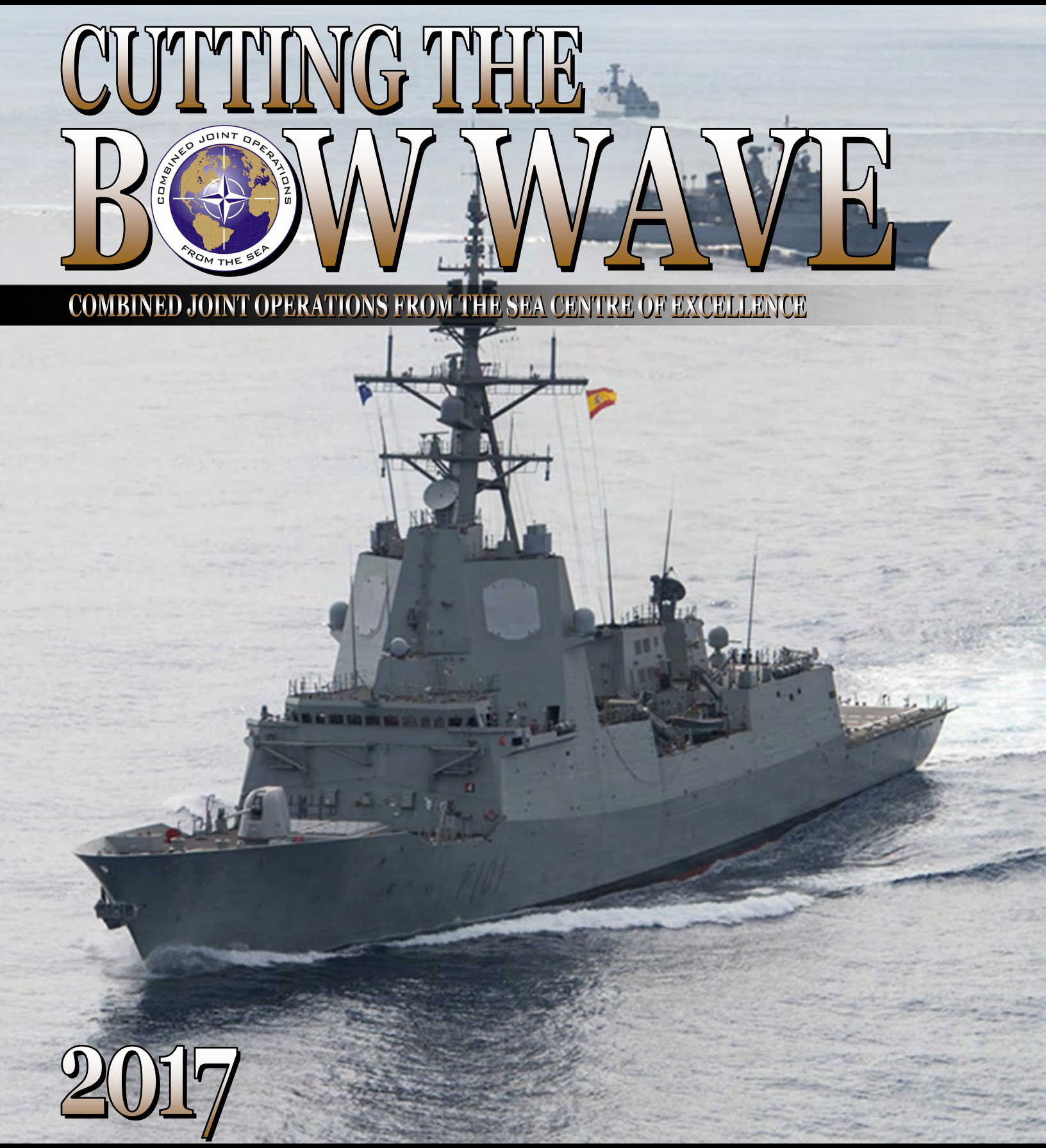
CUTTING THE BOW WAVE

COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE



2017

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 Navy participating in NATO group passing exercise (PASSEX); leading the formation is the Alvaro de Bazan (F101). Photo source: NATO

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

Associate Editor:
Colleen Hazlehurst

USFF.CJOS.COE@NAVY.MIL

TABLE OF CONTENTS

Source: NATO

NATO Exercise BRILLIANT MARINER 2013.

As I complete my first year as the Director, I would like to take an opportunity to reflect on the importance of CJOS COE's work as navies across the world evolve and adapt to the ever changing maritime environment. The maritime environment is growing more complex daily; we have the chance to steer the Alliance and partner navies with purpose and direction to a cohesive and interoperable readiness. CJOS COE is uniquely positioned to play a lead role in achieving this interoperability as we look to the future.

It is often said that it is not the strongest of the species that survives, nor the most intelligent that survives. It is the one that is most adaptable to change. The challenge before us is how quickly can we adapt to the changes presented by the adversary, specifically in the maritime domain? Challenges to sea lines of communication and freedom of the seas in every area of the world will have significant ramifications inside and outside the Alliance.

The maritime environment is shifting from one focused in limited domains with line of sight weapons to one where sea control may be contested across multiple domains to include space and cyber capabilities. The rapid evolution of technology and information sharing is dramatically increasing the threat's power and influence. As the adversary's regional advantage grows with the ability to project force and influence at greater range more quickly, we must adapt through distributed maneuver warfare – on the seas.

Embracing the principals of integration, distribution and maneuver will allow us to lead turn our adversaries. We must empower our commanders with the tools and skills to incorporate these principals into a multi-domain battle for sea control. This will enhance our ability to operate inside contested environments while challenging our adversaries' calculus with greater uncertainty, operational complexity and increased risk. Effectively maneuvering and integrating a distributed force that encompasses partner forces requires exceptional cooperation and interoperability.

Renewed focus on interoperability initiatives and information sharing, coupled with exploring new opportunities for combined operations and training will be critical to achieving the necessary interoperability. The rapid pace of change and increasingly complex nature of our maritime challenges offer an opportunity gain advantages over potential adversaries. However, we must be bold enough and creative enough to seize the initiative or potential adversaries may beat us to the punch. ☸

★ ★ ★

Vice Admiral Richard Breckenridge graduated from the U.S. Naval Academy in 1982 with a Bachelor of Science in Aerospace Engineering. He also holds master's degrees in engineering acoustics and electrical engineering from the U.S. Navy Postgraduate School.

Breckenridge served on USS Hammerhead (SSN 663), USS Florida (SSBN 728) (Gold), and USS Philadelphia (SSN 690). He commanded USS Memphis (SSN 691) in Groton, Connecticut, where he conducted a U.S. Central Command deployment in support of Operation Iraqi Freedom. Breckenridge also served as commodore of Submarine Squadron (SUBRON) 4 and commander of Submarine Group 2 in Groton.

His staff assignments include special assistant to the secretary of defense; special assistant to the director, Naval Reactors; chief of staff, Force Structure, Resources and Assessment Directorate (J8) on the Joint Staff; deputy director, Submarine Warfare Division (N87); director, Undersea Warfare Division (N97); and director, Warfare Integration (N9I) on the staff of the chief of naval operations.

Breckenridge's decorations include the Distinguished Service Medal, Defense Superior Service Medal, and Legion of Merit.

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 24 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 2015 contained 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 become 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 70). 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!

For the past year, CJOS COE has pushed forward working the seams and tension points that surround the delivery of maritime expeditionary power. As Deputy Director, I have learned much and, more importantly, 'observed' these seams and tension points as they are played out amongst Nations, Alliances and Coalitions. Like all Centres of Excellence, CJOS COE is structurally situated on the side of NATO's Allied Command Transformation Headquarters (ACT HQ) and as a result of its NATO accreditation is tasked, in part, by Chief of Staff to NATO ACT. However, CJOS COE is unique and privileged to an extent that it is the only NATO accredited COE located outside Europe and the only COE hosted by the United States. These two points of circumstance offer a privileged position and have allowed the team the opportunity to develop thoughts and understanding as we watch (and help) Maritime Expeditionary Warfare policy and tactics develop.

This edition of *Cutting the Bow Wave* draws out some of these thoughts and, hopefully, gives the community a sense of the value we offer, and the contributions made by this small team. Contemporary issues such as Hybrid and Cyber Warfare in the Maritime Domain are discussed alongside more traditional topics that will be familiar to many. I am particularly grateful to the contributions made by people and organisations outside of CJOS COE, without them the magazine would simply be a reflection of our 'in-tray' and we would all perhaps not learn as much.

But above all I am blessed by a dedicated team of colleagues whose single aim is to make a contribution to support those at the front line; wherever that may be. I am ever impressed by this varied and rich team of subject matter experts from our 13 sponsoring nation. Their drive, investment and varied contribution from differing cultures always radiates here in Hampton Roads. Ultimately, I am grateful for the leadership and guiding headmark set by our framework nation and, in particular, the United States Navy. ☸

★

Commodore Phillip Titterton joined the Royal Navy in 1981 and qualified as a submarine officer in 1983. Eager to develop and expand his warfare experience, he served in a variety of submarines before his selection to the Royal Navy's Submarine Command Course (informally know as the Perisher) in 1994. On completion of his Executive Officer tour, Titterton was promoted Commander and enjoyed the Command of two submarines, HMS SCEPTRE and HMS TIRELESS. The culmination of his seagoing operational career was recognized in 2004 when he was gazetted and appointed as an Officer of the British Empire (OBE).

After an enjoyable appointment at the United Kingdom Ministry of Defence (MoD), where he served as a desk officer responsible for submarine combat systems and sonar, Titterton was honored with a teaching and mentoring assignment responsible for training and qualifying future submarine Commanding Officers.

Promoted Captain in 2008, Titterton returned to the MoD as Captain of Navy Plans and spent a demanding 3 years helping the Maritime case through the 2010 U.K. Defense Review. He then spent 2 years delivering collective training as Captain of the Joint Tactical Exercise Planning Staff, then assumed the role as the Deputy Assistant Chief of Staff for Royal Navy Operations responsible to Commander Operations for the day-to-day execution of command for the Royal Navy.

Titterton joined the team at the Combined Joint Operations from the Sea, Centre of Excellence July 2014 as the Deputy Director. He is responsible through his U.S. Navy Director to the 13 Nations who fund the organization.

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.

Source: U.S. Navy

Forty-two ships and submarines representing 15 international partner nations maneuver into a close formation during Rim of the Pacific (RIMPAC) 2014.

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 Defence and pooling subject matter experts.
- Through broad intellectual engagement thereby supporting the Connected Forces Initiative.

ODU
IDEA FUSION

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 Jonathan Sims, USA-N
Email: usff.cjos.coe@navy.mil
Tel: +1 (757) 836-2463

CJOS COE DEVELOPS MARITIME ISR DOCTRINE

CDR Michael DeWalt, USA-N
CJOS COE

Source: NATO

ISR Op Center supported by 17 nations during Exercise UNIFIED VISION 16.

Intelligence, Surveillance and Reconnaissance (ISR) capabilities are critical to ensuring the maritime security of sea faring nations. During the recent Maritime Surveillance and Reconnaissance conference sponsored by Defense IQ in Rome, several maritime nations expressed deep concerns in conducting surveillance and reconnaissance operations targeting coastal border protection. Many nations presented ISR issues, in particular Italy, Portugal and Canada provided in depth briefs on the issues concerning ISR in maritime operations. Africa Command (AFRICOM) expressed concern in establishing ISR capabilities amongst African nations to patrol their coasts. Each nation may have an existing maritime ISR capability and some nations are in the process of expanding maritime ISR capability. AFRICOM is working with Western African nations to establish ISR capabilities to patrol their Exclusive Economic Zones (EEZ) in an effort to protect their natural maritime resources. With different national ISR reporting requirements in the operational and intelligence communication channels, there are little to no standardized procedures for NATO nations to follow. If we look at how Italy, Portugal and Canada are positioned to conduct maritime ISR, each nation has a specific way of performing ISR tasks to address national security concerns. One aspect that continues to plague nations is funding ISR capabilities. As funding issues vary from country to country, protecting EEZs and coastal boundaries has the potential to remain unchanged. Conducting maritime ISR operations collectively amongst nations can alleviate some of the funding issues when ISR information can be shared. For ISR information to be collected and shared, a standardized collection and sharing mechanism needs to be put into place via doctrine. The Combined Joint Operations from the Sea (CJOS) Center of Excellence (COE) is in a unique position to provide doctrine standardizing ISR capabilities amongst the NATO nations. As we examine Italy, Portugal, Canada and AFRICOM, the common thread is the need for Maritime ISR doctrine.

Italy has expressed concern over the issue of migrants at sea off their coast which has become problematic in recent years. The Italian Navy is responsible for a significant portion of the Search and Rescue (SAR) capability in the Mediterranean Sea. Centrally located in the Mediterranean and an ideal staging location of SAR operations, Italy is in the forefront of SAR operations. The greatest drain on the Italian Navy SAR resources is the influx of migrants at sea from destabilized countries. Contributing to this problem are the Northern African nations electing not to participate in providing SAR assets for the water space governed by their nations. Libya, Egypt and Tunisia are reluctant to contribute to

SAR operations. Libya and Syria have been significant culprits with the most migrants at sea coming from these two nations due to the destabilization of the governing body in each of these nations. Migrants from these two countries traverse the Mediterranean on vessels that are overcrowded and not in the best seaworthiness condition. The simple solution is apprehending the vessel in open ocean and returning the vessel to the nation of origin. This can become exponentially harder when an overcrowded migrant vessel begins to deteriorate transitioning into a SAR scenario. Coordination during a SAR can be very complex in a dynamic environment. Obtaining accurate information, rapidly verifying the information, sending rescue vessels to the SAR scene and closing out the SAR operation encourages the use of rapid ISR collection capabilities. ISR assets reduce the time the Italian Navy can verify and move SAR vessels into position to affect the rescue. In the case of simply returning the vessel to the country of origin, intelligence collection on the individuals being rescued needs rapid assessment to ensure that the individuals get returned to their country of origin. Cooperation in SAR events is binding for all ships on the open ocean that can provide assistance. Once the individuals have been rescued the process of determining what to do with the refugee needs to be assessed. ISR in the maritime environment is difficult at best due to bandwidth constraints and processing capability. The number of migrants at sea in the Mediterranean has increased since the early 1990's peaking most recently in 2014. The culmination was a result of the events unfolding in Libya and then in Syria. The increase in SAR events has tapped the Italian Navy capabilities to the limit. The need to coordinate with other nations in identifying and rescuing migrants has come to the forefront amongst the nations. Maritime ISR will be a significant force enabler to saving the migrants and returning them to a safe environment. By having a standardized maritime ISR doctrine that NATO nations and NGO's can follow will assist in bringing rescue capabilities from different navies together quickly to affect rapid rescues at sea. CJOS COE is drafting doctrine to resolve this issue.

"With different notional ISR reporting requirements in the operational and intelligence communication channels, there are little to no standardized procedures for NATO nations to follow."

Portugal desires to move away from a "need to share" to a "need to be involved" ISR environment to ensure a safe, secure future maritime environment. Portugal covers a large portion of the Eastern Atlantic Ocean and geographically has responsibility for SAR coverage in the Sea Lines of Communications (SLOCs) supplying countries in the Mediterranean and Europe. Today, 90% of the world's trade uses the SLOCs while 70% of national imports come by sea. Having to keep the maritime environment in the Eastern Atlantic safe and secure can be a daunting task for Portugal alone. Portugal is concerned with piracy, terrorism, narcotics, human smuggling, Weapons of Mass Destruction (WMD) and SAR. A great deal of maritime vessel traffic passes through Portugal's Area of Responsibility (AOR) on a daily basis. The need for good maritime ISR coordination would help to identify the bad actors on the high seas. Using organic assets and external agencies within the Portuguese government allows synergy of all ISR assets to monitor and assess maritime vessels in their AOR. However, the sole use of Portuguese assets may not be enough to ensure the safety of the Portuguese maritime AOR environment. When issues arise in the maritime environment, Portugal may require assistance. Portugal's vision of moving toward the "need to be involved" model highlights the need for other NATO nations to become more interoperable when conducting maritime ISR operations. The maritime ISR capability of each

nation is an enabler during operations amongst NATO nations. When Portugal conducts surveillance operations of ships in the SLOCs and another NATO nation joins the operation there is no standardized maritime ISR collection procedures. The gap in maritime ISR can be fulfilled by Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) ongoing efforts drafting maritime ISR doctrine.

Canadian forces have a very large area to cover in the Pacific, Atlantic and Arctic maritime environments. Satellite coverage has been the most effective way of conducting ISR in the cold harsh Canadian maritime environment. Canadian forces have been able to develop a Common Operating Picture (COP) by sharing satellite ISR information between different Canadian government agencies to ensure a safe and secure maritime environment. The Arctic region has recently come under scrutiny with bordering nations postulating how best to take advantage of all the resources the Artic region has to offer. Satellite and big data analytics have assisted the Canadian maritime community to identify targets of interest. Targets of interest in the harsh Canadian environment can consist of conducting SAR operations in extremely cold waters that have the potential to rapidly diminish survival rates the longer survivors remain immersed in frigid waters. Once identified, the surface unit deploys to the location to meet the maritime asset needing assistance. The transition to organic ISR assets in the open ocean becomes necessary to conduct the SAR mission. One of the biggest challenges is sifting through all the data from satellite imagery and big data analytics in order to show a maritime picture that has the relevant information to prosecute targets of interest. The SAR data alone creates too many contacts in the region and needs to be merged with other systems to ensure a clear concise picture is developed. Maritime ISR capabilities merged with other nations supporting the mission can become an enabler in conducting a SAR operation in the Canadian waters. However a standardized maritime ISR procedure is needed to cover the doctrinal gap.

