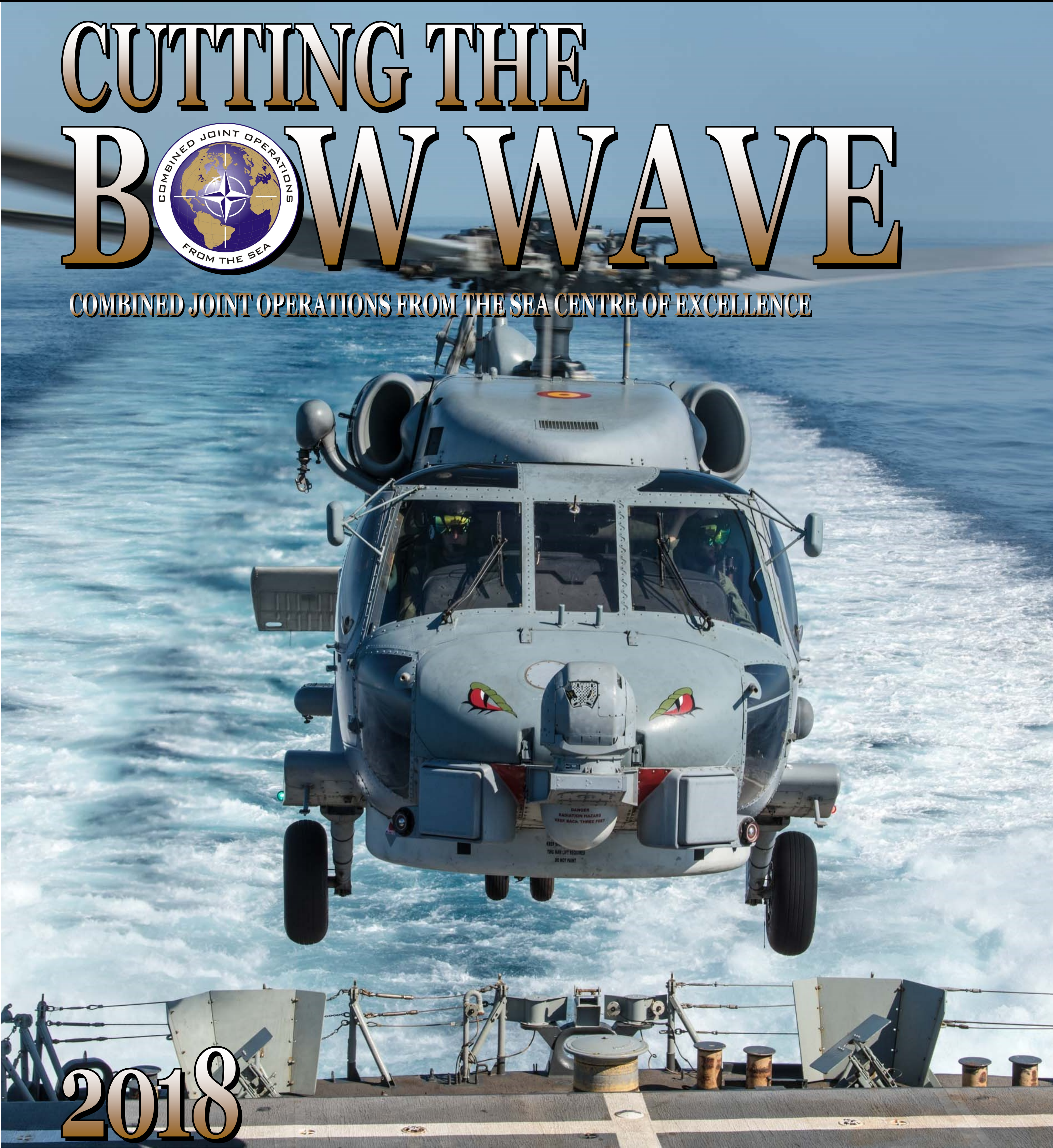
CUTTING THE BOW WAVE

COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE



2018

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. Fleet Forces Command, CJOS COE, NATO, ACT 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: Spanish SH-60 Sea-Hawk lands on ESPS NUMANCIA as it comes back from a passenger transfer while participating in naval operations during BRILLIANT MARINER 2017 exercise.

TABLE OF CONTENTS

Publisher's Note

Cutting the Bow Wave is an annual publication by Combined Joint Operations from the Sea Centre of Excellence, United States Fleet Forces Command, Building NH-39 in Norfolk, Virginia. For publication purposes, all articles and materials submitted become the sole property of CJOS COE. For copies and information, mail request to:

CJOS COE
ICO Bow Wave Editor
1562 Mitscher Ave. STE 250
Norfolk, VA 23551

Managing Editor:
CAPT Dermot Mulholland, CAN-N

Deputy Editor:
CDR Jonathan W. Sims, USA-N

USFF.CJOS.COE@NAVY.MIL

DIRECTOR'S MESSAGE

MARITIME SECURITY

MARITIME GLOBAL

MARITIME TRANSFORMATION

ANNUAL REPORT

DIRECTORY

Source: British Ministry of Defence

HMS Queen Elizabeth is the first of a new class of aircraft carriers that will be the biggest and most powerful warships ever constructed for the British Royal Navy.

MESSAGE FROM THE DIRECTOR

As I begin my tour as the Director of CJOS COE, I am impressed by the scope and intellectual depth of CJOS COE's portfolio. The organization thrived under VADM Rick Breckenridge's guidance for the past couple of years and I aim to continue that stellar reputation. From concept and doctrine development, to maritime futures, and exercise support; this small but powerful international team is firmly focused on improving NATO's interoperability across the maritime domain. NATO's continuing transformation and adaptation to the ever changing threats requires the Alliance to become increasingly interoperable.

Today's maritime environment is increasingly dynamic and we face ever more sophisticated and challenging threats, especially from the sea. In addition to the more traditionally recognized areas of war-fighting we now routinely consider threats from the cyber and space domains. Our adversaries are looking for advantages to challenge the alliance, and the cyber domain in particular has seen an exponential increase in activity. Further complicating the challenge is today's world of instant information sharing and rapid spread of technology. We must be able to innovate more quickly than our adversaries in order to stay ahead of developing threats if we are to maintain dominance in the maritime environment. This increasingly dynamic environment requires diligence and focus to ensure we maintain an effective, interoperable NATO team, and CJOS COE is well positioned to play a leading role in this vital effort.

Through our robust program of work, collaboration with other COEs, and partnerships on both sides of the Atlantic; we strive to make a substantive difference in NATO's warfighting effectiveness and ability to meet the many security challenges we face. CJOS COE has embraced this role and I look forward to our continued success in 2018 and beyond. As in previous years, CJOS remains focused on interoperability and information sharing. The most assured way to stay ahead of and defeat the threats that we face is through a well-integrated and exercised force. The CJOS staff has an impressive resume of exercises, projects, and activities that support integration and interoperability. I aim to ensure that our Centre of Excellence continues to focus on tasks that strengthen and grow our NATO alliance. ☸

Source: NATO

Coalition and allied maritime forces in formation during Exercise DYNAMIC MONGOOSE 2017.

Vice Adm. Bruce Lindsey graduated from the U.S. Naval Academy in 1982 with a Bachelor of Science in Mathematics and was designated a naval flight officer in 1983. He is a graduate of the Joint Forces Staff College and the Navy's Nuclear Power Program. Lindsey holds a Master of Arts in National Security and Strategic Studies from the Naval War College in Newport, Rhode Island, and earned a doctorate in public policy from George Mason University in Fairfax, Virginia.

His initial at-sea assignments were with Antisubmarine Squadron (VS) 21 aboard USS Enterprise (CVN 65) and on the staff of commander, Task Force 70/75/77 embarked in USS Midway (CV 41). His aviation department head tour was with VS-21 assigned to Carrier Air Wing (CVW) 5 forward deployed to Atsugi, Japan, operating from USS Independence (CV 62). From 2005 to 2007 he served as the executive officer of USS Theodore Roosevelt (CVN 71).

At sea, Lindsey's first command was VS-29 flying off USS Carl Vinson (CVN 70) during the first 72 days of Operation Enduring Freedom. His first ship command was USS Dubuque (LPD 8) during Operation Enduring Freedom deployment to the Persian Gulf, North Arabian Sea and Red Sea. He commanded Carl Vinson while completing a change of homeport from Norfolk to San Diego, providing humanitarian assistance and disaster relief to the people of Haiti during Operation Unified Response and executing a deployment to the Persian Gulf and North Arabian Sea in support of Operations Enduring Freedom and New Dawn. He commanded the first Optimized Fleet Response Plan Carrier Strike Group (CSG), CSG-10/USS Dwight D. Eisenhower Carrier Strike Group. He additionally served as commander, Carrier Strike Group 4.

Ashore, Lindsey served as aide to the chief of staff, commander in chief, U.S. Naval Forces Europe in London; as the operational test director and analyst at Air and Evaluation Squadron (VX) 1 in Patuxent River, Maryland; and as a senior operations officer at the National Military Command Center on the Joint Staff (J3) in Washington, D.C. His first flag assignment was deputy director for Operations, J3, Joint Staff. He most recently served as commander, Naval Air Force Atlantic.

Lindsey received the 1997 Naval War College President's Award for Academic Achievement and Community Service, and the 2007 Adm. Jeremy Boorda Award for Outstanding Integration of Analysis and Policy.

COMBINED JOINT OPERATIONS FROM THE SEA
CENTRE OF EXCELLENCE
CJOS COE MISSION
WORKING IN CONJUNCTION WITH THE COMMANDER, U.S. FLEET FORCES, THE CJOS COE WILL PROVIDE A FOCUS FOR THE SPONSORING NATIONS AND NATO IN IMPROVING ALLIED ABILITY TO CONDUCT COMBINED JOINT OPERATIONS FROM THE SEA IN ORDER TO ENSURE THAT THE CURRENT AND EMERGING GLOBAL SECURITY.
COMBINED JOINT OPERATIONS FROM THE SEA
CENTRE OF EXCELLENCE
CJOS COE VISION
THROUGH CLOSE LIASON WITH LOCAL U.S. ENTITIES AND SPONSORING NATIONS TO BECOME THE PREEMINENT ORGANISATION DEVELOPING MARITIME CONCEPTS AND DOCTRINE IN A JOINT ENVIRONMENT.

In November 2017, Vice Adm. Lindsey assumed duties as Director, CJOS COE and Deputy Commander, USFFC.

MESSAGE FROM THE DEPUTY

Having assumed the role of Deputy Director in the late summer, I have been struck by the range and depth of the work of this dynamic international team and I would like to pay tribute to the excellent work of my predecessor Cdre Phil Titterton and wish him well in his next endeavor. It is clear that CJOS COE is a powerful weapon and it is my intent to ensure that it well positioned and properly aimed to deliver real, tangible effect in support of our Sponsoring Nations and NATO's strategic and operational goals. Whilst continuing to serve our customers as before, this year has seen the advent of the revised Request for Support process through ACT which has undoubtedly led to better coordination and collective endeavor. In that context, CJOS COE aspires to make a real difference in support of the Alliance's deterrence and defence posture by working across a federated network of civilian and military Subject Matter Experts, COEs, government and non-government agencies, academia, and industry. I cannot overstate how important effective collaboration is in these increasingly challenging times.

This edition of Cutting the Bow Wave aims to provide a sense of the value that we add and the contributions made by this small team. As well as constant efforts in the traditional areas of Warfare, developing areas such as Cyber Warfare and the importance of Space in the Maritime Domain are coming increasingly to the fore, both in the important conceptual development process and practically in validation exercises, as seen for example in the recent Trident Javelin. As always, the reflections of our own team are enriched by the addition of contributions from some of our many partners, for which I am enormously grateful.

With CJOS COE now heading into its 12 year, the original rationale for its inception remains as valid as ever; perhaps even more so as dominance in the North Atlantic returns to the forefront of strategic debate. But of course we keep a keen eye on maritime challenges wherever they affect NATO interests and alongside the other NATO Maritime COEs will work to improve capability wherever our help is needed. Whilst we do have a full Programme of Work for 2018, do bear in mind that we exist to support the NATO maritime endeavor; if you identify a challenge, we are well positioned to help – do give us a call! ☸

Tom Guy is fortunate to have served in a wide variety of ships, from patrol craft to aircraft carriers, as well as enjoying some rewarding operational, staff and command roles ashore in the UK and abroad. Early appointments included Fishery Protection duties, the initial commission of the Type 23 Frigate HMS IRON DUKE and the role of Navigating Officer in the Hong Kong Squadron and the Type 22 Frigate HMS BATTLEAXE. As a Principal Warfare Officer (Underwater), he was Operations Officer of the Type 23 Frigate HMS MONTROSE and then Group Warfare Officer in the Carrier HMS INVINCIBLE. He commanded the Minehunter HMS SHOREHAM, bringing her out of build and then commanded the Type 23 Frigate HMS NORTHUMBERLAND, fresh out of refit as one of the most advanced ASW frigates in the world.

He has held several Operational Staff appointments, including service in the Headquarters of the Multi National Force Iraq (Baghdad) in 2005. He was Chief of Staff to the UK's Commander Amphibious Task Group, including the formation of the Response Force Task Group and its deployment on Op ELLAMY (Libya) in 2011. Other operational tours have included the Balkans and the Gulf, both ashore and afloat. Shore appointments have included the Strategy area in the MOD, a secondment to the Cabinet Office and Director of the Royal Naval Division of the Joint Services Command and Staff College. Latterly, he had the great privilege of serving as Captain Surface Ships in the Devonport Flotilla followed by the role of DACOS Force Generation in Navy Command Headquarters. In 2016-17 he was the Deputy UK Maritime Component Commander in Bahrain, working alongside the US Fifth Fleet Headquarters. He assumed the role of Deputy Director of the Combined Joint Operations from the Sea Centre of Excellence in September 2017.

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 25 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, United States Fleet Forces, 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 30 permanent staff and 20 U.S. Navy reservists, 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.

HOW WE ARE TASKED

Shortfalls in current maritime capabilities/procedures are identified by Allied Command Transformation (ACT), NATO, individual nations, or institutional stakeholders who then request CJOS COE's support. Once the requests are approved by the CJOS COE Steering Committee, they are reflected in our Annual Programme of Work (POW). CJOS COE's POW is a wide spectrum of proposals with strong focus on interoperability of global allies, maritime security initiatives, and working to deliver coherent operational Concept of Operations (CONOPS). Our aim is to be a pre-eminent source of innovative military advice on combined joint operations from the sea.

We continue to raise our profile by collaborating with high profile, leading edge institutions, publishing high quality, well researched products, and validating them through experimentation and exercise. This is made possible through our close relationship with U.S. Fleet Forces Command which provides the appropriate validation opportunities thus making maximum benefit of our unique position embedded in their command structure. We continue to work with non-military entities leveraging existing knowledge to share best practices on maritime issues and enhance global maritime security.

If you are interested in receiving project support from our staff, simply submit a Request for Support (RFS) to CJOS COE (refer to page 58). Complete instructions and details are available at www.cjoscoe.org. RFS nominations can be submitted to any CJOS COE staff member POC or the CJOS COE Directorate Coordinator available 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 the pre-eminent, 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 provide a focus for the sponsoring nations and NATO to continuously improve the capability to conduct combined and joint operations from the sea. Our aim is to ensure that current and emerging maritime global security challenges can be successfully addressed across the full spectrum of maritime operations.

CJOS COE VISION

Through a managed network of sponsoring nations, academia and industry, CJOS COE will support the development of maritime concepts and doctrine in a combined and joint environment.

Source: NATO

Belgian and Spanish Navy participating in NATO exercise NOBLE MARINER 2016.

CJOS COE will accomplish its mission:

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

DELIVERING ON CJOS COE MARITIME CYBER SECURITY REQUEST FOR SUPPORT PROJECT

CDR Michael DeWalt, USA-N
CJOS COE

Source: Open Source

There are many correlations between the cyber and maritime domains.

The Global Supply Chain (GSC) has tentacles reaching almost every corner of the world supplying consumers with products from Nike shoes to Chiquita bananas. The maritime portion of the GSC has a vast array of vessels and port facilities working in the maritime supply chain. An interruption in the Just In Time (JIT) GSC can have an impact on consumers receiving goods or services. It is also a target rich environment waiting for a devastating cyber-attack. The type of cyber-attack could have a range from incapacitating to taking full control of a merchant ship. When will the merchant shipping industry realize that cyber-attacks affect the JIT GSC? When will the process of hardening merchant vessels and port facilities against a cyber-attack commence? Will a catalyst similar to the Russian cyber-attack on Estonia be required in the merchant shipping industry before being called into action? An analysis of the areas in the merchant shipping industry specifically looking at cyber risks needs to be conducted to determine areas needing “cyber defense shoring up.”

> **“ The type of cyber-attack could have a range from incapacitating to taking full control of a merchant ship.”**

The cyber environment is very similar to the maritime environment. Both are global commons used by all, both are used in free trade and communications and lastly, both take effort to ensure freedom of use. The merchant shipping industry today could take a lesson from history. During the “Golden Age of Piracy,” the maritime commons were combed by pirates finding lucrative targets to extract and amass goods. To end piracy on the high seas required two actions. First, go after pirate safe havens - like Port Royal. Second, nations had to combine efforts to pursue and bring pirates to justice - like the Declaration of Paris signed in 1856. The Declaration was signed by forty two nations and required signatory nations to actively pursue pirates and bring them to justice. These two actions squashed piracy allowing the maritime commons to be used again without fear of piracy grossly affecting trade. Today, cyber pirate safe havens exist in the form of black markets. Cyber pirates can purchase malware or use internet service providers friendly to cyber pirates.[1] Cyber space can be used in the merchant shipping industry by cyber pirates. In the port of Antwerp cyber pirates took control of the port facility container tracking system. They tracked containers holding several kilos of illegal drugs and unloaded the contents at a time of their choosing.[2] Will the merchant shipping industry need to band together, like nations did in 1856, to find common ground to defeat cyber piracy and share best cyber defense practices? Will the cyber police be able to seek out cyber pirate safe havens and eradicate cyber pirates?

Source: NATO

ESPS NUMANCIA conducts a Combat Damage and Control exercise while participating in naval operations during Exercise BRILLIANT MARINER 2017.

There are many examples of cyber attacks in the news today. The number of attacks does not appear to be slowing down and, in fact, appear to have infiltrated most aspects of daily life. Since the maritime supply chain is the life line of many nations, the need for special attention in the cyber arena is necessary.

The Combined Joint Operations from the Sea (CJOS) Center of Excellence (COE) was tasked by the Romanian Naval Headquarters (RNH) and the NATO Maritime Command (MARCOM), in conjunction with an ongoing Maritime Cyber Security (MCS) research project, to analyze a disruption to the maritime supply chain through the cyber-threat lens. In a very broad scope, the CJOS COE MCS charter describes identifying cyber-vulnerabilities to safeguard critical infrastructure against cyber-threats and improve cyber-resilience in the maritime transportation system to include energy (oil & gas) and vital goods. The Romanian Request for Support (RFS) describes identifying cyber-vulnerabilities in ship and port operator systems, particular to the Black Sea region. Lastly, the MARCOM RFS desires an analysis and evaluation for methods safeguarding critical infrastructure in the maritime supply chain. To meet the intent of the CJOS COE charter, the RNH and the MARCOM RFS, CJOS COE determined a risk management approach was best suited to provide the MCS analysis. The risk management process from the International Standards Organization (ISO) publication 27005 was selected. The ISO 27005 risk management framework defines a nine step risk assessment process.

For the purposes of this report, the risk assessment will include three of the nine steps outlined in the ISO 27005. The three steps are risk identification, risk analysis and risk evaluation. The risk assessment will analyze the systems onboard three different types of ships: a cargo container, a liquid natural gas container and a cruise ship. The assessment will then analyze two different port facilities: an "as is" port facility meaning crane operation is not automated and a "to be" port facility meaning crane operations is automated. Completing the risk assessment in this manner, provides a window into the larger maritime community that would be more at risk to cyber-attacks.

