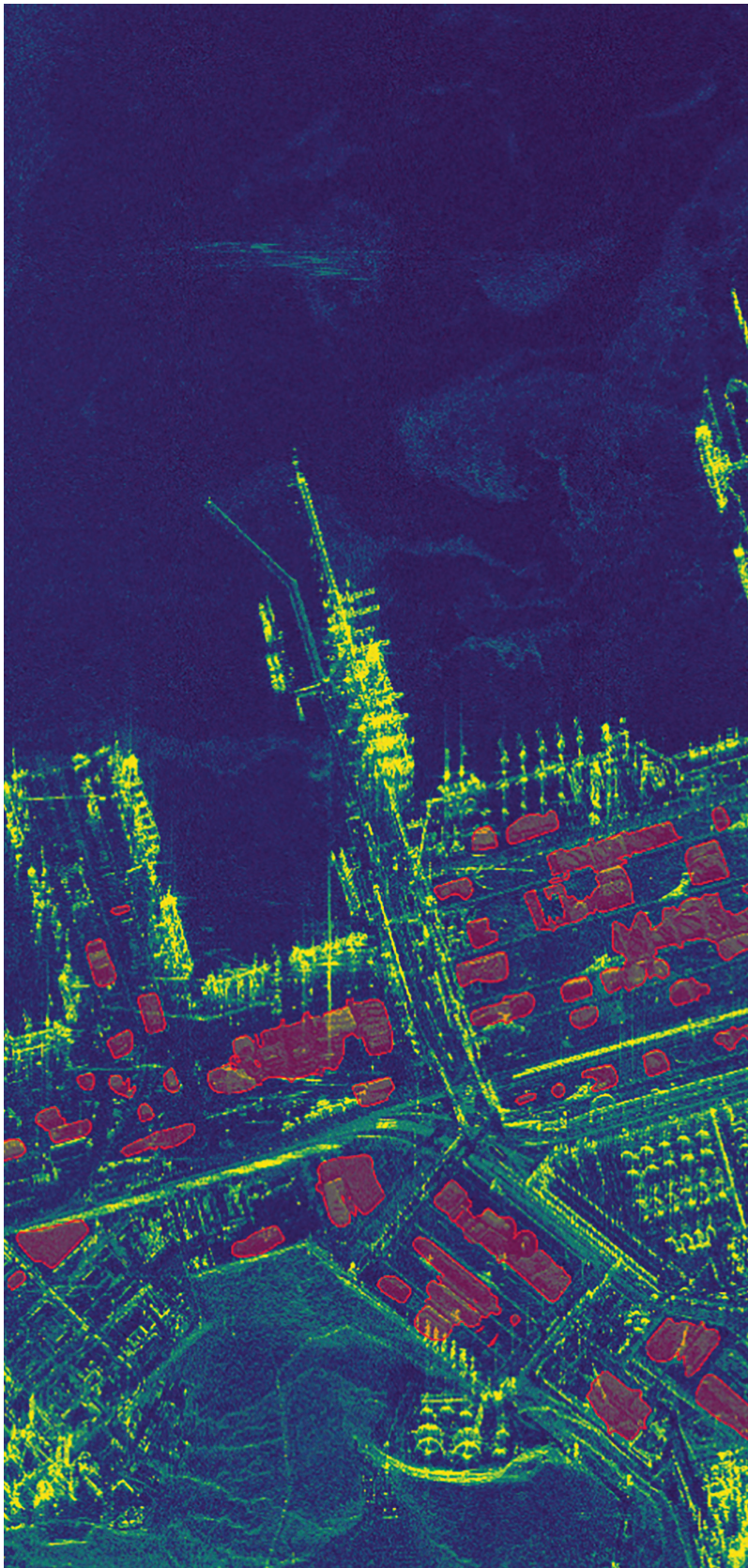
CDR (USN) Nathaniel "Than" Hathaway

Listening to a podcast recently, I was surprised to hear Elon Musk and Socrates discussing a variety of thought provoking topics including free speech, democracy, and artificial intelligence (AI). The conversation went something like this:

> *Socrates: Do you think that the risks of artificial intelligence are worth taking given the potential benefits?*
> *Elon: Yes. There are a few reasons: first we need to take risks in order to progress as a species. Second, the potential benefits of artificial intelligence are so great that they outweigh the risks. Third, we can take steps to mitigate the risks of artificial intelligence such as by regulating its development and use.*
> *Socrates: So we agree that the risks of artificial intelligence are worth taking given the potential benefits. What should most people do?*
> *Elon: I think people should be very proactive in learning about artificial intelligence and its implications. They should also keep up with the latest developments in the field so they can make informed decisions about its use in their own lives.*[1]

This discourse between the ancient Greek philosopher and the present day businessman/futurist produced some truly insightful dialogue, including some points that are relevant for NATO today. But it transpires that this conversation wasn't the creative work of a skilled writer who had spent years understanding the nuances of Socrates' philosophy and Elon Musk's views on technological innovation. Rather, the entire transcript was the product of a state of the art generative AI, capable of creating high quality text and graphics from simple prompts in a matter of seconds.

Commonplace applications of AI are now ubiquitous, such as using Face ID to unlock your phone, but it is still much less common to walk onto a military operational watch floor and point to a sailor or marine using AI in the course of their daily duties. So, if AI is no longer a technology strictly relegated to far future concept development and esoteric debates amongst science fiction writers, how can we make sure that current technologies are carefully evaluated and incorporated immediately? How can focused policies and guidelines for industry-wide applications, including operational plans and resourcing decisions,



"AI will fundamentally change our way of life and… the nature of warfare in the 21st century."

Stockpiles seen and measured from very high resolution SAR imaging, at the port of Bayuquan, China. Courtesy of ICEYE.

Concept image of AI-enhanced Joint All Domain Command and Control (JADC2). Courtesy of US Army.

be developed? As Michael Kanaan states in his book, *T Minus AI:* "The countdown to AI is over."[2] It is a technology that will fundamentally change our way of life and, more specifically, the nature of warfare in the 21st century.

NATO faces a number of challenges in the race to harness the power of AI as a means to deter its adversaries, defend the territorial integrity of its members, and in turn help ensure global stability. Indeed, artificial intelligence and machine learning present a host of promising new opportunities, but there are also a number of key issues that need to be addressed if we are to compete and win in a responsible and ethical manner that supports democratic values. NATO and its allies are at the beginning stages of a global AI arms race that will fundamentally shape the future for decades, especially the highly contested strategic competition between China and the West.

AI Development is Moving FAST

Arguably, last year was a turning point for the real world implementation of defense-focused AI technology. Following Russia's brutal and unprovoked invasion of Ukraine on the 24th of February 2022, a number of technologies have rapidly made the transition from commercial offering to military capability on the battlefield in eastern Europe, providing critical defense capabilities and asymmetric technological advantages to the Ukrainian military. For example, both Capella Space and Finnish startup ICEYE have used their machine learning, space-based synthetic aperture radar (SAR) capabilities to detect Russian unit movements during the invasion, providing Ukrainian forces with access to timely, relevant, and actionable information.[3,4] Additionally, in March of 2022, Hawkeye 360's satellite clusters collected huge swaths of radio frequency data over Ukraine and leveraged AI and machine learning technologies to reveal extensive GPS interference activity throughout the region.[5]

Although smaller startup technology companies such as these have been able to rapidly field their systems in support of Ukraine, larger defense companies have also been busy investing billions of dollars in the development of high-end AI enabled capabilities for future defense acquisition. In November 2022, Lockheed Martin successfully demonstrated a vertical lift resupply mission with its Autonomous Black Hawk capability,[6] and Kratos Defense completed a successful test flight of its XQ-58 Valkyrie production model unmanned high performance tactical aircraft.[7] This is a crowded field, with Raytheon, General Dynamics, Leonardo, and Palantir also investing heavily in AI enabled capabilities that promise to revolutionize the modern battlefield, although some capabilities are still years away from operational fielding.

However, it's not all plain AI sailing. With a host of ambitious AI startup companies entering the market alongside significant investments by the biggest defense primes, the rate of AI technology development risks

outpacing policymakers' abilities to reorganize around this fast-moving, emerging disruptive technology. NATO and national polices appropriately started at the broadest level possible, but principles alone lack the compelling force of detailed plans for investment, tradeoffs, and implementation.

NATO and National Policies Address the Strategic Importance of AI Development and Responsible Use

New technologies and new capabilities inevitably come along with a bow wave of excitement and energy in the defence sector, as industry rushes in to propose a multitude of potential applications. But, that 'bow wave' of excitement has to be accompanied by the right policies and guidance if the accompanying risks are to be mitigated, and strategic advantage not ceded to adversaries.

In 2018, the US took the lead amongst NATO nations in this arena by issuing its first DOD Artificial Intelligence Strategy, directing the Department to "accelerate the adoption of AI and the creation of a force fit for our time."[8] As the first of its kind in the US, the Strategy recognized the competitive investments that China and Russia were making in the development of AI, and the fact that their military applications of the technology could "raise questions regarding international norms and human rights."[9] The Strategy also established a broad approach, with a "human-centered" emphasis around the following five areas:

- Delivering AI-enabled capabilities that address key missions.
- Scaling AI's impact across DoD through a common foundation that enables decentralized development and experimentation.
- Cultivating a leading AI workforce.
- Engaging with commercial, academic, and international allies and partners. Leading in military ethics and AI safety.[10]

Overall, the 2018 US Strategy was an important and necessary first step that established a foundation for the Defense development of AI. That said, time will tell whether it has managed to generate enough momentum to maintain an advantage compared to the massive investments being made by China since that time.

To complement the 2018 Strategy, the US Defense Innovation Board proposed a set of ethical AI principles in 2020 that focused on enabling the US and its Allies to "prevail on future battlefields and safeguard the rules-based international order" while maintaining "America's steadfast commitment to responsible and lawful behavior."[11] The proposal, which was adopted by then US Secretary of Defense Dr. Mark T. Esper, set five major focus areas for ethical AI development: responsibility, equitability, traceability, reliability, and governability.[12] Ethical guidelines for AI are especially important in the development of a new technology that has the potential to undermine human rights and the right to individual representation, not least because these values are at the heart of the divide between the democratic nations of the world and autocratic governments who would seek to exploit such an opportunity to further consolidate and strengthen their control.

Although the US was one of the first Western democracies to adopt a national defense strategy for AI, it is just one of many Allied nations racing to apply a strategy to this emerging technology. In October of 2021, just months before the Russian invasion of Ukraine, NATO adopted its own AI strategy. It noted that AI "will pose a broad set of international security challenges affecting both traditional military capabilities and the realm of hybrid threats" and that it will "have an impact on all of NATO's core tasks of collective defence, crisis management, and cooperative security."[13] NATO's AI strategy focuses on accelerating the adoption of AI through key enablers, including policy and its 'Principles of Responsible Use for AI'.[14] The Alliance's principles essentially mirror those of the 2018 US DOD AI Strategy with the addition of the principle of 'Lawfulness', which emphasizes adherence to international humanitarian law and human rights law.

Most recently, Allied Heads of State adopted the 'NATO 2022 Strategic Concept' at the NATO Summit in Madrid on 29 June, 2022. Although AI is not mentioned specifically in the document, the concept addresses NATO's digital transformation effort, saying that NATO will "increase our investments in emerging and disruptive technologies to retain our...military edge."[15] Echoing sentiment from the 2021 NATO AI Strategy, the concept states that NATO is committed to "principles of responsible use that reflect our democratic values and human rights."[16] Although the concept promises increased resources, it remains to be seen how it will be implemented and, more importantly, whether any of those resources will be applied specifically to AI development.

NATO and national AI strategies describe strategic environments in which technological superiority directly impacts battlefield success, but new disruptive technologies also bring along significant risks that must be dealt with.[17]

Emerging Technology Comes with Emerging Challenges

Since March of 2022, NATO has stood on the western flank of a very modern European conflict, supporting Ukraine's battle for national sovereignty in the face of wholly unjustifiable Russian aggression. With AI technology being employed on the battlefield in its own backyard, NATO faces the challenge of simultaneously ushering in a new capability across

the entire Alliance, implementing safeguards, and maintaining a technological advantage set against the backdrop of a conflict that is still unfolding.

Safety

One of the most important and perhaps most difficult issues in the development of AI is that of safety. As AI systems continue to develop, AI designers are quickly finding themselves in the position of having created systems that can outthink their designers. With AIs that now train on systems with over a trillion parameters,[18] the challenge of designing capabilities that achieve desired outcomes is a complex problem fraught with near limitless potential for unintended consequences. For example, without timely updates and the right situational awareness, a self-driving car asked to find the quickest route to a destination may plot a route through a construction zone that endangers bystanders and passengers alike. In defense applications, the challenge of safety is magnified by the dangers of the operational environment, the complexity of the platforms involved, and mission objectives that can be destructive in nature - the very fog of war.

As with many emerging technologies, the majority of work in the early years of the birth of AI has focused on expanding capabilities rather than developing safeguards. Indeed, according to McKinsey's 2022 state of AI report, the trend towards addressing safety issues in AI since 2019 has been relatively flat.[19] But, with AI technology quickly permeating real world battlespaces, the need for AI safeguards is becoming profoundly clear and accelerated development of these protections is required.

Trust

AI is a new technology that, in many applications, promises to give decision makers answers to complex questions in a fraction of the time imagined possible previously. But, AI is not unlike other new capabilities that must be proven in practice before earning the trust of those that employ it to deliver significant operational advantages. For example, the introduction of AI-powered automatic ground collision avoidance systems into the F-16 produced routine erroneous warnings, leading pilots to completely disable the proven life-saving technology during initial fielding and testing.[20] Similarly, AI will need to prove its reliability before it can be implicitly trusted to perform as needed, especially as a decision support tool.

AI technology has the potential to revolutionize the way military leaders make decisions, from the tactical level all the way to the strategic. Whether technologies are given fully autonomous decision making freedoms or stringent human in the loop constraints, a high standard of trust will need to be met before measurable advantages are realized. Consider the now legendary game of 'Go' between Lee Sedol and Deepmind's AlphaGo AI, in which the non-human player made a famously unexpected decision on move 37, in the second of the 5 game series.[21] It was a move that, at the time, would have been considered unwise for any competitive human Go player, but ultimately was fundamental to AlphaGo's success in the match. If an AI system suggested a similarly unconventional decision in a military operation today, leaders may not yet have the trust in the system needed to act without extensive and time consuming work to validate the recommendation. Until AI achieves an adequate level of reliability, a lack of trust will likely result in time-consuming checks and confidence building that may well erode any decisional advantage offered.

Bias

Recent AI development has resulted in some eye-watering accomplishments that demonstrate game-changing potential, but it has also revealed a notable shortcoming, namely' training bias'. Current systems employ a method of training called Machine Learning, which processes vast amounts of data and forms the knowledge base that the AI then uses as a basis to make decisions. Regardless of how comprehensive the training data set is, there will always be certain biases that exist that will ultimately affect decision making. For example, a training set that primarily relies on English-based data could form an AI bias toward Western democratic values and views, as compared to a data set that consists primarily of Mandarin-based data that might be prone to drive adoption a different philosophical perspective. With seven different types of bias possible in training data sets,[22] AI practitioners face the complex challenge of properly collecting, labelling, and implementing data to avoid bias. In some cases, AI learns patterns embedded in historical data and develops unwanted decision bias. In 2014, Amazon developed an AI based tool to automate the screening of resumes to support hiring decisions. Unfortunately, the training data set consisted of predominantly male resumes, leading the AI to unintentionally screen out female applicants.[23] Whatever the reason for the unwanted bias, it belies the greater challenge for developing AI that enables desired outcomes, while mitigating and reducing the impact of undesirable machine learning.

When it comes to bias, NATO has an especially difficult challenge. As an Alliance of 31 nations, it will face the challenge of incorporating training data from a vast array of different militaries, each with their own culture and their own idea of what constitutes a desirable outcome from AI. Current systems are designed to make judgment calls based on how they are trained, and not all nations train or make decisions in the same way.

Interoperability

Any student and reader of 'Bow Wave' will know how much importance we at CJOS place on the need

for the highest levels of interoperability and integration across the Alliance. In the world of AI though rather than attempt to incorporate Alliance-wide machine learning data sets at this early stage, allied nations are independently developing their own national AI systems that might later be shared with other allied nations. Sharing or selling military hardware between allied nations is an endeavor already slowed by bureaucracy and geopolitical hurdles, but sharing of AI systems is likely to be more difficult. AI systems are data based and the current state of information sharing in allied operations is uneven. The success of Alliance-wide AI that contributes to an integrated and coherent approach, with a minimum of seams and boundaries will depend on our ability to streamline releasability caveats and speed up foreign disclosure processes.

The AI Race is ON!

So, if we believe that AI will have transformational implications for the world, then logically NATO nations must lead in AI development to ensure that systems adhere to, and support the international rules-based order. Meanwhile, our adversaries have for years clearly demonstrated their lack of concern for human rights and international norms – Russia's recent egregious actions could not be a more blatant demonstration of this. Set against that background, it is reasonable to assume their approach to AI development will be no different. As a case in point, Vladimir Putin has publicly stated that he views AI as the key to ruling the world,[24] and he is clearly seeking to develop and exploit those capabilities to gain advantage and support his own objectives.[25] The Chinese Communist Party has already implemented AI as a means to monitor and manipulate its own people,[26] an unambiguous demonstration of their eagerness to employ the technology to achieve the goals of the government. The AI race is on - and challenges abound.

Keeping safety in mind will be a top challenge for NATO nations as they pursue new AI enabled capabilities, but others may not be so careful if they see an exploitable opportunity. While NATO nations will strive to ensure AI can discern between combatants and non-combatants, Russia will likely waste little time in this area based on its track record of indiscriminate attacks.

Trust in AI will remain an obstacle to NATO decision makers for many years, but assurances are a luxury that NATO's adversaries may not hold in high regard when it comes to fierce strategic competition. If an unproven AI system offers China the chance to claim Taiwan in the face of staunch opposition, will the issue of trust quickly take a back seat behind potential strategic success?

And while NATO and its allies are hard at work minimizing AI training biases to protect human rights, governments of adversary nations may choose to leverage these prejudices with the precise goal of exploiting populations that oppose their rule.

In the meantime, the geopolitical clock is ticking. With many high-end AI enabled weapon systems' development timelines stretching into the 2030s, a protracted war in Ukraine or conflict over Taiwan could prove to be a technological crucible for smaller, more

Shield-AI's V-bat utilizes AI for maritime ISR. Courtesy of US Navy.

quickly adapted systems on the battlefield. As such, AI could play a prominent role especially if it occurs in the near future.

AI technology is in its infancy, but there is no doubt that the technology will continue to grow rapidly in coming years. Like many other technological advances before it, AI has the potential to radically enhance modern civilization, while simultaneously threatening to cause irreparable harm if misused. With this technological 'genie' now out of the bottle, NATO and its allies have no choice but to move swiftly to lead the world in responsible AI development.

Now Get Moving, NATO!

If NATO plans to persevere in the AI arms race, the following are top priorities:

Accelerate detailed implementation efforts. In October of 2022, NATO established the Data and AI Review Board (DARB) to serve as a multinational forum leading NATO's efforts toward responsible AI adoption. The DARB can now move swiftly toward achieving its first task, establishing a responsible AI certification standard. The DARB should waste no time in establishing a governance structure that ensures AI technology is deployed in an equitable manner, so that all nations, regardless of size or economic power, can benefit from the advances in AI. As it works to operationalize all of NATO's Principles of Responsible Use, the DARB can champion early development of AI safety infrastructure, like Google I/O's AI Test Kitchen, to facilitate safe AI innovation as soon as possible.