NATO has expressed a desire to expand beyond the traditional boundaries of the European nations over growing concerns on the world scene especially Russia's expansion into Crimea One area of concern for NATO is developing partnerships with Europe's Southern continental partners that shares the Mediterranean- the African nations. AFRICOM's strategy and planning division is leveraging the Gulf of Guinea countries to build capacity and capability in the maritime domain. This includes combined maritime law enforcement operations between African host nations and the United States Coast Guard. The need for improving and establishing maritime ISR capabilities to patrol the EEZ's off the Gulf of Guinea coast will protect the natural resources used as part of the countries sustainment. Countries that have limited numbers of ships will need to partner with other nations to have continuous oversight of the EEZ. Conducing maritime ISR would be easier if there were standardized procedures to ensure EEZ success. The efforts of CJOS COE's maritime ISR doctrine will assist NATO nations in working with non-NATO nations conducting maritime ISR operations and will increase and expand partnerships outside of NATO.

"The efforts of CJOS COE's maritime ISR doctrine will assist NATO nations in working with non-NATO nations conducting maritime ISR operations and will increase and expand partnerships outside of NATO."

Imagine how the Italian, Portuguese and African Nations Maritime ISR capabilities would merge together to form a cohesive maritime ISR Task Force (TF) or fall under a Maritime Component Commander (MCC) to conduct a SAR operation? In response to a Request for Support from NATO, CJOS COE has led the charge to establish a foothold in the maritime

Intelligence, Surveillance and Reconnaissance (ISR) doctrine community by to drafting NATO doctrine on the subject.

In 2014, CJOS COE added maritime ISR improvement to its annual Program of Work (POW). After a year of intense research a Standardization Proposal (SP) was drafted by CJOS COE and submitted to the Maritime Operations (MAROPS) Working Group (WG). While the MAROPS WG considered the proposed SP, doctrine covering the Joint ISR (JISR) process was under development by NATO Allied Command Transformation (ACT). In 2015, Allied Joint Publication 2.7 (AJP 2.7) "Joint Intelligence, Surveillance and Reconnaissance" and Allied Intelligence Publication 14 (AIntP 14) "Joint Intelligence, Surveillance and Reconnaissance (JISR) Procedures in support of NATO Operations" were drafted and ratified by the nations. The nations agreed that a gap in maritime ISR doctrine remained after the ratification of the JISR doctrine. The Military Committee Maritime Standardization Board (MCMSB) tasked the MAROPS WG to develop doctrine in maritime ISR and issued a Standardization Task (ST) in June, 2016. The ST designated CJOS COE as the maritime ISR project lead with deadline for completion in less than two years. The title of the proposed maritime ISR doctrine is the ATP-102 "Maritime Intelligence, Surveillance and Reconnaissance." ATP-102 is a significant milestone as this is the first Allied Publication assigned to CJOS COE for custodianship. This means CJOS COE will be responsible for the initial draft and any future updates.

Source: U.S. Marine Corps

NATO E-3A Sentry AWACS patrolling over Germany.

CJOS COE envisions that ATP-102 will be employed at the tactical level by maritime units. It will contain standardized procedures, aligned with the joint process, to develop sustained and persistent maritime ISR procedures for the maritime environment. It will address the concerns of the Maritime Component Commander (MCC) or the maritime Task Force (TF) commander conducting activities with organic ISR assets. Non-organic assets for ISR outside of the maritime domain are addressed in AJP 2.7 and AIntP 14. Additionally, the ATP-102 will outline how to enable decision making to improve joint operational effectiveness and efficiency against potential threats to the NATO Alliance. ☸

CDR Michael DeWalt 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.

EXAMINING HYBRID MARITIME THREATS

Dr. Ian M. Ralby
I. R. Consilium

Source: NATO

NATO stepping up cooperation to address new security challenges and threats.

Discourse on hybrid threats has been evolving for over a decade, but relatively little attention has been directed toward hybrid aggression in the maritime space. Now that "little blue sailors," hostile posturing toward underwater cables, and a variety of other maritime-related activities are entering the discussion, a growing chorus of military experts, including retired U.S. Navy four-star admiral James Stavridis, a former supreme allied commander of NATO and dean of the Fletcher School of Law and Diplomacy at Tufts University, is calling for rigorous analysis of both existing and potential maritime hybrid threats. Conducting such an examination, however, is less about applying traditional naval expertise than it is about having in-depth familiarity with the low-level activities that would be involved and the maritime law enforcement context in which they would likely take place. Indeed, as the present analysis reveals, sophisticated understanding of the nuances of maritime law may actually provide military strategists with sufficient insight into future hybrid aggression in the maritime domain to be able to formulate effective means of countering it.

At its 2014 Wales Summit, NATO defined hybrid threats as situations in which "a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design."[1] This definition, however, is extremely broad and could even be used to describe some more classical military campaigns. Alternatively, the most famous definition of hybrid threats from an academic standpoint is that of Frank Hoffman from the U.S. National Defense University:

> *Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both states and a variety of non-state actors. These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of conflict. The effects can be gained at all levels of war.*[2]

This definition, too, focuses on the expansion of options for military tactical engagement within a theater of operations. In other words, there needs to be a war in order for this form of hybrid threat to manifest. But in the maritime space, an increasing number of examples suggest the existence and

potential proliferation of hybrid threats and hybrid aggression, even in the absence of an identifiable conflict.

A new definition, not yet published in any literature, helps focus the consideration of hybrid maritime activities and reveals possible avenues for addressing it. At the NATO Center of Excellence in Confined and Shallow Water's 4th Annual Operational Maritime Law Conference in Turku, Finland on 5 October 2016, NATO Maritime Command's Political Advisor Professor James Bergeron identified four key elements of hybridized aggression applicable in the maritime space. First, the initiator must be a major power. Small or weak states may engage in conduct similar to hybridized aggression, but the state must pose a true military threat in order to produce a genuine hybrid threat. Non-state actors can also engage in similar conduct, but again, such activity does not constitute a hybrid threat, as it lacks the backing of a conventional military force – a necessary starting point for the very notion of "hybridization." Second is the paradox of attribution or "implausible deniability." In other words, the activity must be clearly associated with the state engaged in the conduct, but not officially or at least easily attributable to them. Third is the hybrid-legal nexus which requires that the action taken be at least partially illegal. Breaking the law in some manner is a core component of hybrid aggression. Finally, the aggressor must have the ability to adapt the activity and dial up or dial down the level of aggression based on the response. While it is not a key component, Professor Bergeron also argued that a fifth element may be a strategic communications approach in which the aggressor uses the values of its opponents in order to create a moral imbalance in its own favor. While the analysis below does not engage that fifth element, it is worth considering in future work on the subject. In recent examples of hybrid maritime activity – both within and outside of the context of war – Professor Bergeron's four cardinal elements are pervasive.

"NATO defines hybrid threats as situations in which a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design."

In perhaps the most extensive analysis of the possibilities of hybrid maritime warfare, Professor Hoffman, together with Professors Martin Murphy and Gary Schaub, recently addressed the potential manifestations of hybrid maritime activity in the Baltic Sea. To contextualize their analysis, they first reviewed Russia's recent Crimea campaign to determine key takeaways regarding hybrid activity. They identified the following:

1. A persistent information warfare campaign directed at audiences in and out of the theatre to sway Russian members of the populace, confuse and divide opponents through disinformation about intentions, and impose revisionist interpretations on established political, legal, and historical narratives;

2. Utilization of paramilitary forces – such as regular coast guards, coastal militia, or guerrilla-style units – directed, coordinated with, or reinforced by regular forces to intimidate opponents while remaining below the level that justifies an armed response;

3. Deployment of high-end conventional capabilities at the periphery of the theatre to deter external intervention;

4. Gaining control over maritime assets, whether port facilities, naval bases, strategic islands, or other key positions that enable control over sea lines of communication.[3]

The elements of Professor Bergeron's definition are evident in these four aspects of the conflict. Russia, a major power, used false narratives and irregular maritime forces to create the paradox of attribution, while violating the territorial integrity of Ukraine – an illegal act – and maintaining conventional forces on the border as a means to dial up or down the level of aggression. In their examination of potential threats in the Baltic Sea, Hoffman, Murphy and Schaub identify a wide range of vulnerabilities, some of which have already been the subject of aggressive posturing by major powers. They classify the areas of susceptibility into political, social and economic vulnerabilities, noting that maritime infrastructure – particularly ports, undersea cables and offshore energy infrastructure – is in many cases vital to national, regional and global economic stability. Hybridized threats to such infrastructure can occur with or without the backdrop of an armed conflict, and are potentially devastating to international security. Indeed, recent examples and imminent possibilities indicate that this type of threat is likely to become a substitute for traditional military hostilities between states.

"Hybridized threats to such infrastructure can occur with or without the backdrop of an armed conflict, and are potentially devastating to international security."

A recent piece at the U.S. Naval Institute by Stavridis argues, as its title suggests, "Maritime Hybrid Warfare is Coming."[4] In it, he describes hybrid maritime war with a series of elements, as follows:

- Creation of real strategic effect at the tactical level (sometimes called impact of the "strategic corporal")
- Use of "soldiers" in unmarked uniforms (sometimes referred to as "little green men"), making their actions ambiguous under international law
- Elevated use of information warfare, propaganda, and the spreading of false and highly inflammatory rumors to destabilize a region
- Heavy presence on social networks generating propaganda and lies
- Special operators acting across the entire spectrum of violence
- Use of insurgent techniques—including car bombs, torture, and kidnapping—to frighten the population
- Incorporation of nonmilitary forces—including police and carabineer—into military operations
- A sophisticated cyber campaign[5]

These elements, again, can be seen to fit within the definition advanced by Prof. Bergeron. Indeed, the example of the South China Sea presented by Adm. Stavridis, as well as the hypothetical he poses, also bears out that definition. In that hypothetical, which draws on recent real-world events, China, a major power, could use "little blue sailors" – non-uniformed sailors providing the veneer of non-state action in what can only be termed a quintessential example of implausible deniability – to illegally attack and disrupt, potentially using non-lethal weapons, maritime commercial activity that is perceived to be against China's interests. The range of armaments from water cannons to actual mines offers a broad spectrum of options for dialing up or dialing down the aggression in pursuit of Chinese interests. While this could be termed "maritime hybrid warfare," it may be done without actually triggering the legal definition of an armed conflict.

Ultimately, Stavridis advances four principle rationales for why a state would chose to engage in such hybrid activity:

- First, it allows a nation to conduct operations to intimidate, degrade, and destroy an opponent's capabilities without certain attribution. This allows greater latitude of activity as it avoids criticism and sanctions from the international community.

- Second, maritime hybrid warfare bestows the advantage of surprise, as a recipient may not suspect the punch that is about to land.

- Third, its techniques give the user effective control of the tempo and timeline of events, given their inherent ambiguity.

- Fourth, it is much less expensive than building the massive and capital expensive platforms needed to conduct conventional littoral warfare.

In concluding, Stavridis writes: "Hybrid warfare is as old as combat itself.… But what is changing is the level of effort put into it by both big and small nations and the tendency to use it for all the tactical and strategic advantages it confers." He therefore argues for new thinking to be applied to how states can effectively counter this emerging threat.

Source: U.S. Army

Navy Admiral James Stavridis (Retired), former commander of U.S. European Command and NATO's Supreme Allied Commander-Europe, speaks during the opening of the 2011 United States European Command and national Guard Bureau State Partnership conference in Garmish-Pertenkirchen, Germany.

Returning to Professor Bergeron's definition, the hybrid-legal nexus may actually present the sort of creative response Stavridis suggests we need. Fundamentally, the question becomes: can the response to hybrid maritime aggression be hybridized itself such that the responding state does not break the law but nevertheless meets the other three criteria? A look at maritime law specifically suggests that such a response is, indeed, possible. Admiralty and maritime law is a niche field. Few law schools teach it and relatively few lawyers practice in it. Often seen as a vestige of a bygone legal era, maritime law is unique in many respects. Ships – as in the vessels themselves, and not just the people on them – can be arrested, sunken treasure is occasionally found, pirates really do exist, and maritime lawyers have to be familiar with a variety of laws that date back nearly a thousand years. In the United States, it is unethical under the American Bar Association's Model Rules of Professional Conduct, as well as the equivalent rules in most states, for a lawyer to declare herself a specialist in any area of law except patent law, which requires a separate bar exam, and admiralty law.[6]

As specialized as admiralty law is, creative application of it seems to be growing rapidly among one particular demographic: criminals. Around the world, a noticeable trend has emerged in maritime criminal activity in that the criminals are increasingly conscious of the law and sophisticated in how they exploit it. Not only are criminals taking advantage of legal nuances and vagaries, however; they have also begun to engage in forum shopping. In other words, their comparative legal analysis – examining both the laws and the legal institutions in a variety of states –

has led them to choose the jurisdictions in which to either commit crimes or allow themselves to be caught for crimes committed elsewhere when an escape is not avoidable. Indeed, some of the hybrid maritime threats, like Russia's brinksmanship in pushing the legal limit for the distance a submarine can be from underwater cables, is an indication that similar thinking is taking place on the part of states that wish to engage in hybrid aggression.[7]

A number of recent cases have indicated two particular developments within the "community" of maritime criminals. The first is a clear effort to exploit both the nuances in maritime law and the gaps in the effective enforcement of it in different jurisdictions. The use of self-inflicted distress to destroy evidence or end up in a specific jurisdiction, for example, has revealed a creative approach to using the life-saving principles of the Safety of Life at Sea Convention (SOLAS).[8] The second, however, is a resort to legal bullying, anticipating that a confidently asserted stance on a bogus legal position may deter the interdiction efforts of navies, coast guards and maritime police with insufficient legal training. In a recent incident, pirates refused to stand down, arguing that the law enforcement operation was actually in violation of international law.[9] In other words, superior knowledge of the law has become a tactic for obtaining a maritime advantage in the criminal context. Applying such superior knowledge to hybrid threats, however, may also reveal creative approaches to countering those threats.

Given that illegal action is at the core of hybrid threats, and given that maritime law offers a broad spectrum of historically-based oddities, unfamiliar even to some seasoned sailors, considerable effort and rigor should be directed to employing creative means of countering hybrid threats using the more unusual aspects of maritime law. While this analysis does not proffer any specific tactical approaches to countering hybrid maritime activity, this strategic stance of employing three of Professor Bergeron's four elements, plus activities that fall within the far reaches of maritime law, may provide states with answers to existing hybrid aggression. Maritime lawyers, familiar with the non-military aspects of maritime law, should work together with naval lawyers to explore options for taking such an approach to hybrid maritime threats. Indeed, legally-grounded creativity is the only way to develop sufficiently hybrid responses to hybrid maritime aggression. ❁

1. NATO Wales Summit Declaration, 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en.
2. Frank G. Hoffman, Conflict in the 21st Century: The Rise of Hybrid War (Arlington: Potomac Institute for Policy Studies, 2007), p. 8.
3. Martin Murphy, Fank Hoffman & Gary Schaub, Hybrid Maritime Warfare and the Baltic Sea Region, Center for Military Studies, Univ. of Copenhagen, November 2016, http://cms.polsci.ku.dk/publikationer/Hybrid_Maritime_Warfare_and_the_Baltic_Sea_Region.pdf.
4. James Stravridis, Maritime Hybrid Warfare is Coming, U.S. Naval Institute, December 2016, http://www.usni.org/magazines/proceedings/2016-12-0/maritime-hybrid-warfare-coming
5. Ibid.
6. Rule 7.4, "Communication of Fields of Practice and Certification," American Bar Association's Model Rules of Professional Conduct (2016). See also, e.g., Rule 7.4, "Communication of Fields of Practice and Certification," Virginia Rules of Professional Conduct (2016); Rule 7.4, "Communication of Fields of Practice and Certification," Massachusetts Rules of Professional Conduct (2016).
7. David Sanger & Eric Schmitt, Russian Ships Near Data Cables are Too Close for U.S. Comfort, N.Y. Times, 25 October 2015, https://www.nytimes.com/2015/10/26/world/europe/russian-presence-near-undersea-cables-concerns-us.html?_r=0
8. Sea Shepherd, Poaching Vessel THUNDER Sinks Under Suspicious Circumstances, 6 April 2015, http://www.seashepherd.org/news-and-media/2015/04/06/poaching-vessel-thunder-sinks-in-suspicious-circumstances-1681; Ian Urbina, A Renegade Trawler, Hunted for 10,000 Miles By Vigilantes, N.Y. Times, 28 July 2015, http://www.nytimes.com/2015/07/28/world/a-renegade-trawler-hunted-for-10000-miles-by-vigilantes.html?_r=0
9. Center for International Maritime Security, Coming of Age of the West African Navies, 7 March 2016, http://cimsec.org/coming-of-age-of-the-west-african-navies/22919

Dr. Ian M. Ralby is a Nonresident Senior Fellow at the Atlantic Council, a 'Key Opinion Former' on Maritime Security at NATO and the CEO of I. R. Consilium. He speaks and publishes widely on matters of international relations, law and security.

THE MARITIME CONTRIBUTION TO NATO'S BALLISTIC MISSILE DEFENCE

CDR Harry de Groot, NLD-N
STRIKFORNATO
CDR Toby Valko, USA-N
STRIKFORNATO
CDR William Hawthorne, USA-N
CJOS COE

Source: U.S. Navy

Aegis-class destroyer, USS Hopper (DDG 70) launches a SM-3 standard missile.

Over the past decades, the world has seen an exponential increase in the manufacture and proliferation of ballistic missiles, as well as constant increases in the range, performance, and effectiveness of those weapons. The total number of ballistic missiles outside the United States, the North Atlantic Treaty Organization (NATO), Russia, and China has risen to over 5,900.[1] Often, NATO's deployed forces are within range of hundreds of launchers and missiles, and the increase in ballistic missile capabilities emerging from the south-eastern flank of the alliance has put NATO nations within range as well. In response to these threats, NATO has incrementally increased its Ballistic Missile Defence (BMD) capabilities.

" As the improvement in the performance, range, and effectiveness of ballistic missiles has increased, so too have maritime BMD capabilities resulting in an increased requirement for overland coordination."