The risk identification portion of the risk assessment contains five steps. The first step is to identify and list all the assets onboard a particular ship or port facility. The Guidelines on Cyber Security Onboard Ships produced by BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO published in February 2016 was used as a starting point for shipboard systems and assets. Step two identifies threats to the assets and the ISO 27005-Information Technology, Security Techniques and Information Security Risk Management published in 2011 was used to provide a list of most likely threats to identified assets. Step three examines existing controls that could possibly mitigate the threat. For example, if the greatest threat to the communications system was a fire in the communications room that could render all communications inoperable then a control that could be implemented would be an automated fire extinguishing system installed in the communications room to prevent fires. Step four recognizes areas of vulnerability within a given system. Analysis is conducted in six high level areas to assess risk to cyber-attack. In this portion of the risk assessment, a more in depth analysis could be conducted on the specific system. This would be more time consuming if access to the system was allowed and for the purposes of the study was not. The last step, and the most critical, in the risk identification is to identify the consequence of the system being rendered inoperative as a result to a cyber-attack. After all five steps are completed the next step is to analyze the risk.

> **" The risk evaluation is the last step of the risk assessment and the most important in determining which system is most at risk to a cyber-attack when compared to all other systems on a ship or port facility."**

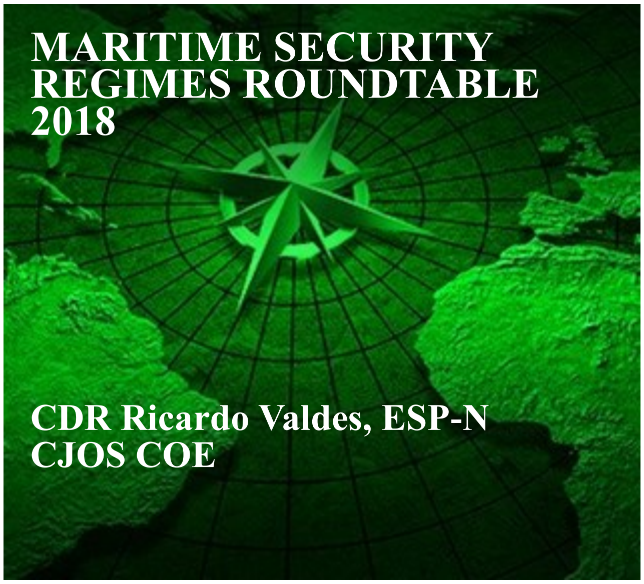
The risk analysis portion consists of three steps. First, assess the consequences meaning what is the impact to the business if each system is knocked out. Next is to look at the incident likelihood, is it likely that a certain action will or will not occur? The last step is to determine the level of risk using a numerical formula. As this phase is completed, each system onboard the ship or port facility will be associated with a number determining the level of risk to a cyber-attack.

The risk evaluation is the last step of the risk assessment and the most important in determining which system is most at risk to a cyber-attack when compared to all other systems on a ship or port facility. After conducting the risk assessment for a given ship, the list of assets can be presented to the Chief Information Officer (CIO) to prioritize resources to combat cyber-attacks on board.

CJOS COE is in the process of conducting the Maritime Transportation Supply Chain cyber risk assessment and will publish the results upon completion within the maritime community. To date two ships and a first draft of the final report have been completed with approval from Romania and Allied Maritime Command. Now it's just a matter of completing the rest of the research and publishing the results. ☸

1. Singer & Friedman, 2014
2. Europool, 2013

CDR Michael DeWalt is a Staff Officer at CJOS COE in Norfolk, VA.



MARITIME SECURITY REGIMES ROUNDTABLE 2018

CDR Ricardo Valdes, ESP-N
CJOS COE

Source: CJOS COE

Maritime Security Regimes Roundtable session at Slover Library, Norfolk, VA.

Maritime Security Regimes (MSR) definition was recognized during Multi-National Experiment (MNE) 7: ‘A MSR is a group of states and/or organizations acting together, with an agreed upon framework of rules and procedures, to ensure security within the Maritime Domain.’ The maritime environment faces threats like terrorism, organized crime, state failure, regional instability, and proliferation of Weapons of Mass Destruction (WMD) and all have a close relation between them. No single country is seen as being able to secure the maritime domain alone. Collaboration and information sharing with partner nations can help to detect, identify, track, and interdict nearly all vessels approaching coastal areas. Space systems utilization and information sharing could be the right steps.

> **“Collaboration and information sharing with partner nations can help to detect, identify, track, and interdict nearly all vessels approaching coastal areas.”**

The Combined Joint Operations from the Sea Center of Excellence (CJOS COE) has been working on different Maritime Situational (Domain) Awareness (MSA in NATO or MDA) projects and getting involved in Maritime Security Conferences and Roundtables since 2008, alone or in cooperation and collaboration with other COEs, especially with COE Confined and Shallow Waters (CSW), since 2011.

‘Define the MSA Network’ requested by MARCOM (Allied Maritime Command) is one of these projects and describes how a comprehensive MSA network to share information can only be established with the support from both Allies and Partners. The purpose of sharing information is to identify the appropriate lines of communications, and exchange mechanisms that ensure the best possible intelligence. Information is shared in support of enhancing NATO MSA as we have, for some time, sought to identify gaps and shortfalls in global MSA. The deliverable product project is to identify what information exchange requirements and protocols should be established for the purpose of building MSA, and develop an engagement matrix.

The way how CJOS COE has been building this matrix and facilitating discussions to figure out possible solutions for gaps identified or information

Source: CJOS COE

Maritime Security Regimes Roundtable 2016.

exchange mechanisms, has consisted of organizing conferences and roundtables with participants considered as key stakeholders (Nations, NATO, IO-International Organizations, NGO-nongovernmental, etc.). One of the most repeated conclusions drawn from the different event reports of proceedings has been the need for better cooperation and understanding between key maritime security stakeholders.

In a recent A2AD (Anti-Access Area-Denial) study written by CJOS COE, we realized the core for MSA at the operational level is a Command and Control system capable of sharing maritime information among stakeholders, integrating unclassified and classified data, and displaying it in a manner defined by the particular users. 'Share information' sounds like an easy achievement but despite the need, information sharing is against the culture of many organizations. It is understandable because there are often good reasons for protecting certain information that poses potential security risks or contravenes individual privacy rights. So, it is important to have the opportunity to continually foster discussion about what information needs to be protected and what should be shared, and to proactively seek the release of information that can enhance the latter goal. As a deliverable of the project 'MSA Review Study', MSA Study Paper was published on 23th of April 2015. After that, the inaugural "MSR Roundtable Meeting" was held in Madrid, Spain, at the Centro Superior de Estudios de la Defensa (CESEDEN) on 9-10 June 2015. The second Maritime Security Regimes Roundtable Meeting 2016 (MSR RT 16) was hosted at the Slover Library, Norfolk Virginia, USA, on 26 and 27 April 2016.

- The purpose of developing MSA is to support well-reasoned and timely decisions - and in the maritime domain, an understanding of time, space, oceanography, geography, weather, the global supply chain, key resources, critical infrastructure and the environment are key - as is an understanding of the nature of risk and the capabilities and methods necessary to effectively manage risks – whether they are related to governance, business operations and supply chain management, or business innovation.
- Preserving freedom of shipping and guaranteeing the constant functioning of land-based infrastructures is fundamental for its direct repercussion in the economic and energy security.
- There is a long history behind 'Define MSA Network' project and CJOS COE is acting pure

MARITIME SECURITY

and honestly in the interests of the maritime community to provide a better information exchange and networking across all stakeholders. Moreover, MSR RT is the main CJOS COE's tool to:

- Discuss MSA concerns; mainly to identify gaps in global maritime security and increase communication between the stakeholders, with a focus on 4 key areas:
  - Creation of a shared network;
  - Development of mutual cooperation;
  - Consensus on the necessity to discuss matters in a forum;
  - Agreement on a regular schedule of stakeholder meetings.
- Keep our level of expertise.
- Get additional contacts for those areas where NATO is not looking.
- Stay a relevant hub enabling connections and thoughts in the area of maritime security.
- Connect different concerns from different projects (Cyber, Sea Control, Big Data, Maritime Intelligence Surveillance and Reconnaissance, Triton, Strategic Foresight Analysis…) with possible practical solutions.

Our event is largely a stand-alone event and it's clearly a follow-up to previous work we have done on the subject and CJOS COE is not a practitioner of maritime security or MSA; we examine problems in the maritime domain and suggest solutions. In this instance we are acting as a facilitator. For the MSR RT 18 at the Norfolk Slover Library, 24-25 April 2018, we have defined these objectives:

- Improve cooperation and promote good governance in maritime situational or domain awareness; and
- Share and exchange best practices to harmonize for better interoperability and standardization in the maritime domain

If you're not already registered and you're interested in joining us, please visit our website (www.cjoscoe.org) to register. On our website you can also get the most up-to-date information. We look forward to seeing you in April! ☸

CDR Ricardo Valdes is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

MANUSCRIPTS WANTED

CJOS COE welcomes unsolicited manuscripts of 1500 words or less in length addressing the theme of "Delivery of Maritime Effect." Selected manuscripts will be featured in the next publication of *Cutting the Bow Wave*! For more information please visit or e-mail us at

www.CJOSCOE.org
usff.cjos.coe@navy.mil

MARITIME SECURITY

NORTH ATLANTIC SECURITY CHALLENGES

CDR Antonio C. Ting, USA-N
CJOS COE

Source: NATO

Forum conducted by NAC member governments on issues affecting security.

The North Atlantic's security is facing a broad spectrum of challenges from conventional to complex and non-traditional threats such as cyber-attacks, long-range and conventional strikes from land and the sea. This continuing challenge to the Alliance highlights the immediate need to develop a comprehensive maritime strategy and fighting capabilities that the Alliance can align with its constantly changing requirements and needs to be one that can overcome the capabilities of its maritime capable adversaries. Russia's recent actions in Crimea as well as its continuing capability development in cyber, space, Anti-Access/Area Denial (A2AD), conventional cruise missiles and long range strike makes it challenging for the Alliance to deter an aggressive combat ready Russian military force. Russia has been developing its conventional capabilities that has been proven difficult to defeat. Each member nation's strategy differs from each other and the current NATO's maritime posture is not enhanced to address the threats of maritime adversaries. The lack of NATO's forward deployed maritime forces and the time it takes the Alliance to assemble a maritime reaction force does not give the Alliance the needed flexibility and capability to rapidly counter Russian forces – this lack of capability actually favors Russia's strategic goals of deterring and defeating NATO's military and non-military capabilities. NATO needs to address this challenge and maintain a rotatable force in the North Atlantic to deter and defeat threats against the Alliance. Sea control, assuring freedom of navigation to include the Sea Lines of Communications (SLOC), undersea surveillance together with logistics resupply capability are fundamental in achieving and maintaining maritime superiority. The member nations need to synchronize their land campaign exercises, develop its maritime capability for delivering strikes from the sea and a comprehensive maritime strategy in employing a combat ready maritime force. Russia has been strategically employing A2AD tactics to prevent NATO forces from intervening if a non-NATO member is engaged into a conflict. Russia can mobilize their conventional forces to execute precise military operations and has the ability to rapidly deploy and employ heavy lethal forces backed with air support - Russia developed these capabilities through a process of programmatic modernization dating back to the turn of the century. Russia possibly intends to shape the political environment and be victorious in local conflicts (victories that would be difficult to overturn quickly); lessen NATO's ability to launch a counterattack and establish a quick fait accompli while controlling the escalation of conflict.[1]

The continued challenge is a clear signal that the Alliance must recalibrate its military posture. NATO needs to identify the gaps and seams between the National and Alliance Maritime strategies and develop a comprehensive maritime strategy of deterrence by improving its combat posture and capabilities to narrow down the deficits in intelligence, operational planning, communications, cyber defenses, interoperability and conventional missile capability through joint exercises and experimentation. Russian deployments of anti-aircraft, land attack, precision guided anti-ship and ballistic missiles to the Northern and South Eastern Europe provides Russia with A2AD capabilities – posing a very serious operational challenge to the Alliance for it not only constrains the deployment of NATO forces from Eastern Europe but it also makes Allied ships and aircrafts vulnerable to anti-ship and surface-to-air missiles. NATO needs to reinforce its Ballistic Missile Defense capability and conventional deterrence posture based on improved capabilities, capacity and effective implementation and display of readiness through coordinated training in the maritime environment, warfare development processes and experimentation utilizing its current framework. The Alliance needs to invest in new generation of long-range, ground-based fires, develop its antitank capabilities, theater air and missile defense, land mines, artillery and institute the constant presence of Alliance forces to make the frontline states unattractive to Russia. Russia's Air defenses would make it difficult for NATO to control the skies and support its ground forces right away in case of a conflict. Having ground-based precision fires in the region will be beneficial in rolling back Russia's A2AD threat and prevent invading forces from achieving a fait accompli.[2]

Deterrence and Engagement. Deterrence by denial has a weighty advantage over deterrence by punishment in the conventional arena. Deterrence by denial is expected to be the most effective method of conventional deterrence, it is based on denying the enemy from achieving its objectives and has been one of the central strategies in preventing a conflict. If a potential adversary is deterred from taking unfavorable actions then conflict has been prevented - preventing a conflict to occur is as important as winning in one. Deterrence needs to be ingrained in the Alliances' security posture and needs to analyze how conventional deterrence and non-nuclear options can be utilized in deterring conventional aggression.

If deterrence by denial fails, then the concept of prompt punishment comes into play – this is the notion that cost would be inflicted on the potential adversary, cost that outweighs the benefits of aggression. If a potential adversary believes that the Alliance has the capability and that the threat is credible then the threat of prompt punishment plays an important role in deterrence. One of the major aspects of deterrence by denial is communicating the Alliances' ability to access and rapidly project its Air, Sea and Land forces into a certain region. If a potential adversary believes that the Alliance does not have the capability to project its forces in a timely manner then it will take certain measures to limit the Alliances' ability by implementing anti-access capabilities. Forward deployed forces and rotational deployments to ensure freedom of navigation and maintain maritime superiority are needed. The Alliance also needs to have a broader missile defense strategy to protect its members against Russia's cruise missile capabilities. NATO needs a strategy on how it will enforce deterrence by denial and if that deterrence fails then the Alliance needs a force designed to perform deterrence by denial to have the capability to transform into a formidable force that can engage an adversary and win in a conflict. The need for the Alliance to strategize the movement of its forces (air, sea and land) that can be rapidly deployed to a theater is of utmost importance. The balance of power between the forces already in the theater and the Alliance' ability to rapidly deploy additional forces to the theater therefore plays a critical role in deterrence.[3]

In order to put together an overall maritime contribution to deterrence, the maritime forces need to have the capabilities and capacity that can be utilized as a clear signal to potential adversaries that the Maritime Forces have the ability to coordinate its actions with Air, Cyber, and Land forces – incorporated into a strategy that allows the Alliance to launch a comprehensive strike not only to deter but also to employ forceful actions if needed.

Command and Control (C2). NATO needs to optimize the use of all available resources for a more effective C2. The Alliance needs to review its current C2 structure and its ability to effectively employ the maritime force of the member nations. This comprehensive strategy requires one unified Joint Task Force

Source: Open Source

The guided missile cruiser USS Vicksburg (CG 69), and the guided missile destroyers USS Roosevelt (DDG 80), USS Carney (DDG 64) and USS The Sullivans (DDG 68) launch a coordinated volley of missiles.

Commander to assume the C2 of NATO forces in order to ensure Unity of Command and Unity of Effort. The Alliance needs to identify differences and barriers between its members' national security concerns and the Alliance' objectives before it can maximize its capacity. NATO needs to establish a synchronized C2 exercise plan – so the maritime force can operate, train and interoperate for the benefit of the whole Alliance.

Capable and Scalable. Credibility in deterrence rests in convincing potential adversaries that the Alliance has the capability to win large scale wars for a prolonged period of time. Fast, proportional and measured responses are important in preventing unintended escalation of conflicts. Scalable forces – combination of Cyber, Air, Sea and Land forces – that can be rapidly deployed to an area of conflict contributes to deterrence not only by its presence and capability but also minimize the risk that a potential adversary can exploit its weaknesses and exploit it. Rapidly deployable but scalable maritime, land and air forces are useful deterrents. The presence and the right mix of combat ready forces readily available to defend and engage potential adversaries sends a clear signal of the Alliance's resolve and ultimately impacts the opponent's belief in the Alliances' defensive effectiveness and offensive power.

Prompt Denial is the Alliance's ability in denying a potential adversary access into a specific location. If a potential opponent knows that it cannot achieve its objectives quickly then deterrence is working. It does not however eliminate the fact that potential adversaries also need to know that the Alliance has a credible capability to win in case of a conflict. In locations where ground forces are not readily available then maritime power will play a major role in enforcing prompt denial especially when it is supported with air assets. Freedom of navigation and air supremacy must be maintained in all possible areas of conflicts.

Reassurance and deterrence through readiness. The Alliance needs to reassure its members and deter Russia from taking aggressive actions by increasing and developing its readiness through technology development, infrastructure building, combined exercises, training with Allied nations and regional partners as well as an increased rotational presence and deployments in the Baltic, the Black Sea, and

Mediterranean for security cooperation, maritime security and crisis response missions. The presence of a maritime force enhance joint access by gaining familiarity with the forward operating areas, establish freedom of navigation and alleviates possible physical and diplomatic obstructions for access. Having forward presence of Naval forces facilitate NATO's missions, maintain sea control which is needed for sustaining the employment of the Alliance joint forces, increases the engagement opportunities within the Alliance and promotes familiarity with the area, collective security and stability and serves as a deterrence to potential adversaries. It is imperative for NATO to build and sustain its capability to interoperate, this contributes greatly to maritime security, deterrence and NATO's maritime force coordination and effectiveness.

> **"A2AD in the cyber world is a real threat; resilience and flexibility are key aspects for defenses."**

Cyber: A new complex form of warfare. Technological advances and our dependence on cyberspace led to the creation of the cyber domain. Questions of proportional responses to cyber-attacks remain unresolved. What level of cyber-attack constitutes as an act-of-war? How fast can we accurately identify the recipient of retaliatory response? What responses are proportional without risking the possibility of escalation? It is tempting to draw red-lines in cyber-attacks but it also provides potential adversaries encouragement in attacking all realms below that red-line. Cyber is a created medium. Somebody owns the nodes, the servers, the lines and infrastructure that enables the attacker to function. Operators need to be able to quickly determine if the network is under attack by installing several layers of defenses and fake vulnerabilities. Another potential option is redundant flexible worldwide networks with capabilities that can quickly isolate and repair the damage. The Alliance needs to develop a wide range of retaliatory options to use against a wide range of threats – an attack on one is an attack on all - applies even in the cyber realm. Alliance needs to maintain a clear strategic advantage on all fronts – Air, Sea, Land and Cyber – to deter potential adversaries from engaging the Alliance into a conflict. Russia have invested in modernizing their conventional capabilities and has exploited vulnerabilities in the cyber domain.[4] Heavy reliance on computers and information networks attract malicious actors from exploiting vulnerabilities for a wide range of reasons. Improved cyber defenses and constant vigilance in denying the adversary access to critical network infrastructure – with hopes that the Alliance defenses are better than the potential adversary's offenses – will hopefully dissuade potential adversaries in attacking. A2AD in the cyber world is a real threat; resilience and flexibility are key aspects for defenses. The Alliance needs a secure, safe and effective deterrent strategy for the future by sustaining and modernizing its cyber capabilities.