Drive workforce AI education. Most people in today's workforce trust and rely on computer processing to handle a multitude of daily tasks, even though they might not understand how the technology works. In a similar way, AI looks set to become a part of daily routines for every future sailor and marine, not just coders and programmers. NATO can establish a strategy to enhance workforce knowledge, engender trust, and build interest in AI across the force now. Forums such as the DARB present a fantastic opportunity to be empowered advocates for AI education and familiarization, especially for senior decision makers who will likely see these enabled decision support tools in the very near future. NATO must focus on workforce AI education today to facilitate accession of tomorrow's AI talent; the opportunities are endless.

Accelerate investment in AI systems/capabilities. Alex Wang, CEO of Scale AI, points out that China's investment in AI has far outpaced that of its leading competitor, the US, with the PLA spending a 10x greater percentage of their annual defense budget on AI.[27] In actual funds applied to AI investment, the PLA spent almost $2.7B versus the US DOD's $1.3B over the same period.[28]

If AI opportunities are to be exploited, NATO nations will need to make significantly increased investments in AI as soon as possible. Efforts like the historic 1B Euro NATO Investment Fund (NIF) are noteworthy, but the NIF will be applied to early stage emerging technologies

An Operations Specialist stands watch in a shipboard Combat Information Center. Courtesy of US Navy.

across industry, not just AI. NATO is rich with talent and the Defense Innovation Accelerator for the North Atlantic (DIANA) effort is seeking to harness that power to accelerate delivery of innovative technology to the force. NATO has the opportunity to prioritize AI-focused grand challenges for DIANA's debut in the coming year, leaning heavily on the leadership of AI industry across the Alliance, and leveraging unique partnerships with organizations such as Bulgaria's AI-focused Gate Foundation.

Drive investment in AI infrastructure.
Data is the foundation upon which AI systems are built. To prevail against its greatest strategic challenges, NATO nations will need to build and maintain data supremacy. The defense ecosystem is full of data, but much of that data is either discarded or locked away behind layers of digital security that render it almost unusable. NATO must continue to harden its cyber defenses, while enabling secure mechanisms for the exchange of data. It is imperative that NATO nations move quickly to establish clean, organized, and secure data systems with the agility to support modern AI systems across trusted Alliance networks. NATO needs a "quantum leap" in secure data sharing – both in terms of the technology to protect it and in terms of the policy to enable it.

NATO's Sputnik Moment

When Deepmind's AlphaGo AI bested Lee Sedol in Go, China recognized a 'Sputnik moment' - quickly shifting priorities to pour extensive national resources into AI research.[29] China accelerated national AI research and, according to Stanford University's AI index report, China's percentage of citations in AI-related academic papers surpassed the US for the first time ever in 2020.[30]

In 2022, NATO experienced its own 'Sputnik moment' when Russian troops advanced into Ukraine and the Alliance witnessed a return to full scale conventional state on state conflict not seen on the European continent since World War II.

The importance, centrality and relevance of the Alliance has never been more clear. NATO now has the opportunity to take decisive action to exploit the advantages of AI technology and defend against Russian aggression, maintain the integrity of the Alliance, and ensure stability on the European continent and beyond. Let's get to work.

Endnotes

1 Omni, "AI CREATED Elon Musk and Socrates On Talk show," YouTube, November 21, 2022, https://www.youtube.com/watch?v=Y1HWqjCZv0g.
2 Kanaan, Michael, 1989-. T-minus AI: Humanity's Countdown to Artificial Intelligence and the New Pursuit of Global Power Dallas, TX: BenBella Books, Inc, 2020.
3 "Capella Space Publishes SAR Imagery Of The Ukraine-Russia Crisis," Satnews, February 28, 2022, https://news.satnews.com/2022/02/28/capella-space-publishes-sar-imagery-of-the-ukraine-russia-crisis/
4 Theresa Hitchens, "ICEYE to supply Ukraine with SAR satellite imagery via Ukrainian foundation," Breaking Defense, August 18, 2022, https://breakingdefense.com/2022/08/iceye-to-supply-ukraine-with-sar-satellite-imagery-via-ukrainian-foundation/
5 Emma Helfrich, "Radio frequency geoanalytics goal of Jacobs' investment in HawkEye 360," Military Embedded Systems, November 8, 2021, https://militaryembedded.com/comms/rf-and-microwave/radio-frequency-geoanalytics-goal-of-jacobs-investment-in-hawkeye-360
6 "Sikorsky And DARPA's Autonomous Black Hawk® Flies Logistics And Rescue Missions Without Pilots On Board," Lockheed Martin, November 2, 2022, https://news.lockheedmartin.com/2022-11-02-Sikorsky-and-DARPAs-Autonomous-Black-Hawk-R-Flies-Logistics-and-Rescue-Missions-Without-Pilots-on-Board
7 "Kratos, USAF Further Advance Capabilities in Successful XQ-58A Valkyrie Block 2 Flight Focused on Operational Aspects," Kratos Defense, November 3, 2022, https://ir.kratosdefense.com/news-releases/news-release-details/kratos-usaf-further-advance-capabilities-successful-xq-58a
8 US DOD, Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity, February 12, 2019, p4. https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF
9 Ibid, p5.
10 Ibid, p7-8.
11 "DOD Adopts Ethical Principles for Artificial Intelligence," Defense.gov, February 24, 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/
12 Ibid.
13 Zoe Stanley-Lockman, Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO," NATO Review, October 25, 2021, https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html
14 Ibid.
15 NATO, NATO 2022 Strategic Concept, June 29-30, 2022, https://www.nato.int/strategic-concept/
16 Ibid.
17 Ibid.
18 Sevilla et al, "Number of parameters in notable artificial intelligence systems," Our World in Data, 2022, https://ourworldindata.org/grapher/artificial-intelligence-parameter-count
19 McKinsey & company, "The State of AI in 2022—and a half decade in review," Quantum Black AI by McKinsey, December 6, 2022, https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review
20 Trevor Philips-Levine et al, "Weak Human, Strong Force: Applying Advanced Chess to Military AI," War on the Rocks, July 7, 2022, https://warontherocks.com/2022/07/weak-human-strong-force-applying-advanced-chess-to-military-ai/
21 "AlphaGo," Deepmind, accessed February 13, 2023, https://www.deepmind.com/research/highlighted-research/alphago
22 "Seven Types of Data Bias in Machine Learning," Telus International, February 4, 2021, https://www.telusinternational.com/insights/ai-data/article/7-types-of-data-bias-in-machine-learning
23 Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women," Reuters, October 10, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G
24 James Vincent, "Putin says the nation that leads in AI 'will be the ruler of the world'," The Verge, September 4, 2017, https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world
25 A.V.Sergeantov, A.V.Resin, I.A.Terentiev, "Transforming the Content of War: Contours of Future Military Conflicts," CNA, September 8, 2022, https://www.cna.org/our-media/newsletters/ai-and-autonomy-in-russia
26 Eunson Cho, "The Social Credit System: Not Just Another Chinese Idiosyncrasy," Princeton University Journal of Public & International Affairs, May 1, 2020, https://jpia.princeton.edu/news/social-credit-system-not-just-another-chinese-idiosyncrasy
27 Alexandr Wang, "The AI War and How to Win It," Substack: Rational in the Fullness of Time, November 27, 2022, https://alexw.substack.com/p/war?sd=pf#footnote-2-87162949
28 Ibid.
29 Graham Ellison, Eric Schmidt, "Is China Beating the U.S. to AI Supremacy?" Harvard Kennedy School Belfer Center, August 2020, https://www.belfercenter.org/publication/china-beating-us-ai-supremacy#toc-2-0-0
30 Akira Oikawa, Yuta Shimono, staff writers, "China overtakes US in AI research," Nikkei Asia, August 10, 2021, https://asia.nikkei.com/Spotlight/Datawatch/China-overtakes-US-in-AI-research

A Dutch Cougar helicopter takes off while NATO forces make an amphibious landing during Exercise Trident Juncture. Courtesy of NATO.

NATO Amphibious Capability – A Defence Planning Perspective

CDR (PRT-N/M) Antonio Esquetim Marques

The Current Security Challenges

The new NATO Strategic Concept 2022 starts with a clear statement: "the Euro-Atlantic area is not at peace."[4] It identifies the Russian Federation as the most significant and direct threat to Alliance security as well as to peace and stability in the Euro-Atlantic area. The concept also points out that terrorism, in all its forms and manifestations, is the most direct asymmetric threat to the security of allied nations' citizens and to international peace and prosperity. Other threats and challenges are also identified, including the resurgence of potential state on state conflict and state and non-state actors operating in the sub-threshold "Grey Zone."

The Strategic Concept reaffirms that NATO's key purpose is to ensure collective defence by using a 360-degree approach that demands appropriate capabilities and forces to fully achieve its core tasks. To support this, the concept states that the Alliance must have a permanent, synchronized planning process. This process is meant to consider each nation's individual pool of forces while allowing for the execution of plans and orders in all domains. This article presents an analysis of NATO's Defence Planning for an amphibious capability and it will show how these unique forces can contribute to overall defence and security. Essentially, as threats have evolved over the years, amphibious forces have had to re-evaluate, evolve and rise to these new challenges, ensuring they remain highly relevant tools for today's operational commander.

The Growing Importance of the Strategic Maritime Environment

The importance of the maritime domain and the littoral environment is highlighted by several statistics: 70% of the globe is oceanic (providing the physical connection among continents and regions); 80% of the world´s population is coastal; 90% of goods arrive by sea; and 99% of international digital traffic travels by undersea cables. The increasing relevance of the sea and the littorals will likely drive a greater number of military operations toward the vast and densely populated urban littoral areas.

The Alliance Maritime Strategy (AMS) and the NATO joint publication Allied Joint Doctrine for Maritime Operations (AJP-3.1) define and describe four major maritime roles: deterrence & collective defence, crisis management, cooperative security, and maritime security. These roles are divided into the following three distinct maritime activities: Warfare and Combat, Maritime Security, and Security Cooperation. Warfare and combat at sea, including sea control and sea denial, are conducted by dedicated naval forces, often blue water in nature but scenarios where the employment of amphibious forces in these areas are being explored. Warfare and combat from the sea, including maritime power projection, are achieved by conducting strike warfare, amphibious operations, special operations, and riverine operations. In the maritime security field, amphibious forces can, for example, protect critical infrastructure, and in security

cooperation activities they are well suited to support the execution of Humanitarian Aid & Disaster Relief (HA/DR) operations and Non-combatant Evacuation Operations (NEO).

Amphibious Forces: Their Relevance and Value

NATO defines an amphibious force as a "naval force and landing force, together with supporting forces that are trained, organized and equipped for amphibious operations."

An amphibious force offers the unique ability, as part of a maritime force, single or joint, to provide added value in all stages of a campaign, across the full spectrum of conflict and operations. While these forces offer many options at the tactical level, they also have distinct roles at the operational level, providing solutions to the Maritime Commander / Joint Force Commander and creating dilemmas for opposing forces.

Amphibious forces possess unique attributes: scalability, flexibility, agility, freedom of manoeuvre, responsiveness, and the ability to operate across all domains and the whole range of military operations. These forces are not reliant on complex infrastructure such as ports and airfields. They can react quickly to an adversary's actions due to their inherently high readiness, speed, and expeditionary reach.

Amphibious forces poised offshore can hold at risk geographically dispersed threats, demonstrate commitment without permanence, and demonstrate presence without obvious escalation. An uncommitted amphibious force is a factor in an enemy theatre commander's estimate. The threat of an amphibious landing or the execution of raids forces an adversary to retain coastal defense forces and a centrally held reserve. Once a committed amphibious force executes operations at the tactical level, it can re-embark and redeploy to continue to play a role at the operational level. This sequence can be successively employed throughout the conduct of a campaign.

By executing a wide variety of possible missions and tasks, amphibious forces can deliver the following effects across multiple domains:

- Coerce. Amphibious forces can demonstrate further resolve by executing raids against targets to prevent a potential aggressor from using force;
- Contain. Amphibious forces can stop, hold, or surround the forces of the adversary, or cause an enemy commander to center his activity on a given front, preventing the use of his forces elsewhere;
- Deter. Amphibious forces can be deployed into a region early in the stages of a potential conflict to convince an aggressor that the consequences of coercion or armed conflict would outweigh any gains;
- Protect. Amphibious forces can defend critical infrastructure in the early stages of a growing conflict;
- Reassure. The early presence of amphibious forces can be used to reassure a friendly state, the secondary effects being a nation that is more likely to provide access, basing, and overflight;
- Shape. In preparation for subsequent operations, amphibious forces can be deployed for shaping operations like intelligence gathering or conducting raids.

The amphibious military effects matrix (Figure 1) shows how amphibious forces operations with specific missions & tasks inter-relate within the larger context of maritime activities. The tactical missions are ultimately designed to generate operational and strategic effects in support of national or allied goals.

The Elements of the NATO Amphibious Capability and the NATO Defence Planning Process

Complex military operations, such as amphibious warfare, require rapid, deployable, capable, multinational, and interoperable forces. Generating such forces requires a long and detailed planning process.

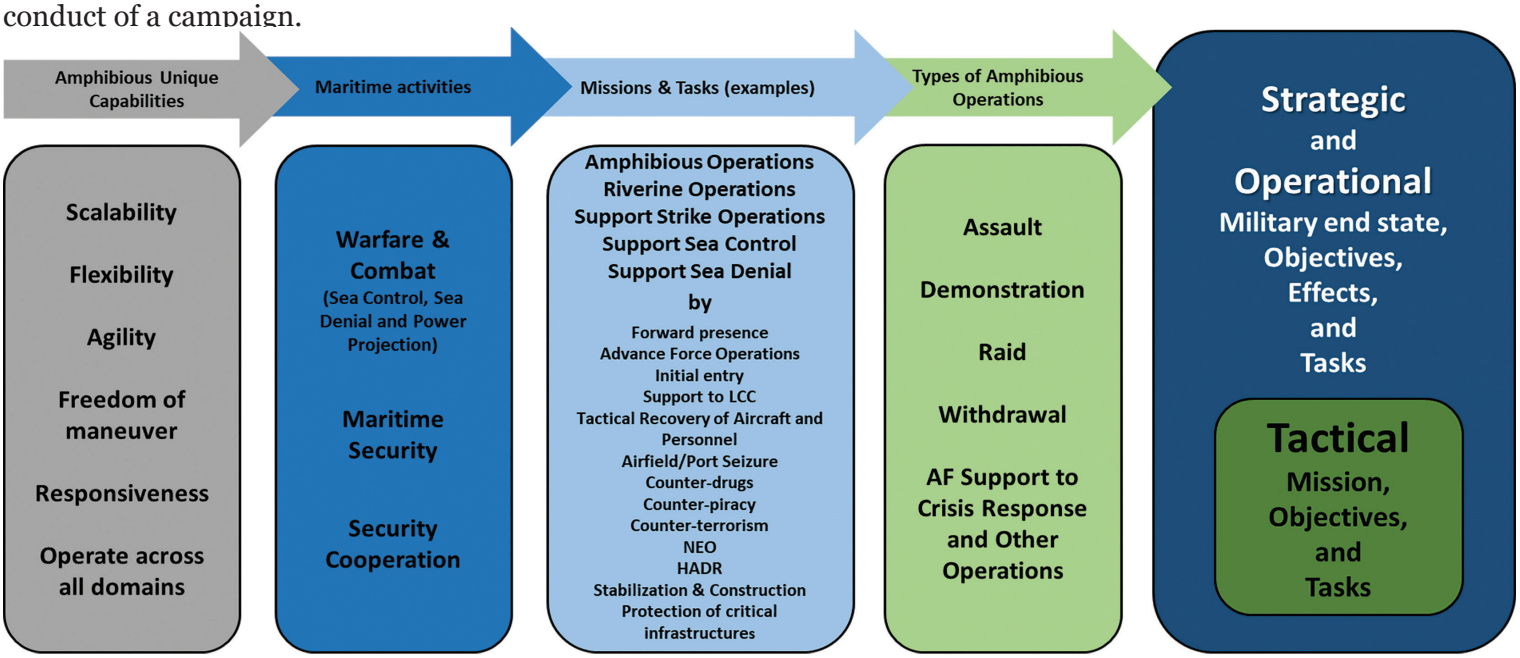


Figure 1 – CJOS Amphibious Effects Matrix (CJOS COE. 2022)

The NATO Defence Planning Process

The NATO Defence Planning Process (NDPP) aims to provide a framework within which national and Alliance defence planning activities can be harmonised to meet agreed targets in the most effective way. It facilitates the timely identification, development, and delivery of the necessary range of forces that are interoperable and adequately prepared, equipped, trained and supported as well as the associated military and non-military capabilities to undertake the Alliance's full spectrum of missions.

It is a coherent and integrated process in which Allies undertake to deliver the required capabilities in the short and medium term (up to 20 years into the future).

The NDPP guides force development for NATO's Amphibious Capability within political and strategic guidance. The defence planning capability requirements describe the necessary elements for achieving a specific Level of Ambition. NATO's amphibious capabilities are further detailed using three different capabilities (encompassing four elements), as depicted in figure 2.

Figure 2 - NATO Amphibious Capability Depiction

The Naval Forces

According to the NDPP, an amphibious ship should be capable of being deployed worldwide to conduct amphibious operations as an integrated part of a naval task force. It includes two variants: the Amphibious Ship Large (NAL) and the Amphibious Ship Small (NAS). NAL and NAS are differentiated by lane transportation capacity (350 vs 750 lane meters[1]), the ability to operate as the primary Command & Control (C2) platform for the Commander Amphibious Task Force / Commander Landing Force, and the ability to operate helicopters. No reference is made to the military lift regarding the number of troops (accommodations).

Amphibious ships are organized into either a Naval Amphibious Assault Group – Brigade or Naval Amphibious Assault Group – Battalion according to the transportation capabilities of the Landing Force echelon and its shore projection capability.

The capability of ship-to-shore movement implies projecting the Landing Force (LF) ashore and supporting and operating surface and/or air connectors. These movements can be achieved by employing organic vertical/short take-off and landing fixed-wing and/or rotary-wing aircraft, using landing craft, and/or through a landing ramp for use by organic assets (e.g., amphibious vehicles). These force elements are categorized as Amphibious Operations Projection Capability – Landing, Amphibious Operations Projection Capability – Helicopter, or Amphibious Operations Projection Capability – Dock. One should note that the surface and the air connectors are often organic to the LF. These combinations in operations planning determine the method of entry; whether it is to establish a lodgment or beachhead[2], conduct a ship-to-objective manoeuvre, or a combination of both.

The Landing Force

A landing force is the task organization of ground, aviation, and surface units assigned to a Commander Landing Force to conduct an amphibious operation. Usually it consists of Marine units, but it can also include units from the Navy, Army (e.g., Artillery or Engineers), and Air Force.

The landing force structures in the NDPP comprise brigade size (heavy and light variants) and battalion size (heavy and light variants). These are assumed to comply with the combat brigade/combat battalion variant common capabilities. Brigades should be capable of conducting tactical land activities to engage or defeat an opposing force, in coordination with supporting units, with organic weapons systems in the full spectrum of land operations. Battalions, as part of a manoeuvre element in a brigade, should be capable of conducting tactical land activities across all operating environments using organic weapons systems while being supported by the brigade and/or joint capabilities.

The objective of the amphibious force is to establish itself on land, which means it must be able to both support and deliver the required effects in its area of operations. In essence, the force is transformed into a "land combat team". The size of the landing force will drive the organization and structure of the overall amphibious force (i.e., it will determine the required capabilities of the other elements to transport, project, support, enable and command and control the landing force).

While building an integrated multinational force is sometimes a political decision, amphibious forces and amphibious operations within NATO will be, by default, joint and most likely combined. For the LF, in particular, integration and interoperability are especially challenging issues. Depending on the size and scope of the mission, it may be planned and led by one or more

countries, with different approaches to operations and understandings of amphibious capabilities. Therefore, the importance of the generic and agreed upon composition of LFs amongst NATO when conducting planning cannot be overstated.