The 2004 NATO Istanbul summit directed the development of a capability to protect NATO deployed forces against short and medium range ballistic missile threats, doctrinally known as Theatre Ballistic Missile Defence (TBMD).[2] TBMD is defined as "The protection of deployed forces and high value assets/areas within the theatre from attacks by ballistic missiles".[3] Work on TBMD was taken forward expeditiously and the NATO Active Layered Theatre Ballistic Missile Defence Programme Office (ALTBMD PO) was created in 2005. The focus of the ALTBMD programme is the upgrade, test, and integration of NATO's command and control (C2) systems and underlying communication network to enable effective information exchanges between various NATO and national missile defence systems. This integrated system-of-systems architecture was designed to create a larger range of detection, communication, and missile defence capabilities for NATO forces.[4] This architecture is realized within NATO's Battle Management Command, Control, Communications and Intelligence (BMC3I) system. The C2 systems and underlying communication networks comprising this "system-of-systems" is funded by NATO, the sensors and weapon systems are national contributions.

The 2010 NATO Lisbon Summit determined that the threat to NATO European populations, territory, and forces posed by the proliferation of ballistic

missiles was increasing. It was decided that the Alliance would develop a ballistic missile defence capability to pursue its core task of collective defence.[5] The aim of a NATO ballistic missile defence capability is to provide full coverage and protection for all NATO European populations, territory, and forces against the increasing threats posed by the proliferation of ballistic missiles. This is doctrinally known as BMD.[6] As a result, in July 2012, the ALTBMD PO was transformed into the NATO Ballistic Missile Defence Programme Office and Services (NATO BMD PO&S) and became part of the NATO Communications and Information Agency (NCIA). The expansion from TBMD to BMD required adjustments to the TBMD architecture and systems. The provision of additional sensors and weapon systems to meet this upper layer requirement remains the collective responsibility of national contributions.

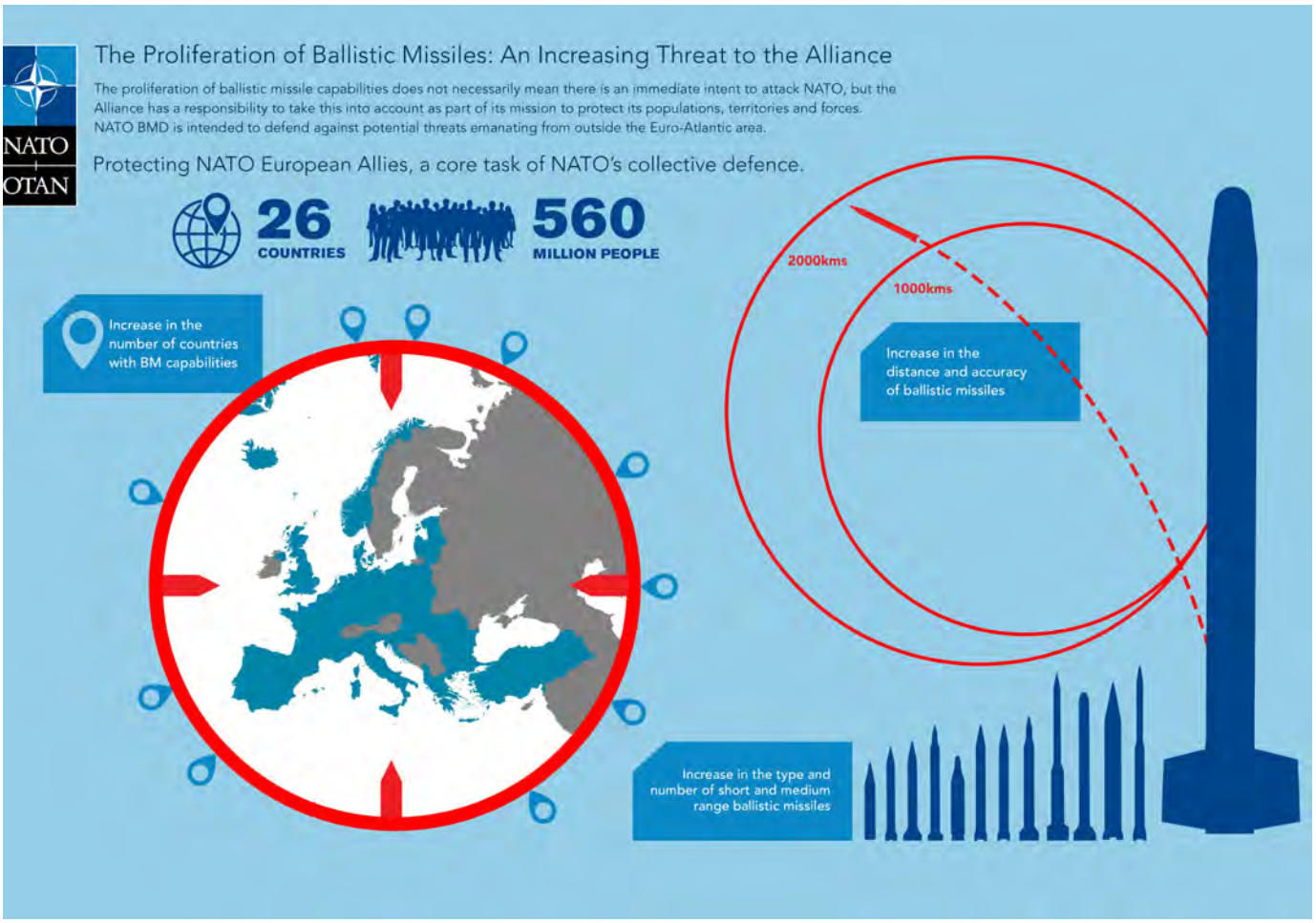
During this evolution, with the prototypes developed for the TBMD capability, NATO was able to install a system in operational headquarters as an interim BMD capability to execute and monitor the initial defence of NATO European populations, territory, and forces. Based on the aforementioned, NATO declared its interim BMD capability at the NATO Chicago Summit in 2012. The main contribution to BMD by the U.S. was accomplished through the European Phased Adapted Approach (EPAA), with phase one of a three-phased programme completed in 2011.[7] The cornerstone of the EPAA programme are the U.S. Aegis systems, sea- and land-based with their Standard Missile 3 (SM-3) interceptors. After improvements were built into the BMC3I systems and prototypes were replaced by industrialized versions together with the additional capabilities brought in by the nations (such as phase 2 of the EPAA program) NATO declared a BMD Initial Operating Capability at the 2016 NATO Warsaw summit.

Evolving Maritime Systems and Land/Maritime Integration

As the improvement in the performance, range, and effectiveness of ballistic missiles has increased, so too have maritime BMD capabilities resulting in an increased requirement for overland coordination. From air defence capable maritime platforms that are capable of defending littoral areas, to BMD capable platforms that are capable of defending areas deep inland, there has also been a growing need for these systems to integrate and coordinate maritime and land based systems. The genesis of these systems began in 1962 with the NATO Air Defence Ground Environment (NADGE), which tied four air defence regions and 18 radar stations together under the Supreme Allied Commander Europe. Over the decades NADGE grew, more and more radar sites were included, computers increased their clock speeds, and commercial off-the-shelf technology enabled the networks to expand. NADGE was renamed as the NATO Integrated Air Defence System (NATINADS) and later renamed as the NATO Integrated Air and Missile Defence System (NATINAMDS). It continues to operate as "systems of systems" to include the BMC3I. Although AD, TBMD, and BMD all fall under the realm of Integrated Air and Missile Defence (IAMD), the C2 networks and systems are used differently. Therefore, comparing them is like comparing apples to oranges. However, they do commonly use the diverse elements of NATO's BMC3I. Although AD and (T)BMD are lumped into the same acronym IAMD, they are not truly "integrated," but rather are "mutually supportive.". In this regard, the integration of land/maritime (T)BMD is further afield than the integration of land/maritime AD, which still relies on the systems and procedures already in place. Considering the advancements made in maritime AD systems and their increased range, further land/maritime integration would serve well the advancement of the overall IAMD within the NATINAMDS umbrella.

STRIKFORNATO and the NATO BMD Mission

Maritime units are a main contributor to the NATO BMD mission, now and in the future. Under the EPAA programme, there are four U.S. DDG's permanently stationed in Rota, Spain. These destroyers are uniquely equipped for the BMD mission through the use of the Aegis radar system and SM-3



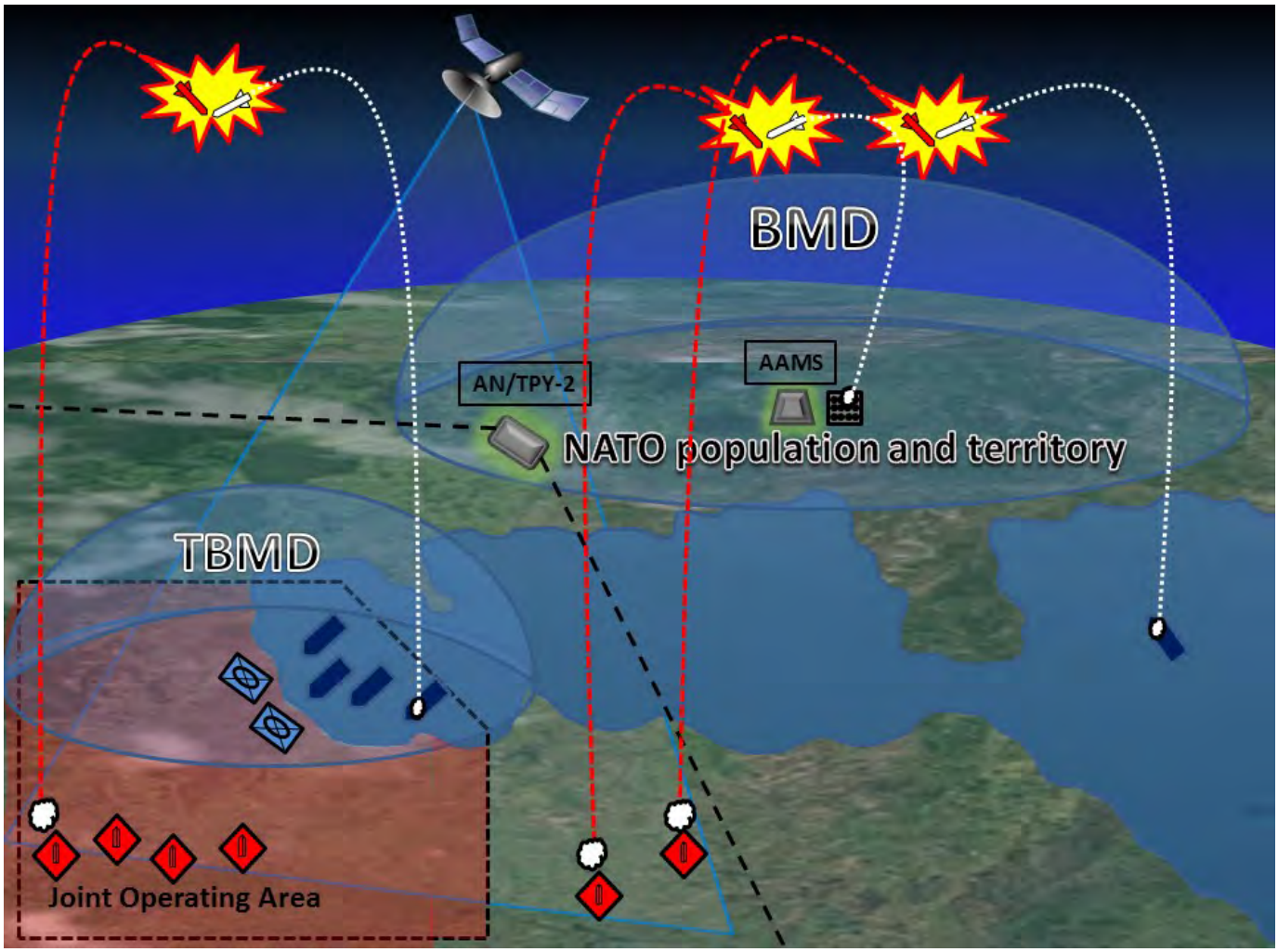
Source: NATO

Figure 1. NATO's Infograhpic illustrating the increasing threat of ballistic missiles to the alliance.

exo-atmospheric missiles. In addition to these destroyers is the Aegis Ashore Missile Defence System (AAMDS) located in Deveselu, Romania, which was declared fully operational in 2016. The AAMDS is literally the deckhouse of a DDG with the aegis radar suite co-located with the vertical launch system and SM-3 missiles. A second AAMDS, currently being built in Redzikowo, Poland, is expected to be fully operational by 2018. Along with the deployment of the SM-3 block IIA, it will complete phase three of the EPAA.[7]

STRIKFORNATO's objective is to integrate U.S. maritime capabilities, such as Carrier Strike Groups and Amphibious Readiness Groups, under NATO command. Because the Aegis destroyers deployed to Rota, Spain are U.S. systems, STRIKFORNATO is in a unique position to draw on expertise and planning support via U.S. Naval Forces Europe, U.S. SIXTH Fleet to support the BMD mission with maritime units. Integrating the Aegis BMD capability fits in the STRIKFORNATO mission to integrate U.S. capabilities.

Within U.S. SIXTH Fleet, STRIKFORNATO works closely with Commander Task Force 64 (CTF-64), which executes the U.S. maritime IAMD mission in Europe. STRIKFORNATO draws upon CTF-64's expertise and planning tools to support execution of the NATO BMD mission in Europe. To do all of this, STRIKFORNATO and CTF 64, under NATO control, provide support to COM AIRCOM for the NATO BMD mission. When called upon, CTF 64 will transfer to NATO and form the core staff of the NATO BMD/IAMD Task Group that will operate under STRIKFORNATO. Arrangements are made to



Source: CJOS COE

Figure 2. A ballistic missile targeting deployed forces is intercepted within a theatre of war (bottom left). Two ballistic missiles targeting NATO populations and territory are intercepted by the Aegis Ashore Missile System (AAMS) and a guided missile destroyer (DDG) (upper right). The AN/TPY-2 radar information can be utilized in both scenarios.

integrate additional maritime NATO contributions from additional nations as such capabilities emerge.

Maritime Units in Support of a TBMD Mission

TBMD is defined as "the protection of deployed forces and high value assets/areas within the theatre from attacks by ballistic missiles."[2] TBMD and BMD have distinct differences, although they are very similar in tactics, techniques, procedures, weapons systems, and sensors,. A Short Range Ballistic Missile (SRBM) typically has a range of 1,000 kilometers or less and stays in the lower layer, while Medium Range Ballistic Missiles (MRBM) and above enter the upper layer. In a TBMD mission, where the geographic defended area is much smaller than a BMD mission, the predominate usage of SRBM's is expected. A BMD mission would typically encompass a much larger geographic defended area against MRBM's and above. The importance in this distinction lays in resource allocation and positioning of maritime and land based units in order to fully leverage high-demand, low-density resources, and provide the most comprehensive theatre coverage possible. In contrary to land based units, maritime units, by their very nature, are "multi-mission" and provide a multitude of options to a Commander. Resource allocation and comprehensive coverage can be optimized through a comprehensive plan that appropriately utilizes the

strengths of all units, land and maritime, thereby enhancing the flexibility and multi-tasking capabilities of maritime units.

Summary

With the ever increasing advancements and proliferation of ballistic missiles, BMD and TBMD have been and will continue to be a "growth industry". As maritime based AD and BMD capabilities have grown, so too has their overlap with land systems and their influence in the IAMD overland environment. We have to lead with the C2 architecture and coordination and get that right in order to fully leverage all of our high demand, low density resources, both maritime and land based, in order to provide the most effective and comprehensive coverage possible in this very complex environment. The requirement to integrate land and maritime systems was taken into account for BMD from design on; however, renewed attention to AD coordination and integration should be provided. The systems are there and, although we have made great strides in the C2 architecture, we must continue to strive for commonality and coordination to fully integrate land and maritime AD, with BMD capabilities. ☸

1. https://www.mda.mil/system/threat.html.
2. 2004 NATO Istanbul Summit: Decision to develop NATO TBMD capability to defend deployed forces against ballistic missiles.
3. TBMD is defined as "The protection of deployed forces and high value assets/areas within the theatre from attacks by ballistic missiles". -Military Concept for the NATO integrated air and missile defence 27 Jan 2012.
4. NATO Communication and Information Agency Ballistic Missile Defence Programme. https://www.ncia.nato.int/BMD/Pages/Ballistic-Missile-Defence.aspx.
5. 2010 NATO Lisbon Summit: Decision to develop NATO BMD capability to provide full coverage and protection for all NATO European populations, territory, and forces against the increasing threats posed by the proliferation of ballistic missiles.
6. Ballistic Missile Defence is defined as "Incorporates all measures to protect territory, populations, and forces against the full spectrum of Ballistic Missile Threats". -Military Concept for the NATO integrated air and missile defence 27 Jan 2012.
7. "Aegis Ballistic Missile Defense," Missile Defense Agency (MDA), https://www.mda.mil/system/aegis_status.html.

CDR Harry de Groot and CDR Toby Valko are Ballistic Missile Defence officers at STRIKFORNATO, and CDR Bill Hawthorne is a staff officer at CJOS COE in Norfolk, VA. For further information on this subject, they may be contacted at h.groot@sfn.nato.int and t.valko@sfn.nato.int, and usff.cjos.coe@navy.mil respectively.

NATO'S CHALLENGE: INCREASED RUSSIAN SUBMARINE ACTIVITY IN THE ARCTIC

CDR Gwenegan Le Bourhis, FRA-N
CJOS COE

Source: USNI

Surfaced Russian submarine Severodvinsk.

Consequences of the climate changes to the Arctic environment are well known and discussed in the maritime community. Shorter routes for shipping activities, exploitation of once inaccessible gas fields, and increasing number of tourists interested in everlasting daylight cruises are all elements showing the increase of the maritime activity in this part of the world.