Future Challenges. Russia is likely to manifest its intentions by derailing further integration of European countries into NATO than launching military attacks against NATO members. Although NATO has greater capabilities overall, it is easier for Russia to assemble and mass its combat forces on its border and threaten a neighbor before NATO can mass its forces in response. Russia's continued intervention on its neighbor's affairs, the annexation of Crimea, presents a continual challenge to NATO. Although the Alliance is committed in taking concrete steps in response, a comprehensive strategy matched with proven and improved capabilities are needed to ensure its intentions are clearly communicated to Russia.[5]

The Alliance is facing growing challenges in gaining access and operating freely in the maritime domain. Russia have been developing its capabilities and technologies that can threaten the Alliance at greater range than before and complicates NATO's access to a number of maritime regions as well as its ability to maneuver within the Baltics, Black Sea and the Mediterranean to include the littoral and landward access. Russia has a robust conventional cruise missile and ballistic capability supported by a command and control structure, electronic warfare and cyber capabilities. The exploitation of Cyber, Electronic Warfare and Space threatens the Alliance's Command and Control. NATO Maritime forces needs to be resilient and be able to operate even when faced with cyber and EW conditions.

NATO needs to examine the significance of all its exercises and identify gaps and seams before it can develop an effective maritime strategy and ensure the current and future maritime security challenges are addressed. The Alliance needs to assess each member's ability to interoperate and address the barriers before it can develop the ability to fight together. NATO needs to collectively take these on and develop a maritime exercise plan that incorporates NATO's objectives and addresses each member's national concerns and ambitions in order to achieve a more effective integration of its forces - resulting in a well-trained combat ready maritime force. If the maritime force can synchronize their efforts with Cyber, Air, and Land forces that incorporates the Aegis ballistic missile defense (BMD) located ashore and afloat to protect its forces will give the Alliance a unique advantage. The Alliance needs to develop its capability in all aspects (Air, Sea, Land and Cyber) in order to defend, deter and destroy an adversary's military forces when necessary.

Conflicts may happen at any point with varying degrees of intensity. The Alliance needs to maintain its readiness and a potential adversary needs to understand clearly that they cannot escalate their way out of a failed attempt if they engage or attack any of the NATO members or its partners. Increased readiness, rotational deployments in the Baltics, Black Sea and the Mediterranean, combined exercises involving the whole Alliance – identifying the gaps in readiness then training and building the capacity in Eastern Europe to close those readiness gaps, infrastructure development and pre-positioning of forces and equipment in vital regions – from a light footprint to heavy presence – are measures that the Alliance can take to reassure its members and partners that it can deter potential adversaries through readiness and proven capabilities.[6]

The Alliance needs to identify operational warfighting and interoperability barriers to enable an informed decision making process. NATO needs to examine all of its national and joint exercises and conduct a thorough assessment of gaps and forces required to compensate for the gaps in capabilities. NATO needs to develop its member's ability to interoperate and address vulnerabilities and critical enablers to achieve maximum influence even under minimum presence. Developing the Alliances' capability to rapidly move combat ready forces – a synchronized movement and engagement of Cyber, Air, Sea and Land forces - from one region into areas where the conflicts are contributes greatly in conventional deterrence and combat engagement when necessary. NATO is stronger when the Alliance operates together with regional partners and Baltic states. The Alliance needs to sustain and modernize its capability and delivery platforms to prove its readiness for defensive measures while ensuring mutual restraints are observed to eliminate the risk of miscalculations. ☸

[1] Putin's Russia and US Defense Strategy; Paul Bernstein and Deborah Ball; Center for Global Security and Research, Livermore National laboratory Center for the Study of Weapons of Mass Destruction, National Defense University, 19-20 August 2015; Washington DC

[2] Breaking Defense; Air, Strategy, Strategy and Policy; How to Secure NATO's Frontline States; Mark Gunzinger and Jacob Cohn; Aug 3, 2016.

[3] Deterrence and Influence: The Navy's Role in Preventing War; Michael Gerson and Daniel Whiteneck; CNA Analysis and Solutions, March 2009.

[4] Strategic Deterrence for the Future. ADM Cecil Haney, USN. Air, and Space Journal Jul-Aug 2015.

[5] RAND Corporation; NATO needs a Comprehensive Strategy for Russia; Olga Oliker, Michael J. McNerney, Lynn E. Davis; 2015.

[6] US Leadership and NATO; Balancing Priorities in America's Europe Strategy; Luis Simon 2016.

CDR Antonio C. Ting is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

MARITIME SECURITY

ANTI-ACCESS/AREA DENIAL (A2AD) CHALLENGES IN THE MARITIME DOMAIN

CDR Ricardo Valdes, ESP-N
CJOS COE

Source: NATO

Destroyer HMS Duncan serving as Standing NATO Maritime Group 2 flagship.

The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) has recently conducted an open-source research to provide the Allied community with an independent vision of the main Anti-Access/Area Denial (A2AD) challenges in the maritime domain. In this domain, the first challenge regarding the term A2AD is to determine if there is something really new that differs from the long-standing doctrinal terms Sea Control and Sea Denial.

Sea control definition as stated in NATO doctrine (AAP 6-NATO glossary of terms and definitions) is ‘the condition that exists when one has freedom of action within an area of the sea for one's own purposes for a period of time in the subsurface, surface and above water environments’. In the meantime, Sea denial refers to ‘preventing an adversary from controlling a maritime area without being able to control that area oneself’.

As there’s no doctrinal definition for the terms A2 and AD, we draw our personal definition: the anti-access (A2) term stands for the scenario where a Force is hampered from entering an Area of Operations (AOO) by an adversary using posture, capabilities, and actions against it. Concurrently the area-denial (AD) term denotes the scenario where once the Force is in the AOO, its freedom of movement is limited and getting worse, elevating a risk evaluation to “unacceptable” (in accordance with the Allied Command Operations Comprehensive Operations Planning Directive-ACO COPD the operational level risk evaluation could be: unacceptable, conditionally acceptable, acceptable).

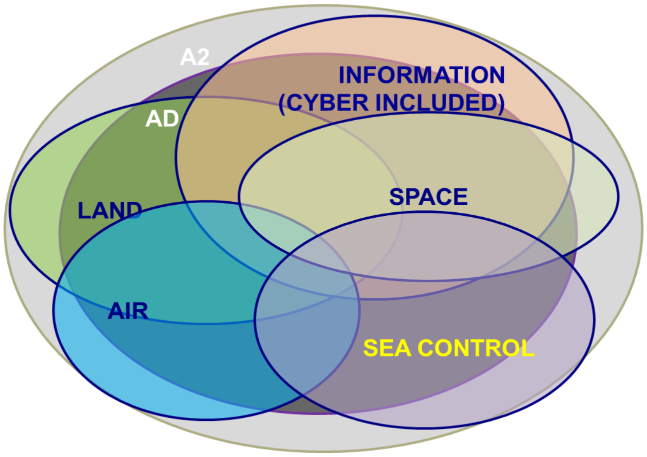
A2AD, Sea Control or Sea Denial, several terms that might be misunderstood based on the terminology and the background of the author of the document. CJOS COE recommends using existing NATO doctrine. Sea Control and Sea Denial are widely accepted and understood doctrinal terms, but the A2AD term doesn’t carry the same doctrinal authority in the maritime domain, particularly in the United States Navy (USN).

For the USN Chief of Naval Operations (CNO) and as he stated in an essay published on October 3, 2016 on The National Interest (http://nationalinterest.org), ‘A2AD is a term bandied about freely, with no precise definition, that sends a variety of vague or conflicting signals, depending on the context in which it is either transmitted or received. He discourages the term A2AD and prefers to use the term ‘contested environment’. A contested environment to any opponent is crucial in his opinion in any strategy development which means that the A2AD term is not a new challenge to the USN. Answers to existing threats should be developed through two ideas. First, a contest in the high-sea area that leads to reviewing how to achieve sea control. Second, a contest in the littoral area that leads to new concept development, as the littoral area is highly evolving and the actions conducted are definitively more joint and inter-agency than those envisioned in the high sea area. To complement this vision is necessary to review the following documents:

Firstly, the Cooperative Strategy for 21st Century Seapower and Navy's Design for Maintaining Maritime Superiority postulates the strategic framework, context and design for establishing enduring maritime superiority in support of US National objectives. This maritime strategy describes how the United States will design, organize, and employ Sea Services (USN, USMC, USCG) in support of their national, defense, and homeland security strategies. This maritime strategy reaffirms two foundational principles. First, U.S. forward naval presence is essential to accomplishing the following naval missions derived from national guidance: defend the homeland, deter conflict, respond to crises, defeat aggression, protect the maritime commons, strengthen partnerships, and provide humanitarian assistance and disaster response. Second, naval forces are stronger when they operate jointly and together with allies and partners.

Secondly, the USN CNO released last year the document 'A Design for Maintaining Maritime Superiority', which describes initial steps toward achieving aims articulated in the revised *Cooperative Strategy for the 21st Century Seapower*. The Design outlines the actions necessary for the fleet to meet its core missions and functions in an era of "great power competition." It specifies four distinct lines of effort (LOEs) that focus on warfighting: strengthen naval power at and from the sea (blue LOE), high velocity learning at every level (green LOE), strengthening the Navy team for the future (gold LOE), and expand and strengthen the network of partners (purple LOE). The CNO deliberately chose to assign each of the four LOEs a different color to avoid the appearance of priority of any individual LOE and stressed that all four LOEs are 'inextricably linked and must be considered together'.

Thirdly, the US Navy Surface Force Strategy-Return to Sea Control document's objective is to achieve and sustain sea control at the time and place of a Commander choosing in order to: protect the homeland from afar, build and maintain global security, project the national power of the United States, and if necessary, win decisively. It is essential to US security and prosperity that the Navy maintains the ability to maneuver globally on the seas and prevent others from using the sea against the interests of the United States and their allies. Additionally, sea control is the prerequisite to achieving the Navy's other objectives of all domain access, deterrence, power projection, and maritime security.



Source: CJOS COE

Figure 1. When understanding A2AD in an operational environment, sea control and A2AD are inextricably linked.

Finally, the USN concept of Distributed Lethality requires increasing the offensive and defensive capability of surface forces, which guides deliberate resource investment for modernization and the future force. Providing more capabilities across surface forces yields more options for Geographic Combatant Commanders who may employ them in dispersed formations across a wide expanse of geography, and generating distributed fires. At the operational level, it operates warships as elements of offensive Adaptive Force Packages that are task oriented and capable of widely dispersed operations. Adaptive Force Packages allow operational commanders the ability to scale force capabilities depending on the level of threat. This approach will constitute a shift from a group-centric operating navy to a fleet-centric operating navy. Fleet commanders will command and control operations conducted by reduced dispersed Task Groups, which may have greater delegation to achieve the expected effect. At the tactical level, it increases unit lethality and reduces the susceptibility of warships to detection and targeting. This way of employment is designed to open the battlespace and enable concealment and deception in order to inject uncertainty and complexity into an adversary's targeting.

Recently three NATO maritime stakeholders (CJOS COE Director, Commander, Allied Maritime Command and Commander, Naval Striking and Support Forces NATO) signed a combined declaration of intent to strengthen the trans-Atlantic response to an Article 5 crisis highlighting our Maritime and Sea control operations are essential to the Alliance's ability to address threats. Consequently, a first approach to future aspects of Sea Control could be based on the type of naval forces or the manoeuver required operating at an acceptable degree of operational level risk evaluation. The US Navy's Surface Strategy or even the lines of effort established by US Navy CNO are not far away from the NATO maritime community ideas so the return to sea control' could be a good starting point for the operationalization of the Allied Maritime Strategy.

Reaching the sea control of an area under area denial asset threat, which is today NATO's strategy, and spreading out your forces into smaller groups to challenge the adversary monitoring and engagement capability, which is the USN Distributed Lethality approach; none seems better than the other. However, maritime planners should be aware that achieving a robust sea controlled area, even temporary and localized, may become a severe challenge facing a near-peer competitor able to implement capable area denial tactics. On the other hand, implementing the Distributed Lethality concept requires to operate groups that are posing a threat to the enemy defended objectives, able to defend themselves, able to survive an attack, and to execute on their own the mission with little or reduced communications

In reference to the NATO publication AJP-3, 'to defeat Area Denial challenges supporting an Anti-Access posture, the maritime force should reach the dominance in the maritime battlespace by both ensuring Sea Control and ensuring maritime freedom of movement in the other joint domains/areas constituting the operational environment'. In a nutshell and graphically, in the maritime domain, sea control (and its component sea denial) and A2AD are inextricably linked as it is illustrated in this representation on ways to defeat A2AD in the operational environment (see Figure 1).

So consequently, A2AD in the maritime domain could be used to describe two different areas:

- The sea area which access is denied by specific maritime defensive means supported by an anti-access posture. This strategy is well-known by the maritime community. Tackling it can be achieved by implementing Sea Control tactics. That is the reason why the US CNO ordered to remove the term A2AD from the USN publications.
- The sea area which access is denied by joint defensive means supported by the same anti-access posture. Tackling it will need the assistance of joint capabilities. That is the reason why the term A2AD remains relevant in the joint community.

It is at the operational level that tactical success in engagements and operations are combined to create desired effects to achieve strategic objectives and attain the desired NATO end state. This tactical success is achieved through understanding the strategic context and the outcomes sought and by applying forces effectively (where necessary, in coordination with other actors). Therefore, the A2AD term seems to be used from the operational level to the political level with the only purpose of adapting to the lexicon of other publications, single services, and agencies and bearing in mind that in the maritime domain A2AD is called Sea Control or Sea Denial. Keeping the term A2AD is recommended to describe among the Joint community the challenges encountered as maritime stakeholders intend to control or to deny the control of the seas. ☸

CDR Ricardo Valdes is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

MARITIME GLOBAL

LEVELS OF COALITION INTEROPERABILITY

CDR Jose L. Garza, USA-N
CJOS COE

Source: NATO

NATO Exercise UNIFIED VISION; testing ability to share and process ISR.

Merriam-Webster's dictionary defines interoperability as: ability of a system (such as a weapons system) to work with or use the parts or equipment of another system.[1] NATO's AAP-06 Glossary of terms defines interoperability as: The ability to act together coherently, effectively and efficiently to achieve allied tactical, operational and strategic objectives. It also defines military interoperability as: The ability of military forces to train, exercise and operate effectively together in the execution of assigned missions and tasks.[2] Whichever definition you use being interoperable is crucial in all aspects in order to be successful.

When news came out that Turkey was buying an S -400 surface-to-air missile system from Russia many questions and comments arose about the deal. How can a NATO country purchase a weapon system from Russia and how will it be interoperable with NATO equipment? Some even welcomed the purchase probably as a possibility to learn more about the system. So far the deal seems to be moving forward with Russia and Turkey finalizing the details of the $2.5 billion purchase. At the end of the day, NATO nations must still be able to operate together and to do so must be interoperable.

The basic level of interoperability is whether countries can communicate with each other. At the lowest common level is whether the countries can verbally talk to each other. NATO's official languages are English and French however on their website you can choose to browse its website in the Russian and Ukrainian language. For the most part the lowest common level of interoperability, verbal communication, is achieved everyday throughout NATO like at news conferences, NATO celebrations, and within the walls of NATO commands throughout the world. More complex interoperability through computers and communications equipment harder to achieve.

Many use interoperability as a buzz word to describe successes or failures within an exercise but the devil is in the details for each exercise. For example, during an exercise in the Mojave Desert the new fifth generation F-35 fighter was able to communicate with the Eurofighter Typhoon over NATO-standard datalink Link-16.[3] The capability for these two fighters to talk to each other is great but what did it take to make the fighters interoperable? Those details, not made available, will allow the audience to make the determination of success or failure. Or take the exercise Formidable Shield 2017 where ships from eight NATO countries participated in a live-fire integrated air and missile defense (IAMD) scenario demonstrating the interoperability of ship defense equipment to intercept multiple targets.[4] The ability to shoot down a ballistic missile or an anti-ship missile shows tremendous interoperability between these ships networks, computers and equipment.

Let's go back to the topic of Turkey buying the

Source: NATO

Ceremony marking the change of command of Standing NATO Mine Counter Measure Group One (SNMCMG1) from Latvian leadership to Belgium leadership on the docks of Zeebruges Marine Base, in Belgium.

surface-to-air missile system from Russia. Here is where the strategic level of interoperability comes into play. Yes, interoperability is something NATO wants but at the end of the day each nation has the right to do what is right for them. In an interview with Reuters, NATO Secretary Jens Stoltenberg said "I spoke with President Erdogan when I met with him in September. I said that the kind of capabilities different nations want to acquire is a national decision."[5] However, General Petr Pavel, the chairman of NATO's Military Committee, put it this way; "The principal of sovereignty obviously exist in acquisition of defense equipment, but the same way that nations are sovereign in making their decision, they are also sovereign in facing the consequences of that decision."[6] Time will tell how interoperability will be affected with the purchase of the S-400 both in the strategic and equipment levels. ☸

1. Merriam Webster, https://www.merriam-webster.com/dictionary/interoperability

2. NATO Multimedia Library, http://nso.nato.int/nso/nsdd/listpromulg.html

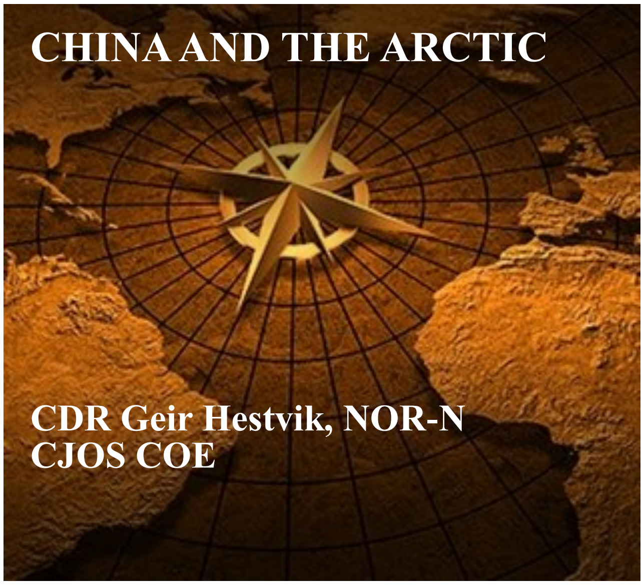
3. Stephen Trimble, "Dubai: RAF talks up Typhoon interoperability with F-35," Flight Global, November 13, 2017, https://www.flightglobal.com/news/articles/dubai-raf-talks-up-typhoon-interoperability-with-f-443219/

4. U.S. Naval Forces Europe-Africa/U.S. 6th Fleet Public Affairs, "Formidable Shield 2017: Ship engages BMD target during NATO exercise, MDA and Navy conduct SM-6 test launch," October 15, 2017, http://www.c6f.navy.mil/news/formidable-shield-2017-ship-engages-bmd-target-during-nato-exercise-mda-and-navy-conduct-sm-6

5. NATO Press Conference, "NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defense Ministers," November 8, 2017, https://www.nato.int/cps/en/natohq/opinions_148417.htm

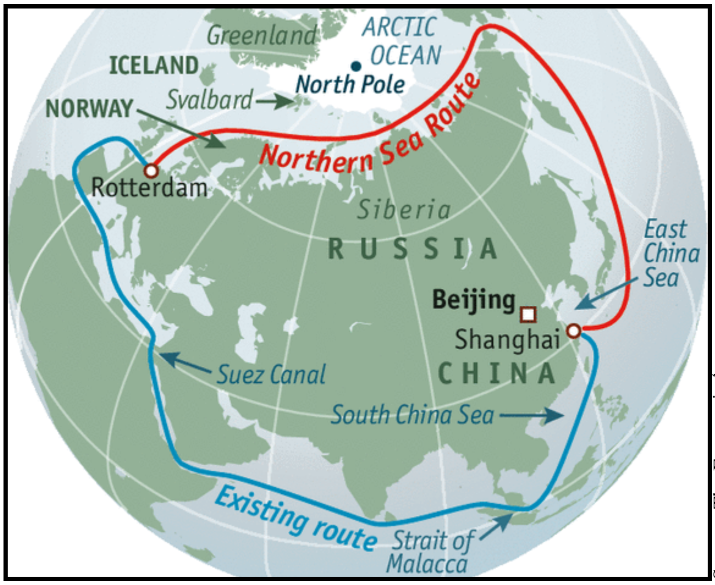
6. Umut Uras, "Turkey's S-400 purchase not a message to NATO: official," Aljazeera, November 12, 2017, https://www.aljazeera.com/news/2017/11/turkey-400-purchase-message-nato-official-171112122033735.htm

CDR Jose L. Garza is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.