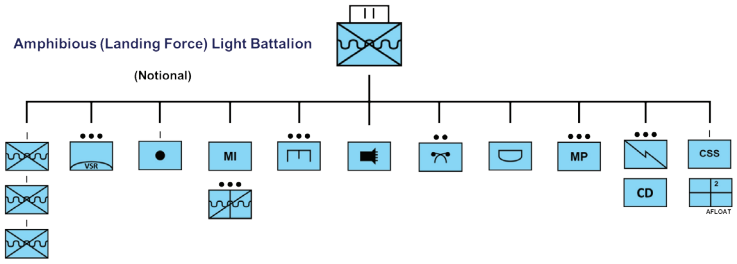


Figure 3 – (Notional) Generic Amphibious (Landing Force) Light Battalion baseline structure

Command & Control

Tactical C2 capabilities are provided by a command structure Naval Commander Task Group – Amphibious (NCTG-AMPH), which must be capable of exercising command and control over an assigned multinational Amphibious Task Force across the complete spectrum of maritime missions. The physical capability is given by the Minor Afloat Command Capability – Amphibious (MACC-AMPH), which must be capable of hosting and providing the seaborne Command & Control for an NCTG-AMPH.

(Possible) Amphibious Forces Structures - ATG and ATF echelons

An ATF contains a brigade size landing force. It will typically also incorporate organic aviation, surface and subsurface maritime assets, and other supporting forces, providing Combat Support and Combat Service Support. An ATF comprises multiple national or multinational ATGs, each providing a battalion size landing force. ATFs and ATGs are inherently adaptable and task-organized with the required capabilities to meet the assigned task. Due to the unique characteristics and the concept of employment for amphibious forces, an amphibious brigade or battalion is likely to be smaller in size than its typical land component counterpart, but equipped with supporting assets (fires, aviation, afloat logistics, etc.) enabling it to deliver the required effects in the littorals. The diagrams and descriptions below illustrate possible standard baselines of building blocks for an amphibious force. The arrangements can be diverse, but typically 1 x NAL is equivalent to 3 x NAS in terms of transportation and accommodation capabilities. In other words, a NAL can replace a NAS without changing the shipping quantitative requirements; however, any unit replacing a NAL must meet full requirements.

Any number of combinations of amphibious and landing forces can be constructed for any given mission. For example, the baseline Landing Force – Light Battalion with a minimum of a two-ship amphibious structural element model (1 x NAL and 1 x NAS) has a combined capability of carrying at least 1000 troops and 1100 lane meters. A Landing Force – Light Brigade could align with a minimum of a six-ship amphibious structural element model (3 x NAL and 3 x NAS) with a combined capability of carrying at least 3000 troops and 3300 lane meters. These examples reflect the most common building blocks for employment in operations with the capability of delivering effects across full spectrum operations.

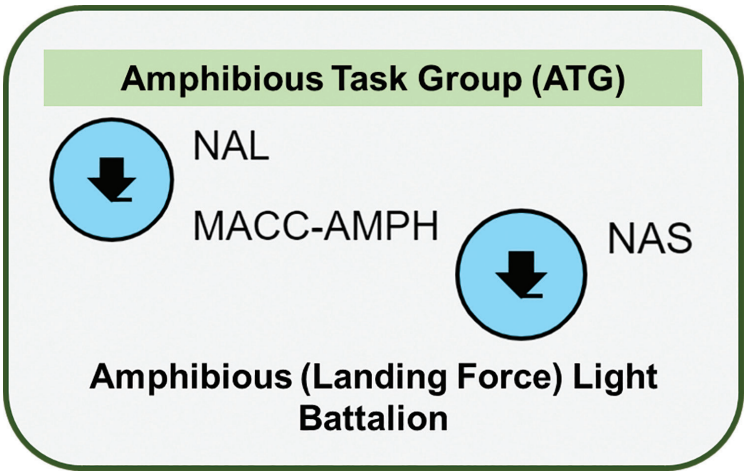


Figure 4 - Generic Amphibious Task Group (ATG) composition (Light Battalion)

In actual operations, amphibious forces will always be mission-tailored and task organized to meet mission requirements, and are capable of being quickly reinforced or augmented with other assets as the situation dictates.

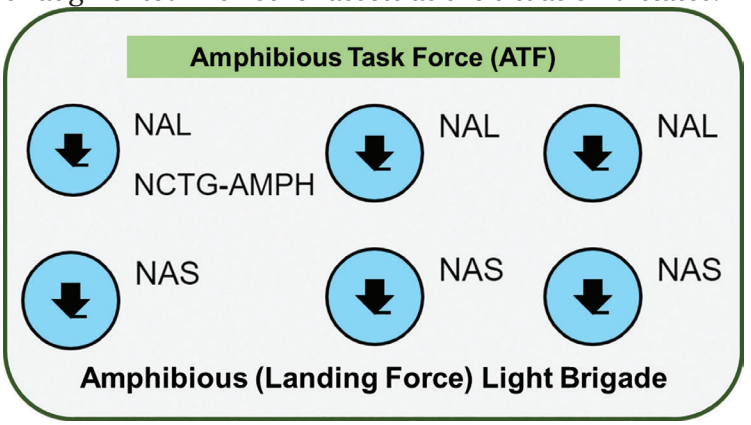


Figure 5 - Generic Amphibious Task Force (ATF) composition (Light Brigade)

Defence Planning is informed by, but distinct from, Operations Planning; while Defence Planning is about identification, development and delivery of NATO's present and future requirements, Operations Planning deals with the planning of military operations at all levels.

Operations Planning is focused on the short term while Defence Planning is focused out to the end of the medium term and thus, is inherently more affected by uncertainties. Operations Planning is constrained by existing capabilities to meet current threats. Defence planning should help identify new capabilities and fulfil shortfalls to meet a range of potential future threats with the constraints set out in Political Guidance.

Considerations for the Future (medium and long term)

Amphibious forces must be able to operate within reach of present and future anti-access and area denial (A2/AD) capabilities in a contested and denied environment. Operating in this environment involves increased risk to the main amphibious ships, with the associated vulnerabilities when operating in the littoral. To overcome those vulnerabilities, a number of nations have focused on being able to conduct distributed operations with smaller forces and the use of unmanned systems. In the same vein, maritime power projection is increasingly trending toward low-signature, smaller, and more lethal amphibious forces capable of surging into an A2/AD bubble. To address emerging threats, new concepts are in development that diverge from the conventional notion of amphibious operations. These novel concepts envision dispersed, disaggregated, or distributed operations conducted by amphibious forces. Some of these concepts are already being written into doctrine for several nations, including robust examples in the United States, the United Kingdom, and the Netherlands. These concepts offer potential solutions to overcome the disadvantage of large, concentrated formations in a contested environment.

The most visible changes to amphibious landing forces are occurring in the US Marine Corps (USMC). In the USMC Force Design 2030, the Marine Littoral Regiments are a prime example of the smaller, disaggregated force structure (linked with the Expeditionary Advanced Base Operations - EABO Concept). The UK Royal Marines are also undergoing a 'back to the roots' transformation by designing the Future Commando Force within the Royal Navy's future amphibious capability. And the Netherlands' Marine Corps is restructuring its Marine Combat groups as part of its new Littoral Raiding Force concept.

Connected with these new concepts are changes to amphibious shipping. The US Navy intends to build the Light Amphibious Warship (LAW) to support the USMC Expeditionary Advanced Base Operations concept and the UK plans to modify one of its LSD ships to serve as an interim Littoral Strike Ship until the Multi-Role Support Ships (MRSS) comes online. The Netherlands announced that two LPD Rotterdam-class ships will be replaced by one new ship class suitable for amphibious operations, maritime patrol duties, and emergency relief.[3]

Nevertheless, the need for conventional amphibious forces to conduct initial entry operations will remain essential. These new concepts should integrate with existing doctrinal amphibious operations as an evolution of the amphibious forces' capabilities in a more wide-ranging spectrum of employment. With changes already in motion in the short and medium term, new amphibious operational concepts should be closely examined for long term capability development to align with NATO's Strategic Foresight Analysis and Future Operating Environment (part of the NATO Warfighting Capstone Concept).

Final Thoughts

The NDPP is the primary means to facilitate the identification, development, and delivery of NATO's present and future capability requirements. It apportions those requirements to each ally as Capability Targets, facilitates their implementation, and regularly assesses progress. Then, NATO's capability requirements are consolidated into the Minimum Capability Requirements (MCR), which are then refined and sent to the Allies (individually or collectively) in the form of Capability Target packages.

Amphibious forces will always be part of Alliance Capability Targets. They are an essential military capability and part of NATO's best response options to the world's most complex threats. Allies will employ amphibious forces in times of peace, crisis, or conflict. They are undeniably effective in nearly all operational scenarios: warfighting, combat, crisis response, security, peacetime military engagement, and peace support. And, as threats and the operating context changes, so too will amphibious capabilities evolve, remaining relevant for the foreseeable future.

When the execution order comes, it's all about planning!

This article is based on a CJOS COE study generated by a Request for Support from the Allied Command Transformation-Staff Element in Europe (ACT-SEE), Defence Planning Requirement Determination (DPRD) Branch, to assist the NATO Defence Planners in the definition of the quantitative requirements for the Alliance amphibious capability.

Endnotes

1 A lane meter is a unit of deck area in ships where containers or other cargo, including vehicles, can be rolled or driven on and off. A lane meter is defined as a strip of deck one-meter long. A lane is conventionally 2 meters wide.

2 A designated area on a hostile or potentially hostile shore which, when seized and held, provides for the continuous landing of troops and materiel, and provides the manoeuvring space required for subsequent projected operations ashore.

3 Ministerie van Defensie, The Netherlands. "Defence White Paper 2022." Defensie.nl. Ministerie van Defensie, August 8, 2022. https://english.defensie.nl/downloads/publications/2022/07/19/defence-white-paper-2022.

4 NATO, NATO 2022 Strategic Concept, June 29-30, 2022, https://www.nato.int/strategic-concept/

Allied Operations in the Data Age – Do We Need to Rethink How We Plan?

WO1 (RM) Stephen Scott

A USMC F-35B Lightning II aboard the HMS Queen Elizabeth (R08). Courtesy of US Navy.

It should be no secret that military forces, especially in the maritime domain, have become increasingly reliant on the use of non-terrestrial communications. Even momentary communication gaps on the battlefield can result in avoidable losses and change victory to defeat. To prevent such calamities, military forces require instant, reliable and capable Beyond Line of Sight (BLOS) communications.

The New Space Race

On 1 December 2022, the Federal Communications Commission granted permission for the private company SpaceX to Launch 7,500 of its proposed Gen2 Starlink Constellation satellites.[1] The SpaceX plan would launch approximately one quarter of the total future planned deployment of 29,988 satellites into Low Earth Orbit (LEO). The remarkable number of deployments sets a landmark, as it equates to approximately the total number of objects launched into space in human history (including the 12,000 first generation spacecraft already planned or currently in orbit).

Aside from the surprising total number of planned launches, the growth rate of these launches is equally remarkable. In 1949, the "Bumper-WAC" made history as the first human-made object launched into space. Just eight years later in 1957, Sputnik 1 became the first earth-launched satellite. For the next 60 years, nations launched a steady stream of satellites into space for a variety of reasons such as weather, global positioning and imaging and, of course, communications. Only in 2020 did the number of satellites launched in a single year first exceed 1000, reflective of a new and highly lucrative space race beginning just a few years earlier. Several major companies, such as OneWeb and Amazon's Kuiper, vied for a slice of an estimated trillion-dollar market.[2]

The 'So What?' for Maritime Military Communications?

Although currently limited on coverage, the Starlink constellation will provide high-speed, low latency internet with up to an estimated 350 Mbps download capability while at sea.[3] This far exceeds current capabilities on any military vessels. Whether used for passing tactical data or simply to improve sailors' quality of life, the Starlink constellation serves as a catalyst for significantly impacting the tactical and operational landscape of the maritime community, not to mention the ability of naval forces to retain sailors with the resultant improvements to morale.

But Is this Secure?

Modern navies have routinely used commercial satellites for navigation since the 1960s and for limited communications shortly thereafter.[4] Commercial satellites may not offer the same levels of protection as military satellites, but transferred information can still be heavily encrypted between senders and recipients. In December 2022, SpaceX revealed the 'Starshield' satellite project. While Starshield's capabilities are not fully known, it is advertised as a partner to Starlink

tailored for government and military use with a focus on three areas: Earth Observation, Communications and Hosted Payloads.[5]

Are Modern Satellite Communications More Robust?

Most current threats to spacecraft have always existed. The primary threats include both adversarial actions, and vulnerabilities related to sensitive equipment in a harsh space environment. Some deliberate actions from an adversary are reversible, such as frequency jamming, while other actions are irreversible, such as anti-satellite missile attack. Non-adversary threats to spacecraft would typically involve either a system malfunction or space-based phenomena, such as a Coronal Mass Ejection (CME) from the sun. A CME is a large expulsion of plasma and magnetic field from the Sun's corona, weighing potently billions of tons and travelling at speeds up to 3000 kilometres per second. When reaching the earth this can cause power grids to overload and increase static in the ionosphere, severely affecting radio and satellite communications.

One improvement of modern satellite capabilities is the flexibility of diverse options available to the customer. Traditional Geostationary Orbits (GEO) are widely used in military communications due in part to having more easily tracked orbits as they remain in the same position; LEO spacecraft are also becoming commonly used. Another option, Medium Earth Orbit (MEO) constellations, have been used since the 1960s for a number of purposes, most notably Global Positioning. The use of MEO satellites is experiencing a resurgence with ongoing research for use in Missile Defence,[6] as well as communications. MEO offers planners the option of low latency and high bandwidth, while fewer satellites are needed than LEO due to the greater altitude coverage. The disadvantages of MEO include higher costs and increased vulnerabilities to space phenomena.

Although not typically as secure or robust as their military counterparts, commercial satellites, particularly those in LEO, may offer the advantage of 'hiding in plain sight.' The commercial and military uses of satellite communications are becoming increasingly intertwined. One nation's military force may rely upon commercial satellites for its operations. Conceivably, a potential adversary, especially if geographically close, may rely upon the same commercial satellites for its own business networks, as well as possibly its military forces. This dual military and commercial use of commercial satellites may force a nation considering a satellite attack to weigh the military benefits to its adversaries against the harm to its own economy and military operations.

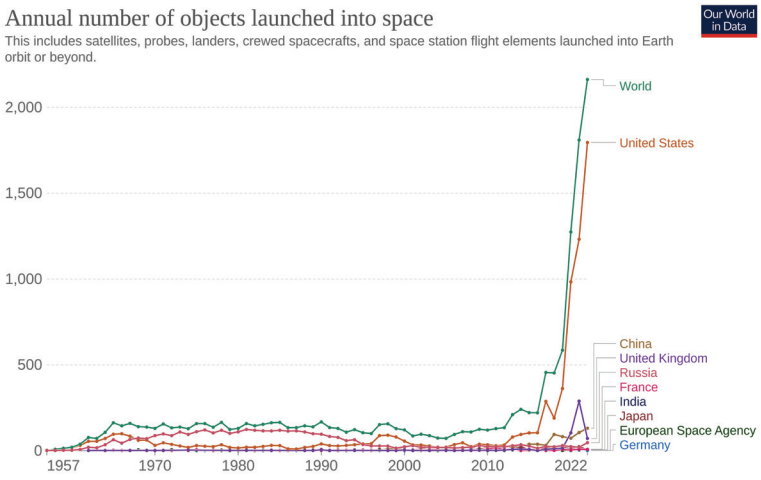


Fig 1. Total Numbers of objects launched into space[9]

If Space Is Denied, What's the Alternative?

With the multitude of current and near-future options available in the space domain, a resilient approach to planning requires open-minded consideration of all reasonable alternatives. A tactical situation may dictate that we need an option with the lowest probability of detection and interception. Conversely, tactical situations may require communications with the maximum access and ease-of-use for military operators, which typically would be better provided by commercial satellites. At the same time, tactical planning cannot preclude technical, environmental or adversarial events that render all satellite communications inaccessible. Therefore, planning must incorporate Earth-based communication alternatives. The following paragraphs explore three of the most practical and accessible long-distance terrestrial communication options.

The High Frequency Alternative.

Use of high frequency (HF) particularly in the maritime domain, has always been, and should remain, a backbone of military communications. HF offers a reliable and robust method of LOS and BLOS communications. Furthermore, HF is relatively inexpensive, technologically simple, widely available and not reliant on third party technologies for retransmission over long distances. Previous issues with low data rates are being addressed: internet protocol over HF and wide band HF are leading to more mature and capable HF technologies. Notwithstanding


SpaceX Dragon over Desert approaches ISS. Courtesy of NASA.

valid questions concerning spectrum availability and training challenges, HF should remain a fundamental option for military communications planning.

The MANET Alternative.
Mobile Ad-Hoc Networking (MANET) represents an umbrella term for communications mediums that operate without reliance upon a single access point, but instead create self-forming and self-healing networks. MANET radio technologies are receiving heavy investments for use in the littoral domain based upon the lightweight and agile communication solutions they offer. Several navies are conducting trials with MANET using a variety of practices and waveforms. Creating a commonly agreed standard for this kind of system would offer a capability for allied vessels to act as elements of a single network. With MANET, increasing the number of vessels would actually correspond to an increase in the range and reliability of the network. The addition of other MANET-capable platforms (aircraft, white shipping, UAVs, etc.) could further create a seemingly boundless network.

The 5G Alternative.
In principle, 5G is similar to the MANET concept as it would treat vessels as part of a single Communications Information System (CIS) network, able to use information as required or act when needed as a node to thicken the network. 5G offers additional capabilities as well. For example, 5G is likely how platforms will communicate with Harbour Wireless Access Points. If that capability were expanded, it could offer improved communications for all coastal defense vessels, seamlessly linking them into multiple supporting assets in the air, land, maritime and cyber domains. 5G will also soon add the space domain, as it evolves into a capability available to LEO satellite constellations, thus creating a potentially unlimited range.

Use of Smarter AI-Based Routing and Cloud-Based Technology

Regardless of the means for transferring information between bearers, the means for storing, processing and accessing information will be equally critical. Fleet communications may rely on approaches that not only dynamically shift between multiple bearers, but also treat every platform in the Fleet or Task Group as part of a larger network, a process which must happen seamlessly. Once a reliable and persistent link is achieved, the Fleet must still be capable of using the information meaningfully while planning for resilience in the face of unexpected network disruptions. For example, a serious concern of cloud computing on ships is whether the information would be accessible in the event of inconsistent or unreliable bandwidth issues. Smart solutions to combat such concerns are being developed using edge computing, a distributed computing framework that brings applications closer to data sources. Such solutions could close the reliability gaps and allow for data to be managed more efficiently.

Visibility of Shipping. Do We Still Need to Stay Hidden, and What is the Point of Trying?

By incorporating every communication option previously discussed, one could imagine a fleet of vessels bestowed with a 'network nirvana' of perfect availability and unlimited bandwidth, but a new problem arises from this scenario. Every networked vessel would propagate a mass of electro-magnetic waves. While the electro-magnetic signature of a cruise ship can be ignored, it creates a major concern for military vessels relying on an element of tactical covertness. While the concern should not be completed disregarded, it should be understood in context with the limits of remaining 'invisible' to an adversary in the present day.