Fully aware of these changes, Russian strategists have reorganized the Arctic Forces under a "new command [that] will comprise of the Northern Fleet, Arctic warfare brigades, air force and air defense units, as well as additional administrative structures."[1] In the maritime domain, the Northern Fleet-Unified Strategic Command will be responsible for protecting Russian shipping, fisheries, and oil and gas fields on the Arctic shelf according to RIA Novosti.

Additionally, there has been a strong increase in the Russian submarine activity and a determined plan to update Russian submarine capabilities. Front and centre during the Cold War, the Russian submarine fleet has been an afterthought by NATO forces during the last decade. Recently, Vice Admiral Clive Johnstone, Royal Navy, the head of NATO's maritime forces, noted that his forces report "more activity from Russian submarines than we've seen since the days of the Cold War."[2] Vice Admiral James Foggo, US Navy (USN), Commander of the 6th Fleet and Commander of Striking and Support Forces NATO, goes even farther by mentioning the "Fourth battle of the Atlantic".[3] With the emergence of Russian submarine activity and the rising of the Arctic as a new area of competition for maritime superiority, NATO faces a growing naval security concern.

"To defend Allied points of interest, NATO forces have to counter the Russian posture by preserving Freedom of Navigation, or in other words, counter the Russian anti-access strategy."

Recent published studies summed up the supposed or claimed maritime Russian strategy.[4] In the undersea domain, the pillars are well known: being a key vector to the nuclear deterrence posture; contribute in the sea domain to a multi-layer defensive area-denial tactic; and being able to challenge enemy sea control by a strategic anti-access posture. Currently undergoing modernization and organized under four

main command structures (Northern Fleet, Baltic Fleet, Black Sea Fleet and Pacific Fleet), the Russian submarine fleet is particularly challenging to NATO sea control operations. Countering this threat in the close and shallow waters from the Baltic and the Black seas is a complex challenge that requires in-depth studies.

Operating in the face of this remerging submarine threat in the Arctic presents a unique challenge. If we consider that diesel and air-independent propulsion (AIP) submarines are located mainly in the littorals, the Arctic is the realm of nuclear-powered attack submarines (SSN) and their capability to support this open ocean strategy.

To quantify the increase in Russian submarine activity in the Arctic, the following rule of thumb can be used. On a daily posture, 25 percent of Russian submarines are under long-term maintenance, 50 percent are in trial or in the certification process for their crew, and 25 percent are deployed. Applying this rule to the claimed Russian Northern Fleet results in two nuclear-powered ballistic-missile capable submarine (SSBN), one nuclear-powered guided-missile capable submarine (SSGN), four SSN, and three diesel or AIP submarines (SSK) currently deployed in the Arctic region. These figures do not include submarines from other fleets that could quickly join the Arctic operations area if needed. Even taking into consideration that the Russian nuclear deterrence strategy may require the two SSBN and two SSN to be tasked elsewhere, NATO forces could still routinely face at least six submarines in the Northern Atlantic or the Arctic.[5] Overtly or covertly tracking these submarines requires the deployment of assets in the vicinity of their areas of operations, starting from their home-based departure in the Barents Sea. Increasing the deployment of anti-submarine warfare (ASW) assets and developing closer coordination between alliance ASW assets, submarines, air assets, and surface combatants still may not be sufficient to guarantee a permanent up-to-date picture of the increased Russian activity.

At a strategic level, NATO maritime posture is well established; protect and deter. That means achieving a certain level of sea control to preserve safe conditions for the maritime enterprise and deterring any opponent to challenge this situation. In the undersea domain, this could be summed up by monitoring submarine activity (mainly Russian) to not cede the initiative to our opponents. Two courses of actions can be implemented to support this strategy: monitor any opponent submarine operating in the area and defend any NATO points of interest. To defend Allied points of interest, NATO forces have to counter the Russian posture by preserving Freedom of Navigation, or in other words, counter the Russian anti-access strategy. To achieve this, NATO must be able to control sea-lines of communication (SLOC), by monitoring and defending choke points access, escorting high-value units, such as aircraft carriers, while they operate in the area, and monitoring and defending undersea cables which support freedom of movement in the cyber domain. All of these actions require the commitment of a large number of highly-capable and well-coordinated assets.

The points-of-interest map shows that during the Cold War one of the key issues for NATO ASW forces was to monitor the GIUK (Groenland-Iceland-United Kingdom) gap, being ready to track any Russian submarine crossing this line. Today, the list of the points-of-interest has grown considerably with additional communication cables laying on the ocean floor and the rising economic activities in the Arctic. Monitoring the GIUK gap, which still remains a tough challenge today, is no longer a sufficient strategy.[6]

How could NATO answer this "new" challenge? VADM Foggo answered "This is not a kinetic fight".[7] In the Arctic, the battle is not on the surface nor in the air, but in the undersea domain. This statement is reinforced by the USN posture which focuses more on submarine activity than on developing ice-breaking surface vessels. Opposed positioning between Russia and NATO fleets could be summed up by the following statement: Russia intends to probe for NATO weakness while NATO wants to ensure the protection of the maritime enterprise and to preserve lines of communication at all times. In this domain, such as in other domains facing Russian provocations in the European theater, there is no peace or war situation, but a gray time zone where very capable

assets are operating in close vicinity.[8] To demonstrate NATO strength and protect key maritime infrastructures, there are different domains that need to be addressed in the short- and mid-term.

In the near term, developing capabilities and capacities to face these challenges will concern all services, but will be particularly relevant for allied navies. Admiral John Richardson, USN Chief of Naval Operations, stated "The Arctic is going to be a different type of theater in the future and if we neglect the fact that we're going to be operating in the Arctic as we design this new class of ship, that's just sort of narrow thinking on our part."[9] The Arctic environment is indeed challenging due to its low temperatures, but also to its high latitudes. This impacts material endurance, system settings, and communication capabilities in all the warfare areas. Technical solutions already exist and need to be commonly explored to determine the most efficient and effective path to follow under the current budget constraint. Maritime Unmanned Systems (MUS) are also considered by many entities to be a part of the solution in the undersea domain. MUS and, namely, Undersea Unmanned Vehicles (UUV) offer significant force multiplication for ASW operations, and are particularly relevant for tasks where near-permanent monitoring is required.[10] UUV can be used for surveillance of geographic areas such as the GIUK gap and for the defense of static infrastructures. By establishing submarine surveillance points without escalating the level of conflict, UUV can greatly enhance the ability of the Commander to achieve and maintain access, independent of the state of hostilities. When it comes to gray zones of confrontation, providing a firing capability to the UUV becomes an issue of interest. Today's lack of effective permanent Command and Control of the submerged UUV may be a drawback to their use. Other development opportunities already exist in the use of variable depth sensors and their combined use with multi-static detecting networks. These sensors are used by some nations to provide large scale detection capability, which could be particularly useful in the quiet Arctic environment. This tracking capability, which comes with less risk of counter-detection and is outside of an enemy's targeting range, poses a greater challenge to an opponent's submarine force.

Source: Open Source

The heavy nuclear-powered GM cruiser 'Peter the Great' patrolling the Arctic.

In the short term, updating doctrine is a necessity. As mentioned, the Arctic environment constitutes unique challenges to the use of materials and the configuration of systems. This has consequences that should be taken into account in NATO doctrine development. The undersea acoustic conditions are distinctive in this region and require development of new procedures and tactics. ASW tactics should also be able to tackle the challenges coming from the "non-kinetic fight" mentioned by VADM Foggo. Operating in a period of other-than-war is particularly demanding

because detecting a contact is challenging, identifying a contact is challenging, communicating or warning a contact is challenging, and not engaging a closing contact is even more challenging. Doctrine updates should address all these issues in this new strategic environment. Only a few allied nations have the experience to contribute to ASW doctrine and any new doctrine proposals need to be experimented before being endorsed by all nations. This process takes time while the Alliance is facing a single opponent not constrained by consensus-based doctrine. Considering the immediate proximity of the threat and the time required to implement efficient counter-tactics, the Alliance must dedicate more focus on the doctrine dedicated to this domain.

Another concern is the organization of ASW Command and Control. Should the responsibility remain at the tactical level under the Officer in Tactical Command of an operating task group, or should undersea be considered a broader concern requiring a united theater answer? Both of these answers may be applicable, depending on the course of action selected by the Maritime Component Commander. Additionally, NATO's efforts to counter the Russian submarine threat in the Arctic must benefit from the unique role of MARCOM to establish a shared undersea picture, enabling deployed task groups to take proper measures to ensure their defense.

Finally, undersea activities and, in particular, ASW, should play a larger part in NATO's training and exercise program. High-level ASW exercises already exist at the tactical level. This community of specialists, who are well aware of the submarine threat challenges, needs to be more connected with the higher level of the chain of command. This is particularly true for Joint planners who usually consider the submarine threat as a single-service concern. Educating these leaders on ASW challenges is a critical step to success. Complicating the matter is the degree of high sensitivity that accompanies this topic due to its close links to national deterrence postures.

Considering the ever-evolving economic environment, coupled with climate change, the Northern Atlantic and Arctic oceans will only continue to increase in strategic importance. In this growing area of operations, capable powers will routinely interact and attempt to counter each others' capabilities. NATO must consider a stronger investment in multi-domain ASW capabilities for a non-kinetic fight, including experimenting with new technologies, updating doctrine, and developing new C2 organizations. This requires will at a moment when most European allies are facing new threats emanating from the South and the US is highly committed to the Asian-Pacific. If the Alliance fails to act accordingly and does not counter the increasing undersea threat posed by Russian activity in the northern flank, the lessons learned may come at a high cost. ☸

1. Russian General staff told the state news agency quoted in Russia to Standup New Arctic Command. www.news.usni.org – D. Majumdar February 18, 2014.
2. Nicholas de Larrinaga, "Russian submarine activity topping Cold War levels," IHS Jane's Defence Weekly, 2 February 2016.
3. Proceedings Magazine - June 2016.
4. JAPCC – Alliance Airborne Anti-Submarine Warfare – June 2016 – CDR W. Perkins, USN CSIS – Undersea Warfare in Northern Europe – July 2016 – under the direction of K.H.Hicks.
5. 1 SSGN, 2 SSN and 3 SSK.
6. CSIS study (Undersea Warfare in Northern Europe – July 2016) recommends reinvigorating this monitoring.
7. Proceedings Magazine - June 2016.
8. April 2016, Russian SU-24 fighter jet made "close-range, low-altitude" passes near the USS Donald Cook while the ship was in international waters in the Western Black Sea. Pentagon spokesman Col. Steve Warren.
9. www.nationaldefensemagazine.org.
10. CJOS COE study - Guidance for developing Maritime Unmanned Systems (MUS) capability - July 2012 - COL A. Evangelio, ITA Air Force.

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.

NATO
Maritime Integrated Air and Missile Defence (M-IAMD) Workshop

5-8 September 2017
Virginia Beach, VA

The Combined Joint Operations From the Sea Centre of Excellence will be hosting the 2nd Annual M-IAMD Workshop at the U.S. Tactical Training Group Atlantic (TTGL), Dam Neck Annex in Virginia Beach, Virginia. Formerly known as the Anti-Ship Missile Defence (ASMD) Panel, the panel was renamed to M-IAMD after the inclusion of Ballistic Missile Defence in 2016. This year's panel will be chaired by the United Kingdom and co-chaired by Germany; the panel will report directly to the NATO Maritime Operations (MAROPS) Working Group Syndicate 2. Established by the Military Committee Maritime Standardization Board (MCMSB), the MAROPS Working Group will initiate and develop the standardization of documents in the field of maritime operations for NATO forces. The MAROPS Working Group will also advise the MCMSB and Military Committee on topics and issues concerning maritime operations.

Workshop calling notice will be released March 2017 and posted to the Naval Special Operations (NSO) unclassified website under "MAROPS - Syndicate 2 Forum"

For more information visit:
www.CJOSCOE.org
CDR Bill Hawthorne, USA-N
Email: william.d.hawthorne@navy.mil
Tel: +1 (757) 836-2429

A NAVAL PERSPECTIVE OF URBANIZATION WARGAMING

CDR Geir Arne Hestvik, NOR-N
CJOS COE

Source: flickr (kathywoolbrightdarza)

Eighty percent of the global population is living within 100 Km of the coast.

The Strategic Foresight Analysis (SFA) and Framework for Future Alliance Operations (FFAO) have predicted that global urbanization will be one of the most challenging trends for NATO. It is expected that cities will contain 65 percent of the world's population by 2040, and that about 95 percent of this urban population growth will occur within developing nation's mega-cities, where most of them will be situated near the coast. With this in mind, NATO's Military Committee initiated a task to investigate the effects of rapid urbanization.

"Currently about 80 percent of the global population are living within 100 kilometers of the coast."

Currently about 80 percent of the global population are living within 100 kilometers of the coast. With the majority of the world's economic and political activity occurring in the littoral, including oil extraction, fishing, mining, banking, and international trade, the impact that continuing urbanization trends can have upon both the maritime environment and maritime operations are evident. The report "Global Maritime Trends 2030" by Lloyd's Register, QinetiQ and University of Strathclyde estimates an increase in the number of floating oil platforms from 270 platforms in 2010 to over 600 in 2030. Likewise the world's total tonnage and vessel numbers will increase for all major ship types, adding to the numbers with probably several thousand more vessels in order to keep up with the population growth, and increased dependencies of transportation across the seas to ensure the flow of commodities. The first part of the Urbanization project was conducted in September 2015, and it is described in the previous 2015 issue of *Cutting the Bow Wave*. A limited objective experiment was conducted in order to bring together subject matter experts, civilian and NATO entities to discuss the possible implications for NATO in the conduct of military operations. These findings were later integrated in a conceptual study that was finalized by NATO Allied Command Transformation (ACT) in March 2016.

The next step was to evaluate the proposed future capabilities in the conceptual study, identify capability gaps and weaknesses across the DOTMLPFI

framework, and identify possible new courses of action and which current capabilities NATO needs to retain. To achieve these objectives an Urbanization wargame was planned and conducted.

HQ Supreme Allied Commander Transformation conducted the NATO Urban Seminar Wargame Experiment at the NATO Defence College (NDC), Rome, Italy from 28th September to 7th October 2016, where more than a hundred military and civilian personnel met. Participants included representatives from a variety of nations, ministries of defence, universities, military commands, and military entities throughout the Alliance. The wargame experiment examined current and future capabilities in a joint full spectrum urban operation, mainly to provide recommendations for further conceptual development and insights for a Joint Urban Doctrine.

A fictitious scenario was developed for the wargame in Rome, with two neighboring countries at war. The year is 2035 and Positania with the mega city Archaria (Naples) as capital, was attacked by its neighbor country Catania. Catania soon took control of most of the country including parts of the capital. After a United Nations Security Council resolution, NATO intervened in the conflict, and conducted a forcible entry into the mega-city Archaria in order to restore peace and stability in the region.

The wargame was conducted with four blue teams playing out three operational vignettes. The vignettes looked at a forcible entry, clearing, and a stabilization operation. The four blue teams, which played the role of a Rapid Intervention Brigade, were first asked to develop a Course of Action (COA) using current military capabilities while facing a red team equipped with future capabilities. This method enabled the teams to assess gaps in current capabilities across the DOTMLPFI framework. After the teams' selected COA were played out against the red team's COA, they were asked again to develop another COA using future capabilities provided by the experiment team and/or capabilities developed by the blue teams themselves. The feasibility and supportability of these COAs were assessed by again playing out the blue versus red COA.

The first vignette is starting at sea; from a number of amphibious ships and vessels taken up from trade, the three Brigades were landed in the mega-city. Sea-control and Air-control were preconditions for success, and not really played out in the wargame. With the number of support and amphibious vessels needed to land, support, and sustain three Brigades, the number of escort vessels would most likely not have been sufficient to provide sea control and proper force protection without being heavily dependent on air support. From a maritime perspective, vignette one should probably have focused more one Catania's most dangerous course of action – namely offensive operations towards the sea lines of communication (SLoC) and the harbor. These aspects seem very often neglected due to the fact that ensuring sea control is very challenging and demands a lot of resources that now are more scarce within the Alliance than twenty years ago. With the naval forces available for NATO and Catania during this wargame, it is quite possible that the NATO operation could have been a failure from the beginning. Even though there was no threat from submarines, Catania could mount almost three times as many fighting ships as NATO. The littoral area outside Positania was further cluttered with more than 3000 small fishing boats and a lot of commercial traffic making it very hard to ensure a recognized maritime picture.

The Catanian Counter Attack at Sea (Not Simulated in the Wargame)

From the bridge on his torpedo boat, Lieutenant Ibrahim Ilyich is looking out on the bow of his torpedo boat as it climbs over the 30 feet high wave, before it is brought thundering down into the deep, black sea. He cannot see the rest of the two squadrons, but, somewhere out in the dark night, 11 other torpedo and missile boats are fighting their way towards the NATO sea-base. Tonight, it's finally time for payback.

The strength and force of the initial attack by the NATO forces had stunned the Catanian Navy. With air superiority, NATO had quickly gained the initiative. The Catanian forces that were tasked to protect the pre-planned minefield and bombard the expected landing areas ashore were wiped out during

the first hours of the attack. Though the squadron with fast inshore attack crafts and small suicide boats were able to neutralize two minesweepers and immobilize one of the amphibious vessels as it entered the port, it was far from sufficient to stop the landing. The post was soon fully operational again, and all of the Catanian forces involved in the attack were cut to pieces by the combined fire from maritime attack helicopters, fighters, and close protection measures from the warships.

Lieutenant Ilyich still remembers the smile on his brother's face as they said goodbye eight days ago. His brother was commanding one of the three C-802 coastal artillery batteries. It was a big disappointment to see them neutralized by NATO's Special Forces before they could take part in the fighting, but tonight its payback time . The remnants of the tropical hurricane surging through the area give excellent hiding and protection – no one will expect an off-coast raid by small fast patrol boats. No drones and hardly any aircraft can operate under these conditions. It is seven hours since the two squadrons left their camouflaged waiting positions, and they would be within weapon range of the NATO sea-base just before dawn. Lieutenant Ilyich only hopes that they will be able to launch their main weapons during these weather conditions.