CHINA AND THE ARCTIC

CDR Geir Hestvik, NOR-N
CJOS COE



Source: The Economist[3]

As Arctic sea ice melts, two international shipping routes have become available.[3]

The change to a multipolar world is very evident in the Arctic where Chinese and Russian footprints grow larger every year. Climate change is gradually melting the polar ice ensuring access to shorter sea lanes of transportation between East-Asia and Europe, and with the Northern European NATO members reduced defense spending in the last decades combined with the United States focusing on the Middle East and Asia have made NATO relatively weaker in the region. The question one could then ask; is Chinese increased diplomatic and economic initiatives in the Arctic, including closer relations and military cooperation with Russia a future threat to the USA and NATO? It`s a complex question to answer and one should be very reluctant to jumping into conclusions. Nevertheless there is a very evident Chinese interest and presence in the Arctic, and the Chinese investments and economic initiatives seems very important to Arctic countries. A statement from the Chinese Rear Admiral Yin Zhou emphasizes this impression.[1]

> **"China must play an indispensable role in Arctic exploration as we have one-fifth of the world`s population."**
> **– CHINESE REAR ADMIRAL YIN ZHUO**

Considering the possible gains by a successful Arctic policy and strategy by China, increased presence and activity in the Arctic should be expected. China`s political culture of long-term central planning gives it considerable endurance in developing relationship and thinking much further along timelines to reach certain economic goals than the short-term focused economic culture of western countries.[2] Access to vast resources of oil and gas, minerals and shorter sea lines of communications between East-Asia and Europe, could have great economic and strategic impact on China. It will ensure increased access to natural resources, diversifying oil and gas suppliers and develop more supply lines making China strategically less vulnerable.

Maritime Trade Routes Prospects in the Arctic

As Arctic sea ice melts, two international shipping routes, the Northwest Passage and the Northeast Passage (NEP) will become increasingly usable for commercial trade. For example, the NEP, which runs along Russia's northern border from the Bering Strait to Nova Zemlya, is approximately 2,500NM shorter from Shanghai in China to Rotterdam in Europe via the Malacca Strait and the Suez Canal.[4] For the People`s Republic of China an open Arctic Ocean provides unique opportunities for the development of China`s international trade; hence changes in the Arctic landscape will undoubtedly have significant impact on the growing interest of Chinese authorities in the region and for the future development of the economy of China.[5] Professor Bin Yang of Shanghai Maritime University estimates the route could save China up to $120 billion annually.[6]

Energy Prospects in the Arctic

The United States Geological Survey (USGS) has estimated that beneath the melting ice lies 25 percent of the world's oil and gas reserves, billions of barrels and trillions of cubic feet.[8] USGS scientific teams and surveys maintain that the Arctic also holds 1,669 trillion cubic feet of natural gas, and 44 billion barrels of natural gas liquids.[9] The USGS believes that some 375 billion barrels of oil rests throughout the Arctic. Their estimate clearly puts the Arctic as the richest in the terms of resource regions in the world. Even Saudi Arabia, long thought to hold the biggest reserves of oil in the world, is estimated to have only reserves of 261 billion barrels.[10]

> **"The deposits contained in the Arctic, the part of the world which is believed to hold over a quarter of the global resources of oil and natural gas, are indeed a serious prize."[11]**
>
> **- Igor Tomberg, Moscow State Foreign Relations Institute of Russian Foreign Ministry**

Chinese Economic Initiatives

Chinese Economic Initiatives in the Arctic weaken U.S. Sanctions, and create closer relationships between China and Russia. Russia sometimes backed up by Chinese investment is building and re-building the Arctic. Many of Russia's cold war military bases have been modernized and manned again, and new infrastructure and oil and gas fields are being developed.[12] For example was the YAMAL project targeted by US sanctions in 2014.[13] This made it difficult to finance construction, but in April 2016 Chinese banks stepped in with loans equivalent to $12 billion. In relation to this, the LNG-tanker *Christoph de Margerie* was delivered in 2017. It is a tanker with ice breaking capacity, the first of 15 planned ice-classed tankers. Designed to rupture ice up to 1.5 meters and withstand temperatures down to minus 50 degrees Celsius, it will ensure the delivery of natural gas from the YAMAL field to Asia and Europe.[14] Fully operational it is estimated that the YAMAL field yearly production alone will be equivalent to 80 percent of China's annual demand by 2021.[15] One could argue that the sanctions imposed by the western countries pushes Russia towards closer cooperation with China, and that may be partly correct, but it would probably have happened anyway. With the recent investments and actions, China is increasing and diversifying its delivery of oil and gas, and if the use of the NEP and building of new oil- and gas pipelines turns out to be successful, China will be less dependent on sea lines of communication through the Malacca strait were about 80 percent of China`s oil- and gas supplies are transported.[16] With a navigable NEP, and easier access to the vast Russian natural resources, China will be less vulnerable in the event of a future armed conflict.

Chinese Investments in the Arctic Countries

The American Enterprise Institute's and Heritage Foundation's is gathering information about Chinese investments worldwide through the "China Global Investment Tracker" (CGIT). According to CGIT, China has invested more than $130 billion in the Arctic countries in the period 2005-2017, not taking into account the investments conducted in the United States.[18] The Chinese investments in the Arctic countries are mainly related to energy, technology, transportation and real estate. In addition to gaining access to western technology, these investments also lead to closer diplomatic relations and cooperation with United States Allies. I would not state that closer diplomatic relations and increased Chinese investments would harm or burden the cooperation between United States and their Allies, but it cannot be ruled out that a prosperous and rich China could reduce US power and influence in the Arctic region. An example on how Chinese use diplomatic- and economic means to reach their goals, are the Chinese-Danish negotiations in relation to the Chinese approval for a permanent observer status in the Arctic Council. In June 2012 Chinese President Hu Jintao conducted a state visit to Denmark. Two months earlier, during the visit of the Chinese Prime Minister, Denmark agreed to support the Chinese bid to gain the permanent observer status in the Arctic Council. China and Denmark signed 11 cooperative documents, which were followed by contracts awarded to Danish companies in China, worth as much as 3 billion USD. For example was the large Danish brewery company Carlsberg allowed to build breweries in the "Center of the World" and the large Danish shipping company Maersk was allowed to develop a major sea port.[19] The amount of money may not seem that impressing, but Denmark without Greenland is a relatively small country, with a population of about 5.8 million people, and in 2015 China including Hong Kong and Macao had about 7.7 percent of the total import to Denmark amounting to around $ 6.4 million.[20] In the same period, about 5.5 percent of Denmark's total export went to China, about $ 5.1 million.[21] I would consider this as a good example on how China attempts to increase its influence in the Arctic countries by using diplomatic- and economic means in order to reach their long-term goals.[22]

Source: Open Source

Chinese Economic Initiatives in the Arctic weaken U.S. Sanctions, and create closer relationship between China and Russia.

Increased Military Cooperation between China and Russia

Since Xi Jinping entered office, relations between China and Russia have grown steadily, and Xi chose Moscow for his first overseas visit after becoming the Chinese president.[23] In view of these closer relations, China and Russia have also conducted several military exercises together. Chinese and Russian officials repeatedly emphasize that the ongoing military cooperation is not directed at any third country, but their exercises have increasingly taken a global character. In 2017, the Chinese people's Liberation Army-Navy and the Russian Navy conducted two Joint Sea 2017 military exercises together. One was conducted in the Baltic Sea, and one in the Sea of

Japan and the Okhotsk Sea. The focuses for the exercises were primarily air-defense, search and rescue, submarine-rescue and anti-submarine warfare, and both destroyers and frigates participated in the exercises.[24] With increased military cooperation between China and Russia, they may in the foreseeable future conduct military exercises together in the Arctic as well. Though Russian skepticism in the short run may negate very close connections with China, Chinese investments and Russian dependence on export of oil and gas, may in the long run change this. Fueled by further Western sanctions towards Russia, and the NATO countries rebuilding their military strength it could not be ruled out that closer military cooperation between China and Russia could evolve.

Conclusion

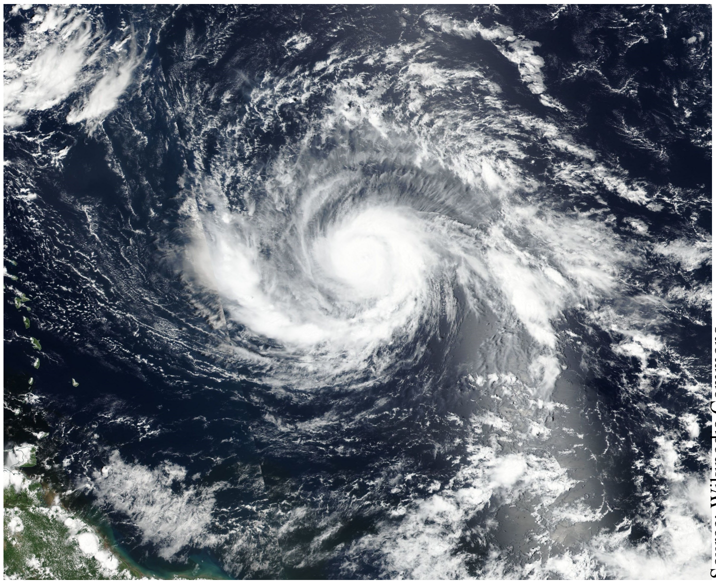
China is a very active nation in the Arctic. China is using diplomatic and economic means in order to reach their goals, and they have conducted several military exercises with Russia. It seems evident that cooperation, partnership and trade with Arctic countries are of strategic importance to China, ensuring increased access to natural resources, diversifying oil and gas suppliers and developing more and shorter supply lines making China strategically less vulnerable. Whether or not Chinese increased diplomatic and economic initiatives in the Arctic countries, including closer relations and military cooperation with Russia is a future threat to the USA and NATO remains to be seen. China has a culture for long-term planning giving it considerable endurance and thinking much longer ahead than western countries normally would do. If we in the future see an alliance between two of the largest, richest, most energy resourceful and most populated countries in the world then their combined strength may surpass the military strength of the United States and NATO. ☸

1. https://thediplomat.com/2010/03/chinas-arctic-play/
2. Diplomacy on Ice, energy and the Environment in the Arctic and Antartic, Rebecca Pincus and Saleem H-Ali, Yale, University Press, 2015, p. 155
3. https://www.economist.com/news/china/21606898-china-pursues-its-interest-frozen-north-polar-bearings
4. China and the Arctic: Objectives and Obstacles, U.S.-China Economic and Security Review Commission Staff Research Report, Caitlin Campbell, 2012, p. 6
5. Hong, 2012, in The High North, Czarny, 2015, p. 107
6. Professor Bin Yang of Shanghai Maritime University, quoted by Byers 2011,www.aljazeera.com
7. http://cimsec.org/chinas-arctic-engagements-differentiating-reality-apprehension/23521
8. Global Arctic, Scott Nicholas Romaniuk, Berkshire Academy Press, 2013, page 24
9. Circum-Arctic Resource Appraisal, United States Geological Survey, 2008, p. 4
10. Circum-Arctic Resource Appraisal, United States Geological Survey, 2008, p. 4
11. Global Arctic, Scott Nicholas Romaniuk, Berkshire Academy Press, 2013, p. 81.
12. http://www.businessinsider.com/r-putins-russia-in-biggest-arctic-military-push-since-soviet-fall-2017-1
13. https://www.forbes.com/sites/timdaiss/2015/11/18/us-led-sanctions-squeeze-massive-russian-gas-project-but-chinese-funds-may-hold-the-answer/#59d95da039c7
14. https://www.ft.com/content/9f7aba98-ddb3-11e6-86ac-f253db7791c6
15. https://www.ft.com/content/9f7aba98-ddb3-11e6-86ac-f253db7791c6
16. http://www.businessinsider.com/this-map-shows-chinas-global-energy-ties-2015-5
17. http://gcaptain.com/russia-to-send-first-arctic-lng-cargo-to-china/
18. http://www.aei.org/china-global-investment-tracker/
19. Global Arctic, Scott Nicholas Romaniuk, Berkshire Academy Press, 2013, page 28
20. https://www.populationpyramid.net/denmark/2017/
21. Ibid
22. Ibid
23. https://thediplomat.com/2017/09/chinese-russian-navies-hold-exercises-in-sea-of-japan-okhotsk-sea
24. https://thediplomat.com/2017/09/chinese-russian-navies-hold-exercises-in-sea-of-japan-okhotsk-sea

CDR Geir Hestvik is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

MARITIME ASSISTANCE WITH HUMANITARIAN ASSISTANCE & DISASTER RELIEF

CDR Jose L. Garza, USA-N
CJOS COE



Source: Wikipedia Commons

A VIIRS satellite image of Hurricane Irma on September 3, 2017.

When we talk about military forces it is usually dealing with combat in Iraq or Afghanistan or it's about the defense budget, or in relation to Russia, China, Iran or North Korea. And if you watch or read any national news outlets the message is the same. But this past year many naval military units were used to support humanitarian assistance and disaster relief (HA/DR) after a very active hurricane season. In fact, HA/DR is a core competency that many navies advertise and exercise on a consistent basis.

The 2017 hurricane season was one of the most active seasons in recent past. There were 17 named storms of which Harvey, Irma and Maria stood out for many reasons. First these storms were the most recent ones so they are fresh in our minds. They were also the most destructive in recent history. All three storms were at least a Category Four when they made landfall in the U.S. and Hurricane Irma was a Category Five when it hit the Caribbean island of Dominica. These storms damaged thousands of homes and businesses and displaced thousands of people. Harvey made landfall twice and dropped 27 trillion gallons of rain throughout its six day period.[1]

But as soon as the storm leaves help begins to arrive. Everything from government sponsored agencies, civilian organizations, the military, and everyday people lend a hand to help where they can. There is usually not enough help to alleviate the suffering but every little bit helps. The military for their part cannot get involved until directed to do so but that doesn't mean that they have not and are not prepared. Many naval units across the world train for disaster reliefs and usually exercise the capability on a continuous basis either annually or bi-annually. However, just like an exercise the event is scripted, performed in a controlled environment and not very dynamic. But a real life disaster provides the ability to test and challenge the training that any military unit has received in relation to a disaster. Although the disaster is a tragedy and any loss of life or property is unbearable, the opportunity for any military unit to help and at the same time gain valuable experience will undoubtedly make that unit a better unit.

Many naval capabilities are used during a disaster relief effort. From the start, once the direction has been given to use military assets, operational level management needs to identify and notify all units to be used. Preparations will take place to ready the units to meet a certain date to deploy and head towards the disaster area. The preparations involve the actual people, ships, airplanes, trucks, gear, food, water, etc. that will be needed for the relief effort plus all the supporting efforts from individuals that handle medical, fuel, supplies, pier operations so on and so forth. It is an all hands evolution that takes place at a steady pace to arrive at the disaster location as soon as

Source: Wikipedia Commons

An aerial view of Ishinomaki, Japan a week after a 9.0 magnitude earthquake and subsequent tsunami devastated the area.

practical.

Once at the disaster site usually the first order of business, beyond the political and jurisdictional wrangling that comes with this size of operation, is search and rescue. This can be done with troops on the ground, aircraft and UASs. Usually helicopters are preferred as they usually have a rescue swimmer that can lower a basket or strap to remove individuals from rooftops or other structures that might be difficult to access from the ground. Although most of the helicopters come from military sources, other helicopters can come from federal agencies and even from new agencies which can raise the level of risk within the operation by keeping the assets geographically separated.

The majority of effort for the military during a HA/DR event is logistical. Everything from moving people to safer locations, to moving pallets of food and water and distributing the items, to clearing debris from roads and rebuilding critical infrastructure. Movement from the ships to land is done by ship-to shore connectors. Whether they are Army or Navy Landing Craft Units (LCUs), these barge looking flat bottom ships can move huge amount of crated supplies or move construction equipment like bulldozers and trucks easily from the ships to land. They can also move people back and forth.

Beyond the high visibility of the ships and the aircraft, the sailors and marines onboard ships become the most valuable asset when it comes to recovering from a disaster. It takes a tremendous amount of manpower to move the supplies inland, setup distribution stations and handout thousands of bottle water and other needed supplies. It is usually up to the federal and local governments to decide where the help is most needed. This manpower can also be used to help family members recover personal items, help setup temporary shelters, and provide basic medical care.

All these efforts are usually an all hands event from the youngest and lowest rank individual to the senior members everyone has a job to make things better. Although, hurricanes are Mother Nature’s doing, it is human nature to help and the maritime community will always lend a hand when they can with the tools they train and use. At the end of the day, the disaster area will receive a helping hand and the maritime establishment will get real world experience that you can’t quite replicate during an exercise. ☸

CDR Jose L. Garza is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

FUTURE ASW: RETURN OF THE COLD WAR?

CDR Gwenegan Le Bourhis, FRA-N
CJOS COE

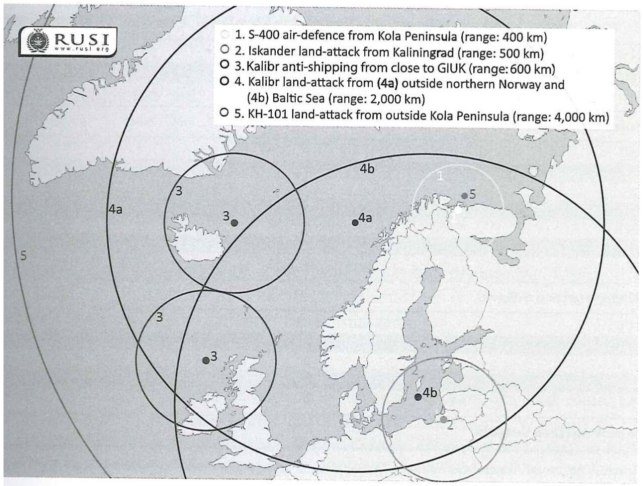
Source: Wikipedia Commons

U.S. Navy P-3C Orion of Patrol Squadron 56 lands at NAS Keflavik, in 1977.

Since the fall of the wall, NATO has enjoyed and expected free transit of the Atlantic. Recent Russian deployments and activity in the Northern Atlantic and along both U.S. and European coasts make it clear that this cannot be assumed in the future.[1] This statement, made by General Philip Breedlove, USAF (ret.), former Supreme Allied Commander in Europe, emphasizes clearly a return to the spotlight for coordinated NATO Anti-Submarine Warfare operations. The end of the Cold War saw NATO focusing on expeditionary campaigns, mainly in Iraq and Afghanistan. The North Atlantic was seen as a region with a reduced likelihood of tension, while the US posture evolved towards a strategic pivot to the Pacific. Consequently, the Alliance has disinvested in maritime capacity and, over time, its understanding of the theatre. Fifteen years after the events of 9-11, NATO has become 'sea-blind'. As mentioned by General Breedlove, recent Russian activities have triggered the alarm, urging the Alliance to return its attention to the undersea domain.

The underwater and maritime environments are becoming increasingly complex and ambiguous. Mirroring the steady growth of trade volume, exploitation of maritime resources continues apace (especially in EEZs) and international competition for assured access to the global commons remains politically, economically and militarily significant. Submarine platforms continue to proliferate, with developments in their capability providing an increasingly versatile and challenging adversary. Today and even more so in the future, submarines will be able to strike critical infrastructure targets from a long range undetected position with cruise missiles; they will also pose a serious threat to key Allied navy platforms (such as aircraft carriers and amphibious decks) and merchant vessels. Key economic infrastructure located undersea, including communications cables, energy wellheads, and pipelines might be threatened as well. Potentially hostile nations are already operating these types of submarines in areas of strategic importance to NATO.