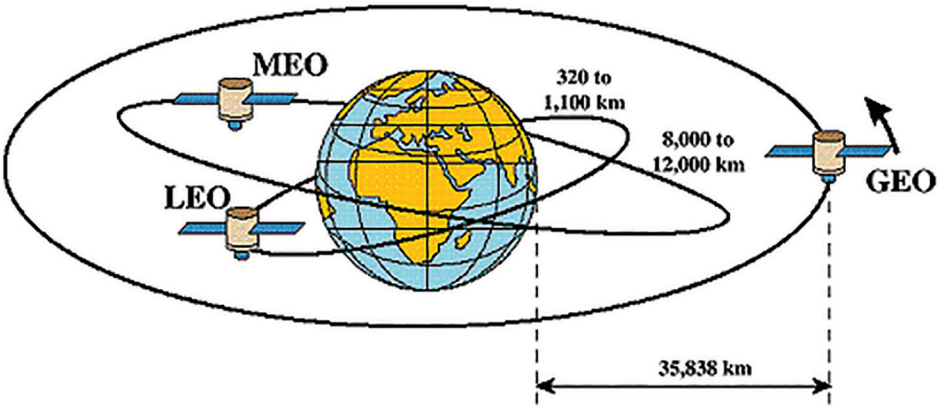


Fig 3. Examples of common types of orbit.

Throughout history, fleets and individual military vessels have balanced the oft-conflicting demands of stealth versus operational effectiveness. Balancing those demands included such choices as day versus night operations, radio silence versus open communications, and the use of direct or traditional routes versus longer ones less expected to be anticipated by an adversary. Similarly, specific tactical situations will demand the risks of electro-magnetic transmissions with the operational benefits of networked communications. For example, the Royal Navy has painted its vessels grey for over a century with an original goal of obscuring the ship and the visual clarity of its vertical structures. But no color would hide the ships from radar.

Of course, the introduction of radar to the maritime battle space naturally produced a new technology race to make ships once again less susceptible to detection from above and below the surface. The U.S. Navy's Zumwalt-class ships serve as excellent examples, where structural and other innovative solutions result in a radar signature as small as a fishing vessel, despite their actual size.

HMS Spey with a camouflage paint scheme. Courtesy of Royal Navy.

USS Zumwalt. Courtesy of US Navy.

Modern satellite surface-monitoring capabilities are various but can thwart attempts to hide with a reduced radar signature. For example, the Moderate Resolution Spectrometer (MODUS) monitors chlorophyll concentration and sea surface to an extent that it can predict and track whale (and, of course, ship) movements. Also, ever-advancing satellite cameras can record images down to centimeters. Tracking even a non-transmitting ship does not appear too difficult with such satellite technologies available to an adversary. The difficulty of hiding is compounded further by the increasing accessibility of information, as exemplified by the Open-Source Satellite capabilities currently used in Ukraine[7] to track Russian military movement on both land and sea. The reality of satellite technologies questions the degrees to which we attempt to hide military vessels and what measures we can take to mitigate this risk.

So, What about the Planning?

Taking all the information above into account, what does this mean for planning methodology? Furthermore, how do we capitalize on the opportunities presented to us, how do we discontinue a dangerous trend of over-reliance on vulnerable technologies, and how do we mitigate known risks when conducting communications planning?

Whether strategic, operational or tactical, communications planning involves the three same processes, at least in general terms. There is first an assessment of the overall situation and the effect to be achieved, which clearly varies based upon the commander's intent. Second there is an estimate process, which involves the planner reviewing and aligning the intent to the CIS assets expected to be available. Finally, the efforts culminate in a concept of how the plan will be realized in the form of an Information Exchange Requirement.[8]

Underpinning these processes at every level are the considerations for interoperability, security, support and resilience. All are weighty subjects in their own rights, and subject to their own research, but the next section of this article focuses primarily on resilience.

How We Plan Now for Resilience

Using the processes and basic principles previously mentioned, planners must consider the mission and available assets, and then allocate those assets to the requirement. A common methodology for allocating available assets and building a robust communications plan is PACE, which can be explained as follows:

Primary – Determining the best and intended method of communication between parties.

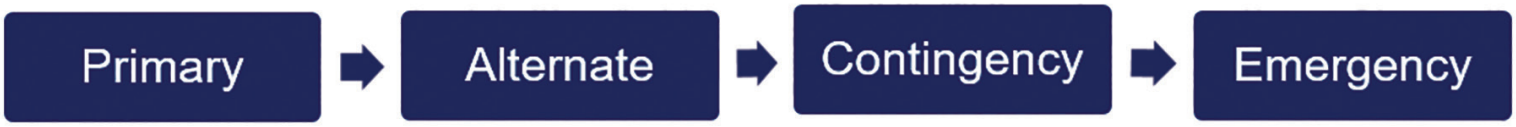
Alternate - A common but less-optimal method of accomplishing the task, often monitored concurrently with primary means.

Contingency - Generally not be as capable or convenient as the first two methods but can accomplish the task.

Emergency - The last resort, typically involving significant delays, costs, and other impacts, and often only monitored if the other means fail.

A typical employment of PACE for BLOS on a maritime vessel could be the following scenario:

- A Vessel plans to operate most circuits on a Primary GEO Satellite Communications Bearer.
- As an alternative in the event of failure, the priority circuits would revert to another LEO or commercial GEO satellite with high availability but lower bandwidth than the SatCom Bearer.
- In the event of those satellites' unavailability, BLOS would be achieved on one or two circuits using HF as a contingency.
- Finally, if HF fails emergency planning could employ a LEO Satellite phone.



PACE planning offers a simple, comprehensive and resilient process that minimizes a planner's likelihood of complete communication failure and allows communications planning that is scalable to requirements. The following paragraphs consider two approaches to applying PACE to Fleet operations.

Option 1: Every Bearer is a Primary Component of PACE
With every vessel maintaining an advanced and automated dynamic routing capability, there could be the possibility of using multiple primary bearers at the same time and managing outputs. What this means is you treat every bearer as a primary and separate the transmission flow over the one that has space at that time. Although this would be impractical with the current PACE methodology where you allocate networks to slow and outdated bearers in order of capability, with the technologies mentioned above that are all high bandwidth and low latency, this could be possible. What this means is that every bearer is a primary bearer, and every bearer mutually supports the other.

Option 2: A Service-based approach
One other proposed method that will be researched by CJOS COE this year is a 'service-based' approach. The basic premise of this approach is to allocate priority to the nets or circuit and let them run 'bearer agnostic', meaning able to pass traffic over any carrier, not necessarily just an assigned one. This will require early planning but could produce great benefits in giving a platform full autonomy over the priority list and then letting the router configure how it is split. In this way the planner would only be concerned about the order of information flow and a system would automatically find a correct path. One exception to this is a separated HF circuit that runs consistently for message traffic. Separating the HF in this way would mean that regardless of faults on the other systems or a technical error with the router, a vessel always has the ability to communicate and fight the battle.

What about Planning for Satellite Denial?

Failing to plan for a satellite-denied environment would seem reckless. For example, if a vessel was operating in reliance of GEO and LEO satellites simultaneously, it is unlikely that an adversary-launched attack would cripple all communications; however, planners must still prepare for the possibility, as there are many ways satellites may be denied. Planners must incorporate terrestrial-based bearers into a plan, leveraging flexibility to achieve improved technological resilience. It is fathomable that a powerful solar event could disrupt satellite communications from all orbits and even render BLOS HF inoperable, or at least disrupted. In such an emergency situation, it would become critical to have backup terrestrial options like a Line of Sight based 5G network. Vessels using a common 5G rebroadcasting standard, thus having multiple points of presence already established, would create a robust or 'thick' network. In the event of a 5G network requiring increased range or resilience, there are methods whereupon it could be temporarily "thickened" further; for example, deploying small, high altitude rebroadcasting UAVs could provide area coverage.

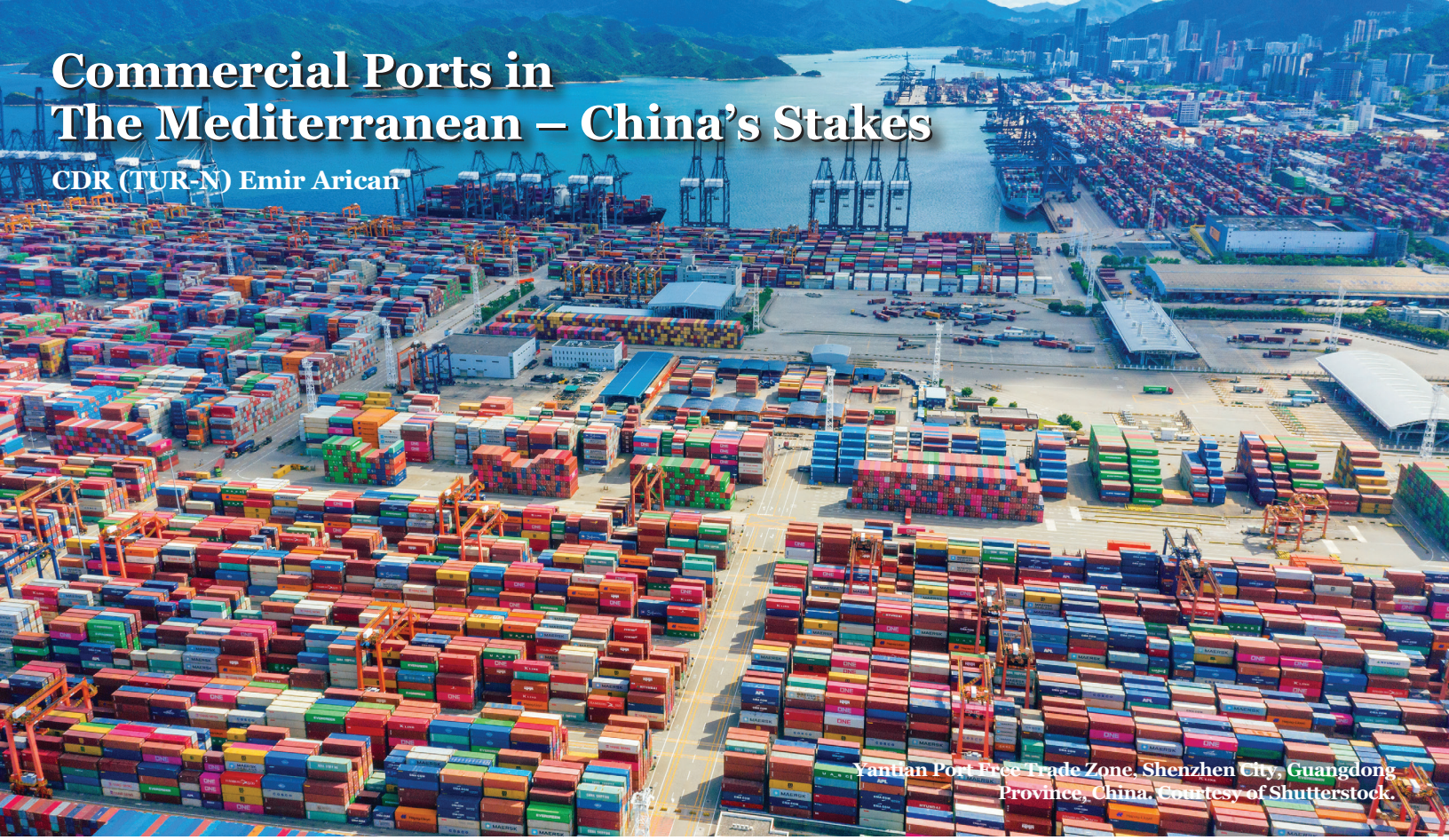
The Next Step

Communication technologies are advancing at a dizzying pace. Increasing corporate levels of investment guarantee further acceleration and changing demands. Communicators, planners, warfighters and technologists working together must accept the changes and embrace new solutions in order to adapt to them. It is critical to consider how we think as well as how we plan to make the most of the new opportunities presented to us. Transforming our current communications strategies in multi-domain operations requires consideration of opportunities to link previously isolated platforms and reshape our view and use of the electromagnetic spectrum. As fleets expand from point-to-point radio links to networks, single networks to internets and whatever lies beyond, they must continuously prepare for threats to communications and the required preparations and planning to respond to those threats.

Endnotes
1 Foust, Jeff. "FCC grants partial approval for Starlink second-generation constellation" December 2, 2022. https://www.spacenews.com
2 Pultarova, Tereza. Howell, Elizabeth. Dobrijevic, Daisy. Mann, Adam. "Starlink satellites: Facts, tracking and impact on astronomy" November 23, 2022, https://www.space.com/spacex-starlink-satellites.html
3 Figures from Starlink Maritime
4 Normanx, Jeremy. "The US Navy Launches NAVSAT, the First Operational Satellite Navigation System," 2023 https://www.historyofinformation.com/detail.php?entryid=106
5 Information from SpaceX - Starshield, 2023.
6 Hitchens, Theresa. "SMC eyes MEO Sats for Missile Tracking". July 2021, https://breakingdefense.com/2021/07/smc-eyes-meo-sats-for-missile-tracking/
7 AEI's Critical Threats Project; Institute for the Study of War; NASA Earthdata; Planet; Telegram; VKontakte; The Economist. Jan- 2023, https://www.economist.com/interactive/international/2023/01/13/open-source-intelligence-is-piercing-the-fog-of-war-in-ukraine
8 Information summarized from AJP-6 Chap 3
9 United Nations Office for Outer Space Affairs, "Annual number of objects launched into space", Jan 2023, https://ourworldindata.org

Commercial Ports in The Mediterranean – China's Stakes

CDR (TUR-N) Emir Arican



Yantian Port Free Trade Zone, Shenzhen City, Guangdong Province, China. Courtesy of Shutterstock.

The Mediterranean has been home to Egyptian, Ancient Greek, Hittite, Phoenician, Roman, Seljuk, and Ottoman civilizations that have shaped history. It has long been a center of culture and art and its ports have served world trade for centuries.

The Phoenicians were the earliest dominant Mediterranean maritime power, developing numerous ports throughout the region and bringing trade from the Near East in 1200 - 800 BC.[1] The Greeks and Romans were the primary beneficiaries of these early merchant pioneers.

Linking the Mediterranean to the far east, the Venetian merchant Marco Polo was first to bring news of Asian cultures to Europe via a book that chronicled his travels along the Silk Road (1271-1295).[2] Subsequently, the silk and spice trade grew to stretch from China to Europe and Africa over a route that traversed Asia's interior. This trade route proved beneficial to both China and Europe, despite suffering interruptions due to wars over the years.

Fast forward nearly 800 years to the present day, the European Union and China are significant markets for each other's goods in global trade of a scale unthinkable in Marco Polo's time. According to 2021 trade information, the European Union supplies China with 10.2% of the products it exports, while receiving 22.4% of its imports in return.[3] The range and volume of goods involved are vast – the machinery, parts, and vehicles sector constitutes about 700 billion Euros in trade annually.[4]

Benefitting from access to resources, a competitive labor market and the governmental control of a socialist market economy, China has become the dominant mass manufacturing center of the world in recent decades. It has steadily driven global reliance on its products by being a high-volume, low-cost producer of goods. In turn, this growth in demand has resulted in an increase in manufacturing volume that has provided China with a consistent annual trade surplus for more than two decades. To support this growth, it has invested in transportation infrastructure to ensure the timely delivery of raw materials to factories, finished goods to market, and energy to fuel industry.[5]

But these infrastructure investments made by China have not been contained solely within its own borders; indeed, for the past 2 decades China has been aggressively providing incentives to nations across the globe to accept Chinese investment, while promoting and influencing its own industry and prosperity. This article aims to examine one arena for Chinese overseas infrastructure investment - its influence over Mediterranean ports. In particular, this article will take a close look at the greater Belt and Road Initiative (BRI) and the possible implications for military and commercial maritime operations.

Belt And Road Initiative

In a bid to guarantee sustained economic growth and drive increased prosperity, President Xi-Jinping announced the "Silk Road and Economic Belt" policy during a speech at Nazarbayev University, Kazakhstan in

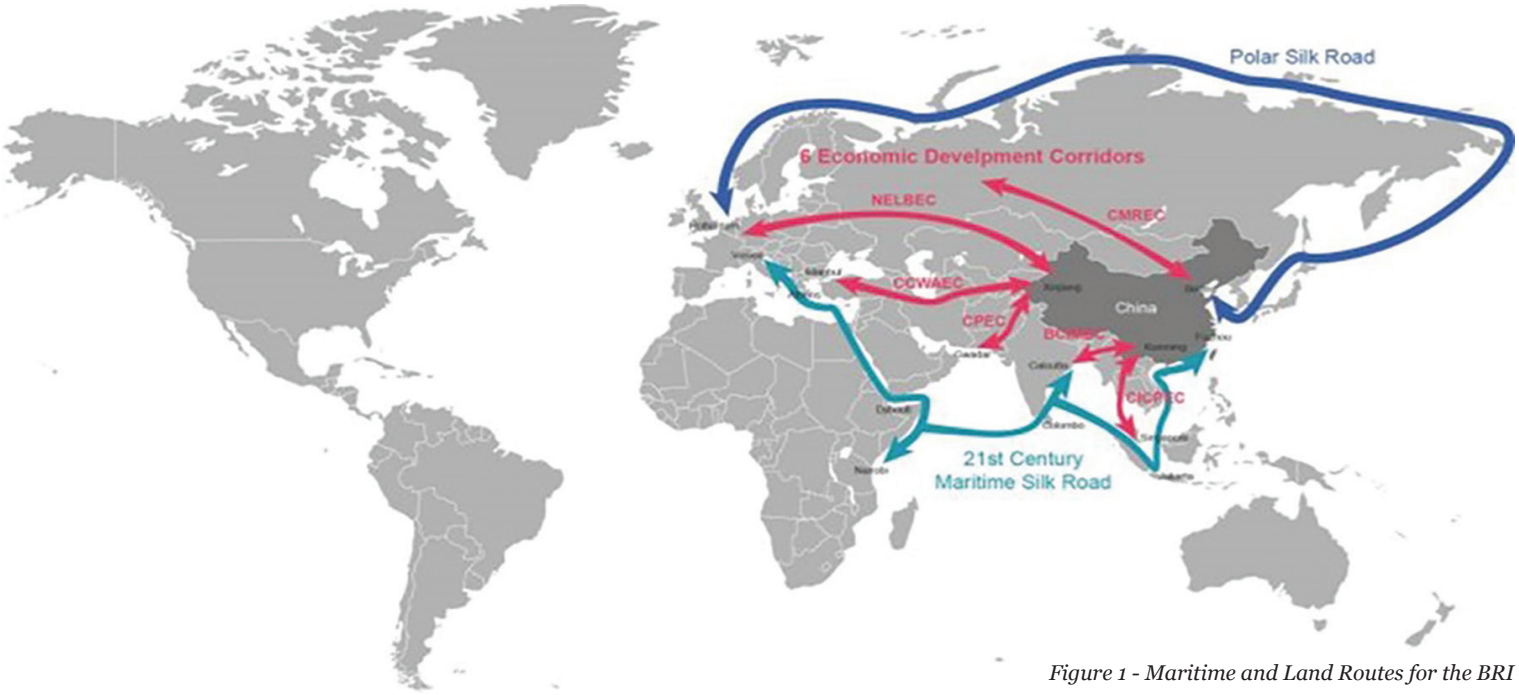


Figure 1 - Maritime and Land Routes for the BRI

2013.[6] In this key development, Central Asian countries were offered a "win-win" proposition in the form of an initiative to rebuild the ancient Silk Road. Now well understood and much commented on, the fledgling policy set out a vision using the term "Belt" to refer to a land route to Europe from China across Central Asia, Russia, and Ukraine. Counter to most people's assumptions, the "Road" in the BRI is actually used to refer to maritime routes to the Mediterranean from the South China Sea, Indian Ocean, and Red Sea.