Suddenly, radio silence is broken; the passive sensor operator is reporting an enemy emitter. The signal strength is high implicating that the enemy is close. The sea is calming slightly as the first morning light appears, and Lieutenant Ilyich can see the NATO sea-base as the two squadrons receive orders to form up and engage. The sea-base is enormous and it covers a vast area of sea, but it is evident that without air support the NATO combat vessels are not able to establish a proper defensive barrier to protect it. In addition, the Catanian torpedo- and missile-carrying fast patrol boats are very difficult targets in the rough seas.

On his starboard quarter, three of his colleagues are neutralizing a NATO frigate. Totally taken by surprise, the frigate was covered with gunnery shells, before it was utterly destroyed by a torpedo at close range. The sea-base now lies directly in front of

Source: Wikipedia

The majority of the world's economic and political activity occurs in the littoral, including oil extraction, fishing, mining, banking, and international trade.

Lieutenant Ilyich. He fires four torpedoes on two targets. Each torpedo has a warhead with 250kg high explosives; every torpedo is a vessel-killer. On his combat management system, Lieutenant Ilyich noticed they lost contact with one of the torpedoes, but the three others are striking home. To his left and to his right, he can see his comrades launching torpedoes, firing surface-to-surface missiles and guns at a frenetic speed. The surprise attack has been ongoing for nearly 10 minutes, and the majority of the sea-base is either sinking or ablaze. The NATO escort vessels stationed farthest away are closing in, and NATO aircraft could be expected shortly. It is time to execute part two of the plan, Lieutenant Ilyich decides, as he turns his vessel around towards the Archarian harbor and increases speed to 35 knots. Increasing his speed, the first NATO aircraft arrives. The Catanian FPB squadrons are engaged, but the small vessels are difficult targets in the rough seas. Lieutenant Ilyich can see that several of his comrades are still fully operational capable as they rush towards the harbor at best speed, firing their anti-air-warfare guns and shooting anti-air-missiles at the approaching aircraft.

The artificial naval battle described was not played out in the Urban wargame. With a skilled opponent able to mount about thirty boats equipped

with torpedoes and surface-to-surface missiles, opposed by almost three times the number of fighting ships provided by NATO forces in this scenario, it would be very hard for NATO to ensure sea control and SLOC . Additionally, if the opponent were to have one or more submarines available, I'm afraid NATO would not stand a chance to fulfil its mission without taking severe losses of ships and soldiers.

In many military discussions and many forums, sea control and the maintenance of SLOC seems neglected. From the 1990's to 2015, the North European countries have reduced the number of fighting ships by 170 units (Norwegian Defence, Maritime Doctrine 2015). The Alliance ability to conduct large scale maritime operations is reduced. Yes, the fighting ships today are more capable than in the beginning of the 1990's, but so are most of the possible future opponent fighting ships. And though the ships are more capable today, many of them must be able to contribute within several warfare areas, which may lead to ships design and manning solutions that are unfavorable. I agree that flexible multi-purpose vessels may seem like a good investment, fulfilling the needs of the nations and the Alliance on the paper, but they are also multi-vulnerable. If neutralized by an opponent, a nation's fighting capability within several warfare areas is reduced. Of the 170 ships that have been taken out of service by the North European countries since the 1990's, many of them are smaller combatants and submarines specialized for littoral operations. With the expected urban population growth in the littoral areas, as predicted in the strategic analysis conducted by ACT, one could question the expediency in this development.

Most of the Alliance nations still have a fair deal of major combatants in service. Frigates and destroyers – the workhorses of navies – can contribute in NATO Standing Maritime Groups, sail worldwide, and show the nations flag around the globe. From a political point of view, that is important in many aspects. On the other side, the nations in the Alliance's decision to remove the vessels that are most capable in littoral operations – the corvettes and fast patrol boats –should maybe be questioned. To man a modern frigate properly, it takes at least 120 sailors and officers. For operations in the littorals, one could man 6-8 smaller combatants each with the same capability to fight in anti-surface warfare operations, giving a naval force increased surveillance coverage, increased weapon load, and increased force survivability. Smaller vessels translate to reduced endurance, but with the expected increased focus on the littoral areas until 2030, it could be unwise not to strengthen the alliance naval littoral capability and capacity. If it is deemed necessary to conduct out-of-area operations, there are always strategic lift resources that can be used to transport smaller combatants into action worldwide.

To foresee the future is difficult . But, the impact on sea borne trade and NATO's future maritime challenges are certain. The large reduction of fighting vessels among the North European countries should be a concern. A reduced number of fighting vessels means reduced surveillance coverage, reduced survivability, and reduced fighting capability for the Alliance. It remains to be seen if the Alliance can meet the future without improving its naval littoral capability and capacity. ☸

1. French Ministry of Defence, Delegation for Strategic Affairs, "Strategic Horizons" 2012, p. 118.
2. IMSM-0543-2014 - NATO Conceptual Study on Urbanization, 28 Nov 2014.
3. NATO, NATO Conceptual study on Urbanization, 2016, p. 39.
4. Lloyd's Register, QinetiQ and University of Strathclyde, Global Marine Trends 2030, 2013, p. 41.
5. Doctrine, Organization, Training, Material, Leadership, Personnel, Facilities and Interoperability.
6. Belgium, Denmark, Germany, Norway, The Netherlands and United Kingdom.
7. Fighting ships are her considered as destroyers, frigates, corvettes, submarines and fast patrol boats.

CDR Geir Arne 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.

AFRICAN FRAMEWORK AND CJOS COE ENGAGEMENT

CDR Ricardo Valdes, ESP-N
CJOS COE

Source: Wikipedia

Assembly of the African Union (AU).

The Combined Joint Operations from the Sea Center of Excellence (CJOS COE) has been working on Maritime Domain Awareness (MDA), or *Maritime Situational Awareness* (MSA) in the NATO lexicon, since its beginnings. Going back to 2011, CJOS COE has published several documents on the subject, most recently the MSA study paper, 'From Fragmented Sea Surveillance to Coordinated MSA.' This paper was distributed last year in concert with the COE for Operations in Confined Shallow Waters (CSW) in Germany, the Maritime Security COE in Turkey, and the NATO Maritime Interdiction Operations Centre in Greece. One of the recommendations from this paper was that "*…the COEs should become more familiar with the breadth and depth of the Global Maritime Community of Interest (GMCOI).*"

CJOS COE is striving to understand the challenge around information sharing and collaboration by first identifying and then working with the main actors in the maritime domain, and then hosting them at meetings to discuss ways to achieve an effective global maritime situational awareness. Finally, CJOS COE is actively building useful networks and consistent habitual relationships with those main actors. Back to the findings and recommendations from Maritime Security Regimes Roundtable 2016 (MSR RT 16), which was held by CJOS COE in Norfolk last April, "Recommendation 8" encapsulated this issue: "*Continue to understand the problem and work towards regulatory barrier breakdown; meanwhile, maintain and develop personal relationships across the MSR to enhance trust.*"

Independent of the NATO Command structure, CJOS COE draws upon the knowledge and capabilities of sponsoring nations, United States Fleet Forces Command, and neighboring U.S. commands to promote best practices within the Alliance. CJOS COE has the unique ability of looking at those maritime areas that are not NATO Areas of Operations. Specifically, we are on the path to obtain regional situational awareness in the following areas of increased interest: West Africa, Indian Ocean, and Southeast Asia.

To begin, consider West Africa, mainly the Gulf of Guinea (GOG), where seas have become one of the most unsafe places in the world due to, among other concerns: armed robbery with hostages taken, illegal fishing, illegal immigration, and maritime pollution. Pirates have been more aggressive in hijacking sailors during attacks, mostly for ransom. Over the past decade piracy and armed robbery at sea have escalated from a minor issue on the global and African security agenda to a major strategic concern. As a result, political leaders have turned their attention to the GOG maritime domain. Consequently, to secure the

maritime domain, a framework has been in development since 2011 with various initiatives adopted at the national, regional, continental and international level.

In November 2011, the AU sent a request to the secretary-general of the UN for assistance in tackling the piracy situation. The UN secretary-general responded by sending a delegation to the GOG to assess the piracy and make appropriate recommendations on how the UN can assist. This led to the adoption of UN Security Council resolutions 2018 (2011) and 2039 (2012), which condemned all acts of piracy and armed robbery in the GOG and emphasized the need for a comprehensive strategy among all affected nations to effectively address the problem.

In 2012, African Heads of States and Governments adopted the 2050 Africa's Integrated Maritime Strategy (AIMS) at the 22nd Summit of the African Union (AU) in Addis Ababa. This is considered the primary framework at continental level which provides a broad framework for the protection and sustainable exploitation of the African Maritime Domain (AMD). It is intended to address current, emerging, and future maritime challenges and opportunities in Africa. It takes into account the interests of landlocked countries, with a clear focus on enhanced wealth creation through the sustainable governance of Africa's inland waters, oceans, and seas. The Combined Exclusive Maritime Zone of Africa (CEMZA) is defined and should allow for the convergence of existing and future monitoring and tracking systems used for maritime safety and security, protection of the marine environment, fisheries control, trade and economic interests, border control, and other law enforcement and defense activities. This Strategy steps toward promoting inter-agency and transnational cooperation and coordination on maritime safety and security.

In June 2013 the heads of state and government of the Economic Community of Central African States (ECCAS), Economic Community Of West African States (ECOWAS), and the Gulf of Guinea Commission (GGC) held a summit on 'Maritime Security and Safety in the Gulf of Guinea' in Yaoundé, Cameroon. This summit focused on developing a regional response to maritime security concerns in the GOG, and agreed upon a declaration on maritime security, a memorandum of understanding, and a code of conduct:

- The declaration of the heads of State and Government of Central and West African States on Maritime Safety and Security in their common Maritime Domain (Yaoundé Declaration) tasked the signatories with the promotion of peace, security, and stability within the GOG maritime area by assuming the responsibility of mobilizing sufficient operational resources. Additionally, it called for encouraging activities aimed at cooperation and coordination, and to share resources among members while continuing to cooperate with international strategic partners.

- The memorandum of understanding aimed to facilitate the coordination and implementation of joint activities, as well as the sharing of experiences and information exchange on suspicious movements and activities at sea. It calls for the harmonization of legislation on piracy and other illegal activities, and control procedures on reinforcing the fight against crimes at sea as well. It also considers the establishment of an inter-regional coordination center for the implementation of the regional strategy on maritime safety and security.

- The code of conduct concerning the repression of piracy, armed robbery against ships, and illicit maritime activities in Central and West Africa points out assurance enough that there is full cooperation in the repression of transnational organized crimes in the maritime domain. It is nonbinding for the first three years, after which a review will take place to establish a timeframe for transforming the document into a binding multilateral agreement; assess its implementation; and share information, experiences and best practices.

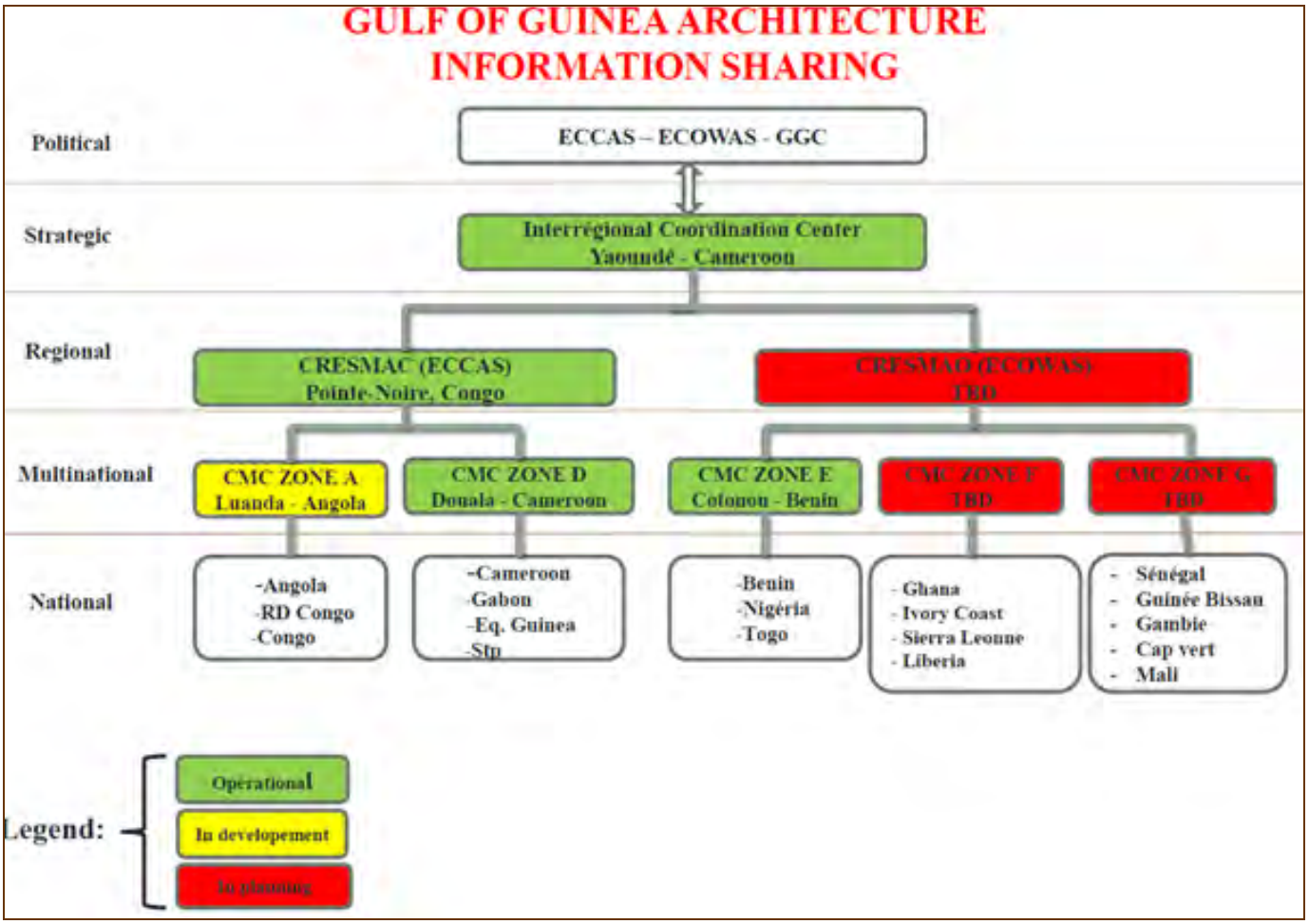


Figure 1. The coordination centers play an important role in promoting information exchange and joint actions in response to piracy and maritime crime in the Gulf of Guinea.

Besides these agreements, the ECOWAS Integrated Maritime Strategy and its implementation plan were adopted in March 2014. ECOWAS and the GGC also planned to develop an integrated maritime strategy. These regional plans should be aligned with the Yaoundé Declaration just to stand behind the best and coordinated regional maritime security response.

In March 2015 the Council of the European Union (EU) adopted the Gulf of Guinea Action Plan 2015–2020, which outlines the EU's approach to helping the region combat its maritime insecurity. This plan intends to provide support at both the regional and the national level towards the ongoing efforts mentioned of ECOWAS, ECCAS, the GGC, and all signatories of the Yaoundé Declaration. The EU envisages that the implementation of this plan will reinforce intraregional cooperation and increase the level of coordination among the EU, its member states, and international partners. The plan states that the Council "…*stands ready to assist West and Central African coastal states to achieve long lasting prosperity through an integrated and cross-sectorial approach, linking the importance of good governance, rule of law, and the development of the maritime domain to enable greater trade cooperation, and job creation for the countries in the region*."

All the navies of the GOG have one common goal, and that is to provide a safe and secure passage way for the ships and crews in these waters. They conduct exercises to build capacity and ensure their readiness. One such exercise is the *Obangame Express*, conducted by U.S. Naval Forces Africa, which is "…

an at-sea maritime exercise designed to improve cooperation among participating nations in order to increase maritime safety and security in the GOG." It focuses on maritime interdiction operation, as well as visit, board, search, and seizure techniques. CJOS COE, as part of its MSA project, is initiating an engagement with exercise planners to put forward objectives for an exercise with focus on anything from information gathering, information sharing, and interoperability.

The long-term effectiveness of these initiatives is difficult to assess at this stage, because many are still relatively new or only partially implemented. However, there is surely a need to continue assessment progress while addressing implementation challenges. Nevertheless, some signs are present. For example, of the 16 planned coordination centers, 10 have been established and are currently operational.

The coordination centers play an important role in promoting information exchange and joint actions in response to piracy and maritime crime in the Gulf of Guinea (see Figure 1). Maritime Security Regional Center of Central Africa (CRESMAC) was created in 2009 and located in the Republic of Congo following a memorandum signed between ECCAS and the Heads of State and Governments of ECCAS countries. CRESMAC has two zones (A, D) and works with CRESMAO's (Maritime Security Regional Center of Western Africa) planned 3 zones (E, F, G) and foreign partners (US, France, Brazil, Germany, Italy, Spain, Portugal, and China). As it was presented in our MSR RT 16, Zone D's mission is to develop a security plan which includes plans of equipment and facilities, monitoring, training, and fighting against illegal immigration, drug trafficking, piracy, and other illegal activity. The Zone D states have a background of strong information sharing.

While there is still so much to be done in terms of improving information sharing and coordination in the GOG, it was agreed at MSR RT 16 that it could be addressed by improving three areas:

- Interoperability of communications or detection means for better compatibility between national users.
- National coordination fusion center to manage timely, secure, and accurate information.
- Common Operations Picture ashore and offshore.