In Anti-Submarine Warfare, some principles will remain valid. Because submarine forces operate with the initiative, this threat could occur with no prior notice and the consequences could be dramatic considering the high lethality of the weapons delivered by a modern submarine. Fighting in the undersea domain is very similar to fighting in the Cyber domain. Aggressions are not easily characterized and the enemy even more difficult to identify, and it is for these reasons that a near-peer competitor will be keen to use submarines while staying calm and peaceful above the wave tops at the political level. Operating a submarine force will remain a heavy challenge for any nation; the acquisition, training, maintenance, and support requirements are demanding even for experienced navies. The decision to employ submarines is a highly political one as these ships may be considered as capital assets in any country's maritime strategy. Without mentioning links with national deterrence policies, this gives immediately to the ASW a strong political flavor, particularly during peace time. These elements underline the revival of interest in ASW, as noted by Admiral Jonathan Greenert, USN (ret.), the former Chief of Naval Operations: "We have to sustain maritime dominance here, particularly in the undersea domain, to assure global economic security. This was particularly essential in the Cold War and applies today."[1] The question is not whether or not NATO should reinvest in ASW, but rather should NATO reestablish the organizations implemented during the Cold War for this purpose or do something else?


RUSI
www.rusi.org
○ 1. S-400 air-defence from Kola Peninsula (range: 400 km)
○ 2. Iskander land-attack from Kaliningrad (range: 500 km)
○ 3. Kalibr anti-shipping from close to GIUK (range: 600 km)
○ 4. Kalibr land-attack from (4a) outside northern Norway and (4b) Baltic Sea (range: 2,000 km)
○ 5. KH-101 land-attack from outside Kola Peninsula (range: 4,000 km)
1
2
3
3
3
3
4a
4a
4b
4b
5
5

Source: RUSI

Figure 1. The significance of the North Atlantic and the Norwegian Contribution.

With the geographic area in question, the same threatening country and the same strategic threat, it seems very natural to look backwards to the Cold War to examine how NATO addressed this threat in past decades. The undersea challenge is still composed of three levels of actions. At the strategic level, both sides would try to deter or prevent any enemy submarine from leaving its homeport, continuously hampering its ability to operate efficiently or receive orders and support from its base of operations. At the operational level, both navies would work to deny to any unidentified submarine access to the Joint Operations Area (JOA), which includes detection, localization, classification, and identification of subsurface contacts in the open ocean. At the tactical level, deployed naval forces operate to deny to the enemy underwater platform the ability to disrupt NATO operations; this includes counter-localization, protection of high-value assets, neutralization of threats, and self-protection of ASW assets. This layered approach requires a shared awareness of the enemy underwater posture based on persistent intelligence, surveillance, and reconnaissance missions at the theatre level. Achieving this challenge at the operational and tactical level also requires continuously updated environmental situation awareness. Considering the immensity of the Atlantic Ocean, a central coordinating authority, responsible for conducting the fight in this area, is a key enabler for delivering the expected effects in the ASW domain. In previous decades, NATO's response to these issues was the Supreme Allied Commander for the Atlantic (SACLANT).

The Mine Warfare area has faced similar challenges during the past decade. To tackle the ongoing mine threat, several Mine Warfare Commanders have chosen innovation via developing modern capabilities centered on unmanned systems. ASW has traditionally been carried out by airborne, surface and undersea manned assets equipped with advanced sensor systems. This approach is costly and explains the reduced number of ASW capable platforms among Allied navies. Today, maritime robotics is an emerging technological area that could enable the development of advanced networks for underwater surveillance. Current and developing unmanned assets are typically composed of small, low-power, mobile systems possessing limited endurance, processing, and wireless communication capabilities. When deployed, these assets should be able to cooperate via a smart network achieving high performance with significant features of scalability, adaptability, robustness, persistence, and reliability. According to several researchers from the Center of Maritime Research and Experimentation (CMRE), "They also introduce new challenges for underwater distributed sensing, data processing and analysis, autonomy and communications."[2] Despite challenges, this approach should strongly be investigated as a way to offset the shrinking number of ASW capable platforms, especially destroyers and Maritime Patrol Aircraft. It reinforces the idea that ASW in the 21st century need not be identical to Cold War ASW approaches.

Today's ASW must be a multilayered and connected capability able to seamlessly operate among Allied forces. The NATO ASW community must be agile enough to maximize existing technology and legacy systems while being poised to exploit emerging opportunities – specifically, those in the fields of information technology, enhanced processing capability, miniaturization, and unmanned systems. The Cold War focus on SSNs and SSKs persists to this day, with our sensors and weapons designed to counter the parameters of those platforms, but the target set is now far broader. ASW traditionally focused on cold, deep blue water capabilities, but there are a significant and growing number of smaller targets and weapon delivery platforms either in service or under development which will be designed to operate in the warm littorals as well as the open ocean. Together with widespread adversary understanding of signature management, proliferation of sensors, acoustic databases, weapon and processing technologies, and improved training, submarines today pose a greater threat than those of previous generations. Recently developed submarine capabilities (improved torpedoes, cruise missiles and anti-air missiles) and new effects that can be achieved by NATO forces in terms of targeting and Cyber/EW domain actions have moved ASW to a Joint endeavor that should be undertaken at the strategic level.

For all these reasons, looking backwards and trying to cope with today challenges only by reinvigorating old strategy may not be the solution. Taking stock of historical analysis and earlier approaches is obviously a part of the solution but future ASW concept should definitively include modern, innovative approaches.

It seems in particular that there are three areas in which ASW should be energized.

In the wide grey areas of modern warfare, undersea domain could become a very interesting and highly contested space where an adversary's determination and political will may be challenged and tested. Similar in posture to the Cyber domain, confrontations in the undersea domain remain masked and difficult to characterize. The main difference with the Cyber game is the extreme lethality of undersea platforms and their direct contribution to national deterrence. Considering the sensitive nature of the ASW mission in early stages of conflict, the ASW Commander must ensure that the Allied ASW force is acting in accordance with political guidance to prevent any escalation in the crisis level. In this area, identification of every contact of interest is a key task in the process to gauging appropriate reactions towards an underwater contact closing the force -- and merely identifying a contact might not always be a sufficient end-state. Neutralizing the threat may not be authorized by restrictive ROE, so the ASW commander must be able to apply other-than-war techniques and tactics to deter the closing threat and preserve the freedom of movement of the Allied force. Being able to operate during the grey phase of a conflict without crossing the kinetic threshold remains a key area for future explorations in terms of capabilities and doctrine.

Unmanned systems will no doubt become great contributors to the ASW fight. However, it is certain that investments in new undersea capabilities will be of little use if the alliance fails to create command and communication nodes to receive, analyze, and disseminate information gathered from these systems. Command and Control of these system architectures will force ASW planners to systematically change their mindset. Interoperability between legacy and emerging systems, and among these new unmanned systems themselves, will be another significant challenge. Conversely, as unmanned platforms are recognized as an opportunity for NATO forces, they should also be considered as an emerging threat when employed by the enemy. In accordance with the recently proposed joint Counter Unmanned Automated System (CUAS) concept, CUAS capabilities need to be developed in the underwater domain, considering in particular the reduced size of the vehicle, their limited autonomy, and their needs for communications in a networked approach.[3]

Finally, and as in many other areas, revisiting the C2 construct in terms of technological limitations, organization, and doctrine will be an all-encompassing endeavor. To ensure unity of effort and ensure the

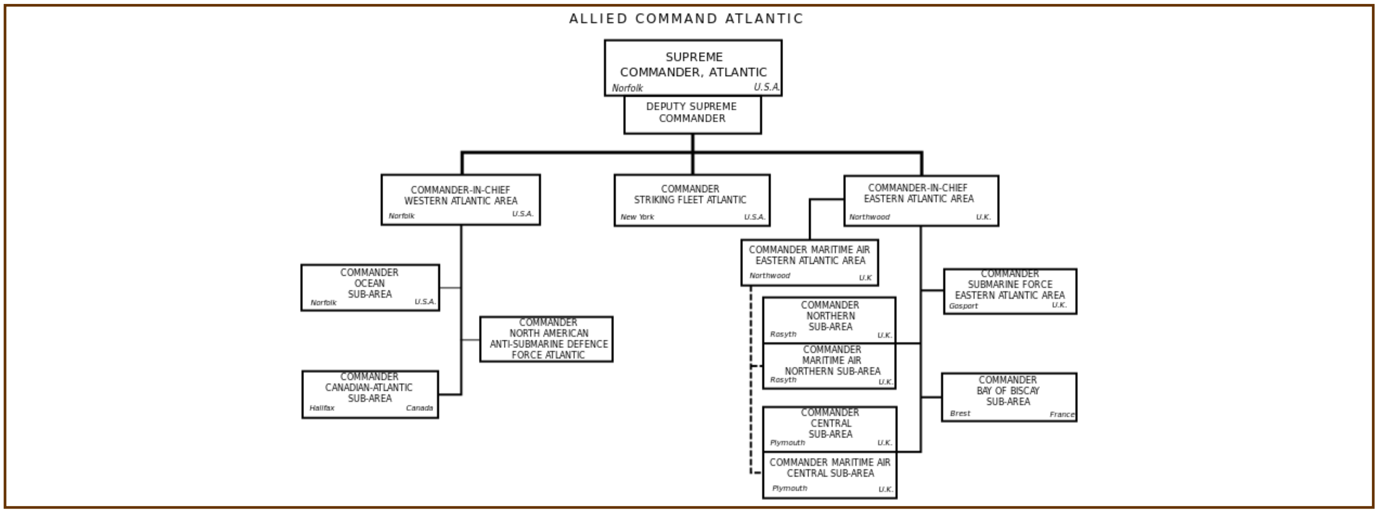

ALLIED COMMAND ATLANTIC
SUPREME COMMANDER, ATLANTIC
Norfolk
U.S.A.
DEPUTY SUPREME COMMANDER
COMMANDER-IN-CHIEF WESTERN ATLANTIC AREA
Norfolk
U.S.A.
COMMANDER STRIKING FLEET ATLANTIC
New York
U.S.A.
COMMANDER-IN-CHIEF EASTERN ATLANTIC AREA
Northwood
U.K.
COMMANDER OCEAN SUB-AREA
Norfolk
U.S.A.
COMMANDER NORTH AMERICAN ANTI-SUBMARINE DEFENCE FORCE ATLANTIC
COMMANDER CANADIAN-ATLANTIC SUB-AREA
Halifax
Canada
COMMANDER MARITIME AIR EASTERN ATLANTIC AREA
Northwood
U.K
COMMANDER SUBMARINE FORCE EASTERN ATLANTIC AREA
Gosport
U.K.
COMMANDER NORTHERN SUB-AREA
Rosyth
U.K.
COMMANDER MARITIME AIR NORTHERN SUB-AREA
Rosyth
U.K.
COMMANDER BAY OF BISCAY SUB-AREA
Brest
France
COMMANDER CENTRAL SUB-AREA
Plymouth
U.K.
COMMANDER MARITIME AIR CENTRAL SUB-AREA
Plymouth
U.K.

Figure 2. Organization Chart to NATO's Allied command Atlantic (ACLANT), circa 1954.

Source: CJOS COE

delivery of strategic-level effects while keeping in full view the political sensitivities of the actions conducted at the tactical level, ASW Command and Control structures should be well established; relationships between the different levels of ASW authorities should be well-understood by all stakeholders. At the strategic level, national ASW decision-makers should be able to coordinate their views, preserving national interests and the interests of the Alliance while maintaining a persistent shared picture. In each JOA, a dedicated ASW Commander should be identified to ensure cross-domain synergies are achieved and common posture and policies are applied throughout the force. This Force ASW Commander must be capable of executing operational control of theatre level ASW assets, such as assigned submarines, maritime patrol aircraft, Surveillance Towed-Array Sensor System ships, and relevant unmanned systems. Considering the size of a JOA, these actions may be delegated at the tactical level to local ASW Commanders in charge of executing a task in a dedicated area. One level of coordination and two levels of command should be sufficient to tackle the ASW challenge in the whole Atlantic and other areas of interest for the Alliance. These relationships must be described in detail in publications dealing with ASW.

In the coming years, the Alliance may face a near-peer threat in the undersea domain. Tackling this threat will be a mandatory endeavor, doing so without escalating the level of conflict will remain an ever-present challenge. To fulfill this task, we should not simply look back and call for Cold War era solutions. Facing a more capable threat in a different context will require deeper consideration: we must revisit NATO C2 organization, ensure interoperability of modern equipment with legacy systems, and experiment new technical solutions. Overcoming these challenges would enable NATO maritime forces to preserve their ability to operate throughout the Atlantic and ensure freedom of access in any other areas where potential adversary submarine forces are in development. ☸

1. Center for a New American Security TTX – Forgotten waters Minding the GIUK Gap
2. Cooperative robotic networks for underwater surveillance: an overview - Gabriele Ferri , Andrea Munafò, Alessandra Tesei, Paolo Braca, Florian Meyer, Konstantinos Pelekanakis, Roberto Petroccia, João Alves, Christopher Strode, Kevin LePage – Institute of Engineering and Technology www.ietdl.org 19 June 2017
3. Multinational Capability Development Campaign (MCDC) 2015 -2016 - Future Capstone Concept on Counter Unmanned Autonomous Systems (CUAxS)

CDR Gwenegan Le Bourhis is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

presents:

The Distinguished Lecture Series

CJOS COE in partnerships with Old Dominion University (ODU) Idea Fusion is proud to present *The Distinguished Lecture Series*. DISCOVER, SHARE, and LEARN from leading subject matter experts from government, military, academia, and industry. The lecture series addresses a wide spectrum of relevant maritime issues with a strong focus on interoperability and all aspects of maritime security. Attendee collaboration and participation is highly encouraged.

Past Distinguished Lectures:

CAPT Ray Toll, USN (Retired), "Sea Level Rise: An Intergovernmental Blueprint for Community Resiliency"
Dr. Ian Ralby, JD, PhD, "Emerging Threats & Trends in Global Maritime Security"
Dr. Heiko Borchert, "Autonomy in Tomorrow's Undersea Domain: Trends, Opportunities, and Challengers"
Mr. Guy Thomas, "Satellite Automatic Identification System"

For more information visit:
www.CJOSCOE.org
CDR Jose L. Garza, USA-N
Email: usff.cjos.coe@navy.mil
Tel: +1 (757) 836-2462

MARITIME ISR: GAINING THE FULL SPECTRUM OF SITUATIONAL AWARENESS

CDR Pavlos Angelopoulos, GRC-N
CJOS COE

Source: NATO

The prosperity and economic development of most countries around the world depend on sea-trade, the unobstructed flow of energy through strategic maritime crossroads and to a great extent on human activities taking place in coastal regions. Maritime transport is essential to the world's economy as over 90% of the world's trade is carried by sea[1]. As of January 2016 the number of merchant ships trading internationally exceeded 50,000[2]. This number is forecasted to increase as seaborne trade is expected to double over the next 15 years[3]. With passenger ships, fishing vessels and ships belonging to navies adding to the number, it is evident the maritime domain is becoming more and more congested.

Considering the multifaceted risks and challenges in the international security environment one could argue that the "sea-generated" prosperity enjoyed by many countries around the globe is quite fragile. It could be easily disrupted by the never-ending competition for resources, the existent maritime territorial disputes (e.g., territorial disputes in South China Sea, tensions in East China Sea, etc.) and possible threats to seaborne commerce, either from rogue nations, extremist and terrorist groups or from transnational crime organizations. Under the current security setting and the clear dependency of world economies on sea-trade, the safeguarding of maritime security (MS) is one of the most important challenges for NATO, European Union (EU) and for all navies around the world.

> **"Considering the multifaceted risks and challenges in the international security environment one could argue that the "sea-generated" prosperity enjoyed by many countries around the globe is quite fragile."**

MISR as an Enabler of MSA and Maritime Security

One of the seven specific tasks identified by NATO under maritime security operations (MSO) is support to maritime situational awareness (MSA). According to this task, where possible, Alliance assets capable of contributing to MSA, should share data and/or information aimed at enhancing the NATO recognized maritime picture (RMP), with other Allies and civilian agencies as appropriate[4]. MSA is singled out on purpose for the reason that it is a prerequisite for maritime security. MSA delivers the required information superiority in the maritime environment by achieving a common understanding of the maritime situation in order to increase effectiveness in the planning and conduct of operations[5].

Achieving situational awareness in the maritime environment requires continuous intelligence gathering, surveillance and reconnaissance (ISR) by all available sensors and assets. These critical navy tasks are described by the broad term of maritime ISR (MISR). MISR is an enabling capability not only of MSA but of the full spectrum of maritime activities. It is a tool at the disposal of commanders at all levels, down to the tactical and unit level, as it supports decision making and improves operational effectiveness.

MISR and its Challenges

The three distinct elements of MISR; intelligence, surveillance, and reconnaissance should cover all domains: land, maritime, air and even cyber. Data, information and intelligence collected through surveillance and reconnaissance activities, assist commanders in making timely but most importantly informed judgments. While surveillance and reconnaissance provide help in answering the questions of "what", "when", and "where", the combined elements of different ISR sources and intelligence collection disciplines provide the answers to "who", "how" and "why".

From a process perspective MISR comprises all activities in the maritime domain focused on the collection of data; information and intelligence gathering; as well as the processing, exploitation and dissemination of the results, in order to build better understanding. MISR should always be considered and planned for as an integral part of the ISR effort at the joint level (JISR), following the same five step process, well known in the intelligence community as TCPED (task, collect, process, exploit, disseminate), but with its own unique characteristics.

ISR in the maritime domain is focused on a three-dimensional operational environment, considering the situation above, on, and below the surface of the sea as well as the littoral. Collection of data and information through surveillance and reconnaissance is not a trivial task for naval forces. The vast area of operations, oceanographic constraints, weather conditions, topographic limitations, electromagnetic spectrum complexity, congestion in littoral areas and traffic volume in critical sea routes, all present difficult challenges to overcome. Satellite communication bandwidth limitation for near-real-time (NRT) transmission of all collected information is also a major challenge for sea-based ISR platforms.

As ISR plays an even greater role in maintaining situational awareness and in the planning and execution of current and future military operations or other mission-specific tasks, the need for NRT data, information and intelligence will often exceed the available organic capability and capacity. In most cases a maritime commander will have a limited number of MISR assets at his disposal. It is therefore critical that all available air and surface joint assets: traditional or non-traditional, organic or non-organic, manned or unmanned, are carefully managed and optimally employed to satisfy the commander's information needs.

MISR Capabilities

There is a continuous need for information regarding the operating environment forcing maritime assets at sea to engage in surveillance 24/7. As a consequence they are able to support MSA and contribute to the ISR effort whether or not specifically tasked to do so. MISR assets could be tasked to collect data and information for many intelligence disciplines through several different sensors. Being equipped with hydrophones and/or SONAR systems, MISR assets and especially submarines, maritime patrol aircrafts (MPAs) and anti-submarine warfare (ASW) helicopters are well-suited for acoustic intelligence (ACINT) gathering. Maritime capabilities include imaging sensors like electro-optical (EO), infrared (IR), full motion video (FMV) and synthetic/inverse synthetic aperture radar (SAR/ISAR) sensors allowing them to contribute to imagery

Standing NATO Maritime Group Two (SNMG2) including flagship Royal Navy Type 45 destroyer HMS Duncan and Turkish frigate TCG Gaziantep, transit the first part of the Straits to the Black Sea on January 30, 2018.

Source: NATO

intelligence (IMINT). Moreover, being equipped with sophisticated signal intelligence (SIGINT) systems, maritime assets are also extremely capable in collecting and exploiting electromagnetic signals or emissions to assess adversary air, surface or subsurface based electronic emitters.

Despite the fact that maritime assets are adequately equipped with systems and sensors allowing them to contribute to the joint ISR effort no single asset can answer every intelligence requirement. Coordinated and joint operations are usually required to maximize the advantages of different types of units and capabilities. Tasking different assets with different collection capabilities to collect against the same information, within the same geographic area, provides flexibility, cross-cueing opportunities, and reduces the chance of deception or errors increasing at the same time the level of confidence in the results.