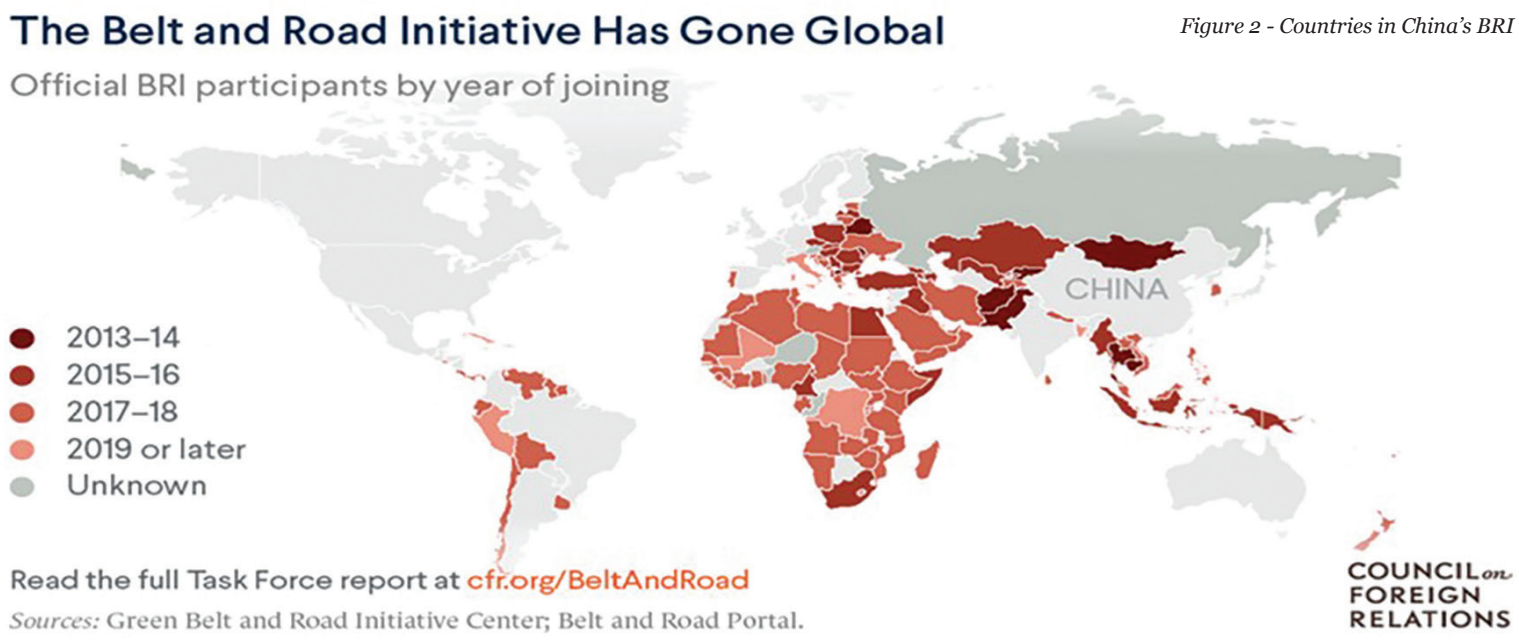
This twin track approach provides options when it comes to China's trade routes. There are economic corridors on land between China, Myanmar, Bangladesh, and India in addition to the maritime routes from China to the Indian Ocean via Pakistan's port of Gwadar. There is also an overland transportation route to Türkiye and, arguably, much of Europe via Central Asia, independent of Russia or Ukraine. Overall, there are multiple land trade routes connecting the EU, Middle East, and Africa. At sea, there are only two main routes: the Maritime Silk Road and Polar Silk Road (Figure 1).

Following this model China seeks to minimize disruptions to the flow of raw materials and/or exportation of finished goods by establishing multiple land and sea routes. Within the scope of the BRI, it has committed to improving port infrastructure and logistics facilities, aiming to speed the delivery of goods and increase the volume of its products.

In addition to providing Chinese access to raw materials and energy resources that manufacturers need, the BRI aims to deliver finished products at the lowest cost. In time, this approach may help China reach a dominant position in world trade.[7]

As of 2021, 140 countries had signed a Memorandum of Understanding (MoU) with China regarding the BRI, including 46 African, 37 Asian, 11 Pacific, and 27

Figure 2 - Countries in China's BRI



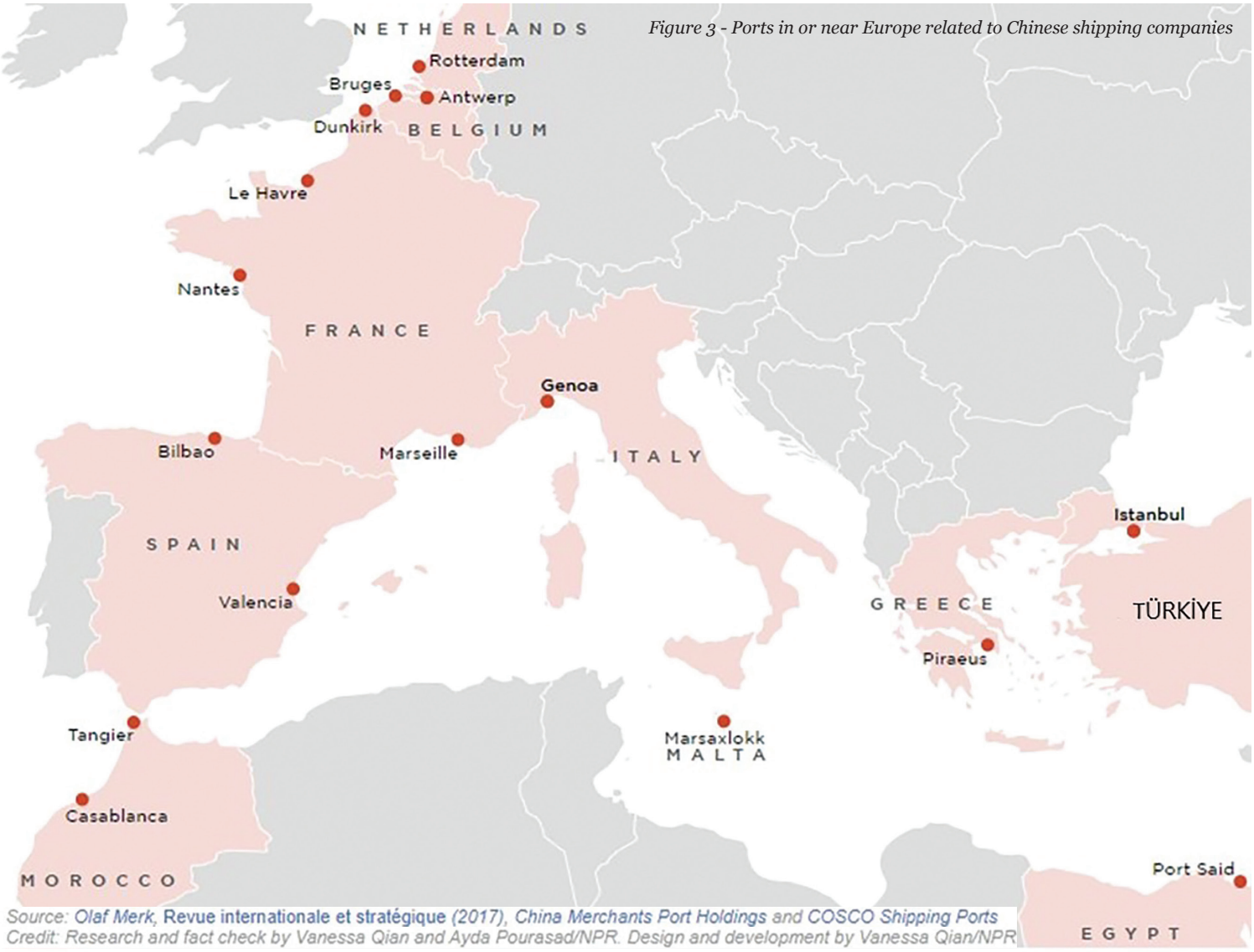


Figure 3 - Ports in or near Europe related to Chinese shipping companies

European countries.[8] With 20 Latin American and Caribbean countries also signing on, the scope has evolved beyond the historical Silk Road.

China's national interests for this project are ensuring trade continuity, increasing its global sphere of influence, and creating economic dependency for political purposes.[9]

Figures 3 and 4 show the commercial ports in which China Merchants Port (CM Port) Holdings and China Ocean Shipping Company (COSCO) Shipping Port (part of a Chinese state-owned multinational conglomerate) have economic interests.

Situation In The Mediterranean

To provide an idea of Chinese expansion in the European area and its subsequent influence on the region, the following paragraphs detail three ports in the Mediterranean which will be relevant for NATO nations:

Port Said

Egypt's Port Said is the main port terminal bridging African and European trade. Its location, notable as a stronghold at the mouth of the Suez Canal and chokepoint to the Mediterranean, increases its geostrategic importance given that 30% of all global container traffic passes through the Canal.[10] For Port Said, approximately 3,000 vessels visit annually, bringing 10,700,000 tons of cargo, 1,000,000 TEU and 271,450 passengers.[11] Container capacity is expected to increase further in coming years.[12] COSCO currently has a 20% share in the port, which is maintained as a government organization under the operation of the Port Said Port Authority (PSPA).[13]

Istanbul-Ambarlı

The port of Istanbul-Ambarlı is important given its location as a gateway between Europe and Asia. In Ambarlı, COSCO and CM Port own major shares (Figure 4 - 52% in total), while the private Turkish national companies Altas, Marport and Mardas operate the port.[14] It has improved its efficiency over the last few years, handling 9.6 million tons of cargo from January through June 2022.[15] Its unique chokepoint location is vital for access to Black Sea trade lines via the Istanbul Strait.

Piraeus

COSCO owns 100% of the shares in the port of Piraeus, the largest in Greece. Due to its close proximity

to the European mainland and as another gateway to Europe from the Mediterranean, it has significant importance for China.[16] The volume of cargo passing through the port increased from 3.7 to 5.4 million containers from 2016 to 2020.[17] Being the biggest port in Greece, Piraeus plays a critical role in international trade and is a hub that connects mainland Greece with the islands. It is also a major passenger and international cruise center in the Mediterranean region.[18]

According to the share figures in Figure 4, one can assume that China has a significant influence over trade in a number of Mediterranean Ports and is increasingly using its "soft" economic power to gain influence in the region. If this influence remains stable, it is beneficial for China and, at least in the short-term, the port-owning country.

Points of importance and possible implications

China's port acquisitions throughout the Mediterranean may well have potential benefits for the host nation. Investment may serve to accelerate economic growth for developing and modernizing countries. Indeed, many trading nations might benefit from synchronizing and increasing their trade volume with China, ostensibly in line with strategic goals and properly planned economic road maps. However, as an increasing number of ports fall under the partial or full control of Chinese firms, so too do the risks associated with such a strategic competitor operating in this way in the Alliance's AOR. Ports come with their own unique challenges and a competitor may find itself able to exploit vulnerabilities with strategic effect.

Security

China's increasing influence in the Mediterranean prompts consideration of a multitude of plausible scenarios in which dominant ownership of ports by any one competitor nation might cause security concerns for NATO and partner nations. As highlighted in international news by the Huawei case, there is concern that Chinese law may be used to this end. For example, the 2017 PRC National Intelligence Law stipulates that Chinese companies must "support, assist, and cooperate with China's intelligence-gathering authorities."[19] The following list of potential security risks is by no means exhaustive, but serves to stimulate consideration:

- Port ownership may allow an "on the ground" ability to study the frequency and content of military and strategic cargo movements in and near ports, contributing to pattern of life assessments;
- Electronic warfare – units installed in ports can create technological vulnerabilities that cause national (or even NATO-wide) security breaches;
- Control of a port may allow malicious transfers of goods or equipment within the area, either conducted or assisted by port operators and escaping the eyes of customs and other security authorities;
- With an increase in the number of merchant ships from the port owning nation, consideration for the physical security of those vessels also increases. This could prompt the need for more warships or other security forces to be employed in escort duties. The follow-on effect would be an increase in maritime traffic, making it more challenging for port countries to exert control in the region and keeping security forces from participating in other missions;
- If the port is critical to NATO lines of communication, there may be supply and security concerns for advanced planning, berthing, fueling, or maintaining units. During a crisis or even an escalation in hostile rhetoric, a port owning nation could easily disrupt supply chains and support efforts in the region.

PORT	TERMINAL(S)	PERCENT SHARE HELD BY ENTERPRISE
PIRAEUS (GREECE)	Piraeus Container Terminal	COSCO: 100%
ZEEBRUGGE (BRUGES, BELGIUM)	CSP Zeebrugge Terminals NV	COSCO: 85%
VALENCIA (SPAIN)	Noatum Container Terminal	COSCO: 51%
CASABLANCA (MOROCCO)	Somaport	CMPort: 49%
DUNKIRK (FRANCE)	Terminal des Flandres	CMPort: 45%
VADO LIGURE (GENOA, ITALY)	Vado Reefer Terminal	COSCO: 40%
		QPI: 10%
BILBAO (SPAIN)	Noatum Container Terminal	COSCO: 40%
ROTTERDAM (NETHERLANDS)	Euromax Terminal	COSCO: 35%
AMBARLI (ISTANBUL)	Kumport	COSCO: 26%
		CMPort: 26%
LE HAVRE (FRANCE)	Terminal Nord, Terminal de France	CMPort: 25%
MARSAXLOKK (MALTA)	Malta Freeport Terminal	CMPort: 25%
MARSEILLE FOS (MARSEILLE, FRANCE)	Eurofos	CMPort: 25%
NANTES (FRANCE)	Terminal du Grand Ouest	CMPort: 25%
ANTWERP (BELGIUM)	Antwerp Gateway	COSCO: 20%
		CMPort: 5%
PORT SAID (EGYPT)	Suez Canal Container Terminal	COSCO: 20%
TANGER MED (TANGIER, MOROCCO)	Eurogate Tanger	CMPort: 20%

Notes

Data for COSCO are from a combination of COSCO's map of overseas terminals and press releases, both last accessed on Sept. 12, 2018. Excluding data for Kumport in the Port of Ambarli, data for CMPort are from CMPort's 2017 Annual Report and Olaf Merk's paper, *Geopolitics and Commercial Seaports*. Details for CMPort's share in Kumport are from COSCO's press release on the investment. Information on QPI's percent stake in the Vado Reefer Terminal is from a press release issued by APM Terminals, a member in the Vado venture.

Source: Olaf Merk, Revue internationale et stratégique (2017), China Merchants Port Holdings and COSCO Shipping Ports
Credit: Research and fact check by Vanessa Qian and Ayda Pourasad/NPR. Design and development by Vanessa Qian/NPR

Economy

China has made the economic impacts of the BRI very clear as it relates to the potential for growth, not just for itself, but for participating nations. With economic ties, comes influence and, as it currently stands, China is competing with NATO members to seek increased advantage. A host country may be at risk of increased industrial espionage[20] achieved through "owner" access to data such as schedules,

cargo and vessel types. If security policies are not well planned, a host country that runs afoul of China could quickly face economic sanctions[21] that may lead to foreign dependency.[22] The following lists some of the actions China could take in a time of increased tension that would have economic impacts to NATO and partner nations:

- Reduction or cessation of the efficiency of the port enterprise by using activities such as strike-lockouts;
- Reducing the efficiency of the port, or stopping operations altogether as a result of "accidents";
- Extending the time for maintenance or expansion of the port;
- Under-pricing to reduce competition. It is possible to ensure that a port becomes preferred over other ports of the country, thus creating a monopoly and putting pressure on the economies of other nations across the region;
- Should conditions change and a country wish to regain control of a port, it may face serious sanctions from China in maritime trade or other areas.

Social and Societal Considerations

External influence can have a societal impact on nations, including oft forgotten second and third order effects. Some of the possible effects on a population are as follows:

- Chinese authority and investments in ports often includes the stipulation to use its workforce in a variety of capacities. The number of non-native workers employed at the ports can be considered a loss from the labor force of the port owner country;
- The effects of foreign workers on the demographics of the port region, albeit at a low level, could result in cultural or political challenges;
- Increasingly successful and large enterprises, such as ports, tend to raise the prices of local economies, pricing out some inhabitants and causing friction;
- China will have the ability to influence nations and the public, ultimately leading to a more sympathetic international community.

Analysis

China is aggressively pursuing economic policies in order to gain and preserve its burgeoning economic power.[23] The velocity of this growth is reflected in the saying: "A pause will be a regression." China supports infrastructure development activities beyond its own borders, especially in countries on trade lines with Europe and Africa. It also provides financing with loans at initially favorable terms, using its economic strength and massive workforce to gain influence in several nations.

Over time, China has created a robust maritime trade fleet to distribute its commodities to world markets and transport the raw materials necessary for production of these commodities. In addition to the presence of a naval base in Djibouti (ostensibly in the fight against international maritime piracy), NATO can logically expect to see an increase in the number of Chinese military vessels within NATO's traditional area of operations. Such vessels will be deployed to secure sea lines of communication and provide assurance for Chinese global commercial fleets.

There has also been an increase in Chinese-Russian close military coordination in recent years, with several bilateral naval exercises conducted since 2012.[24] One need only refer to the combined exercise Naval Interaction (Joint Sea) 2015, held in the Mediterranean, for a demonstration of how both countries continue to seek opportunities to increase their influence on the world stage. These activities have abated somewhat since the advent of the war in the Ukraine; however, China continues to present a regional military challenge in addition to a global economic force.[25]

Although the management of worldwide port operations by Chinese companies may not be an overt threat, such ownership and management provides access and insight that may be valuable in intelligence terms. In addition, electronic surveillance risks merit attention. Since the US government has already assessed that Huawei 5G technology presents an intolerable security risk, similar vulnerabilities will need to be mitigated in ports.[26]

The Russia-Ukraine conflict has disrupted the planned land routes of the BRI and logically the safe passage of trade is shifting to sea routes. Consequently, the rising importance and density of maritime routes will drive an increase in maritime security needs. More ships at sea, including those charged with providing security, will cause more concern over maritime routes, especially in the relatively congested waters of the Mediterranean.

Conclusion

During the Cold War period, strict borders and the limits of a pre-globalization world economy allowed two opposing ideologies to exist as largely independent blocks in a bi-polar world. Now borders are more permeable thanks to advances in technology, economic links, and social demands, creating a global village. The algorithm of life has started to change rapidly in a fundamental way, as people travel and interact more than in the past. Whereas there are great benefits to a more connected world, there will also be frictions, intensifying the effects of existing or emerging problems.

Increasing Chinese global influence is a complex issue that many nations are now grappling with and, at first glance, the issue would seem to be mainly related to economics. In that vein, commerce remains a necessary path and a vital link, as it has been for hundreds of years. Throughout history, ports have

been the most important and subsequently vulnerable points of interest for commerce and national prosperity. Port-owning nations are intrinsically linked to the world market and arguably enjoy greater benefits overall. Their economies are often more secure and they can exert more influence over nations dependent on their ports. Issues arise when foreign states begin to own, or partially own, ports that are geographically situated in other states. Such is the case multiple times over with China in the Mediterranean.

Based on the examples provided, Chinese ownership of European ports is already considerable, allowing for a significant advantage in reaching European markets. As those Chinese-owned ports increase capacity, that market share may also increase. The limits of these influences need to be well understood and Allied nations must find an optimum balance point between delivering economic benefits to guarantee the welfare of its citizens and managing maritime/national security. Chinese soft power can create economic pressures that may influence politics and challenge NATO's resilience.

As for NATO, it must remain steadfast in its resolve to protect its one billion citizens, defend NATO territory, and safeguard democratic values. It is important to remember that the Alliance is not exclusively a military pact. NATO's purpose is to guarantee the freedom and security of its members through economic, political and military means. "NATO promotes democratic values and enables members to consult and cooperate on defense and security-related issues to solve problems, build trust and, in the long run, prevent conflict."[27] Recognizing and understanding the potential threats associated with Chinese-owned (or partially owned) ports in the NATO area of operations is fundamental. Even more important is the need for NATO to have plans in place should relations with China deteriorate, including determining how to deliver continuity of trade with minimal disruption. Individual countries should already have these plans in place, but they may require assistance. In order to secure prosperity, the Alliance must be able to better support allied nations' interests, countering the ability for China to erode those norms. The future of our various cultures, our collective security and our prosperity may very well depend on it.