Knowing that difficulties with information sharing in the GOG are based on:

- Lack of communication between different country's MOCs.
- Difficulties of HF communication between ships.
- No AIS (Automatic Identification System) or internet on most ships.
- Low radar coverage of the GOG

As a recommendation from our study paper, 'From Fragmented Sea Surveillance to Coordinated Maritime Situational Awareness', the Centers of Excellence (COE) should become more familiar with the breadth and depth of the GMCOI (Global Maritime Community of Interest). Hence, the COEs are in the process of identifying a number of key MSR (Maritime Security Regimes) stakeholders to either bring them together for regular meetings, or respectively to attend and support established GMCOI stakeholder events to foster MSA collaboration. CJOS COE is working to improve global MSA, and we have a great challenge facing us: continuing the successful engagement with African stakeholders working in the Maritime Security/Maritime Situational Awareness activities in Africa. Stakeholders of improved maritime conditions include African States, local communities, specialized regional institutions and associations, the African maritime private sector, strategic development partners, and the international community as a whole. This activity will further support the MSA project endeavors conducted over several years at CJOS COE. ☸

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.

STRENGTHENING THE EUROPEAN UNION AND NATO AMPHIBIOUS CAPABILITY AND INTEROPERABILITY

CAPT Massimiliano Nannini, ITA-N
CJOS COE

Source: ITA Navy

Exercise EMERALD MOVE 2016 (ERMO 16) held in the Tyrrhenian Sea.

On 5 December 2000, the Ministers of Defense of the United Kingdom, Netherlands, Italy, Spain and France signed a letter of intent with the title "European Amphibious Initiative" (EAI) with the aim of enhancing amphibious capability, primarily through establishing greater co-operation and progressively improving interoperability between existing European Union and NATO forces. With this initiative, the five signatories intended to group a set of capabilities to allow the EU and NATO to have a significant force in the amphibious field.

"The European Amphibious Initiative is also working to integrate the European amphibious component in the NATO Response Force (NRF) and in the European Union Battle Group (EUBG)."

At the organizational level, EAI is driven by the Steering Group (SG), who tasks the Working Group (WG) to develop concepts, plan common exercises and organize a symposium for the member nations' Force Commanders or the Commanders of Amphibious Task Forces and Commanders of Landing Forces (CATF / CLF). EAI is also working to integrate the European amphibious component in the NATO Response Force (NRF) and in the European Union Battle Group (EUBG). Over the last decade, interest in EAI has grown with other European amphibious-capable partners participating, including Germany, Portugal, Sweden, Denmark, Turkey and Norway. Following the April 2014 SG meeting, Portugal, Sweden and Belgium applied to join the initiative as well. Italy chaired the last WG meeting held in London this past February, at which, the initiative decided to draft of a new Declaration of Intent (DoI), which was subsequently signed at the Chief of European Navies meeting (CHENS) held the following month.

Since 2002, the initiative has resulted in several common exercises. At the tactical level, the main objective of these exercises is to check the amphibious capability expressed by member nations. Additionally, the exercises are to ensure interoperability between the participating forces, with a particular focus on the conduct of initial entry operations, non-combatant

Source: CJOS COE

Exercise EMERALD MOVE 2016 involved the deployment of more than 3,000 men and women , from 10 European countries, in the waters of the Tyrrhenian Sea central and Capo Teulada, Italy.

evacuation operations (NEO), humanitarian assistance, and land and amphibious folding maneuver. The initiative held its first common exercise, NEO Tapon, in June 2005. The CATF/ CLF exercise was held off the coast of Gibraltar and was attended by all member states.

This past September, EAI conducted its most recent common exercise known as Emerald Move (ERMO). ERMO was founded to test the inter-European expeditionary capacity from the sea and increase synergy and interoperability between the European amphibious components. The aim of the exercise is to constitute a brigade-level force available to the international community able to operate under the auspices of the European Union. Starting from the initial planning phase, up to the subsequent conduct of operations, the Italian Navy guided the exercise at sea and ashore aboard the amphibious task force. Rear Admiral Salvatore Vitiello, Commander of the Third Division, served as the CATF, while Rear Admiral Bruno Cesare Petragnani, Commander of the Navy Brigade San Marco, served as the CLF.

Italy participated with ITS Cavour, ITS Carabiniere, ITS San Giorgio, Submarine Venuti, an aliquot of 400 riflemen of the San Marco Marine Brigade and 71 Italian Army "Lagunari". The other participating countries were France, with LHD FS Mistral and 200 marines, the Netherlands, with HNLMS LPD Rottherdam and 117 marines, Spain with SPS LHD Juan Carlos I, FFG SPS Numancia and 400 marines,

Source: ITA Navy

The Italian 1st San Marco Regiment (1° Reggimento San Marco) conducting amphibious landing during ERMO 16.

Turkey with the LST Osmangazi and 80 marines, the UK with 28 marines, Portugal with 90 marines and Belgium with 121 marines. In addition to marine and ground units, an air component consisting of nine Italian and Spanish AV8B Plus and 18 helicopters, took part in an exercise.

The training activity developed in several stages, starting from planning, through the integration of forces, and the deployment of naval units in the waters off Cape Teulada. Training missions included the execution of amphibious assault activities, constituted by the initial infiltration of the Recon and Target Acquisition Team and Underwater Demolition Team (UDT) released by the Submarine Venuti. The UDT was followed by four waves of amphibious vehicles, coming from their parent units, all conducted with the support of fixed-wing and rotary-wing aircraft. The training also included a medical evacuation and the evacuation of non-combatants, aimed at improving integration and standardizing procedures.

Although EAI has made great strides in improving the amphibious capability and interoperability of its member nations, the political popularity of a European expeditionary force remains low. As a result, EAI faces limited funding of new assets or training to improve capabilities. This is especially true for those nations with a smaller GDP. With this premise, Marine Forces Europe/ Africa (MARFOREUR/AF) have recently been working closely with EAI to develop a synchronized way ahead for allied amphibious forces to meet today's and tomorrow's challenges. The concept is to look at the actual European amphibious capability, generate a force up to a division size, and to apportion the appropriate naval assets to this force in a tactical interoperable way.

This concept of a multinational amphibious force in support of NATO for collective defense, crisis management, and cooperative security was presented at the Allied Leaders Expeditionary Symposium (ALES), hosted this past October by MARFOREUR/ AF in Stuttgart, Germany. Amphibious leaders from all EAI member nations were in attendance, as were representatives from Naval Striking and Support Forces NATO (STRIKFORNATO). Potentially the most challenging aspect of this concept will be the Command and Control (C2) construct that will apply to both training and operations in the scope of a force up to a division in size which may be NATO, UN, US or European-led. This complicated C2 construct, as well as the relationship between the MARFOREUR/ AF-led symposium and EAI will be the subject of the next ALES to be held May 2017. ☸

CAPT Massimiliano Nannini heads the Transformation Branch at CJOS COE in Norfolk, VA. For further information on this subject, he may be contacted at usff.cjos.coe@navy.mil.

MARITIME SECURITY REGIMES ROUNDTABLE 2016

CDR Ricardo Valdes, ESP-N
CJOS COE

Source: U.S. Navy

Norfolk, VA - Maritime Security Regimes Roundtable '16 hosted by CJOS COE.

Situational Awareness contributes to all phases of the operations planning process (OPP) by providing a holistic understanding of the environment. Likewise, Maritime Situational Awareness (MSA) contributes to all phases of the maritime expeditionary operations planning process by providing a holistic understanding of the Maritime Domain. The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) has, for some time, sought to identify gaps and shortfalls in global MSA. CJOS COE, along with many others in the Global Maritime Community of Interest, has been actively engaged in determining the ways and means to address these gaps by improving the effectiveness of global Maritime Situational (Domain) Awareness.

In June 2015, the first Roundtable (RT) forum was held in Madrid (Spain). CJOS COE facilitated and organized this historical inaugural meeting between regional and global maritime security stakeholders, with the objective of encouraging dialogue, sharing best practices, and initiating future cooperation. Some 30 Maritime Security organizations across the globe were represented by regional and local stakeholders who enjoyed a varying degree of cooperation between one another.

We believe that dialogue has the potential to leverage wider regional and inter-regional maritime access and enhance maritime security. Therefore, the second Maritime Security Regimes Roundtable 2016 (MSR RT 16) was hosted by the CJOS COE at the Slover Library, Norfolk, Virginia (USA), on 26 and 27 April 2016. Civilian and military professionals were invited from throughout the global MSA community. The attendees represent a strong cross-section of government, non-government, military, academic, and industry stakeholders from around the world who play a leading role in maritime security affairs in their respective nations or geographic regions.

"CJOS COE facilitated and organized this historical inaugural meeting between regional and global maritime security stakeholders, with the objective of encouraging dialogue, sharing best practices, and initiating future cooperation."

		Finding	Recommendation
CHALLENGES	1	Operations outside the law	As threats are still increasing, it's more necessary than ever to create a shared network amongst regimes in the field of maritime security
	2	Regulations	Try to discuss, and perhaps agree, what should be the framework to develop future regulations by identifying key points
	3	Procedures	Each organization parametrizes data to fit its needs. Develop a procedure that permits every regime to jump from one layer to another (local, regional, global)
	4	Sharing	Ensure and facilitate engagements across cultural barriers for involved players and authorities sharing similar concerns and interests
COOPERATION	5	Cooperation vs Building	Identify the need that permits to overcome any lack in the MSA cycle
	6	Coordination	Support those initiatives committed to develop coordination
	7	Core tasks	Understand that holistic solutions will contain elements from each (influence, response, awareness) core bin
IMPROVE	8	Pitfalls in information sharing	Continue to understand the problem and work towards regulatory barrier breakdown; meanwhile, maintain and develop personal relationships across the MSR to enhance trust
	9	Develop plans	Recognize the mechanisms which have achieved success and work towards expansion
	10	Information is not the same as intelligence	Continue efforts to share actionable intelligence between multiple organizations, agencies, and structures
BUILD	11	Capacity building	Identify who to develop capacity building beside our recommendation 5 related to lacks
	12	Mutual Trust	Continue with the firm implementation of regular maritime security regimes meetings on relevant levels
	13	Common Information Sharing Environment	Look for those ways that permit information and data exchange. Determining where to implement it and what should be exchanged.
	14	Enterprise solution	This should include: • Define (and share) stakeholder interests and decision-making culture; • Determine (and share) critical information requirements (through security and business lenses); • Adopt a repeatable "information exchange and triage" process and encourage voluntary collaboration; • Apply scientific rigor to define surveillance requirements; • Harmonize/simplify reporting requirements
	15	Cooperation with commercial companies	The shipping industry is part of the solution and should always be included in any MSR-related meetings/deliberations
	16	Commitment to cooperate	Establish, now, a MSR cooperative enterprise, emphasizing collaboration in a global approach to regional maritime security changes

1 Figure 1. Findings and associated recommendations, drawn from MSR RT 16.

"From Unconnected Regional Maritime Surveillance to Effective Global Maritime Situational Awareness" was the theme of this forum. The forum was structured around four panels, each tasked to discuss a different sub-theme (Challenges, Cooperation, Improve, and Build) and several different perspectives on the current and emerging threats, towards achieving effective maritime security.

The principal objectives in MSR RT16 were:

Identify and share best practices and practical solutions to address identified challenges; and

Form the basis of an agreed framework for improved information sharing and collaboration among the MSRs from across the Global Maritime Community of Interest.

Were these objectives achieved? Good examples were set forth through the many success stories from different organizations. Most of the discussions came back to the requirement for, and challenges to, effective information exchange, with the only purpose of getting the right piece of information to the right people at the right time. So it seems, the first objective was achieved. The second objective is more than ventured, but a remarkable acceleration and build momentum would be achieved if three things are done:

- Agree once and for all whether improved information sharing and collaboration at the inter-regional level is a problem which needs to be addressed.
- Agree on an approach to the information sharing/collaboration problem (if it is a problem).
- Finally, and perhaps, the biggest problem is an agreement on who is going to build a framework to support the chosen approach. A leader is needed.

Throughout MSR RT 16, the following list summarizes and identifies what the participants viewed as the main challenges to achieve effective global maritime security:

- Identify, track, and apprehend actors operating outside the law.
- Update regulations.
- Establish procedures to facilitate information exchange.
- Share timely information with those who need to know.

Our analysis has been developed by taking into account panel presentations and discussions, and consulting previous research related to the conference theme. This includes: the conference notes from MSR RT 15; the CJOS/CSW (Centre of Excellence for Operations in Confined Shallow Waters) MSA Study paper (published in April 2015); the MSR and Enterprise Manual (2011); and, conference proceedings from maritime security conferences hosted by CJOS COE since 2011. The resultant analysis has been condensed to its most relevant determining factors, which then form the findings for each element of the four main sub-themes of the conference. These 16 findings and associated recommendations, drawn from MSR RT 16 are illustrated in Figure 1.

We are now at the point where the representatives of the global MSRs and other stakeholders have to commit to regularly scheduled meetings, agree on collaborative information sharing tools to enhance meeting effectiveness (portals, email, websites), and create terms of reference (or constitution) to provide a meeting structure. This basic next step will help achieve the following goals which were highlighted repeatedly during MSR RT 16:

- Build useful networks and consistent habitual relationships.
- Incentivize information sharing by sharing, at meetings, what information is actually important to the various MSRs.

Meanwhile, CJOS COE will be working to that end; acting as a facilitator like in the past; providing support to those who request it; and championing best practices between MSRs. It's worthwhile to continue making this effort because, as it was mentioned several times during MSR RT 16, the main purpose of situational awareness is to support good and timely decisions. At the end, decisions will be taken if the piece of information is transferred from one organization to other, on time. So CJOS COE will contribute to it by helping to build a simple, but self-sustained international structure linking maritime security regimes around the world, without further facilitation by non-stakeholders or outside agencies. ☸

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.

COMMAND AND CONTROL CENTRE OF EXCELLENCE SEMINAR

CDR Jonathan W. Sims, USA-N
CJOS COE

Source: U.S. Navy

Norfolk, VA - C2 COE Conference '16 hosted by C2 and CJOS COE.

The NATO Command and Control Centre of Excellence (C2COE), in cooperation with the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) and NATO Allied Command Transformation (ACT), presented it's annual 2016 seminar entitled "C2 in Future Emerging Warfare – Challenges for the Alliance and Coalitions". Nearly 150 participants representing 25 nations and organizations provided various views and issues related to the topic of the seminar hosted in Norfolk, Virginia, USA.

The purpose of the seminar was to support NATO nations and international institutional organizations by providing subject matter experts (SME) on all aspects of the Command and Control process with a concentration on the operational environment. Moreover, offering the Alliance with the most relevant contributions in the field of C2; permitting the Alliance to be properly prepared for a fast-paced and dynamic atmosphere with new centric areas and challenges.

General Denis Mercier, French Air Force, Supreme Allied Commander Transformation, opened the seminar by delivering the keynote address: "The Importance of Command and Control to the Alliance". In addition, subject matter experts throughout NATO administrations, embassies, lead work centers (LWCs) and civil companies such as TNO, ADS and BAE briefed the audience on challenges related to C2 in Emerging Warfare.

The seminar touched various concerns such as challenges to the Alliance and Coalitions both present and in the future. Imminent conflicts will require cooperation between combined joint military forces and civilian organizations. Hence, the reason why the seminar approached this vigorous subject from civil, maritime, land and air perspective. Conceptually, the seminar participants received a comprehensive understanding of future C2 challenges. The seminar examined how C2 would evolve in the next 5 to 10 years given the fast pace of technology development and ever evolving emerging warfare threats.

"Future conflicts will require cooperation between combined and joint military forces and civilian organizations."

During the seminar, a panel of experts was

assembled to share ideas and theories concentrated on the following questions:

- Who will be our adversaries?
- What will be the battlefield?
- How will our adversaries fight in the future?
- What will be the consequences of worldwide urbanization and the impact of advance weaponry?

Based on these range of questions, the C2 Seminar was divided into three segments:

Segment I: Focused on the future environment; seminar participants explored NATO's future as well as the enemy's future with regards to the exercise of authority and direction of attached forces in the accomplishment of the mission. Also, discussions elevated the topic of C2 systems and encounters with regard to urbanization and megacities.

Segment II: Focused on the present warfare ecosystem; outlining investigating current issues encompassing operations and warfare and interoperability. Seminar participants considered systems and platforms the alliance employs presently and in the near future (i.e. Theater Ballistic Missile Defense (TBMD), Joint Maritime Expeditionary Operations, and the F35 A/B Joint Strike Fighter).

Segment III: Re-visited the future environment to ask ourselves "What do we have to do now, in order to prepare for the future?"

The seminar was an effective example of the truism that C2 is integral to all domains. The subject matter experts brought together by the C2COE in concert with the maritime themes introduced by CJOS COE, furthered participants understanding of the integral necessity of C2 as a multi-domain enabler.

In 2017, C2COE will be hosting another dynamic seminar "NATO C2 in a Civil Environment" hosted in Valencia, Spain, 13 to 15 June, supported by Headquarters NATO Rapid Deployable Corps Spain. This seminar will address the key decisions made at the 2016 Warsaw Summit to project stability in the Euro-Atlantic area and beyond. To accomplish this directive, the seminar will address what NATO must do to enhance its ability to undertake effective C2 across the full spectrum of missions, especially in those where partnering with civilian organizations is required. Projecting stability from a C2 perspective means a focus of effort on: ensuring interoperability, enhancing situational awareness, adapting to challenges and threats, and keep sustainable structures with partners. ❁

Source: NATO

Improving interoperability was a key topic throughout the seminar; methodologies were presented ensuring the effective use of a partnership interoperability "toolbox" and that exercises, education and training adequately support NATO functionality focused objectives.