MISR Shortfalls

It is clear that navies are perfectly suited for ISR tasks. Actually, these tasks are considered to be among the traditional or core navy tasks. In the current security environment with Russian Federation's ambition to restore the Russian Navy as a blue water force with a permanent naval presence in the Mediterranean as well as increasing its naval presence in the Black Sea, Atlantic, and Arctic oceans, NATO should make sure the existing MISR capabilities are not only preserved but also adapted accordingly[6]. It is also pressing for the Alliance and its member and partner nations to stop the decline in certain crucial capabilities. This is especially true considering the inability of NATO to counter the increasing presence of Russian submarines in the Baltic Sea and the North Atlantic due to diminished anti-submarine warfare capabilities (e.g. submarines and MPAs)[7]. The reported capability shortfalls allow Russia's submarines to project power achieving a strategic effect that is disproportionate to the resources committed.

According to a Joint Air Power Competence Center (JAPCC) study on "Alliance airborne anti-submarine warfare" there has been a net reduction of approximately 120 MPA across NATO compared to the inventory in 1985[8]. Respectively, the submarine fleet of North European NATO nations with access in the North Atlantic and the Baltic Sea has decreased by almost 40%[9]. This is a serious shortfall taking into account that submarines constitute a critical MISR capability and a force multiplier as besides locating and tracking adversary submarines they are capable of performing a plethora of other critical tasks such as covert surveillance and reconnaissance, intelligence gathering, landing of special operation forces, etc[10].

Management of MISR Assets - Procurement of New MISR Capabilities

The loss of crucial MISR capabilities like MPAs and submarines is mainly attributed to defense budget cuts across most European NATO nations. As defense budgets are not expected to increase it is necessary to efficiently manage the existent ISR capabilities, especially the high end ones (e.g., unmanned surface, sub-surface and aerial systems), but also make plans for upgrades or procurement of new sensors and systems in order to be able to carry out the full spectrum of NATO activities.

Interoperability is the key for the optimal management of multinational MISR assets pooled together for a NATO operation. Although it's easier said than done interoperability should be sought at the greatest extend possible by making sure current and future MISR capabilities, produce data following common standards, use the same processes to exploit collected information as well as the same security protocols and communication interfaces to transmit and share the resulting products, at a timely manner. Interoperability is also achieved when NATO forces use the same standards for training and exercise together on a regular basis in different and demanding scenarios. The Alliance should take advantage even more of the new and increasingly sophisticated MISR technologies which are proliferating across the battlespace. Unmanned systems launched from the sea are invaluable in gathering intelligence or providing surveillance and reconnaissance. These systems are stealthy, have an ever increasing operating range and endurance, pack more potent sensor and weapons payloads and at the same time they provide a safer environment for the operator by minimizing mission risk.

For the research, development and procurement of new MISR assets NATO should focus on high-payoff, low-risk, low operating and maintenance cost systems designed to penetrate and survive in a range of operational environments including anti-access and area denial environments[11]. Future MISR sensors will generate data at an overwhelming amount. The transmission, reception, processing, and analysis of this volume of data create unique challenges that should be carefully considered during the development of new ISR systems.

Current and under development sophisticated technologies provide new attack vectors that need to be protected. With the digitalization of the battlespace practically all major systems on ships, maritime aircraft, submarines, and unmanned systems are "networked" to a varying degree. As such, cyber-attacks could have a detrimental effect in the conduct of maritime operations. The potential vulnerabilities of some widely-used maritime systems (e.g., ECDIS, AIS, GPS, digital communications, etc.,) highlight the need for MISR assets capable of withstanding cyber- attacks and for commonly accepted cyber security procedures to be in place. Furthermore, sensor and system operators should train and exercise in identifying and responding to the new security threats.

Conclusion

Operations in all warfare domains rely on accurate and timely intelligence to develop understanding and situational awareness. ISR in the maritime domain is an enabler of MSA and of the full spectrum of maritime activities. As such, NATO MISR assets should be interoperable and readily available to be integrated in a coalition force. Critical capability shortfalls should be mitigated with the development and procurement of new platforms, sensors and systems taking advantage of new and emerging technologies.

1. UN-Business Action Hub, IMO Profile, https://business.un.org/en/entities/13
2. Statista, https://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/
3. USN, USMC, USCG, A Cooperative Strategy for 21st Century Seapower, March 2015
4. MC 0588, MC Concept for NATO Maritime Security Operations (MSO), 21 Apr 2011
5. MCM-0140-2007, NATO Concept for Maritime Situational Awareness, 14 Jan 2008
6. http://cimsec.org/new-russian-naval-doctrine/18444
7. According to the commander in chief of the Russian Navy, Adm. Vladimir Ivanovich Korolev, his submarines reached a level of operation not seen since the Cold War as his crews had spent more than 3,000 days on patrol in 2016. (http://www.independent.co.uk/news/world/europe/russia-submarines-patrols-highest-levels-cold-war-attack-putin-fleet-a7664841.html)
8. https://www.japcc.org/portfolio/alliance-airborne-anti-submarine-warfare/
9. https://www.csis.org/analysis/undersea-warfare-northern-europe
10. ASW was identified as one of the critical capability shortfalls at the 2014 Wales Summit. https://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease
11. Intelligence, Surveillance and Reconnaissance, Joint Force 2020 White Paper, June 2014

CDR Pavlos Angelopoulos is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

STREAMLINING MARITIME COMMAND AND CONTROL

CDR Ovidiu Portase, ROU-N
CJOS COE

Source: NATO

Named after the messenger god of the sea, NATO's project TRITON.

Throughout its existence, and especially after the end of Cold War era, NATO has continuously changed focus on why and how to conduct maritime operations. In addition to collective defense and deterrence, the main core task and role, the focus of NATO maritime operations expanded to counter new types of threat (e.g. proliferation of weapons of mass destruction, terrorism, piracy, migration at sea) in order to provide direct and indirect support to crisis management, to promote cooperative security and to contribute to maritime security.

A Need for Change

To address the challenges brought by these new focus areas, NATO underwent major internal reforms to adapt military structures and capabilities, to equip members for new tasks and to deepen and extend its partnerships in accordance with the framework set by the strategic concepts, political and military guidance. In the maritime domain, the Allied Maritime Strategy and the Allied Maritime Governance, along with new and emerging concepts, revised allied publications and other capstone documents established new ways to these ends for maritime forces, which require new or refined means or add more stress on existing ones. Nowadays, maritime C2 stopped to be seen and understood as merely a tactical matter, but a necessary, mandatory and integral part of the operational and strategic thinking required by a comprehensive approach.

Regardless if it is to perform an activity in support of fulfilling a NATO permanent task or as part of a major joint operation, the maritime element of NATO forces and headquarters should be always capable to carry out its command and control (C2) function effectively and efficiently. Agile C2 structures, modern C2 capabilities, standardized operating procedures and up-to-date communication and information systems (CIS) are prerequisites and key enablers in establishing C2 superiority and achieving mission success. Currently, NATO forces and headquarters and some NATO nations use Maritime Command and Control Information System (MCCIS) and Maritime Situational Awareness Demonstrator Prototype (MSA/ BRITE) as the main C2 systems to support C2 in maritime operations.[1] With one of them developed decades ago, these systems are quite specialized, stove-piped systems, and have started to show their operational and technological limitations.

Still fairly capable, MCCIS remains more tactical C2 oriented, hardware dependent, using a client/ server architecture. Based on newer technologies and on a service oriented architecture (SOA), MSA/BRITE is a fusion platform that process larger amounts of information from multiple data sources (e.g. national, industrial, open sources), offers better visualization and analytical tools, and allows an iterative, scalable development. Even though a more modern system which delivers C2 support via a web based set of integrated C2 services, MSA BRITE's prototype status limits systems' availability to the unclassified domain and to a single site only. Despite notable improvements brought by multiple updates and upgrades delivered during their life cycle, the lack of a consolidated system has prevented existing maritime C2 from being as seamless as it could be.[2] These types of limitations and sometimes obsolesce of existing NATO C2 systems, demand modernizations of these systems and their supporting infrastructure or development of new C2 capabilities, systems and services. Moreover, such changes will allow a better and on a larger scale integration with newer NATO and national systems and services.

> **" By taking advantage of the wide-scale adoption of cloud computing technologies in NATO and other benefits provided by NATO IT Modernization (ITM) project, TRITON will provide the NATO maritime community of interest with an integrated, robust, and flexible capability ..."**

A New Solution Called TRITON

In the maritime domain, one solution to the problems related to maritime C2 systems is provided by the collection of maritime information services to be delivered under project TRITON.

A NATO common-funded project within the Bi-Strategic Command Automated Information System (Bi-SC AIS) architecture, project TRITON is the name given to all implementation activities associated with the delivery of services in support of maritime C2. Part of a larger capability package for C2 functional services, TRITON aims to replace the operational level functionality of current NATO maritime C2 systems and through its services to provide the tools for NATO operational users to plan and execute maritime missions in a joint environment. By taking advantage of the wide-scale adoption of cloud computing technologies in NATO and other benefits provided by NATO IT Modernization (ITM) project, TRITON will provide the NATO maritime community of interest with an integrated, robust, and flexible capability throughout the Bi-SC AIS and its deployable and national extensions.[3]

TRITON will provide functionality related to NATO Recognized Maritime Picture (RMP) and White Shipping Picture (WSP), Water Space Management and Prevention of Mutual Interference (WSM/ PMI), as well as a variety of decision aid and operational support functions. Through its services TRITON will enable NATO maritime headquarters and forces to share a common view of the battle space, will improve their situational awareness and decision-making processes and will contribute to an enhanced NATO Common Operational Picture.

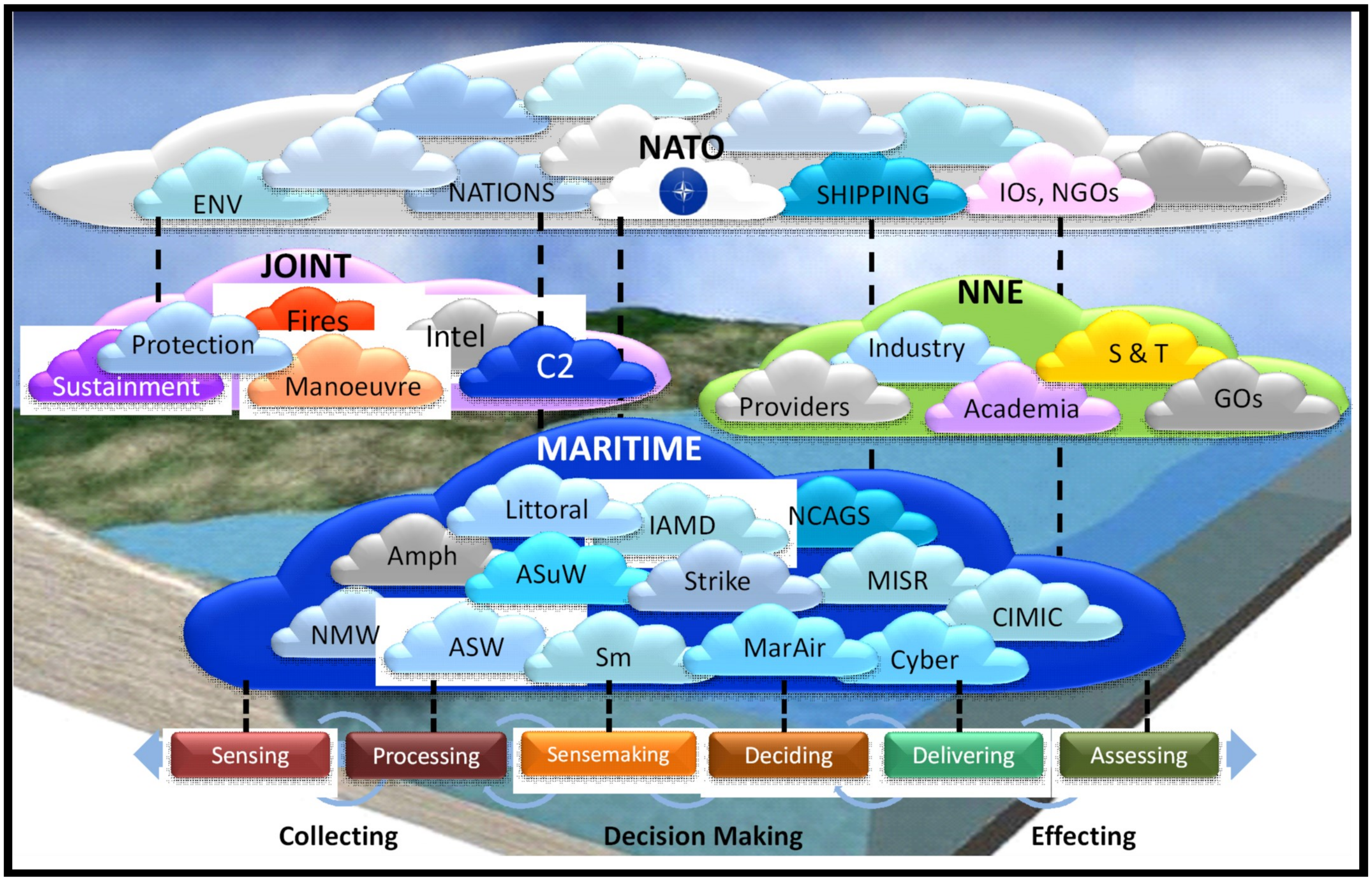
A new system based on modern software architecture and technology, Triton will allow authorized operational users to access its functions from any location using a web-based application. Supported by the NATO's centralized Core Enterprise Services, this capability will be interoperable with national systems and in full compliance with the Federated Mission Networking (FMN) specifications.[4] A deployable kit will support afloat users to have access to TRITON services even in the difficult conditions of a low bandwidth communications.

TRITON capabilities and functionalities will be developed and made available using an incremental approach. By complying to C3 taxonomy and FMN frameworks, it will allow a smooth transition towards new C2 concepts (e.g. ACT's C2 capstone concept).[5,6] During its incremental development, TRITON will increase its level of support to operational and tactical users to provide situational awareness, support for operational planning, tasking, execution and assessment for maritime warfare areas.

Increment 1 of Project TRITON will primarily provide MSA and replace the aging MCCIS and MSA/BRITE. Its main functions include building and disseminating NATO RMP and WSP within the MSA capability, WSM/PMI function of Maritime Operational Planning capability, and a variety of decision aid tools for Maritime Operational Support functions.

Among further improvements, TRITON's second Increment will focus on maritime operational planning and execution, and the complete implementation of Naval Mine Warfare planning, execution and evaluation. Future increments of TRITON will cover more C2 capabilities across other naval warfare areas.[7] Once TRITON reaches its full operational capability, it will become the main platform for supporting C2 of NATO maritime operations throughout the entire Alliance. NATO structures and national forces and commands will be able to share their maritime information live, in a consolidated system, mutually benefiting from data sharing.

At the request of Allied Command for Transformation (ACT), CJOS COE is conducting an operational analysis on the use of TRITON as the main maritime C2 capability. In addition, CJOS COE will develop a draft TRITON concept of employment in collaboration with representatives from Supreme Headquarters Allied Powers Europe (SHAPE), Allied Maritime Command (MARCOM), NATO Communication and Information Agency (NCIA) and other NATO organizations. Based on the initial results of the operational analysis, it can be stated that even though TRITON is merely a material solution, TRITON is a game changer with implications in almost all DOT-MLPFI lines of development. At NATO level, TRITON capability will have a major impact mainly



Source: CJOS COE

Figure 1. A comprehensive approach that might provide the maritime communities of interest a more integrated and federated collaborative working environment based on a new technologies (e.g. cloud computing).

on the business processes/ SOPs at the MARCOM and some of the NATO education and training facilities, while at national level, TRITON will have a significant impact at maritime headquarters, maritime component commander and maritime tactical command levels, especially for the nations which use MCCIS as their national maritime C2 system.[8]

A Starting Point for the Future

The permanent changing nature of the operational environment requires a continuous adaptation and evolution of the ways and means used by NATO maritime forces to conduct operations. New operational needs will trigger and shape the requirements for future maritime C2 capabilities and new technologies (e.g. artificial intelligence) will lead to new engineering solutions. New C2 systems and services, functionalities and concepts of operations will be developed as a resultant of these two vectors, by taking advantage of emerging solutions and capabilities (e.g. federation of clouds, unmanned systems, new operational and protected business networks) which can lead to paradigm shifts.

By moving away from highly proprietary hardware dependent systems and a rigid client/server architecture to a SOA, TRITON opened the path for more agile solutions, solutions which will allow an easier integration of current or future maritime information services and products (e.g. MNMIS - Multinational Maritime Information Services developed under NATO Smart Defense Initiative). The technologies and solutions applied by current and planned NATO CIS capabilities allow a quicker capability development process and subsequently a faster implementation of best practices and lessons learned from previous NATO operations and exercises.[9]

Since its awarded contract in December 2017, TRITON has become a reality and has set the chart for the development and implementation of a new suite of products. Even though this contract addresses just Increment 1 of the project, this moment is a landmark in the future of maritime C2 systems, both NATO and national systems, because its deliverables will set the foundation for next TRITON increments and future maritime information services. ☸

1. MCCIS – Maritime Command and Control Information System, MSA/ BRITE - Maritime Situational Awareness/ Baseline for Rapid Iterative Transformational Experimentation)
2. NCIA Communication, The Messenger of the Sea, 06 February 2016, https://www.ncia.nato.int/NewsRoom/Pages/triton.aspx
3. Matteo Tomasina, NATO signs milestone contract for IT modernization, 30 March 2017, https://www.ncia.nato.int/NewsRoom/Pages/170329_itm.aspx
4. ACQ and C2 Service Line, NCI Agency awards contract for project TRITON, 21 December 2017, https://www.ncia.nato.int/NewsRoom/Pages/21122017.aspx
5. The Consultation, Command and Control (C3) Classification Taxonomy is a tool used to synchronize all capability activities for C3 in the NATO Alliance by connecting the Strategic Concept and Political Guidance through the NATO Defense Planning Process to traditional CIS architecture and design constructs. This taxonomy links CIS capabilities to operational context and it 'charts' the NATO C3 'landscape' by capturing concepts from various communities and mapping them for item classification, integration and harmonization purposes at NATO Enterprise level.
6. Support to ACT C2 Focus Area, https://c2coe.org/policy-development/support-to-act-c2-focus-area/
7. NCIA Command and Control Service Line, Project TRITON Invitation for Bid released to industry, 19 May 2016, https://www.ncia.nato.int/NewsRoom/Pages/160519_TRITON.aspx
8. DOTMLPFI (Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities, Interoperability) is a framework used by NATO for capability development.
9. Sandra Jontz, Sweeping Acquisition Changes on Horizon for NATO Agency Reshaping How it Buys Software, 30 June 2016, https://www.afcea.org/content/?q=Article-sweeping-acquisition-changes-horizon-nato-agency-reshaping-how-it-buys-software

CDR Ovidiu Portase is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

SPACE INTEGRATION WITH NATO OPERATIONS AND PLANNING

CDR William Hawthorne, USA-N
CJOS COE

Source: NASA

A series of satellites with stereo solar panels deployed.

The conclusion of a NATO Strategic Command (Bi-SC) report on the dependencies of space exclaimed, "There is no single NATO operation which does not depend on space."[1] The Space community has a common euphemism that space is "Congested, Competitive and Contested." Access to space services is not guaranteed, and in a conflict with a "near-peer competitor" will most certainly be contested. NATO does not own any space assets, but relies on national contributions for space provided services. So why should NATO care about space support in operations? More specifically why should a Maritime Component Commander (MCC) at the high tactical/low operational level care about space support in operations? How can a MCC mitigate the effects of operations in a space denied or degraded environment? This article will explore the answers to these questions, focused at the Maritime Component level.