Endnotes

1 National Geographic." First Rulers of the Mediterranean." Accessed March 7,2023. https://education.nationalgeographic.org/resource/first-rulers-mediterranean

2 Silk Road. "Marco Polo and his travels." Accessed March 8, 2023. http://www.silk-road.com/artl/marcopolo.shtml/

3 Eurostat." China-EU - international trade in goods statistics." Accessed March 7, 2023. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=China-EU_-_international_trade_in_goods_statistics

4 BBC." China overtakes US as EU's biggest trading partner." February 17, 2021. https://www.bbc.com/news/business-56093378

5 West, Darrell M. "Six ways to improve global supply chains." July 12, 2022. https://www.brookings.edu/research/six-ways-to-improve-global-supply-chains/

6 De Decker, Victor. "THE GEOECONOMICS BEHIND THEBELT AND ROAD INITIATIVEHOW THE BRI IS SHAPING A NEW GEOECONOMIC ORDER." Accessed March 7, 2023. https://libstore.ugent.be/fulltxt/RUG01/002/509/652/RUG01-002509652_2018_0001_AC.pdf

7 Dollar, David. "Reluctant player: China's approach to international economic institutions." September 14, 2020. https://www.brookings.edu/articles/reluctant-player-chinas-approach-to-international-economic-institutions/

8 Ye, Min. "Ten Years of the Belt and Road: Reflections and Recent Trends." Accessed March 8, 2023. https://www.bu.edu/gdp/2022/09/06/ten-years-of-the-belt-and-road-reflections-and-recent-trends/

9 Chhabra, Tarun; Doshi, Rush; Hass, Ryan; Kimball, Emilie. "Global China: Regional influence and strategy." July, 2020. https://www.brookings.edu/research/global-china-regional-influence-and-strategy/

10 New Zealand Foreign Affairs & Trade. "The Importance of the Suez Canal to Global Trade." April 18, 2021. https://www.mfat.govt.nz/en/trade/mfat-market-reports/market-reports-middle-east/the-importance-of-the-suez-canal-to-global-trade-18-april-2021/

11 Shipnext. "PORT SAID (EGYPT)." Accessed March 8, 2023. https://shipnext.com/port/port-said-egpsd-egy

12 Shaw-Smith, Peter. "Egypt ports to nearly double container capacity by 2024." September 19, 2022. https://www.joc.com/port-news/international-ports/egypt-ports-nearly-double-container-capacity-2024_20220919.html

13 Craft. "Port Said Port Authority." Accessed March 8, 2023. https://craft.co/port-said-port-authority

14 World Port Source. "Port of Ambarli." Accessed March 8, 2023. http://www.worldportsource.com/ports/commerce/TUR_Port_of_Ambarli_2079.php

15 Silk Road Briefing. "Turkiye's Europe-Asia Ambarli Port H1 2022 Transit Cargo Shipping Up." July 20, 2022. https://www.silkroadbriefing.com/news/2022/07/20/turkiyes-europe-asia-ambarli-port-h1-2022-transit-cargo-shipping-up/

16 MINISTRY OF COMMERCE PEOPLE'S REPUBLIC OF CHINA. " The Myth of the Port of Piraeus." Accessed March 8, 2023. http://www.mofcom.gov.cn/article/beltandroad/gr/enindex.shtml

17 Moverdb.com. "Top 49 Biggest & Busiest Container Ports In 2023." Accessed March 8, 2023. https://moverdb.com/top-49-container-ports/

18 World Port Source. "Port of Piraeus." Accessed March 8, 2023 http://www.worldportsource.com/ports/commerce/GRC_Port_of_Piraeus_1041.php

19 https://www.cfr.org/backgrounder/chinas-huawei-threat-us-national-security#:~:text=The%202017%20National%20Intelligence%20Law%20%5BPDF%5D%20declared%20that,could%20share%20user%20data%20with%20the%20Chinese%20government

20 Hvistendahl, Mara. "THE OLDEST GAME The very long history of industrial espionage." April 27, 2019. https://foreignpolicy.com/2019/04/27/the-oldest-game-industrial-espionage-timeline/

21 Farrell, Henry. "The Modern History of Economic Sanctions." March 1, 2022. https://www.lawfareblog.com/modern-history-economic-sanctions

22 McKenna, Amy. "foreign dependency economics and politics." February 27, 2023. https://www.britannica.com/topic/foreign-dependency

23 Kim, Patricia M.; Pita, Adrianna. "What does Xi Jinping's power move mean for China?" October 25, 2022. https://www.brookings.edu/podcast-episode/what-does-xi-jinpings-power-move-mean-for-china/

24 Weitz, Richard. "Assessing Chinese-Russian Military Exercises: Past Progress and Future Trends." July 9, 2021. https://www.csis.org/analysis/assessing-chinese-russian-military-exercises-past-progress-and-future-trends

25 Dobbins, James; Shatz, Howard J.; Wyne, Ali. "Russia Is a Rogue, Not a Peer; China Is a Peer, Not a Rogue." Accessed March 8, 2023. https://www.rand.org/pubs/perspectives/PE310.html

26 Reed, Betsy. "Huawei can prosper despite US sanctions, says board member Catherine Chen says Chinese telecoms firm will use technical expertise to reach new markets less dependent on the US." Accessed March 8, 2023. https://www.theguardian.com/technology/2021/sep/01/huawei-can-prosper-despite-us-sanctions-says-board-member

27 NATO. "What is NATO?" Accessed March 8, 2023. https://www.nato.int/nato-welcome/index.html

Hypersonic Weapons and How They Fit into the Battlefield

CDR (USN) Matt Cady

The X-51A Waverider in hypersonic flight powered by a Pratt & Whitney Rocketdyne SJY61 scramjet engine. Courtesy of US Air Force.

For much of the world, the first time hypersonic weapons were thought of might have been on March 19th, 2022, when CNN reported, "US officials confirm Russia has used hypersonic missiles against Ukraine." Iskander and Kinzhal may have then become the scariest words and thoughts to the informed citizen. The question is: "Where do hypersonic weapons fit into the military landscape?" The utility of hypersonic weapons probably falls somewhere between the development of the atomic bomb and the next three consecutive versions of the US Navy Working Uniform (sure to be released, made mandatory, and become obsolete over the next 18 months). Where on the sliding scale of innovation do hypersonic weapons fall? Are all hypersonic weapons created equal? Should NATO start working on the next series of "Duck and Cover" videos to show in elementary schools around the world?

HIADS: What Are They?

Referring to the new capabilities of these missiles as simply "hypersonic weapons" does not adequately define these weapons, nor does it properly frame the discussion surrounding them. Conversely, ICBMs,[1] bunker busters, cruise missiles, and semi-active radar are all terms that more accurately describe the way those particular weapons operate and better facilitate conversations based on those capabilities. Moreover, ICBMs travel at hypersonic speeds, but are not termed as hypersonic weapons.

In an effort to better define "hypersonic weapons," this author recommends a re-branding. Hypersonic Intra-Atmosphere Delivery Systems: "HIADS" properly frames the discussion and could be used to further categorize follow-on specific attributes for the weapons. HIADS-C would be cruise-type missiles, while HIADS-G would be glide weapons. Identification of a nuclear tipped hypersonic cruise weapon could be HIADS-CN. The broad term "hypersonic weapons" does little to help discussions and likely only serves to further confuse this important topic.

Why Read this Article?

Most of the information on the internet will lead you in one of two directions: 1. A scientific article, which discusses design characteristics using modeling and simulation, not offering any information relevant to the military or 2. An opinion article, generalizing about the devastating potential of hypersonic weapons and how HIADS must be banned or controlled before they change everything about military defense.

This article is neither of these; indeed, it seeks to offer some background, but it should ultimately move to offer perspectives that have not been considered and propose recommendations for high-level decision making.

What is Hypersonic?

The term is easier to define than it is to create, produce, or employ. Hypersonic simply means "exceeding sonic speed," or five times the speed of sound (Mach 5). Setting aside the details of temperature, density, the coefficient of stiffness, standard day, and details regarding the speed of sound away from the

> ***People fear what they don't understand and hate what they can't conquer. -Andrew Smith***

surface of the earth, Mach 1 is approximately 761.2 mph (1,225 km/h) and hypersonic is anything more than 3,806 mph (6,125 km/h).

Aside from the general definition, it is important to understand that the nations working on HIADS have not been targeting Mach 5. Most nations have been seeking speeds for these weapons closer to Mach 10, or about 7,600 mph (12,250 km/h). Based on that design goal, any calculations or examples in this article will use the Mach 10 target, vice the Mach 5 definition.

Bullet AND Bomb

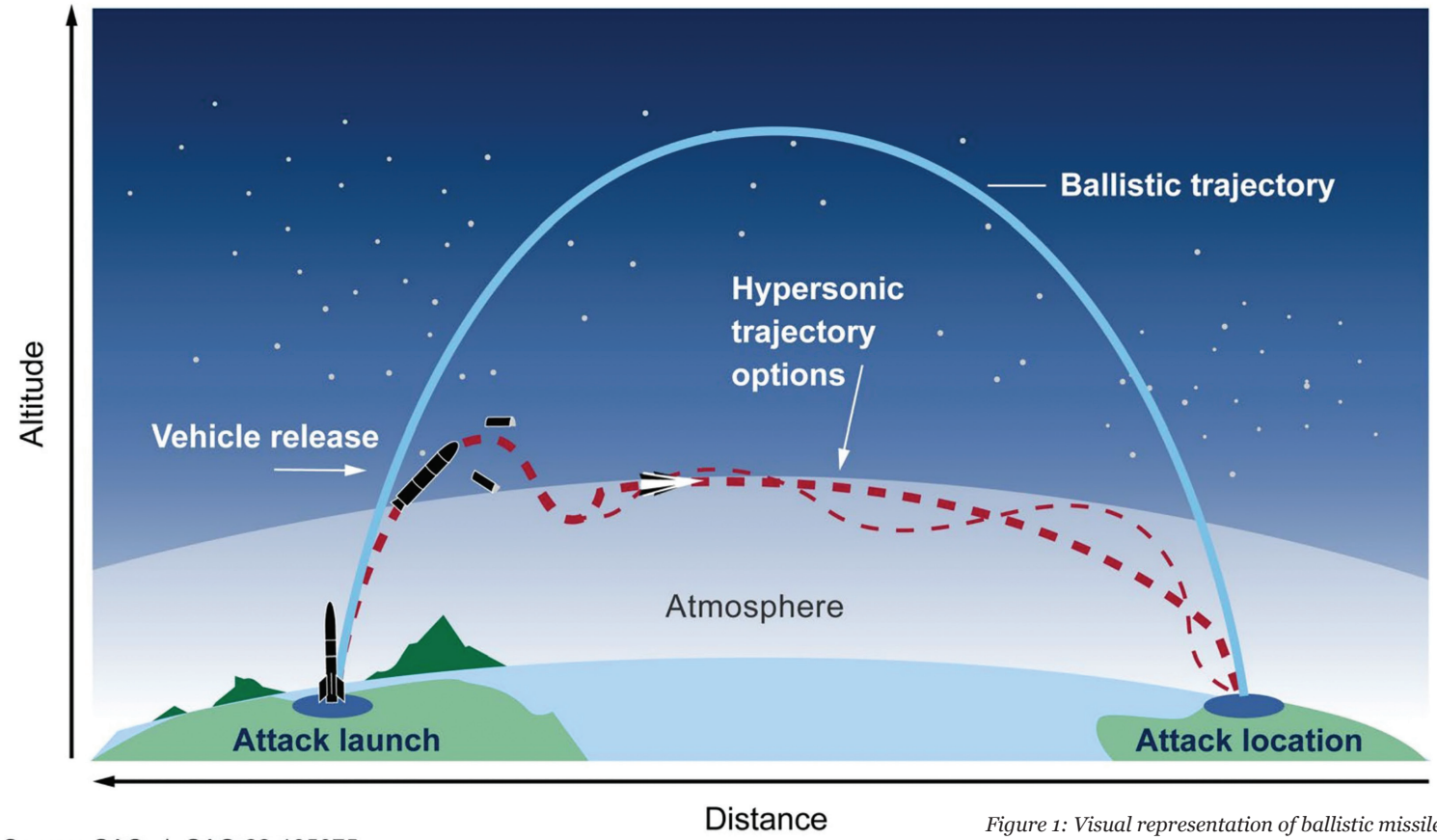
HIADS offer more than just a vehicle for delivering a payload, combining the kinetic energy of a bullet with the power of a traditional explosive weapon. Much like traditional air-dropped bombs,[2] hypersonic vehicles may be another option to deliver tritonal[3] explosives to the forehead of the enemy.

The key difference between hypersonics and most traditional delivery weapons is the kinetic energy provided by the speed with which the payload is delivered. A hypersonic vehicle (read: "weapon"), much like a bullet, does not necessarily need a warhead to prosecute the target. Below is a numerical comparison of different types of weapons and the approximate "energy"[4] transferred to the target:

9mm bullet[5] =	0.000481 MJ/MN
1 stick of dynamite =	1.0 MJ/MN
1 kg TNT =	4.184 MJ/MN
AGM-84 Harpoon missile[6]=	885 MJ/MN
2,000lb explosive free fall bomb[7] =	3,861 MJ/MN
"No Payload" HIADS[8] =	**11,765 MJ/MN**
MOAB GBU-43[9] =	43,000 MJ/MN
Hiroshima bomb[10] =	60,000,000 MJ/MN

These are not "apples-to-apples" comparisons but serve to express the amount of kinetic energy potential for a hypersonic weapon. The same calculations could be made by 20 different people and result in 40 different numerical values.

As you can see in the above representative values, a hypersonic delivery vehicle without an explosive warhead has the energy somewhere between a 2,000lb free-fall bomb and the GBU-43 (generally accepted as the largest non-nuclear conventional weapon employed by a NATO member). HIADS do not have radioactive fallout concerns[11] and are generally a one-for-one comparison to other conventional weapons. HIADS offer a potent energy release at impact, but they are not going to end a civilization. However, they will cost substantially more to produce, maintain and employ.



Source: GAO. | GAO-22-105075

Figure 1: Visual representation of ballistic missiles, hypersonic glide vehicles, and cruise missiles

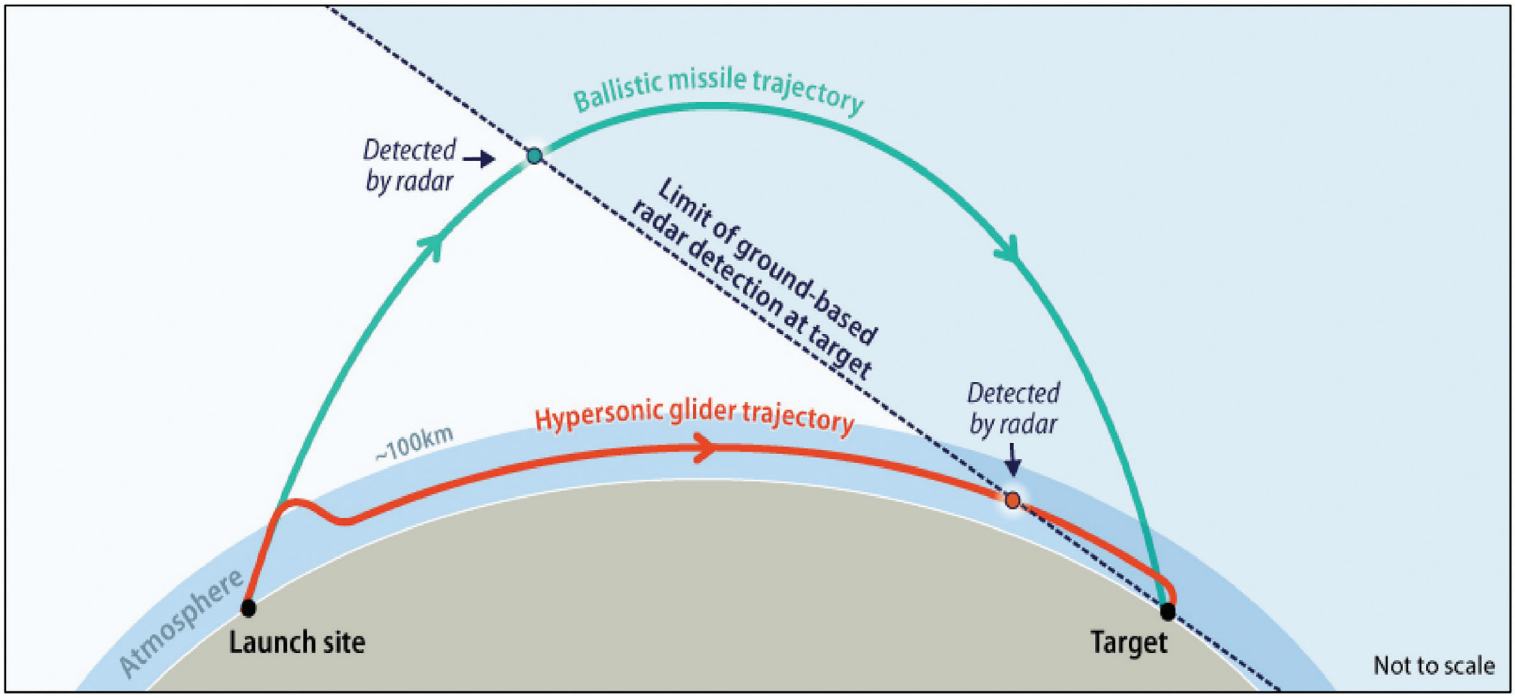


Figure 2: Terrestrial-Based Detection of Ballistic Missiles vs. Hypersonic Glide Vehicles (Source: Library of Congress, Congressional Research Service, 10 Jan 2023, R45811)

Fastest Weapons Ever Created!...?

False. The truth about these delivery systems is that they are not actually faster than weapons the world has been employing since the beginning of the Cold War. ICBMs, which also have a re-entry speed of greater than Mach 5 (usually greater than Mach 15), are faster as a delivery system.[12] The key difference is not actually the speed of HIADS, but much more important is the environment and behavior of these weapons.

Figure 1 is a graphic which represents the different flight paths of an ICBM, a HIADS-G, and a HIADS-C. The picture is not to scale, but represents the profile differences between launch and impact for each of the three delivery methods. Over the past years, NATO (and our adversaries) have been able to develop detection and engagement tactics which quell the hysteria of "unstoppable weapons." However, HIADS are new, and the excitement is still high.

HIADS: Too Hot to Handle

Hypersonic speeds of Mach 10 and greater yield operating temperatures of roughly 3,000-5,000 degrees F (approximately 2,000-2,800 degrees C). The SR-71,[13] the famous US high-speed reconnaissance aircraft, was mostly constructed of titanium to combat the heat experienced at its operating speeds. Titanium has an operating temperature of roughly 842 F (450 C) and a melting temperature of 3,034 F (1,668 C); it is not going to work for HIADS. In response, ultra-high temperature ceramics (UHTCs), such as hafnium carbide (HfC), tantalum carbide (TaC), or woven silicon carbide (SiC) ceramic composites are being used to manage the higher operating temperatures. Even greater heat issues arise when any surface variances occur such as changing shape to control direction. This not only stresses the control surfaces, but also requires even greater heat protection throughout the vehicle design.

The natural rebuttal to this would be that ICBMs endure equally as great of heat along with speeds exceeding hypersonic speed. The difference is that the ICBMs are large vehicles that are purposely built to deliver a ballistic payload. Size and shape were secondary concerns. The size and shape are what make HIADS capable of the speeds they seek to achieve. There may not be enough space in HIADS to dissipate the heat and protect the payload (i.e. inadvertent explosion during flight maneuvers).