CDR Jonathan W. Sims 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 EXPEDITIONARY OPERATIONS CONFERENCE

LT Clarissa Butler, USA-N
CJOS COE

Source: ITA Navy

Oeiras, Portugal - Maritime Expeditionary Operations Conference (MEOC) 2016

During the third week of July, Naval Striking and Support Forces NATO (STRIKFORNATO), together with Combined Joint Operations from the Sea, Centre of Excellence (CJOS COE), hosted the bi-annual Maritime Expeditionary Operations Conference (MEOC) in Oeiras, Portugal. The timing of the conference was opportune – the Warsaw Summit was held the week before, reaffirming the Alliance's three core tasks: collective defense, crisis management, and cooperative security. The MEOC was able to capitalize on a maritime theme and contribute to the Summit's two key pillars: protecting citizens through modern deterrence and defense, and projecting stability beyond borders.

The conference brought together over 170 representatives from NATO Command and Force structures, academia, and national military commands from Allied and Partner Nations. Over the two days, attendees listened to five panels evolving from current threat, application of maritime expeditionary warfare, exercises and training, and the role of maritime partnerships.

Each panel featured four distinguished Officers and/or Senior Executives and the highlight of the conference were three Keynote Speakers [i]: General Petr Pavel, CZE-A, Chairman of the Military Committee (MC), Admiral Michele Howard, USA-N, COM Allied Joint Forces Command Naples (JFCNP), and Admiral Manfred Nielson, DEU-N, Dep Supreme Allied Command Transformation (SACT).

The goals of MEOC 16 were to define the future role of Maritime Expeditionary Operations (MEO) and how the capability can best be delivered to contribute to assurance and adaption measures in the evolving geopolitical sphere in light of emerging security challenges faced by the Alliance. During the five panel discussions, three themes came to the forefront: sources of instability, importance of joint and combined training, and partnership inside and outside the Alliance.

Sources of Instability in the East

Day 1 was largely dedicated to the maritime element of NATO's adaptation to the surrounding borders of the Alliance. Arguably, Russia maintains a competitive advantage over the Alliance through rapid decision-making, strong public support of military actions, and the use of operations in the perceived grey space below the threshold of war. Recent moves by Russia have tested NATO's unity and the Alliance should pay particular attention to the Baltic and Black Sea regions.

To counter this aggressive posture, the first panel recommended the Alliance adapt a posture of constraint and engagement while maintaining the

moral high ground through transparency. Credible and visible deterrence can be achieved through intensified Maritime Expeditionary Operational exercises such as the recent BALTOPS exercise, in which 14 NATO nations participated along with partners Finland and Sweden.

Both the Baltic and Black Sea regions require a tailored solution that takes into account regional diversity while providing a cooperative and inclusive approach. In particular, the Black Sea's importance as a strategic crossroads and cradle of Russian aggression requires cooperation with as many nations as possible including partners Ukraine and Georgia.

Sources of Instability in the South

Socioeconomic instability along the southern peripheries of the Alliance has caused mass migration and terrorist attacks to rise to an unprecedented level. The second panel focused on the effects of the deteriorating security situation in the Middle East and Africa and how the impact on NATO members will necessitate a review of NATO's Area of Responsibility.

As evolving threats continue to put new pressures on resources and priorities, NATO cannot act unilaterally in the region; it must cooperate with regional partners such as the African Union and Arab League to provide support. In the context of Maritime Expeditionary Operations, NATO can best provide a supporting role in functions such as maritime domain awareness, freedom of navigation, and port security. However, in a relatively new strategic direction for the Alliance, NATO must commit to understanding the complex environment to the south prior to proposing specific means of engagement.

Importance of Training

Day 2 focused on maritime exercises, training, and the role of maritime partnerships. NATO's two primary maritime objectives are to deny use of the sea by adversaries and to deliver effects ashore. The former is an easily understood mission, but the latter includes multiple missions to include power projection, humanitarian assistance, noncombatant evacuation, and newer effects such as cyber warfare. In the event of invoking Article V, the most difficult situation for the Alliance at sea is operating Carrier Strike and Amphibious Tasking simultaneously with an appropriately agile and interoperable Command and Control Structure.

Without the historical context of a past Article V mission at sea, the Alliance is left to develop trust and interoperability through training and exercises. One senior official was quoted, "trust cannot be surged," it must be developed over time with quality training opportunities. All but 10 out of the 25 Alliance navies have fewer days at sea than planned per year. Allied navies must increase the number of large scale, unscripted combined and joint exercises while maximizing return on investment for the time and money spent by individual nations. Integrating the maritime and land forces of allied countries will allow the Alliance to train how it will fight.

Partnership

Partners offer regional expertise and experience that NATO can leverage to execute the Alliance Maritime Strategy. For example, Sweden's in depth understanding of operations in the littoral environment or Japan's grasp of the shifting military balance in East Asia can benefit Alliance security. Each potential maritime partner will have a unique relationship with the Alliance, each with its own political guidance and tailored cooperative engagements.

Potential areas of cooperation with partners in the maritime domain include supporting rule of law, joint exercises, deeper intelligence sharing, capacity building, defense of sea lines of communications, joint capability development, and participation and training in NATO's Centres of Excellence.

Ultimately, partnering with other nations will drive the Alliance to be globally aware, agile, and enable NATO Maritime Expeditionary Operations to face emerging threats within and beyond the traditional NATO Area of Responsibility. ☸

LT Clarissa Butler is a Staff Officer at CJOS COE in Norfolk, VA. For further information on this subject, she may be contacted at usff.cjos.coe@navy.mil.

CYBER RISK WITHIN THE MARITIME DOMAIN

CDR Ovidiu Portase, ROU-N
CJOS COE

Source: Wikipedia

Port Jebel Ali located in Dubai, United Arab Emirates.

Technology, automation and digitization dominate maritime domain, where integrated, customized, and high performance solutions make ships, ports, and offshore installations more efficient, safe, and profitable. More information and communication technology (ICT) and operational technology (OT) systems interconnected via cyberspace are now capable of performing complex tasks, more rapidly and virtually error-free, with little or no human interaction. But this progress has generated some new challenges.

"Due to the global nature of cyberspace, we must not forget that a cyber threat actor doesn't have to be within the maritime domain to generate a maritime catastrophic incident."

Various hazards and threats could expose or exploit, intentionally or not, existing vulnerabilities of these cyber systems and trigger cyber incidents that put at risk maritime organizations' missions, goals, and objectives.

Sensitive or classified information disclosure, physical destruction or denial of access to data, maritime systems or networks could lead to material and financial loss, inoperative industrial systems, catastrophic pollution, disruptions in the global supply chain or even loss of life, incidents which might have a high level of impact on people welfare, environment, economic activities or even maritime and national security.

In addressing hazards and threats to maritime cyber systems, both intentional and non-intentional sources of threat must be considered. Natural elements, human errors (including structural failures), technical failures, or partnering organizations can inadvertently generate maritime cyber incidents. Therefore, safeguards should be put in place against such undesired and accidental effects. For example, Hurricane Sandy made ICT and OT systems and services unavailable for terminal operators, pilots, and others stakeholders of Port of New York and New Jersey in 2012. Also, the human error and primarily reliance of an inaccurate Digital

Nautical Chart lead to grounding of USS Guardian in 2013. These are just two examples of such incidents.

On the other side, insiders, competitors, hacktivists, criminal organizations, cyber terrorists or nation-states could intentionally conduct untargeted or targeted attacks on ICT and OT systems and networks operated by maritime organizations.

Single individuals or ad-hoc or well-structured organizations can execute attacks ranging from apparently inoffensive network monitoring to more elaborate attacks (APT - Advanced Persistent Threat). Whether they be a state trying to steal financial records, customer data, and shipment manifest, or hackers employed by pirates to get information about their next target, they all can generate maritime cyber incidents with serious impact on maritime organizations and beyond.

Due to the global nature of cyberspace, we must not forget that a cyber threat actor doesn't have to be within the maritime domain to generate a maritime catastrophic incident.. An easy target or a good return of investment from a third party will always attract cyber threat actors, regardless of whether or not they belong to the maritime domain. However, cyber threat actors can't generate cyber risk without the existence of a vulnerability they can expose or exploit to create harm.

As ships are increasingly adopting degrees of automation that decrease the size (and expense) of ship's crews, they become more vulnerable to cyber-attacks and less equipped to deal with the after effects of one.

To make automation more efficient, integrated systems are required to interconnect more systems together and allow exerting control from one or multiple locations, locally or remotely, with or without human presence. Every device, equipment, and system brings with it its own inherent vulnerabilities, not to mention the potential vulnerabilities brought by any configuration change after a component upgrade or addition.

Because ships navigate in isolation and exchange increasing amount of data, multiple wireless communications and Internet connections are more common on board ships now, enabling access to information or remote functions. As these connections to ships become faster and more reliable, hacking into the connections becomes much easier. Regardless of its purpose, to send data back to organizations ashore to monitor or remote maintenance, the almost permanent Internet connectivity and broadbands of 50 MB could facilitate cyber intrusions and attacks. Moreover, Internet use for non-operational purposes increases the risk of contamination or infiltration of the ships network.

But ship cyber vulnerabilities are not limited only to technical aspects of ship systems and their data and information flows. Smaller crews; the absence of cyber threats from ship security assessments; inadequate roles, responsibilities, plans and procedures to address maritime cybersecurity incidents; and other similar organizational failures could open the path for uncontained propagation of adverse effects across the organization and beyond.

Without being limited in size like ships, ports are larger and more complex organizations. Even though they don't operate in isolation and are merely regulated by national legal frameworks, the variety of their components make cybersecurity a more challenging task. An interface between the maritime domain and its connecting rail, road, and air transportation networks, this element of critical infrastructure uses a combination of maritime and land -based cyber systems.

Similar to other domains, common ICT and OT system solutions are used for their daily operations, business, and administrative activities. A cyber attack on an ICT system might lead to corporate breaches, compromised office computers, or stolen business information, which could be devastating to any company and industry. Sector specific OT systems are used to operate land based facilities and installations (smart buildings, power plants, transmission and distribution networks, oil and gas terminals, railways network, etc.), where similar vulnerabilities are encountered and should be addressed.

In addition, vulnerabilities related to maritime-specific systems should be addressed. Maritime systems existing onboard ships and common to port systems (radars, AIS, GPS, etc.), port operations

specific systems (Terminal Operating Systems, Equipment Control Systems, Automated Stacking Cranes, etc.) along with electronic and digital aids to navigation, coastal maritime communications systems, satellite ground terminals have their own cyber vulnerabilities and are prone to cyber incidents.

The current trend to evolve to modern multimodal gateways connecting the maritime transport system with the other transportation systems (rivers and their adjacent ports, railway, road, air, etc.) is an operational challenge given not only by the extension of their dependencies, but also by their aggregated effects.

Together with ships and ports, similar weaknesses of the maritime cyber systems or cyber enabled systems specific to offshore installations, waterways, littoral infrastructure, etc. along with their security procedures or internal controls are other opportunities for a threat actor to achieve its objectives. The absence of a common approach, regulated at international and national levels, implemented by a single organizational entity and based on a consolidated set of policies, procedures and mechanisms for a clearly designated area usually might lead to no or limited awareness and understanding of the environment, disunity of effort and lack of effective and efficient reaction.

Not fully aware of the causes and potential impact of a cyber incident, the global maritime community was initially reluctant to accept cyber risks existence in the maritime domain. But, reports on cybersecurity issues in the maritime sector released by prestigious institutions in Europe in 2011 and in the U.S. in 2013, along with the media coverage of major maritime cybersecurity incidents made the community take action.

In 2016 , companies or groups of companies from the maritime industry developed and published guidelines on cybersecurity onboard ships or risk-based management program to apply best practice cybersecurity, automated systems safety, data integrity and software verification cybersecurity guidance notes for the marine and offshore Industries, where a risk-based approach to identifying and responding to cyber threats is proposed and where the plans and procedures for cyber risk management are seen as complementary to existing security and safety risk management requirements contained in the International Safety Management Code (ISM) Code and the International Ship and Port Facility Security (ISPS) Code.

At the international level, the nations proposed voluntary guidelines to enhance maritime cybersecurity to be discussed within Facilitation Committee and Maritime Security Committee of the International Maritime Organization (IMO), which recently released its first circular on maritime cyber risk management.

As recommended by this IMO document, a holistic cyber risk management could be more effective in addressing the challenges of interdependencies of maritime systems as a whole, and not just separately solving individual aspects of maritime cybersecurity.

An adequate cyber risk management in the maritime domain should start with defining and adoption of an appropriate framework and process, both adapted to the existing maritime context. A key element in achieving cyber resilience, a good risk assessment should properly identify, analyze, and evaluate all maritime related cyber risks so effective solutions for risk treatment are developed, implemented and used. Equally important, a continuous monitoring, review, communication and consultation are indispensable within this risk management process.

Maritime cyber systems should be developed from their inception with cybersecurity requirements as part of the system development life cycle, supported by a redundant, distributed infrastructure that could ensure continuity of operation with little to no disruption with a low cost of development and maintenance.

Cyber incidents should be part of business continuity and disaster recovery planning of maritime organizations. A correct anticipation and full understanding of the potential consequences of a cyber incident is impossible within the limited time during a crisis or disaster. Alternate contingency plans and well-planned back-up plans are required along with a solid cyber defense. Roles and responsibilities, procedures, and tools to address the challenges of a maritime cybersecurity incident should be addressed

well in advance. Moreover, these should regularly be exercised and reviewed in order to keep them effective and efficient, and to develop the required skills and expertise within the organizations.

Maritime cyber resilience is the resilience of maritime systems and organizations to cyber incidents. Along with technical solutions made available by industry, maritime specific regulations should establish specific principles of governance, roles and responsibilities, specific measure and activities, information sharing, and compliance mechanisms.

To address maritime cyber risks successfully and ensure cyber resilience, a comprehensive, multilevel, holistic risk-based approach, integrated within the existing maritime safety and security frameworks and processes is required.

Cyber risks should be always part of a continuous risk management process, where existing management strategies are permanently assessed and reviewed, to be capable of addressing the challenges brought by new technologies and systems (such as machine learning, artificial intelligence, unmanned vehicles, Internet of Things, Industrial Internet of Things, etc.) so the cybersecurity objectives of confidentiality and integrity can be chieved, and risk can be contained permanently within acceptable levels. ❁

1. Mark Szakonyi, , “US Coast Guard takes lead to address cyber risks at ports”, The Journal of Commerce, Apr 01, 2015, http://www.joc.com/regulation-policy/transportation-policy/us-transportation-policy/us-coast-guard-takes-lead-address-cyber-risks-ports_20150401.html.

2. Department of the Navy, “Command investigation into the grounding of USS Guardin (MCM 5) on Tubbataha reef, Republic of the Philippines that occurred on 17 January 2013”, 22 May 2013, www.cpf.navy.mil/foia/reading-room/2013/06/uss-guardian-grounding.pdf .

3. Kurt Marko, “How a Scanner Infected Corporate Systems and Stole Data: Beware Trojan Peripherals”, Forbes, 10 July 2014, http://www.forbes.com/sites/kurtmarko/2014/07/10/trojan-hardware-spreads-apts/#169e934e4342.

4. J ames Rogers, “From high seas to high tech: Pirates hack shipping company”, Fox News Tech, 02 March 2016, http://www.foxnews.com/tech/2016/03/02/from-high-seas-to-high-tech-pirates-hack-shipping-company.html .

5.Wendy Laursen, “Many Operators Open to Simple Cyber At tack”, The Maritime Executive, 10 June 2015, http://www.maritime-executive.com/article/many-operators-open-to-simple-cyber-attack .

6. European Union Agency for Network and Information Security, "Cyber Security Aspects in the Maritime Sector". Last modified December, 19, 2011. https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1.

7. Kramek, Joseph. ”The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities”. Last modified July, 3, 2013. http://www.brookings.edu/research/papers/2013/07/03-cyber-ports-security-kramek.

8. Jeremy Wagstaff, "All at sea: global shipping fleet exposed to hacking threat", 24 April 2014, http://www.reuters.com/article/tech-cybersecurity-shipping-idUSL3N0N402020140423.

9. BIMCO. “Cyber security guidelines for ships launched today”, 4 January 2016, https://www.bimco.org/News/2016/01/04_Cyber_security_guidelines.aspx.

10. American Bureau of Shipping, “ABS Expands Comprehensive Industry-First Cyber System Guidance”, 6 September 2016, http://ww2.eagle.org/en/news/press-room/2016/ABS-Expands-Comprehensive-Industry-First-Cyber-System-Guidance.html.

11. International Maritime Organization, “Maritime Safety Committee (MSC), 96th session, 11-20 May 2016” 25 May 2016, http://www.imo.org/en/MediaCentre/MeetingSummaries/MSC/Pages/MSC-96th-session.aspx.

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.

HOW MARITIME IS KEY TO UNITE THE EFFORT TO COMBAT GLOBAL CYBERSECURITY CHALLENGES

Dione Lee
QSE Solutions

Source: Pixabay

Cyber threats are fluid, versatile, and globally shared,

Maritime activity globally connects all of us through its fluidity of movement, versatility, and ability to share resources. Cargo transported by sea represents 90% of world trade, including the food we eat and the energy we use.[1] Cyber threats are also fluid, versatile, and globally shared, and could greatly inhibit and disrupt commerce and security. Who better to address these issues and achieve positive security outcomes than the maritime community, experienced in assuring safe and secure passage of people, assets and cargoes by forming key partner relationships, shared infrastructure, and frameworks for continual improvement?

This collaboration and leveraging of resources has been a lynchpin in commerce, safety, environmental protection, and our security for quite some time. National economies are dependent on the safe and secure transport of cargo. Instead of reinventing a framework and processes to address cyber threats and attacks, why not plug in cybersecurity as a risk category within pre-existing maritime safety management system elements, like the International Safety Management (ISM) Code?