> **"NATO does not own any space assets, but relies on national contributions for space provided services."**

NATO's Dependency on Space

Space Support is unique because it cuts across all domains and functions. Whether it is logistics, Intelligence Surveillance and Reconnaissance (ISR), weather, planning, navigation, precision strike, or Satellite Communications (SATCOM), there is no single NATO operation which does not depend on space. In 2014, the Supreme Allied Command for Transformation (SACT) tasked the NATO Communications and Information Agency to conduct the first comprehensive study into NATO's dependencies on space. This study revealed a "high and pervasive dependency on space sourced data, information, and services". The main conclusions of the report are as follows:

1. All NATO operations depend on the availability of Position Navigation and Timing (PNT). PNT includes information necessary for targeting, precision attack, force movement and asset tracking, and precision location of resources.

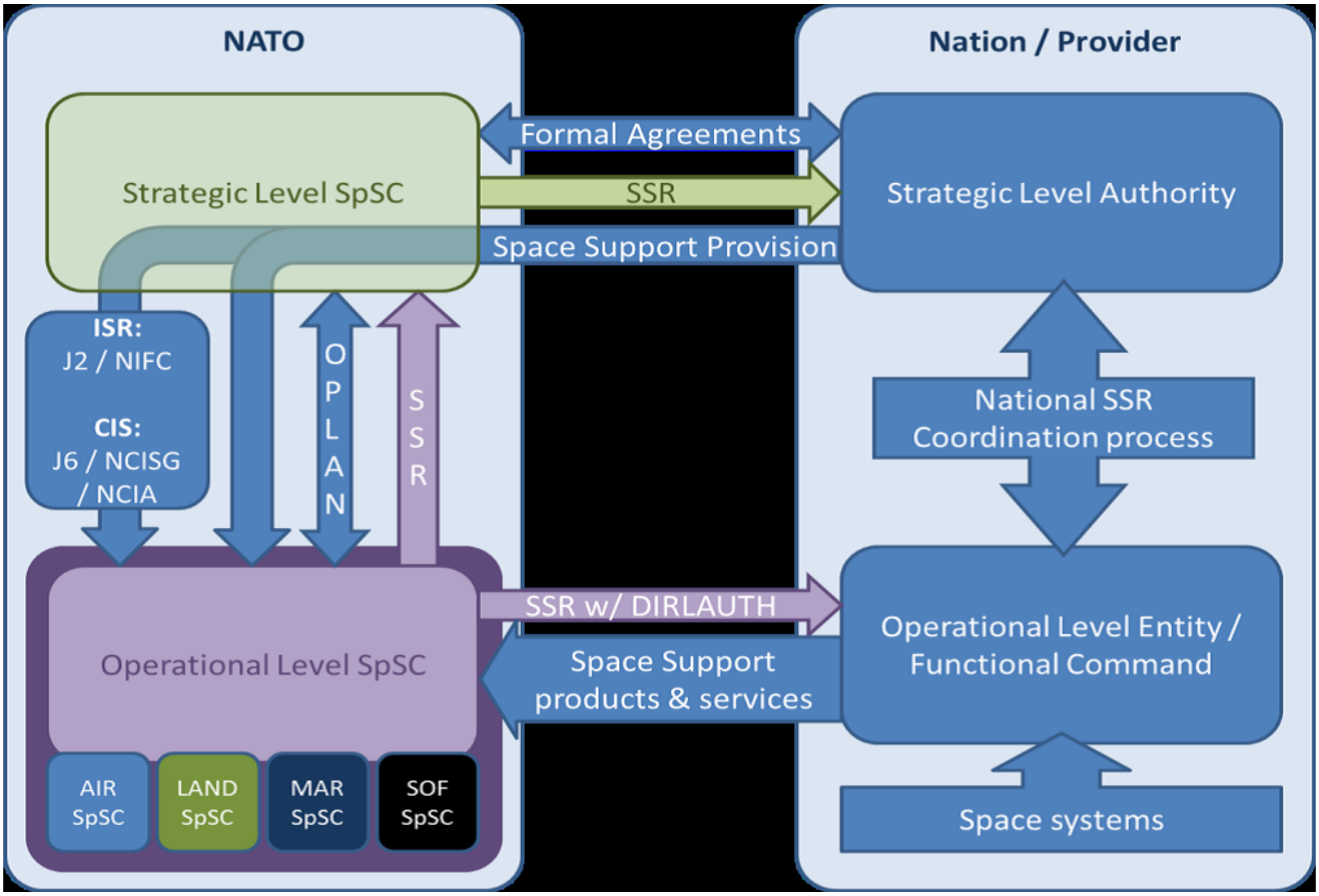
2. Space-based communications are essential in all NATO mission types with the exception of the Anti-Terrorism (AT) mission. The maritime domain is particularly dependent on Space Based C2 due to the tyranny of distance in maritime theatres of operation.

3. All NATO mission types, except AT depend on space based ISR which supports intelligence and

situational awareness for the planning and conduct of missions and operations. Because there is no sovereignty in outer space, space based ISR is unique in the sense that it does not require permission for over-flight rights. It also provides the advantages of providing ISR to areas that could be contaminated such as radiologically or biologically, and wide area surveillance due to the unique vantage point from space.

4. Space-based systems provide a capability to monitor missile launches in peacetime, "Collective Defence of NATO territory is the most serious form of all considered NATO mission types". Space based Overhead Persistent Infrared (OPIR) is essential to the early warning of ballistic missile launches.

5. All NATO mission types except AT depend on weather information provided by space-based sensors. The maritime realm is particularly dependent on space based weather information due to the lack of weather sensing stations in the oceans and seas.



Source: NATO

Figure 1. Illustration of the hierarchical network of Space Support Coordination Elements (SpSCE).

Space is Congested, Competitive, and Contested

It is hard to imagine outer space as congested, isn't space infinite? However in order to operate effectively in space there are certain locations, specifically orbital belts where the satellites need to be depending on the type of satellite and task it needs to accomplish (i.e. communications, weather, and ISR). A detailed orbital mechanics discussion is beyond the scope of this article but in a brief summary, satellites need to be in the ideal location to do their job depending on what type of job that is. These locations are defined by orbit type such as High Elliptical Orbit (HEO), Low Elliptical Orbit (LEO), and Geosynchronous or Geostationary Orbit (GEO). This is the first element that restricts satellite operations. The radiological effects of the Van Allen belt restrict certain orbits for certain types of satellites. Further restricting orbits are orbital debris; over 9,000 man-made objects softball sized and larger, an estimated 40,000 golf-ball sized objects, and millions of smaller objects. To explain the effects of orbital debris, a small 10 centimeter paint chip may seem innocuous, however when traveling at 17,000 miles per hour it poses a significant threat to space craft. With the exponential increase in the number of space craft in orbit resulting in an ever shrinking space, the first one (Sputnik) launched in 1957 to over 2500 today, space is becoming more and more congested and competitive.[2]

Space is contested. The Treaty on the "Use of Outer Space" has been signed or ratified by every space-faring nation, and states in Article IV "States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner."[3] It does not however prohibit the targeting of objects in space, except that any nation would be "liable for damages" to another nation's space craft. Threats to spacecraft and their payloads range from "reversible to non-reversible" and proportionally "easy to difficult" to achieve. Space Weather such as coronal mass ejections occur naturally and have varying effects on satellites and communications. Cyber attacks, and GPS and SATCOM jamming, are relatively inexpensive, easy to achieve threats available to any adversary. Ground based high-powered lasers are more expensive/sophisticated threats, and Anti-Satellite Weapons (ASAT) capabilities at the high end of the threat spectrum are difficult and expensive, but possible.

> **"With over 9,000 man-made objects softball sized and larger, an estimated 40,000 golf-ball sized objects, and millions of smaller objects, space is becoming more and more congested."**

What Space Support in Operations Means to the Maritime Component Commander

With the knowledge of NATO's dependencies on space, the dangers of space, and the fact that it is congested, competitive, and contested, what does this mean to an MCC? If NATO doesn't own any space assets, how does it access space supported information and services? The answer is through a network of space support coordinating efforts that is a budding but rapidly evolving NATO process. The Space Support Coordination Elements (SpSCE) collect, understand and process requests for space support through the NATO established mechanisms (see Figure 1).[4] The method for processing requests for space support is via the Space Support Request (SSR), a form filled out by a Space Support Operator and forwarded to nations via established channels in the space support network. There is a SpSCE at the Strategic level, Operational level, and at each of the component levels. The breakdown and size of a SpSCE varies from component to component but are all similar in that they are task organized to integrate within the staffs. The members of the SpSCE include space experts and non-experts who establish relationships with the component directorates, bring awareness of space capabilities, and optimize battle rhythm involvement to effectively inform the Commander's Decision Cycle. In some instances the SpSCE will be able to provide space based products to enhance planning and operations, other times they may simply bring situational awareness that aids in providing a more complete picture of the operating environment. Space products can include such things as friendly and enemy satellite fly-over times, expected GPS precision dilution, space weather affecting SATCOM and HF communications, and soil moisture content and ice density.

The SpSCE also provides an "in-house" expertise on all things space related. Because space operations can be very highly classified and specialized it is valuable to have an expert involved in the battle without a space background. Often times a staff member may be aware of a space product but not know how to access it. For example the joint effects branch may be aware that there are satellite fly-over products, or products that show GPS expected accuracy but may not know how to access the data. The SpSCE at the component level is networked into the larger space support organization that acts as a conduit to provide timely, accurate products.

These products and information can enable a commander to "fight through" a space degraded/denied environment, but there are limitations to overcome adversary actions. GPS or SATCOM may be jammed and there may be nothing that can be done, but the awareness of this information informs the commander of when his units may need to "fight beneath" in a space degraded/denied environment. This may influence how his orders are written with increased de-centralized execution, or when to be prepared to execute alternate, contingency, and emergency communication and control plans. HF communications may become the primary means of communications and if it is how would the space weather affect those communications? If some of the commander's units don't possess HF capability that may influence task organization if a space denied/degraded environment is expected. This awareness should also inform exercises and how to best prepare for collective self-defence in a space denied/degraded environment. How proficient are units at executing Emission Control (EMCON) plans, operating without GPS, or recognizing when their navigational systems are being "spoofed"? All of this information enables the component commander to wage a two pronged approach to dealing with a space denied/degraded environment to be able to "fight through" and "fight beneath".

Conclusion

Space is congested, competitive, and contested and that trend will only continue to accelerate as nations launch more satellites, the commercial space sector grows, and militaries continue the trend of reliance on space based products and services. In the event of a conflict, the space environment will be degraded or denied to varying levels depending on the competitor. Through continued integration of space support in NATO operations and awareness, NATO can be better prepared to "fight through", "fight beneath", and win. Space Support in Maritime Operations is one more enabler that enhances and informs the commander's decision cycle. Much like cyber, space cuts across all operational domains and disciplines; air, maritime, land, logistics, planning, operations. Also like cyber, space support is an enabler that is evolving into a formalized structure designed to continue to enable and remain resilient. There is no single NATO operation which does not depend on space and as NATO continues to evolve space support in operations it will be better prepared for future conflicts. For more information on space support in NATO operations and space education opportunities please visit the BiSC space page on NSWAN at https://dnbl.ncia.nato.int/Space/SitePages/Home.aspx.

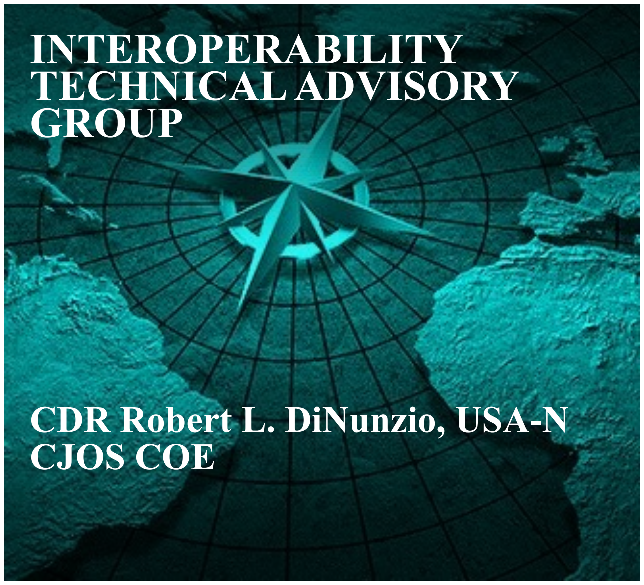
[1] SH/J3SPOPS/14-305625 3400/TSC MDX 0070/TT-10435/Ser:NU0018 'SPACE SUPPORT TO NATO OPERATIONS: NATO DEPENDENCIES ON SPACE'

[2] Orbital Objects, https://www.nationalgeographic.com/science/space/solar-system/orbital-objects/

[3] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies; https://www.state.gov/t/isn/5181.htm

[4] NATO Allied Joint Publication 3.3 (AJP3.3)

CDR William Hawthorne is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.



INTEROPERABILITY TECHNICAL ADVISORY GROUP

CDR Robert L. DiNunzio, USA-N
CJOS COE

Source: British Ministry of Defence

HNOMS Helge Ingstad seen from the Lynx of HMS Montrose.

The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) has been involved in improving allied, coalition and joint operations through observation of exercises specifically focusing on interoperability issues and challenges. In 2014, CJOS COE stood up the Interoperability Technical Advisory Group (ITAG) to formally bring together key stakeholders to collectively identify specific tasks that will lead to improved interoperability of U.S., allied and coalition maritime and expeditionary forces.

> " Today, with NATO and its partners conducting more operations together, interoperability is more important than ever. And there's good news: much can be achieved without great expense."[1]
>
> \- Hans Binnendijk

Primarily through observing the Bold Alligator amphibious exercise series, the ITAG identified nine gaps in terms of training, doctrine, C2 and operations. 2017 proved to be the most productive year for the ITAG - mainly through the collaboration, cooperation and dedication of the key stakeholders in closing each of these gaps. Key activities and highlights of the past year include:

Training

United States Fleet Forces Command (USFFC) training directorate (N7) developed USN training objectives in primary warfare areas for NATO exercises. Additionally, in preparation for the US to lead the Standing NATO Maritime Group (SNMG-1) in 2019, N7 developed a training plan for the SNMG staff to better understand NATO operations and procedures to include a customized program focused on NATO-centric academic and synthetic wargame vignettes.

Doctrine

In coordination with the Navy Warfare Development Command (NWDC), the ITAG contributed to the update of the Allied Tactical Publication Eight (ATP-08 Vol 1) - Doctrine for Amphibious Operations, agreed to by NATO Nations in March 2017.

Source: Open Source

The goal of the Interoperability Technical Advisory Group is to identify a means that will allow U.S., allied and coalition maritime and expeditionary force commanders a means to employ decision making unity of effort and speed of command with mission partners at any time within the same security domain.

Command and Control

USFFC N6 directorate assists in the establishment of the transfer of the Recognized Maritime Picture and Common Operation Picture of maritime positional information between the US Navy Maritime Operational Center (MOC) and NATO's Allied Maritime Command (MARCOM).

Operations

Through the development of a classified portal on the NATO Secret Wide Area Network (NSWAN), USFFC N3 can post relevant OPTASK Link and Communication joining instructions between U.S. Navy and NATO maritime and expeditionary forces.

Continued Way Ahead

While much progress had been made during the past year, CJOS COE continues to monitor allied, and coalition training opportunities to include Composite Training events and Fleet synthetic training evolutions involving NATO nations. Exercise TRIDENT JUNCTURE will be a key event later in 2018 to observe interoperability issues as the exercise will have the aim of certifying the NATO Response Force 2019, strengthening relationships with NATO forces highlighting the USMC capability to support NATO amphibious operations. ☸

CDR Robert L. DiNunzio is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

1. Hans Binnendijk, "For NATO, True Interoperability Is No Longer Optional," http://www.defenseone.com/ideas/2017/12/nato-true-interoperability-no-longer-optional/144650/?oref=d-river

CJOS COE ANNUAL REPORT 2017-2018

CAPT Dermot Mulholland, CAN-N
CAPT Bruno Scalfaro, ITA-N
CJOS COE

Source: NATO

View from the bridge of the HMCS Halifax.

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, an organization outside the NATO Command Structure, 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 2017-2018 CJOS PoW is summarized below:

Maritime C2 Programme (NATO TRITON Project)

TRITON is a software intensive capability to provide Maritime Command and Control (C2) Information Services and it will replace NATO's current maritime C2 capabilities. At the request of NATO Headquarters Allied Command Transformation (HQ ACT) and Supreme Headquarters Allied Powers Europe (SHAPE), CJOS COE is conducting an operational analysis for the use of TRITON as the main Maritime C2 capability. Working together with representatives from Allied Maritime Command (MARCOM), NATO Communication and Information Agency (NCIA) and other NATO commands, CJOS COE will develop a Concept of Employment considering TRITON capabilities and the new C2 architecture for static and afloat commands.

Interoperability Technical Advisory Group (ITAG)

In response to the CUSFFC request for CJOS COE to contribute to improving interoperability in combined and joint operations, the COE, in coordination with USFFC, stood up the Interoperability Technical Advisory Group (ITAG). The working group, consisting of stakeholders such as USFFC N3, N6, N7, N8/9, NWDC, MARFORCOM, CNSL, CNAL, CSG-4, and STRIKFORNATO, meets bi-monthly to identify and close interoperability gaps across doctrine, lessons identified, training, capabilities and experimentation. Most recently, the ITAG conducted its' quarterly working group meeting and reviewed the progress made in 2017. Improvements in allied situational awareness, training for the Standing NATO Maritime Group and mission network enterprise solutions were discussed.

NATO Mission Thread Concept Implementation

The NATO Federated Mission Networking Implementation Plan (NFIP), Vol I, identified the need for a mission thread-type approach. The use of this methodology to establish consistent content and context for interoperability, training, planning and mission activities would enhance the effectiveness of future operations and inform FMN implementation.   As a result, this document called for the Military Committee to task the strategic commands to produce a NATO Mission Thread Capstone Concept.   This concept paper, developed in response to that tasking, is the result of significant analysis and several years of internal discussion within various NATO communities.

The NATO Mission Thread (NMT) Capstone Concept will provide a coherent definition of mission threads and detail the expected operational benefits of this common approach.   Furthermore, it will also address some general aspects of implementation in light of NATO's level of ambition and in support of other broad key initiatives, such as the Readiness Action Plan. Following the Concept endorsement an implementation phase, development of the Doctrine, Organization, Training, Standards will commence; require content contributions and participation in validation events for specific mission areas.

NATO Urbanization Concept

Since 2014, Allied Command Transformation (ACT) has been working on an “Urbanization Project” to support their examination of the future security environment through the Strategic Foresight Analysis (SFA) and the Framework for Future Alliance Operations (FFAO). In this context, ACT with support from Allied Command Operations (ACO) was tasked to develop Both Strategic Commands (Bi-SC) Conceptual Study examining challenges to war/warfare in mega cities and large urban areas. CJOS COE greatly supported this work. ACT presented the findings and military advice to the Military Committee (MC) late March 2017. The MC then gave further tasking to ACT/ACO to produce a capstone concept on Urbanization. The concept should be ready for implementation in 2019.

Support to Joint Allied Lessons Learned Command

CJOS COE is working with NATO Supreme Allied Command Transformation in providing support to Joint Allied Lessons Learned Command (JALLC) on their analysis projects. SACT is collecting Analysis Requirements for the JALLC in Lisbon on a semi-annual basis and CJOS COE will provide assistance to JALLC in conducting analysis reviews in support of their Programme of Work.

NATO Maritime Integrated Air and Missile Defense (M-IAMD) Panel

The M-IAMD panel is the successor to the Anti Ship Missile Defense (ASMD) panel and reports directly to the NATO MAROPS Syndicate 2. The M-IAMD panel meets annually in the fall to develop and refine M-IAMD standardization documents in order to enhance IAMD interoperability of NATO forces. CJOS COE is the secretariat for the panel.

Support to Capability Requirement Review 2019 Planning Process

CJOS COE will provide Subject Matter Experts (SMEs) for the planning phases of the Capability Requirement Review (CRR19). This effort will contribute in identifying NATO/Allies capabilities, and discovering shortfalls preventing the fulfillment of NATO’s Level of Ambition (LoA).