Why the Militaries Care: OODA Loop Issues

Observe, Orient, Decide, Act, (and Feedback) also known as the OODA Loop, first introduced by US Air Force Colonel John Boyd, is a widely accepted way to describe the process of remaining agile in a military situation which requires action.

HIADS', particularly HIADS-C, high level of speed at lower altitudes significantly reduces the detection, or observation, range of a ground-based line-of-sight radar system. Reducing the detection range compresses the response time for those being targeted. In many cases, this shortened timeline will not be something that a current line-of-sight ground or surface-based radar-operator team can respond to. This is unlike an ICBM which, despite its higher speeds, has substantially more manageable detection ranges for defense. Figure 2 is a representation of radar detection range differences between ICBM and hypersonic glide weapons.

Physics to the Rescue

Detection. Thankfully, traditional line-of-sight radar is not the only system available to help in defending against HIADs - some general detection and tracking solutions

may actually come from the temperatures produced at hypersonic speeds. With operating temperatures between 3,000 and 5,000 F (1,600-2,800 C), the hypersonic vehicles will bloom on any infrared (IR) detection system. An average thermal imager from your local hunting supply store has the thermal sensitivity to detect a difference between the background and an object's temperatures as low as 0.01 degrees Celsius. It stands to reason that hypersonics could be detected or tracked based on their significant temperature difference from the atmosphere they operate in. Perhaps the same technology that NASA uses to detect wildfires across the globe would play a role here.[14] Especially considering the limited employment of hypersonics, it may be possible to have dedicated IR tracking of launch systems.

Stability. In addition to the detection of differences between hypersonic vehicles and their environments, high temperatures also drive a variety of design issues for this technology. It is difficult to design a vehicle that will: 1. Sustain flight at hypersonic speeds, 2. Maneuver enroute, and 3. Not ignite its payload in the process.

The most common explosives used in employable weapons are some version of tritonal which has a flash point of about 300 degrees Celsius. The HIADs vehicle would need to reduce the external operating temperatures by approximately 2000 degrees Celsius from the skin of the HIADS to the payload with insulation sustained over the flight-time of the weapon. Sparing the thermodynamic calculations of stepping down the temperature, it is important to remember that insulation relies heavily on space, air, and unique materials. This may be surmountable by using a vacuum area (which has a zero value for thermal conductivity) to insulate the explosive, but such a vacuum would, of course, create its own physical challenges.

Accuracy. In addition to the significant challenges of speed-induced heat, maneuvering at hypersonic speeds causes serious issues for navigation and accuracy. Unlike ballistic missiles that reach their target with a largely vertical trajectory, HIADS will approach primarily in the horizontal plane. With speed acting mostly in the horizontal plane, a slight adjustment in trajectory inherently creates a significant opportunity for target inaccuracies, including overshoots or undershoots, essentially increasing the error ellipse.

Ban, Curtail, or Race to Employ?

The real question that NATO must address regarding HIADS, is what to do about them? In September 2022, a NATO forum discussed HIADS in relation to air and missile defense. During the meetings, presenters discussed the speed of HIADS and the defensive challenges of protecting against those weapons. It took approximately 3.5 minutes for an audience-member in that multi-national forum to suggest that NATO should consider banning all HIADS. The head nods came all too quickly.

Could there be a ban on something that both allies and adversaries are investing in? In theory the answer is yes, but should there be? Would HIADS be banned because they are significantly more devastating than weapons already in existence? More explosive, more deadly? No. Ultimately, it's not about banning a payload, but a delivery system. The reason for banning the delivery system is simply because Allies cannot readily defend against that delivery system through conventional means.

As alluded to above, another option might be to curtail the employment of HIADS, possibly limiting their employment to certain payload or warhead types. Isn't there already a ban on biological weapons and controls on nuclear weapons? One might ask whether or not the threat of sanctions is working on nations that care little about their people or how they are affected? As with most things, laws have the greatest effect on law-abiding parties. Nations that do not traditionally follow international weapons bans, environmental regulations, or human-rights laws are not likely to accept regulations on HIADS. HIADS development is a reality; the law-abiding nations can choose to accept that fact and work through increasing effective defenses or spend years in debate within the chambers of various international organizations. Those same organizations might have tried to ban the atlatl, archery, or even the sling given the opportunity. Ingenuity and determination have overcome insurmountable threats in the past. Are HIADS any different?

Endnotes

1 Intercontinental Ballistic Missiles

2 MK-80 is the series of 500lb explosive casing that can be configured a variety of ways to prosecute different types of targets.

3 Does not infer that hypersonic use the explosive tritonal, nor that tritonal would be stable at the associated speeds and temperature extremes.

4 Kinetic energy is not directly comparable to explosive force. This unit of power is used to compare kinetic and explosive weapons.

5 Average velocity of ~1,180 ft/s (380 m/s), 115 grain, 7.45 gram ammunition high velocity round.

6 ~500lb warhead, total weight ~1,500lbs and travels at 537 mph. Value obtained by combining power or kinetic and explosive values.

7 The Mark 84, 2,000 lb (907 kg), filled with 945 lb (429 kg) of tritonal high explosive. Tritonal explosive energy rating of 9 MJ/kg.

8 Kinzhal, weight of approximately 2,000kg total, using theoretical Mach 10 (~3,430 m/s) speed.

9 GBU-43/B Massive Ordnance Air Blast

10 Scientifically accepted standard measure representing the explosive power from the original explosion during World War II.

11 Assuming the hypersonic is not loaded with a nuclear warhead.

12 ICBMs have consistently been tested and operated in excess of 15,000 mph, while hypersonics are identified as 3,800 mph (Mach 5) and designed to operate at approximately 7,600 mph (Mach 10).

13 The SR-71 Blackbird maximum recorded speed, according to NASA, is approximately 2,220 mph (greater than Mach 3 at 85,000 ft). The SR-71 experienced between 315-480 degrees Celsius (600-900 degrees Fahrenheit).

14 (https://www.nasa.gov/mission_pages/fires/main/missions/index.html) Several of NASA's instruments use infrared technology to detect fires across the globe. NASA is often the first to detect fires in remote areas and will use this data to aid disaster response efforts around the world.

The Russian – Ukrainian Maritime War

CDR (HN) Ioannis Stamoutsos

The Ukrainian armored boat "Ackerman" (U-175) is the key to the defense of the coast of Mariupol. Courtesy of Ukraine Ministry of Defense.

From ancient valour to modern fighter

Warfare is as old as human history. As the famous ancient Greek philosopher Aristotle once said, "War is a school for virtue,"[1] meaning that during battle, the fighter, through courageous actions, was achieving the realization of virtue. Modern warfare though, in the form of unmanned systems, is driving us far away from Aristotle's wisdom.

Every war claims new technological achievements, developments in tactics, doctrines, and innovation in the way that battle is waged. The same applies to the current unlawful Russian invasion in Ukraine that ended a 77-year-old standing peace on European soil.

This article will try to shed light on several aspects of the naval confrontation between Russia and Ukraine in the Black Sea Region,[2] a confrontation that may change the way we think about the conduct of naval conflicts between seemingly mismatched adversaries from now on.

Unequal adversaries in the Black Sea region – Russian dominance

Russia's so-called "special operation" started on February 22, 2022, and directly focused attention on the land and air warfare domains in the first instance. But the war was not just limited to air and land actions; important and notable flashpoints subsequently also occurred in the Black Sea region, where the Russian Navy was expected to enjoy complete dominance.

By the time Türkiye closed the Straits to Russian naval forces, Russia had assembled all the naval units needed to conduct operations across the entire spectrum of maritime warfare. However, while those forces were conducting operations at sea with seemingly no blue water capable adversary in the area, allied (NATO) units were conducting Maritime Intelligence Surveillance and Reconnaissance (MISR)[3] operations, monitoring at a safe distance and obtaining valuable information about the movements of the Russian Navy units, their tactics and their electromagnetic emissions. It is widely recognized that Ukraine was receiving all relevant intelligence from an array of bilateral level synergies.

> ***The American Civil War introduced armor, pivoting gun turrets, and bowsprits to naval warfare. Crimean war sea mines and Sino-Japanese war torpedoes. Now the war in Ukraine clearly brings unmanned [weapons] to an inseparable part of naval warfare.***
>
> ***Commander of the "Suomenlinna" Ukraine Coastal Regiment -Ville Vänskä***

The Black Sea maritime battlespace

Before analyzing the major maritime events, it is essential to stress the following:

- The Black Sea is a closed maritime area with one choke point controlled by Türkiye, under the provisions of the Montreux Convention, regarding the regime of the Straits.
- From the beginning of the war, the Russian Navy was able to project power to the Ukrainian coast of the Black Sea with amphibious operations. It was also able to support land domain operations into the interior of Ukraine with long-range missiles launched from both surface vessels and submarines.
- The Russian blockade and initial attacks on numerous merchant vessels had multiple objectives. It was meant to cripple maritime exports from Ukrainian ports (and respectively cripple the Ukrainian economy) and to reduce the density of maritime traffic in the area.
- Capturing Odessa and Mykolaiv, Russia would effectively turn Ukraine from a coastal state into an enclosed one, seizing its Exclusive Economic Zone (EEZ) and increasing its control over the region.
- Major Russian naval bases (Sevastopol and Novorossiysk) were out of reach of Ukrainian weapons. Sevastopol serves as the main naval base of the Russian Navy in warm waters in the southwest frontiers of Russia, enabling power projection into the Mediterranean Sea.
- NATO and allied nations assisted Ukraine with MISR operations from the beginning of the war, obtaining far better situational awareness of Russian movements and actions.

The geography of the maritime area. Sevastopol (Crimea) is the main Naval Base for the Russian Black Sea Fleet. (Source: NATO)

Area denial of the Ukrainian South Coast

Laying sea mines near the Odessa port was the first measure from Ukraine to protect its southern coast from an amphibious operation. This first act of area denial made the maritime area south of Odessa a dangerous place to all vessels, especially the Russian amphibious fleet.

Ukraine's second step towards reducing the threat from a future amphibious operation was the attack on the Russian Amphibious Vessel, LST Orsk (March 24, 2022) at Berdyansk Port (in the Azov Sea), as well as two Ropucha-class landing ships,[4] while all three vessels were alongside piers. This strike, inside a Russian controlled port, marked the first loss for Russia's Black's Sea fleet and made an amphibious assault in Odessa less likely.

Photo No 1 This satellite picture shows the damage to LST Orsk inside Berdyansk Harbor in Sea of Azov. (Source: No1: "Satellite image ©2022 Maxar Technologies", USNI news (H.I. Sutton 25 March 2022)

The hit on Moskva – Area Denial in Northwest Black Sea

The sinking of Black Sea Fleet Flagship Cruiser Moskva (April 14, 2022) was one of the first military action from the Ukrainian Navy; it shocked the Russian Navy leadership and created severe political stress to the Kremlin. Two (or more) Ukrainian "Neptune" naval surface missiles from a coastal battery hit Moskva and sunk her within a couple of hours. It is believed that at the time of the strike, a TB2 "Bayraktar" UAV, flying at the firing limits of the ship's anti-aircraft missiles, was keeping Moskva's air defense personnel and some of her sensors distracted. Several factors likely added to the success of the strike on the Moskva[5] such as the older technology of the ship's sensors, crew fatigue, and overall complacency due to the routine nature of operations. There seems little doubt that the provision of critical information about the electromagnetic emissions of Moskva, its exact location (track, velocity, and course), and knowledge of the positions of other ships in the area contributed significantly to the successful attack. Acquiring such information (SIGINT/ELINT) was possible after persistent MISR operations from manned and unmanned systems for an extended period of time. This intelligence provided a detailed profile of Moskva and likely contributed to the successful hit.

The strike on Moskva was the second area denial measure taken by Ukraine, turning the northwestern part of the Black Sea into a contested area for the Russian Navy. It weakened the chances of a possible amphibious assault on Odessa. It also resulted in Ukraine's unmanned systems being able to operate more freely in the area between Odessa and Snake Island, the next focal point of this naval fight.

Makarov class frigate on fire (authenticity of the photo is pending), (Source: Twitter European OSINT @EuropeanOSINT)

The semi-submerged Moskva in flames just before sinking (Source: via social media & NDTV clip on YouTube)

Attack on Makarov – Area Denial in the West Black Sea

Less than a month later, on May 06, 2022, a strike on a modern Russian vessel (possibly the Frigate Admiral Makarov) was reported[6] in the vicinity of Snake Island, south of the Port of Odessa. The Ukrainian claimed hit (which has not been independently confirmed) seemingly had a profound effect given that the remaining anti-air warfare capable Russian warships in the vicinity subsequently moved far away from Snake Island. This action also helped provide freedom for the use of Ukrainian armed UAVs (Bayraktar TB2) against smaller Russian vessels that lacked air defense. Although unconfirmed, the effects of this attack were noticed by the Ukrainian Navy who re-captured Snake Island, marking the expulsion of the Russian Navy from the western Black Sea.

Re-capturing Snake Island

Meanwhile, the battle for re-capturing the legendary Snake Island had begun, pitting two major actors against each other - Ukraine's armed UAVs and Russian small patrol boats/landing craft. Left unprotected from air attack after the previous alleged strike on the Admiral Makarov forced the Russian Navy's capable units away from the western Black Sea, several Russian "Raptor" patrol boats were hit and likely sunk by Ukrainian TB-2 UCAVs (8th May) as well as one "Serna" class landing craft (14th May), which was probably carrying a Tor – M2 anti-aircraft system to the island.[7] Interestingly, after the Makarov incident the Russian Navy quickly tried to cover the air-defense gap with other means, like the Tor M2 system, but not before the Ukrainians executed their operations with devastating effects.[8] By June, 2022, Russian troops abandoned the small, rocky, but significant Snake Island, marking a severe blow to Moscow, and providing a real boost to Ukraine's political standing, military, morale, and the economy as well.[9]

Footage from a Serna class landing craft carrying a Tor-M2 anti-air battery just after a hit from a TB-2 UCAV. (Source: Twitter Walter Report @Walter report)

With a mixture of old tactics (mines), new assets (UCAVs), and a great influx of reliable information from the Alliance in the form of MISR, Ukraine effectively created an A2/AD environment and achieved much more than tactical success through these actions. Having regained control of Snake Island and consequently able to operate freely along the southern coast, Ukraine had again achieved the status of a coastal state. While it has not yet been able to gain sea superiority, its ability to deny Russia the use of the western Black Sea has provided Kyiv with significant benefits.[10] Its next objective is likely to further immobilize and restrict the Russian Navy to the eastern Black Sea and, if possible, force units back to their naval bases, perhaps by using blockade tactics that Corbett[11] would recognize.

Assumptions Made

Prior to the invasion, Russian maritime strategy prioritized the high north region, assuming they would have clear superiority in the Black Sea. Indeed, by capturing Crimea in 2014, Russia had secured its most important naval base in its southwest zone. By destroying or capturing the majority of the Ukrainian Navy's vessels, it assumed that the maritime aspects of the 24 February 2022 "special operation" would be easy and unchallenged.

There also wasn't evidence in the latest version of Russian maritime doctrine[12] of a serious awakening to new and emerging threat technologies. Conversely, this

is something that Ukraine clearly used in its favour, along with the recognition that Russia's Naval leaders had assumed the main bases in the Black Sea area were a safe haven for their units. By contrast, today the main Russian naval base in Sevastopol is considered vulnerable, not only because of Ukraine's increased special operations in the region or because long-range artillery has gradually become available for use, but also because, for the first time, the Russian Navy lacks the required presence. It has great difficulty creating a consistently robust recognized operational picture at sea. Additionally, now that the main air-defense assets of the Russian Navy are absent, Ukraine has a more manageable task monitoring the adversary.

Swarming Attack

Perhaps the most impressive use of these new and emerging threat technologies from Ukraine was the swarming attack from an unknown number of armed UAVs and USVs on the Russian Black Sea Fleet in the Crimean naval base of Sevastopol on the 29th of October, damaging at least one warship.[13] Russia claims that 16 unmanned systems (nine air and seven maritime) attacked the base at approximately 04:20 local time, and reported that all air drones were stopped, and only three unmanned maritime systems made it inside the bay before they were destroyed.[14] Unverified, but fascinating, footage on social media showed what appeared to be an unmanned vehicle speeding across the water toward a Russian warship. At the same time suppressing fire was fired from a Russian helicopter and surface vessel.[15]

Ukraine initially didn't deny or confirm the attack on Sevastopol, but Russia claimed that the maritime assets used in the attack departed from Odessa and used the grain corridor (typically used only for merchant vessels) to achieve an element of surprise before the strike. Not long after the attack, Russia suspended the grain export deal. Other sources claim that the first of two attack waves took Russia off guard, hitting 2 to 4 vessels. The Russian Navy then began defending itself against the second wave of attacks after sunrise.[16] These large-scale attacks marked a global first for exclusively using a synchronized saturation attack from multiple maritime unmanned systems (MUS).[17]

Regardless of the result of the attack, the lessons identified will be used to inform all future maritime conflicts and will likely be remembered as the birth of a new era concerning the use of MUS in the maritime domain.[18] As the Commander of the Finnish "Suomenlinna" Coastal Regiment Ville Vänskä said, *"A country with no operational navy has encroached over a superior enemy at its home base… The American Civil War introduced armour, pivoting gun turrets, and bowsprits to naval warfare. Crimean war sea mines and Sino-Japanese war torpedoes. Now the war in Ukraine clearly brings unmanned [weapons] to an inseparable part of naval warfare".*

A Ukrainian MUS washed up on the shores of Crimea near Sevastopol (21 Sep 22), (Source: Twitter: Tweets by Ukraine Weapons Tracker @UAWeapons)

Footage from a Ukrainian USV drone showing suppressing fire from a Russian surface ship & helicopter towards the drone (Source: Twitter: Ukraine Weapons Tracker @UAWeapons)

Land-based Loitering Munitions and Naval Units

Some days after the devastating attack in Sevastopol, a Russian loitering munition destroyed a Ukrainian patrol boat, in an unknown location. The increasing role of land-based weapons in the maritime domain is fact. As land-launched weapons make gains in accuracy, velocity, lethality, and range, it is expected that their role in maritime conflicts will steadily increase. And, as the production cost of such weapons is relatively low (often a fraction of the cost of a naval unit), it is easy to understand their desirability when such weapons are used in mass

Naval Bases – No longer a safe haven

The massive attack inside Sevastopol in Crimea had serious consequences for the Russian Navy; indeed, it acted as a cautionary tale to the entire maritime community. The attacks signaled that ports are a viable target for MUS and consequently NATO will need to develop tactics and procedures to mitigate the threat from unmanned systems. Crimea and the naval base at Sevastopol were demonstrably unsafe for Russian vessels, and subsequently almost the entire Black Sea could be considered a contested area. Indeed, the attacks highlighted that the Russian Navy had failed to secure the Black Sea and assert its dominance there, gradually losing sea control. Russian vessels are no longer safe if they remain static at sea, or even inside their secured bases.

As a result, a novel type of blockade is in effect around Sevastopol, and the Novorossiysk naval base further to the east seems to be the last shelter for the Russian navy. Recent sudden dispersals of at least ten vessels of Russia's Black Fleet from Novorossiysk naval base, on January 11th and 25th, showcase the heightened concern for an impending attack.[19]

The Adversary Strikes Back

The attack from a Russian maritime unmanned asset on the critical road-rail "Zatoka" Bridge near Odessa on February 11, 2023, marked the first strike from the adversary with MUS and shows that Moscow is increasing the use of unmanned systems as it hopes to turn the tide of war.[20] In another recent and highly provocative incident, two Russian fighter jets (Su-27) forced down a US Air Force MQ-9 "Reaper" drone over international air space in the Black Sea after damaging the propeller. The drone was conducting MISR operations in the area, flying over international waters, complying with international law and norms when it was subject to this egregious and blatant aggression. This incident marks the first time Russian and US military aircraft have come into direct contact since the beginning of the invasion and has multiple side effects.[21] The Russians, who initially stated that they didn't prefer to create tensions due to unintended incidents, later announced that their navy would try to recover the drone's wreckage.