Strategic Foresight Analysis (SFA)

The SFA Report provides a wide-ranging shared understanding of the future security environment that is expected to unfold out to 2035 and beyond. The Report depicts political, social, technological, economic, and environmental trends and their implications. The latest report was released October 2017. Work has started on the next SFA update report, and CJOS COE will contribute as subject matter experts (SMEs) in the process, ensuring that the project has a valid input on maritime aspects and developments.

Framework for Future Alliance Operations (FFAO)

The FFAO proposes how Alliance forces might plan to transform, and recommends abilities that these forces may need to develop over the next 15 years. FFAO is intended to directly inform all steps of the NATO Defense Planning Process (NDPP). CJOS COE has contributed to the FFAO development by providing SMEs, advice and drafting/editing services. The FFAO report is due for release 2018.

Exercise Support

Exercises BRILLIANT MARINER (BRMR), TRIDENT JAVELIN (TRJN), and TRIDENT JAGUAR (TRJR) are tactical and operational level headquarters training exercises designed to practice and certify the coordination between NATO Command Structure (NCS) and NATO Force Structure (NFS) entities. CJOS COE will provide a subject matter expert to support the maritime element of the exercises and gather observations enabling further post-exercise analysis.

Maritime Intelligence, Surveillance, and Reconnaissance (MISR)

CJOS COE is the custodian of a new Allied tactical publication (ATP) describing NATO procedure for maritime intelligence, surveillance and reconnaissance (MISR). The new publication (ATP-102) is developed to address the identified gap in NATO doctrine in MISR as the existing joint ISR doctrine (AJP-2.7) doesn’t address the ISR issues in the maritime domain. The first study draft of the document is completed and is currently under review by the NATO nations. ATP-102 is expected to be ratified by the end of 2018.

Counter-Improvised Explosive Device in Maritime Environment

CJOS COE is supporting investigations on Improvised Explosive Device (IED) threats and countermeasures in the maritime domain. For CJOS COE, the goal is to identify capability shortfalls along the Doctrine, Organization, Training, Material, Personnel, Facilities (DOTMLPFI) spectrum and identify ways to mitigate these shortfalls. For this purpose, CJOS will strive to identify ways to strengthen each of the three C-IED pillars: Prepare the Force; Attack the Network; Defeat the Device.

Maritime Situational Awareness (MSA)

Having held two previous roundtable (RT) forums, at Madrid in June 2015 and at Norfolk in April 2016, the third forum, 2018 Maritime Security Regimes Roundtable (MSR RT 18), has been scheduled for 24-25 April 2018 in Norfolk, Virginia, USA, at the new Slover Library. The theme of this international forum is: ‘Exploiting Synergies to Improve Delivery of Global Maritime Situational Awareness’. The agenda will seek to build on the last roundtable discussions from Norfolk with the aim of agreeing a framework for effective sharing of MSA between global MSRs. The forum will be conducted at the unclassified level and the audience will be drawn mainly by invitation from the international MSA community, representing a strong cross-section of government, non-government, military, academic and industry stakeholders.

Theatre Anti-submarine Warfare (TASW)

During the 2012 Submarine Commanders Conference (SCC), Commander of Submarine Forces NATO (COMSUBNATO) was tasked in by the Maritime Operations Working Group to develop an Alliance TASW concept. A draft was approved by SCC in 2013 and presented to Maritime Operations Working Group (MAROPSWG) in 2014. The TASW concept is an operational level application for ASW. The goal of TASW would be to eliminate the threat that adversarial submarines could bring into a theatre or operation. CJOS COE support was requested to review the TASW concept, develop a BI-SC arrangement and a MC concept.

Multinational Maritime Information Systems Interoperability Board (M2I2)

M2I2 is a U.S. led user's forum for the Combined Enterprise Regional Information Exchange System (CENTRIXS) Maritime. M2I2 is the only coalition maritime governing body that enables C2, mission planning, situational awareness and information sharing/exchange for the U.S. and Coalition Partners. M2I2 is a body consisting of those Countries and organizations that represent and support operational forces and provide technical, information assurance, requirements, and planning associated with Internet Protocol (IP) networks and associated services in the form of Operations and Planning applications. It is recognized that M2I2 provides the forum for enhancing and addressing CENTRIXS Maritime operational interoperability, this is particularly relevant now given the operational environment of the future is perceived to be one of Coalitions, which are flexible in their constitution and unlikely to be constrained to regular Allied partners. CJOS is seen as a key member to the M2I2 forum than can impose impartiality whilst ensuring interoperability remains its focus.

Joint Battlespace Management

Throughout several exercises it has been a challenge ensuring the effective coordination and/ integration of all elements of a joint force. Introducing long range anti-ship missiles with the capacity to fly over land has hampered coordination of different needs in the Battlespace area; especially in the coastal and littoral environment. NATO was well underway to develop a stand-alone doctrine for Joint Battlespace Management (AJP-3.20). However, based on comments from nations the decision was made to stop this development and instead focus on implementing required aspects of Joint Battlespace Management into the revised AJP-3 (Allied Joint Doctrine for the Conduct of Operations). CJOS COE has been part in the writing team of this significant publication. Draft version is available on NSO forum, and the publication is due for release 3rd Quarter 2018.

Maritime Cyber Security

Cyber Security has been recognized as a growing concern all over the world. In the maritime domain cyber security has been lagging behind the financial sector. The Maersk shipping company cyber attack was the catalyst that work up the merchant shipping industry to the very real cyber threat to the maritime domain. The possibility of a cyber-attack being directed towards the maritime supply chain is very likely, and the impact of that attack could be financially catastrophic. Cyber risks within the maritime domain need to be analyzed and evaluated to create a cultural awareness, to reexamine the priorities and methods for safeguarding maritime critical infrastructure and improve cyber resilience within the Maritime Domain. Continued cooperation and collaboration among different stakeholders, military and academia are a necessity to identify and tackle those risks. CJOS COE is working in cooperation with various stakeholders, military, and academia to identify the risks that will have an impact on the maritime domain.

NATO Maritime Operations Working Group (MAROPSWG)

Develops standardization in doctrine, tactics and tactical instructions and procedures in maritime operations to improve the effectiveness of NATO forces. The MAROPSWG is the largest Maritime Standardization Board Working Group and is responsible for a wide range of tactical publications. National Maritime Tactical Schools are strongly represented - mainly at the Naval Captain level. The MAROPSWG operates with four Sub-Groups: Heads of Delegation, Syndicate 1 - Under Water Warfare, Syndicate 2 - Above Water Warfare and Electronic Warfare, and Syndicate 3 - Maritime Communications and Information Exchange. Together their focus is standardizing Maritime Operations by NATO Forces to include, but not be limited to Submarine Warfare, Anti-Submarine Warfare, Above Water Warfare, Tactical Communications, and maritime Electronic and Acoustic Warfare. In support of MAROPSWG, CJOS COE is deeply committed in playing an active role providing WG

Chairmanship and subject matter experts for the Syndicate Sub-Groups.

Amphibious Operations Working Group (AWG)

AWG's focus is standardizing Amphibious Doctrine, Techniques and Training Methods, Equipment for use in Amphibious Operations, Communications and Operational Intelligence, Support for Amphibious Operations, and Command and Control relationships. As an independent, multinational source of innovative advice and expertise on all aspects of maritime operations, CJOS COE collaborate with developing and promoting maritime concepts and doctrine. Regarding amphibious, CJOS COE has also been collaborating with Amphibious Leaders Expeditionary Symposium (ALES) and RAND Corporation on the potential development of a large scale multinational amphibious force within NATO framework.

ATP-08 Volume III Riverine Operations

CJOS COE is collaborating with US Navy Warfare Development Command (NWDC), on the writing of ATP 08 Volume III. As part of the ATP 08 Amphibious Operations, this new volume describes riverine tactics, techniques, and procedures and provides guidance for the execution of riverine operations. This volume details elements build off of Volume II - Tactics, Techniques and Procedures for Amphibious Operations, and how riverine operations may tie into an amphibious operation or subsequent phase of actions ashore across the range of military operations from humanitarian assistance to offensive action. The second review meeting will take place in Amsterdam, Netherlands in April 2018.

Integration of Unmanned Aerial System (UAS) into Maritime Operations

CJOS COE provides support to MARCOM in developing solutions for the integration of UAS into maritime operations (asset de-confliction, battle space management, and maritime situational awareness).

NATO Prevention of Mutual Interference (PMI) - doctrine for Unmanned Underwater Vehicles (UUV)

CJOS COE currently provides support to MARCOM/CONSUBNATO for the creation of PMI NATO-doctrine for suite of both military and non-military UUV. This action item has been endorsed by all Alliance submarine operating nations during the Submarine Commanding Conference of 2016.

Dual Use of Military Defense Capabilities for Non-military Purposes (DuMDC)

CJOS COE provides support to the Italian Defense Staff for the development of a Multinational Capstone Concept on DuMDC, in order to explore and study possibilities to optimize economical resources, find new/alternative ways to sustain military capabilities, render AF more flexible, robust and responsive, support resilience and civil preparedness.

Review ATP-17 Naval Arctic Manual (Chapter 14) Submarine & Antisubmarine Operations

CJOS COE is working with COMSUBNATO to improve the utility of ATP-17 for arctic operations. The purpose is to provide detailed information for submarines and ASW assets operating in the constrained operational environment of the arctic. Ultimately the goal is to develop meaningful tactical data for each unit to include practical guidance for sonar operations, counter-detection and evasion.

Anti-Access Area Denial Study

Anti-Access Area Denial (A2/AD) tactics challenge NATO's ability to conduct maritime operations throughout its AOR CJOS COE has produced a classified study paper to identify these threats that will subsequently lead to the development of NATO tactics, techniques and procedures for use in an A2/AD environment.

Interoperability Handbook

CJOS COE will release the updated Allied Information Handbook in 2018. The interoperability handbook is designed to facilitate operations between Allied navies. The handbook is divided into two sections that provide overview of US exercises and ship training curriculum and historical interoperability issues from past experiences. Look for the handbook to be posted on the CJOS COE website in 2018.

Partnering with Academia

Through several bi-lateral Memorandums of Understanding CJOS COE has been able to create mutually beneficial academic relationships with Old Dominion University and the Romanian National Defense University. Within the framework of these MOU’s CJOS COE is able to directly connect its work with academia and promote the free exchange of ideas across the gap between the uniformed services of NATO and some of the world’s top research institutions. CJOS COE co-hosts a bi-annual lecture series with ODU that is focused on maritime security issues and has addressed such complex topics a coastal resiliency and space based-AIS.

Geographic Focus Areas

Embracing the idea that NATO’s AOR is global, CJOS COE has ventured to develop its expertise in areas that present unique challenges to the Alliance: Artic, West Africa, and South East Asia. As such, CJOS COE has engaged with regional entities such as Association of Southeast Asian Nations (ASEAN) in Asia and Maritime Organization for West and Central Africa (MOWCA) in Africa. Through these relationships CJOS COE has been able to build much needed regional expertise that has been vital to broadening NATO’s reach – specifically in cyber space and in the area of global maritime security.

Big Data

Based on Gartner's definition, "big data" could be considered as "high volume, high velocity and high variety information assets that require new forms of processing to enable enhanced decision making." There are two areas that challenge naval warfare development: the use of ashore cloud based networks and the administration of data security permission. CJOS COE is working with other NATO accredited COE's, warfare development commands, industry and academia to draft a white paper stating "big data" issues particular to the maritime environment.

Space Support to Maritime Operations

Although NATO does not own or operate space assets, it is a consumer of space information that cuts across all domains. NATO's Maritime Command (MARCOM) desires to significantly increase its integration into the space domain through education, training, and doctrine development. CJSO COE is assisting a larger Bi-Strategic Command effort to include space support to operations at the JFC and component levels including the Maritime Component Command (MCC). CJOS COE provided subject matter expertise and manning augmentation to MARCOM during exercise TRIDENT JAVELIN 2017, marking the first dedicated space support to operations for a NATO MCC. CJOS COE is currently developing an MCC Space Support to Operations Standard Operating Instruction (SOI).

Collaborative Anti-Submarine Warfare (ASW) – Maritime Unmanned Systems in ASW

The development of autonomy and unmanned platforms has followed a dynamic path in the recent years. Supreme Allied Commander Transformation (SACT) has asked CJOS COE to update and develop the Alliance

Source: British Ministry of Defence

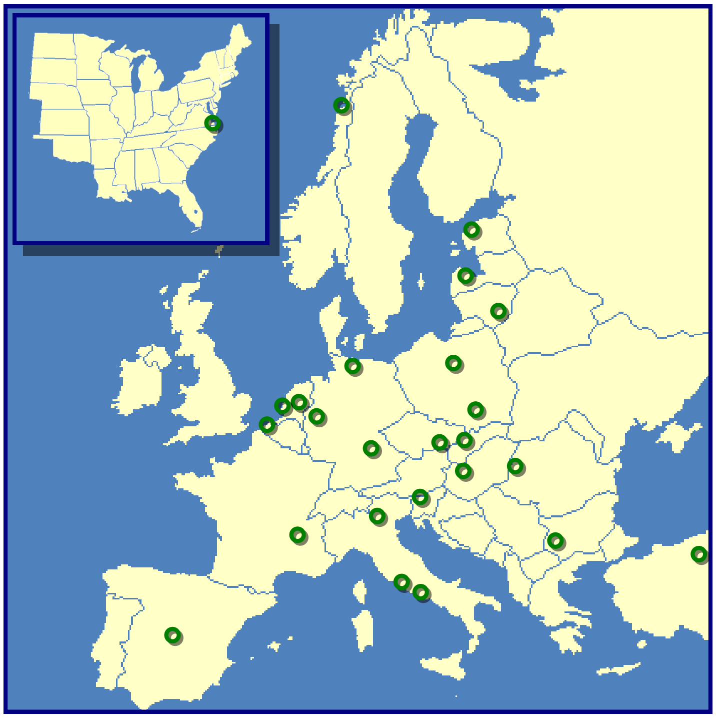
Lynx Mk8 helicopter firing all 60 of its flares over the type 45 destroyer HMS Dragon.

awareness on this matter, and develop potential Concept of Operations for such systems in ASW. Connected with several companies, as well as the NATO Centre for Maritime Research and Experimentations (CMRE), CJOS COE delivered a study to answer this request. The result should contribute to a better understanding between warfighters, scientists, and systems' designers to increase NATO ASW capability in the near future. ☸

CAPT Bruno Scalfaro and CAPT Dermot Mulholland head the Transformation Branch and Strategic Plans and Policy Branch, respectively, at CJOS COE in Norfolk, Va. For further information on this subject, they may be contacted at usff.cjos.coe@navy.mil.

CENTRE OF EXCELLENCE FACT SHEET

A COE is a nationally or multi-nationally sponsored entity, which offers recognized expertise and experience to the benefit of the Alliance, especially in support of transformation. COEs are not part of the NATO command structure, but form part of the wider framework supporting NATO Command Authority. They support transformation through Education and Training, Analysis of Operations and Lessons Learned, Concept Development and Experimentation, and Development of Doctrine and Standards. ☸



There are 25 NATO accredited COEs:

Joint Air Power Competence Centre (JAPCC/DEU)
http://www.japcc.de

Defense Against Terrorism (DAT/TUR)
http://www.coedat.nato.int

Naval Mine Warfare (NMW/BEL)
http://www.eguermin.org

Combined Joint Operations from the Sea (CJOS/USA)
http://www.cjoscoe.org

Civil Military Cooperation (CIMIC/NLD)
http://www.cimic-coe.org

Cold Weather Operations (CWO/NOR)
http://www.forsvaret.no/coe-cwo

Joint Chemical, Biological, Radiological & Nuclear Defense (JCBRN/CZE)
http://www.jcbrncoe.cz

Air Operations Analysis Simulation Centre (CASPOA/FRA)
http://www.caspoa.org

Command & Control (C2/NLD)
http://c2coe.org

Cooperative Cyber Defense (CCD/EST)
http://www.ccdcoe.org

Operations in Confined & Shallow Waters (CSW/DEU)
http://www.coecsw.org

Military Engineering (MILENG/DEU)
http://milengcoe.org

Military Medicine (MILMED/HUN)
http://www.coemed.hu

Human Intelligence (HUMINT/ROU)
http://www.natohcoe.org

Counter - Improvised Explosive Devices (C-IED/ESP)
http://www.coec-ied.es

Explosive Ordnance Disposal (EOD/SVK)
https://www.eodcoe.org

Modeling and Simulation (M&S/ITA)
https://www.mscoe.org

Energy Security (ENSEC/LIT)
http://enseccoe.org

Military Police (MP/POL)
http://www.mpcoe.org

Crisis Management & Disaster Response (CMDR COE/BGR)
http://cmdrcoe.org

Mountain Warfare (MW/SVN)
http://mwcoe.org

Stability Policing (SP/ITA)
http://nspcoe.org

Counter Intelligence (CI/POL)
http://www.cicoe.org

Strategic Communications COE (STRATCOM/LVA)
http://www.stratcomcoe.org

Security Force Assistance (SFA)
http://www.esercito.difesa.it

CJOS COE REQUEST FOR SUPPORT
(Continued from page 7, “*How We Are Tasked*”)

Originator:

Nation	
Name	
Service	
Telephone Number	
E-mail Address	
Signature & Date	

Point of Contact/Subject Matter Expert: (Provide information if different from the originator)

Name/Rank	
Command/Branch	
Service	
Telephone Number	
E-mail Address	
Signature & Date	

Requested Task:

Additional Information: (Provide details to why this task is important)

Background: (Identify the aim of the task, what benefit will result from this task for the requesting nation, NATO, and/or other organization)

CJOS COE STAFF DIRECTORY

NAME	POSITION	TELEPHONE # +1 (757) 836-EXT DSN 836-EXT
	STAFF HEADQUARTERS	
VADM Bruce Lindsey, USA-N	Director	2997
CDRE Tom Guy, GBR-N	Deputy Director	2452
CDR Antonio Ting, USA-N	Fiscal Officer	2457
LT Jesse Nerius, USA-N	Flag Aide	2452
CDR Jarrod Mosley, USA-N	Directorate Coordinator	2611
YNC Shonka Houston, USA-N	Admin Assistant	2453
	STRATEGIC PLANS AND POLICY BRANCH	
CAPT Dermot Mulholland, CAN-N	Strategic Plans and Policy Branch Head	2450
CDR Joerg Maier, DEU-N	Strategy and Policy Analysis Section Head	2464
CDR Jose Garza, USA-N	SPA SO	2462
CDR Geir Hestvik, NOR-N	SPA SO	2440
CDR Ricardo Valdes, ESP-N	SPA SO	2442
CDR Michael DeWalt, USA-N	Strategic Communications and Knowledge Management Section Head	2461
CDR Ovidiu Portase, ROU-N	SCNO SO	2451
CDR Jonathan Sims, USA-N	SCNO SO	2463
ITCS Stephen Wheeler, USA-N	SCNO SO	2467
	TRANSFORMATION OPERATIONS BRANCH	
CAPT Bruno Scalfaro, ITA-N	Transformation Operations Branch Head	2449
CDR Gwenegan Le Bourhis, FRA-N	Expeditionary Operations Section Head	2446
CDR Jose Conde, PRT-M	EO SO	2444
CDR Josh Heivly, USA-N	EO SO	2454
LTCOL Jos Schooneman, NLD-RM	EO SO	2443
Lt Col Luca Bertonati, ITA-AF	EO SO	4080
CDR Pavlos Angelopoulos, GRC-N	Maritime Operations Section Head	2537
CDR William Hawthorne, USA-N	MO SO	2429
CDR Robert DiNunzio, USA-N	MO SO	2445
WO1 Jack Cuthbert, GBR-RM	MO SO	2960

Mailing Address:
CJOS COE
1562 Mitscher Ave. STE 250
Norfolk, VA 23551
USA

CJOS COE

NATO
OTAN
COMBINED JOINT OPERATIONS FROM THE SEA
ODU
IDEA FUSION
UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”
UNITED STATES FLEET FORCES COMMAND

TRANSFORMING ALLIED MARITIME POTENTIAL INTO REALITY