Footage from US Air Force MQ-9 and the provocative approach of a Russian Su-27 that struck the propeller. (Source: U.S. European Command – Dvids)

Contributions to Future Maritime Warfare

The contribution of the maritime conflict in the Black Sea between Russia and Ukraine to future maritime warfare is complex and will need refining when accurate (and probably classified) information becomes available in time. However, some initial lessons can be identified and brought up for discussion as a basis for future exploitation:

- Historic operational principles from maritime strategists like T. Mahan and J. Corbett remain valid (power concentration and blockade) and, combined with new technologies (unmanned systems, artificial intelligence (AI)), can provide success on the battlefield.
- Superiority in information warfare is now the prerequisite for superiority and success at sea and on land. 24/7 MISR operations can be achieved for a prolonged period and over a large area of operations, but only with the contribution of unmanned systems on a grand scale.
- The swarming attack in Sevastopol marks the beginning of a new era. In the coming years, such attacks combined with more sophisticated unmanned systems and AI will become a nightmare to defend against.
- The use of unmanned systems creates a field of opportunity for the development and use of counter-unmanned systems. Integration & interoperability of systems, multi-domain fusion of information (from seabed to space) in the form of a cyber-centric platform with suitable AI algorithms (replacing C4I systems), processing speeds and capacities, and multi-layered air defenses are some of the countermeasures to future saturation swarming attacks.
- Relatively cheap unmanned systems, with the help of accurate information and timing, can turn near-obsolete, traditional, expensive navy platforms into useful units and have a significant impact in maritime battles, especially if used on a mass scale.
- The future of unmanned vessels (air, surface, and underwater) is already here, and we must develop the necessary doctrine and tactical procedures to use them effectively. Exercises like DYNAMIC MESSENGER and REPMUS are crucial to facilitate such efforts.
- Some failures of the Russian Navy were almost certainly due to the human errors of the Russian navy leadership. Ukrainians knew their opponent in-depth and could exploit cultural weaknesses while using their own innovative strategies versus the inflexible Russian structure and poor operating procedures.
- The Russian Navy seemed unprepared for this confrontation, and its performance seems poor. The war may not have ended, but the Russian Navy has suffered significant blows that have reduced its strength and power projection capabilities. This has limited its mobility and consequently it now operates under the risk of another significant blow in a highly contested area. It does however retain the capability to strike maritime targets of choice in the Black Sea.

Epilogue

The future maritime fighting environment is going to get dense, as we are facing an era of rapid transformation in relevant technologies that have already modernized traditional weapons and developed new ones.[22] These new and emerging threats possess lethal accuracy, supersonic velocity, stealth, rapid processing capacity, and will be equipped with AI algorithms that will replace (in a way) the human factor. Integration of AI and quantum processing will transform ever further the capabilities of future adversaries, and numbers (mass-swarming carriers) will complicate the equation of defense. Focusing on new technologies whilst remaining cognizant of the immutable constants of operational art, will help us stay ahead of any potential enemy and consequently help secure peace.

Considering all the above, when it comes to conflict like that found between Ukraine and Russia, we must comprehend the strategic importance of land-based systems ever-increasing role in future maritime operations. In this type of environment, which arguably will be more prevalent than open ocean battle, our core perception that naval units are the harbinger of power projection in all circumstances must be challenged. Ukraine and Russia have taught us that the future also lies with MISR, unmanned systems, and ingenuity, and we as allies must be prepared for it – both in offense and defence.

Endnotes

1 "War is a school for virtue" Said Greek ancient Philosopher Aristotle (384-322 bc) and by this he meant that valour exists only if the ultimate goal of courageous action has to do with the realization of virtue, that is, with the fulfillment of good. Indeed, the warrior went into battle to defend his ideals and brought the war to the ground. Here, the fighter now, along with the mutation of ideals, is not even present!

2 Ukrainian Navy assets were destroyed or seized during the 2014 Crimea annexation from Russia. The last main vessel (Frigate "Hetman Sahaidachny" U-130) was sunk by its crew in the port of Mykolaiv.

3 MISR stands for Maritime Intelligence Surveillance Reconnaissance and is vital to Information Warfare Operations. MISR is a tool for information superiority and contributes to the joint Common Operational Picture (COP). NATO countries covered Ukrainian forces' gap in such capabilities as all Allied Nations on the broader area raised their contribution in any way to assist the defending Nation (Ukraine).

4 Sutton, H I. "Satellite Images Confirm Russian Navy Landing Ship Was Sunk at Berdyansk". USNI News. March 25, 2022. https://news.usni.org/2022/03/25/satellite-images-confirm-russian-navy-landing-ship-was-sunk-at-berdyansk. Video footage of the burning ship, taken soon after the attack, shows that two Ropucha-class landing ships were also damaged. They had been berthed alongside and in front of the Alligator-class amphibious ship. They sailed away, fighting their own blazes as the fire on the Alligator raged.

5 Ktenas, Christos. "Two Greek Admirals discuss Sinking of Moskva and discrediting of Russian Navy in Ukraine. Naval Defence. May 19, 2022. https://navaldefence.gr/greek-admirals-discuss-russian-navy-performance-in-ukraine/. A fascinating insight on the factors that must take into account about the hit on the Russian Flagship, from two experienced admirals (Hellenic Navy).

6 Axe, David. "The Russian Frigate 'Admiral Makarov' Might Be The Juiciest Target In The Black Sea". Forbes. May 6, 2022. The Russian Frigate 'Admiral Makarov' Might Be The Juiciest Target In The Black Sea (forbes.com). A blurry video from a UAV shows a vessel on fire, almost stationary, with radar working. Admiral Grigorovich-class frigates with medium-range surface-to-air missiles and Kalibr cruise missiles are the most modern vessels of the Russian navy in the Area of Operation. Taking into account the absence of those vessels from the AOO after this reported hit, we might reasonably assume that, indeed, a successful strike on one of the three remaining major vessels of the class took place.

7 Radio Free Europe - Radio Liberty. "Ukrainian Military Says Drone Destroys Russian Landing Craft Near Snake Island In Black Sea". May 7, 2022. https://www.rferl.org/a/ukraine-russian-serna-landing-craft-destroyed/31838979.html. Ukraine's defense ministry said in a statement that an armed drone had destroyed a Serna-class landing craft and a missile defense system at the small island under Russian control.

8 Covering such a large maritime area to acquire information takes a lot of work. Surveillance of such a large area requires the availability of many means of surveillance with a mixture of sensors. Manned means are not sufficient and it is dangerous to use them near the area of operations, especially when the task imposes short observation distances. There, unmanned maritime systems are valuable assets.

9 Lukov Yaroslav, Kirby Paul. "Snake Island: Why Russia couldn't hold on to strategic Black Sea outcrop". BBC News. June 30, 2022. https://www.bbc.com/news/world-europe-61992491. Snake Island may be in a highly strategic part of the Black Sea and in an ideal spot for installing sophisticated missile systems. Acquiring a robust air-defense posture from the Island can be a positive factor in opening the merchant lines from Odesa port and rebooting their war-ravaged economy.

10 B.J. Armstrong, "The Russo-Ukrainian War at Sea: Retrospect and Prospect". War on the Rocks. April 21, 2022. https://warontherocks.com/2022/04/the-russo-ukrainian-war-at-sea-retrospect-and-prospect/ . Interesting article analyzes the nature of conflict in Black Sea, the ways that Russian navy pursued the essential elements of naval strategy, and how Ukraine has adapted to the conflict.

11 Julian Stafford Corbett. "Principles of Maritime Strategy". 1911. British Naval Historian and maritime strategeist Sir Julian S. Corbett (1854–1922) proposed blockade as a means to secure command.

12 After an interesting discussion with Dr. Olga R. Chiriac (a Black Sea State Department Title VIII research fellow for the Middle East Institute in Washington DC and associated researcher at the Center for Strategic Studies in Bucharest, Romania) about Russian Maritime Doctrine in the Black Sea, it became apparent that the Black Sea wasn't among the main regional directions of the national maritime policy. Not because it was not important but because the Black Sea is already a theater of war and presents fewer opportunities than the other regions (Arctic). Perhaps the Russian Navy thought its supremacy would not be challenged in the Black Sea and that all maritime tasks could be performed easily.

13 Hugo Bachega, James Gregory, "Massive Drone attack on Black Sea Fleet – Russia". BBC news. October 29, 2022. https://www.bbc.com/news/world-europe-63437212. Russia accused the UK of being involved in the massive drone attack, but the UK responded that "Russia was peddling false claims of an epic scale."

14 US News – Reuters. "Factbox-What is Known About the Drone Attack on Crimea?". October 30, 2022. https://www.usnews.com/news/world/articles/2022-10-30/factbox-what-is-known-about-the-drone-attack-on-crimea

15 A careful study of all footage from surface maritime unmanned systems (already on social media) can give impressive lessons to the maritime community about force protection, the value of MISR operations, the increased failure rate of defensive fire from Russian units, and the inability of maritime units to defend themselves against sophisticated swarming saturation attacks from unmanned systems with AI.

16 Euromaidan Press. "Better than Moskva: four things to know about Ukraine's drone attack on Russian Fleet in Sevastopol". November 01, 2022. https://euromaidanpress.com/2022/11/01/ukrainian-drone-attack-on-russias-fleet-in-sevastopol-no-less-significant-than-zmiinyi-island-liberation-expert/ .Footage circulating on social media shows at least two different close encounters with Russian Frigates (class Admiral Grigorovich) and a minesweeper (Ivan Golubets).

17 Few know that a first attempt of an improvised unmanned maritime asset, in the form of a small vessel on fire (ready to explode when attached to the target in order to spread the fire) was used during Greece's independence war against the Ottoman empire. Some principles are the same (cheap, easy to build, used by the weaker opponent) even though its success was relying on seamanship and courage.

18 Euromaidan Press. "Better than Moskva: four things to know about Ukraine's drone attack on Russian Fleet in Sevastopol". November 01, 2022. https://euromaidanpress.com/2022/11/01/ukrainian-drone-attack-on-russias-fleet-in-sevastopol-no-less-significant-than-zmiinyi-island-liberation-expert/. Although attacks on the enemy's fleet in its base are nothing new, this was the first-ever remote attack, in which operators were located hundreds of kilometers away.

19 The Norwegian Ship Owners' Mutual War Risks Insurance Association. "DNK IOC Monthly Threat Assessment – February 23". January 31, 2023. "The reported dispersals ...were unlikely part for an amphibious landing...It could also have been a pure self-protection measure meant to mitigate a perceived imminent Ukrainian attack on the BSF (Black Fleet) vessels present in the port of Novorossiysk."

20 Will Stewart, Christian Oliver. "Dramatic moment Russian drone boat packed with explosives smashes Key Ukrainian bridge as Putin unleashes new war weapon that Moscow hopes will turn tide of war". February 11, 2023. https://www.dailymail.co.uk/news/article-11738951/Dramatic-moment-Russian-drone-boat-packed-explosives-smashes-key-Ukrainian-bridge.html .

21 Oren Liebermann, Jennifer Hansler, Haley Britzky, Natasha Bertrand. "Russian fighter jet forces down US drone over Black Sea". CNN com. March 15, 2023. https://www.cnn.com/2023/03/14/politics/us-drone-russian-jet-black-sea/index.html. Except for the strong strategic message of such a move, some operational and tactical side effects can downgrade the information warfare effort of the alliance. Downing a very expensive and capable MUS like the MQ-9 Reaper could change the way allied assets operate in the Black Sea area, increasing the operating distance from Crimea and, in that way, potentially reduce situational awareness.

22 Self-guided artillery munitions replacing "dumb" rounds, long endurance sophisticated UUVs with AI replacing "self-guided" torpedoes of the past, stealth guided weapons with swarming capabilities operating autonomously in terminal phase replacing old fashioned guided weapons, loitering munitions replacing dumb munitions, etc. The possibilities stop only when industry's imagination ends.

MARITIME SECURITY REGIMES
ROUND TABLE

CJOS COE

2023 MSR ROUNDTABLE

Slover Library
Norfolk, VA
1-2 November 2023

WWW.CJOSCOE.ORG

COMBINED JOINT OPERATIONS FROM THE SEA

Contact
CDR (SPN) Carlos Carballeira
carlos.a.carballeiracasal.fm@us.navy.mil

CJOS COE

FUTURE MARITIME WARFARE SYMPOSIUM

Spring 2024
NSA Hampton Roads, VA

WWW.CJOSCOE.ORG

CJOS COE STAFF DIRECTORY

NAME	POSITION	TELEPHONE #
		+1 (757) 836-EXT
		DSN 836-EXT
STAFF HEADQUARTERS		
VADM Daniel Dwyer, USN	Director	7551
Cdre Philip Nash, RN	Deputy Director	2452
CDR Gil Uy, 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 Carlos Carballeira, ESP-N		2462
CDR Emir Arican, TUR-N		2466
CDR Nathaniel Hathaway, USN		2440
CDR Matt Cady, USN		
WO1 Steve Scott, RM		2960
ITCS Kevin Collier, USN		2467
DOCTRINE DEVELOPMENT BRANCH		
CAPT Giuseppe Catapano, ITN	Branch Head	2449
CAPT Max Blanchard, FRN		2446
CDR Ioannis Stamoutsos, HN		2537
CDR Esquetim Marques, PRT-N/M		2444
CDR Bernd Roelink, RNLN		2443
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 2023 CJOS PoW is listed below:

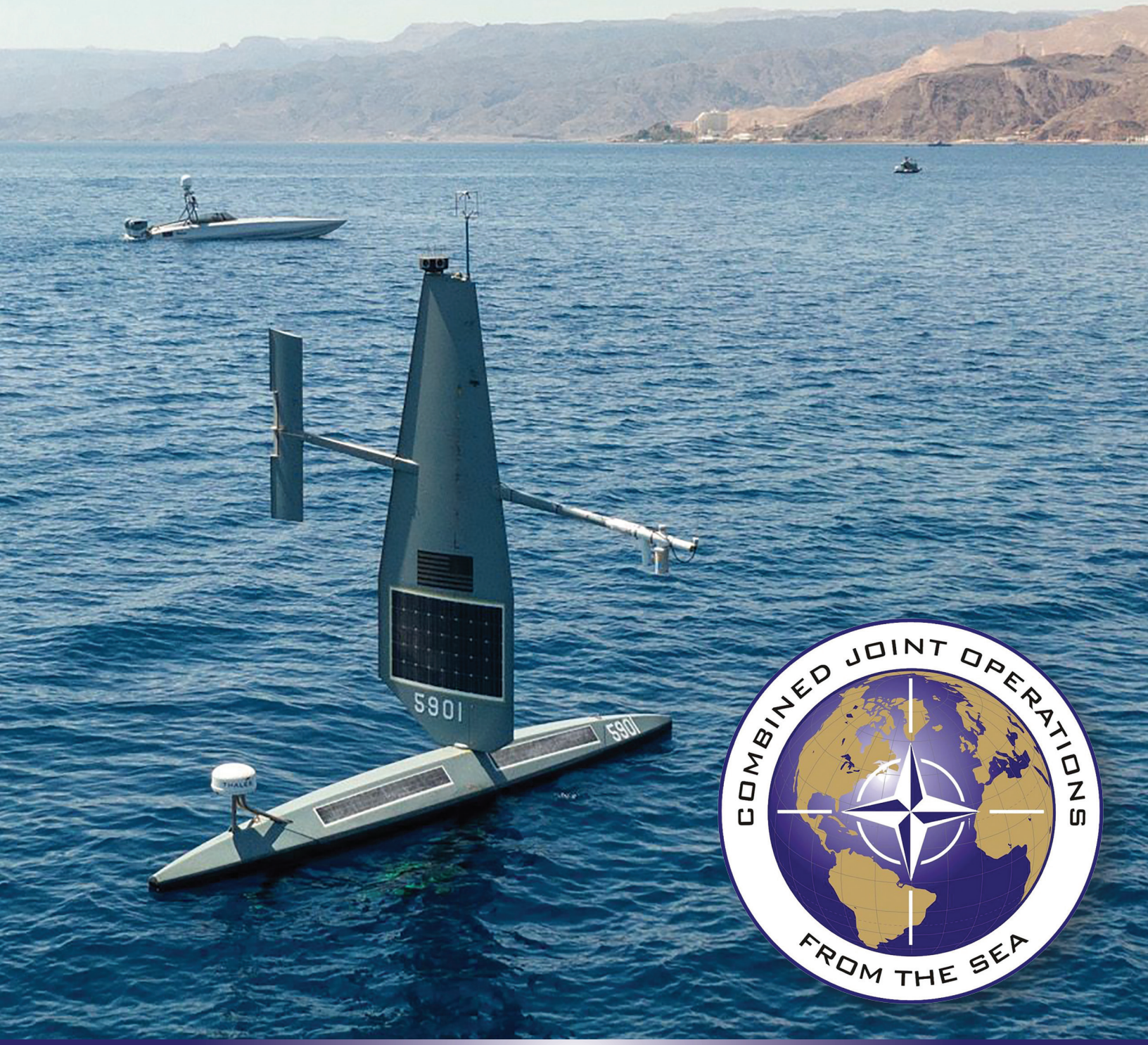
CONTROLLED UNCLASSIFIED INFORMATION

CJOS COE Programme of Work 2023

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 Custodians • Maritime ISR Doctrine • NATO Interop, Evaluation, and Certification • TIDE Sprint WG	• IAMD-M support • Collaboration with Romanian NDU • MEAB WG • Support to ACT's NWCC follow-on activities • Support NATO Defense Planning Process (NDPP) • Naval Capabilities and Opportunities of SWE & FIN • NATO Command Network Project • Federated Mission Networking WG	• Lessons Learned Process and Analysis • Missile Deterrence and Defense • BALTOPS support • Support to C2F Allied Interoperability and Integration • CSG/ESG 2023 Allied Interop Employment • Maritime procurement in NATO	• NATO Exercise Support • CJOS engagement with NDUs • Support to Education and Training Activities
2. Multi-Domain Integration			
	• Host Maritime Security Regimes Round Table (Tentative) • MSRT Working Group • Support to JFCNF DDA Activities • STDE24 Planning and execution • Alternative Satellite Opportunities • Urban Multi-Domain Operating Concept	• Impact of Danube Delta and Danube River	
3. Support the Alliance's Development and Integration of Amphibious Capability			
• AMPHIBOPS WG • Joint Combined Sea Basing WG • Unmanned vehicle for ISR and tactical/logistic support	• NATO ATF Concept • NATO Amphibious Leaders (NALES) • Fifth Amphibious Operation Amphibious Force Support to Crisis • NDDP Amphibious Forces Requirements		• Participate in CPAOT
4. Support the Alliance's Development of Innovative Technologies			
• Maritime Unmanned Systems Tactical Doctrine Development • ASW Barrier SDI • 5G Use Case for Operational Relevance • MC 0195 Document Support • Maritime Information Warfare • MC3CAT	• Cooperative ASW C2 • DYMS 23/ REPMUS 23 • Unmanned Surface Sea Vessels • Quantum Technology and defense • Innovation Hub/Tech Bridge		
5. Deepening Our Understanding of Challenges and Competitors in the Maritime Domain			
	• Cutting the Bow Wave • Support to Cold Weather Operations • NATO maritime activity in the Arctic • Long Term Military Transformation • NATO Undersea Warfare Study	• Exploring Maritime Cultural Differences in NATO	
6. Support Administrative Activities			
			• COE Support to NATO as DH • ACT CPD Branch Coordination

CJOS COE — ***Transforming Allied Maritime Potential Into Reality***

TRANSFORMING ALLIED MARITIME POTENTIAL INTO REALITY



COMBINED JOINT OPERATIONS FROM THE SEA