“Cyber threats are also fluid, versatile, and globally shared, and could greatly inhibit and disrupt commerce and security. ”

Cybersecurity Challenges with Proposed Action Items

To avoid overcomplicating this already confusing topic, we need to design a simple and streamlined solution to better manage risk, turn the tide toward prevention, and strive toward a generative security culture resulting in zero cybersecurity incidents. We can attempt to manage risk by summarizing cybersecurity challenges and their proposed action items in a well-organized table. (see Table 1). The more robust we get with organizing, consolidating, and disseminating cybersecurity information, the more effective we will be at managing the threat of cyber attacks. The maritime community has the framework

(Continued on page 54)

Table 1. Cybersecurity Challenges and Proposed Action Items

Challenges	Proposed Action Items
Lack of common terminology – is cybersecurity one or two words? Is it a cybersecurity incident or a cyber attack?	• **Determine universal cyber security terminology, working with such organizations as ASTM International – ASTM has a draft "Best Standard Practice/Guide for Cyber Security, for Cyber Attack Mitigation for Marine and Mariner Use." [2]**
Lack of Overarching Goal/Objective	• **Zero tolerance – Work together towards eliminating all cybersecurity attacks.**
Lack of cohesive cybersecurity leadership	• **Expand Company Security Officer (CSO), Vessel Security Officer (VSO), and Facility Security Officer (FSO) roles, responsibilities, and authorities to include cybersecurity.** • **Identify and communicate clear governance when it comes to cybersecurity – who is responsible for what.** • **Create a single industry-wide consortium to develop cyber security best management practices.**
Lack of a cybersecurity plan	• **Include cybersecurity in existing security plan.** • **Include risk and opportunity assessment function to develop plan. Review Cyber Risks in the Marine Transportation System the U.S. Coast Guard Approach, which includes a helpful Cyber Risk Bowtie Model.[3]** • **Conduct unified research to better understand the threat. How do you provide strategic directions if you do not know what the risks are? Risk assessments at all levels should be conducted to include cybersecurity in job Hazard Analysis (JHA), shoreside management risk assessments, and enterprise and/or business continuity risk assessment.** • **Review the U.S. Coast Guard Cyber Strategy, June 2015.[4]**
Lack of resource allocation for cybersecurity	• **Include cybersecurity in the planning and budget process.**
Lack of operational policies and procedure that address cybersecurity at the deckplate	• **Review the ABS Cybersecurity Guidance Notes for the Marine & Offshore Industries.[5]** • **Implementing the following best practices provided by "an Operator's Perspective" Robert Sheen, Vice President, Operations, Ocean Shipholdings, Inc. during the SOCP 2016 Fall Meeting:** ° **Share information throughout the organization that more modern ships with networked systems and automated information replication to shoreside facilities are more vulnerable than more modern ships, and the same is true for shoreside automation. Reverse the trend, make important systems stand-alone from other systems, and resist the network integration urge.**

Table 1. Cybersecurity Challenge and Proposed Action Items (continued)

Challenges	Proposed Action Items
Lack of operational policies and procedure that address cybersecurity at the deckplate (continued)	◦ **Provide examples of cyber intrusions so people understand and are able to counter these threats with risk assessment and develop protective actions.** ◦ **Ensure that the crew communications system is "standalone" and not networked with any other systems.** ◦ **Ensure that automated ship to shore communications systems are encrypted and that a protocol exists to ensure the authenticity of the Communication.** ◦ **Ensure that operating systems are locked down and any passwords are closely kept.** ◦ **Disallow the connection of flash drives to the systems without password protection, virus scans, and authentication protocols.** ◦ **Set up strong user access control.** ◦ **Set up strong network access control.** ◦ **Perform back-ups.** ◦ **Test recovery plans.** ◦ **Make sure any anti-virus software is kept up-to-date.** ◦ **Ensure that firewalls exist throughout the network and are updated to reflect current threat profiles.** ◦ **Set rules and communicate to the crews and shore staff as to what kind of information is sent back and forth between ship and shore and how this information is to be sent and how it is to be protected.**
Lack of "cyber threat" awareness	• **Provide cybersecurity information in a simple and easy to understand format on a regular basis.** • **Provide cybersecurity information to share with families to ensure cyber threats at home do not cross pollinate to work products.** • **Circulate information and alerts provided by outside sources like the National Security Institute's weekly NewsWatch.[6]** • **Encourage trade associations to include cybersecurity panels.** • **Attend industry events that discuss cybersecurity by incorporating business, government, education, and labor perspectives with actionable outputs as a result of collaborative input during the meetings, such as the Ship Operations Cooperative Program bi-annual meetings.[7]**

Table 1. Cybersecurity Challenges and Proposed Action Items (continued)

Challenges	Proposed Action Items
Information overload	• Ensure relevancy of information and provide comprehensive assimilation of information in an organized format prior to distribution.
Multiple unclear Laws, Regulations and Standards from multiple agencies	• Employ electronic "chain of custody" best practices to ensure confidential data in your keeping is protected. • Determine which regulatory agencies impact your organization. • Review the United States Coast Guard's document *Cyber Risks in the Marine Transportation System*, which outlines cybersecurity authorities within the United States federal government.[8]
Constantly changing threats	• Ensure malleable and simple processes for managing information efficiently and effectively. For example: risk management, document control, non-conformance control, audits, corrective action and preventive action.
Lack of cybersecurity being covered in school curriculums	• Integrate cybersecurity topics into all appropriate maritime training classes, starting as early as K-12. • Integrate cybersecurity issues into simulator scenarios, like the Navigation Skills Assessment Program (NSAP®).[9] • Include cybersecurity competency standards
Lack of cybersecurity in emergency planning	• Include cybersecurity in Business Continuity Planning • Develop a cybersecurity breach contingency plan, similar to an oil spill response plan • Conduct cybersecurity drills for threats and attacks
Lack of cybersecurity as a risk factor when proposing change	• Incorporate cybersecurity in Management of Change Process • Critically think through the process if an IT solution is the appropriate action to take – it may be more efficient and cost effective in the short term, but will it be effective long term?
Lack of cybersecurity incident investigations	• Include "cybersecurity" as an incident category to track, trend investigate, and analyze.
Lack of cybersecurity engagement of employees	• Increase cybersecurity awareness and how it could impact them.
Lack of cybersecurity Inspections	• Develop routine inspections to monitor cybersecurity onboard and ashore. • Include cybersecurity as a preventive maintenance item. • Expand scope of surveys to include cybersecurity.

Table 1. Cybersecurity Challenge and Proposed Action Items (continued)

Challenges	Proposed Action Items
Lack of cybersecurity control measures being audited	• **Establish control measures and audit to ensure the control measures have been implemented and are effective in reducing the risk of cyber threats and attacks.** • **Include cybersecurity in internal management system audits and required security audits.**
Lack of vendor / OEM cybersecurity audits	• **Include cybersecurity quality assurance when vetting vendors / Original Equipment Manufacturers (OEMs).**
Lack of cybersecurity leading and predictive indicators to prevent occurrence	• **Track, trend, and analyze cybersecurity incidents and near misses to monitor and measure the risks.** • **Educate mariners to understand what a cybersecurity threat is and solicit their support to report.** • **Determine how to monitor and manage without breaching privacy rights and creating distrust.**
Lack of Cyber Security Culture	• **Use the same framework for developing a safety culture**

and existing systems in place for managing cybersecurity; they just need to be utilized. The biggest effect maritime can have on cybersecurity is the industry's collaborative and cooperative spirit to join in an all-out effort to stop cybersecurity incidents from happening in order to keep us and our families safe, secure, and out of harm's way. ☸

1. International Maritime Organization, https://business.un.org/en/entities/13.
2. ASTM International, https://www.astm.org/ABOUT/overview.html.
3. Cyber Risks in the Marine Transportation System the U.S. Coast Guard Approach, https://www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf.
4. United States Coast Guard Cyber Strategy; https://www.uscg.mil/seniorleadership/DOCS/cyber.pdf.
5. Cybersecurity Guidance Notes for the Marine & Offshore Industries; http://ww2.eagle.org/content/dam/eagle/publications/2016/Cybersecurity_16053_LR.pdf.
6. National Security Institute; https://www.nsi.org/.
7. Ships Operations Cooperative Program, SOCP Spring Summit; http://www.socp.us/article.html?aid=188.
8. Cyber Risks in the Maritime Transportation System; https://www.uscg.mil/hq/cg5/cg544/docs/USCG_Paper_MTS_CyberRisks.pdf.
9. Navigation Skills Assessment Program; https://nsap.com.

Dione Lee is President of QSE Solutions and a freelance writer. For further information contact dione@qsesolutions.com.

U.S. NAVAL WAR COLLEGE DEVELOPS INTERNATIONAL MARITIME OPERATIONS TRAINING

Michael Hallett
U.S. Naval War College

Source: U.S. Naval War College

USNWC broadens international training with I-MSOC.

The International Programs department at the US Naval War College has developed an International Maritime Staff Operators Course (I-MSOC) in order to answer the demand signal from partners for operational level focused maritime training. The first session of the course will be held in Spring 2018. As described in the course overview, "The International Maritime Staff Operator Course (I-MSOC) is a non-classified, twelve week course jointly produced by the United States Naval War College (USNWC) International Programs and the College of Operational and Strategic Leadership, to provide international naval officers the knowledge and skills needed to support the planning and execution of maritime operations and integrate with existing operational planning teams. Designed to meet the learning needs of O3-O5 (NATO OF-2 to OF-4) maritime officers, the course uses the US Navy Maritime Operations Center (MOC) as an organizing concept, and is informed by NATO, UN joint and US Naval doctrine, with a special emphasis on the US Navy Planning Process as described in Naval Warfare Publication Navy Planning 5-01." This article describes the I-MSOC development process as a preliminary high-velocity learning (HVL) implementation case study. For the purposes of this article, HVL experiences are powered by three "engines" or design principles: competency development focus, multidimensional assessment, and metacognitive awareness. This article describes the I-MSOC use of these design principles.

"The course introduces maritime component staff's baseline fundamentals and develops key competencies in students that enable them to comprehend, analyze and apply maritime operational level process and procedures necessary to plan, prepare, execute and assess combined maritime operations."

Competency Focus

The focus on competency development is the first HVL engine, or design principle. The course is

Source: U.S. Naval War College

The I-MSOC development process is a preliminary high-velocity learning (HVL) implementation case study.

modeled upon the extremely successful competency-based USNWC Maritime Staff Operators Course (MSOC) which, in accordance with the US Navy MOC standardization guidance, has prepared staff officers for service with US Fleets since 2007. Building on the MSOC model, "The course introduces maritime component staff's baseline fundamentals and develops key competencies in students that enable them to comprehend, analyze and apply maritime operational level process and procedures necessary to plan, prepare, execute and assess combined maritime operations."

This I-MSOC focus on competency development contrasts with much of the current non-military educational system as described by Michelle R. Weise and Clayton M. Christensen in "Hire Education: Mastery, Modularization, and the Workforce Revolution," as follows: "The current education system separates learning to know and learning to do. Rather than giving students broad, interdisciplinary problems to solve, colleges and universities channel students through narrow specializations that have become artificially separated from one another."

In contrast, I-MSOC is built on a series of increasingly complex scenarios within which the students act, and through acting, learn. As Weise and Christensen write, "By being presented anomalies and real-world problems, students must be able to connect ideas on their own without necessarily knowing that different solutions come from different disciplines. Identifying how a body of understanding fits together is more useful than understanding the boundaries between disciplines." In the I-MSOC case, the course learning experiences are explicitly focused on shaping the maritime operational level "body of understanding."

Powerlifting offers a metaphor for the competency development process. A powerlifting coach provides an overall description and demonstration of a movement (a deadlift, for example), and then breaks down the movement into its discrete parts. The athlete practices each part using a PVC pipe until they can do the movement correctly. Once the competency in the low risk PVC pipe use is demonstrated, the athlete performs the movement using an unloaded bar and finally, upon demonstrating proper technique at each step, begins the process of developing increased competency at ever higher loads.

Similarly, the I-MSOC instructor demonstrates the staff skill or step in the planning process for the students. He or she then provides a lecture, or leads a discussion about a doctrinal reading to enrich the student's knowledge of the step. Following this the students are given the opportunity to perform the task (for example, center of gravity deconstruction during mission analysis) with the instructor there to ensure the students are executing the processes just described to them appropriately. By guiding the student through demonstration, analysis, synthesis and practice, the instructor enables the students to translate their initial hesitant understanding into fluent competency mastery.

Based on the MSOC model, I-MSOC is designed to develop multinational staff officer competencies in six areas: current operations (COPS), future operations (FOPS), future plans (FPLANS), assessment, planning, and staff skills. Weise and Christensen explain the utility of this approach: "By breaking down learning into competencies – not by courses or even subject matter – these [courses] can cost-effectively combine modules of learning into pathways that are agile and adaptable to the changing

labor market." The "labor market" in this case is the global network of maritime security organizations that attend the Naval War College. I-MSOC adds multinational elements to the competency set in order to ensure the course meets Partner's learning needs as an international course, and not as a U.S. course simply delivered to an international set of students.

Source: U.S. Naval War College

United States Naval War College in Newport, Rhode Island.

The course enables students to develop mastery in facilitating the commander's decision cycle within the maritime operations center (MOC) by acquainting students with the bundle of knowledge, and giving the opportunity to practice the skills in a realistic context that constitutes the required staff competencies. This focus on mastery, rather than time spent in the classroom, as the measure of effectiveness, enables learning cycle compression. This compression generates the "high" in HVL. I-MSOC Mastery demonstration requires multidimensional participation in course activities, such as lectures, operational planning team discussions, and performing MOC tasks during the battle lab. However, students develop mastery at different rates.

If a student appears unable to execute the cognitive tasks associated with, for example, the mission analysis step of the navy planning process, the faculty intervenes to provide additional explanation. This interaction takes place unobtrusively, and ensures that no student gets 'lost in the shuffle" and finds that the course has moved on to the fourth step of the Navy Planning Process while he or she has still not completely grasped the first. These focused, personalized instructor interventions substitute instructor effort for class time, ensuring each student receives the support necessary to master the skills and knowledge bundles associated with each phase of the course.

Multidimensional Assessment

In order to support competency development, the second HVL design principle, multidimensional assessment (of students, faculty performance and the course design itself) persistently informs I-MSOC. Observation of student action, discussion, and evaluation of formal brief delivery by the faculty occurs continuously (not only upon course conclusion) in order to assess the degree of student mastery. For example, briefs are delivered both informally within operational planning teams and formally to the entire class, providing students multiple opportunities to demonstrate their command of the briefing competency bundle, and instructors with insight on where additional guidance is necessary.

The timeliness of the continuous assessment enabling the provision of rapid support tailored to the student's individual learning needs constitutes a major advantage of the competency based approach over the time based instruction model. While in traditional instruction the student receives periodic feedback in the form of tests, such as a midterm and final, the feedback provided is often too late and insufficiently granular for the student to act on effectively. A poor grade on a midterm or final provides only an indication of a learning deficiency. It does not reveal to the student the root cause of the deficiency – poor study habits, a misunderstanding of a fundamental point, or sloppiness. Just as on the ship a Sailor is not sent before a qualification board without completing their personal qualification standard and a preliminary board administered by their mentors, in I-MSOC the student who performs poorly in a brief to the Operational Planning Team is assisted in improving his or her briefing skills before providing the decision brief to the Commander in front of the entire class. Thus the continuous assessment within the competency based approach provides meaningful feedback and gives the student the opportunity to reengage with the task until mastery is achieved.

In addition, faculty performance and the structure of the course itself are assessment targets. A student's inability to demonstrate increasing mastery of a competency provides signals concerning not only student, but more importantly, faculty performance. Student failure to achieve mastery generates a requirement for the faculty to adjust their teaching style in order to more effectively transmit the content in ways that facilitate student incorporation of the material. The competency-based approach, unlike schedule dependent testing (such as midterm or final exams) provides valuable feedback to the instructor side of the learning equation in time for the feedback to inform the instructional process and thus benefit students.

Metacognition

The third HVL engine is the surfacing of metacognition, or thinking about thinking, within the learning experience. According to Paul R. Pintrich in "Metacognitive Knowledge in Learning," metacognitive knowledge can be divided into three main types. He explains, "strategic knowledge refers to knowledge of strategies for learning and thinking. Knowledge of tasks and their contexts represents knowledge about different types of cognitive tasks as well as classroom and cultural norms. Finally, self-knowledge is a critically important component of metacognitive knowledge." The metacognitive activities in I-MSOC include discussion of mental models especially pertinent to the competency focus area, such as the steps of the Navy Planning Process and tips on how students can examine their own learning styles. This metacognitive awareness enables students to learn more efficiently and effectively, and thus increase their overall learning velocity.

Conclusion

Through application of the three HVL engines, I-MSOC generates a high speed, low drag, exciting learning experience for the global maritime community. For more information about the course (MASL P179622), please visit https://www.usnwc.edu/Departments---Colleges/International-Programs.aspx or write to I-MSOC@USNWC.edu. ☸

Pintrich, Paul R. (2002). The Role of Metacognitive Knowledge in Learning, Teaching and Assessing Theory Into Practice (Vol. 41): Taylor & Francis, Ltd.

Weise, Michelle R., & Christensen, Clayton M. (2014). Hire Education: Mastery, Modularization, and the Workforce Revolution Retrieved from http://www.christenseninstitute.org/wp-content/uploads/2014/07/Hire-Education.pdf

Michael Hallett is Subject Matter Expert with Netsimco at the U.S. Naval War College, International Programs. For further information contact michael.hallett.ctr@usnwc.edu.

IMPACTS OF CLIMATE CHANGE TO THE MILITARY

Ray Toll
Old Dominion University
Gregg Nakano
University of Hawai'i Manoa

Source: U.S. Air Force

U.S. has increased research of the climate change impacts on national security.

September 2015, the entire world was shocked as pictures Alan Kurdi, a 3-year old Syrian refugee who drowned fleeing the civil war, were splashed across news outlets.[1] The picture not only highlighted the risks migrants take in putting their lives in the hands of smugglers who promise to get them across the water; but also the collective failure of Western governments to help those fleeing the poverty and warfare destroying countries in Africa and the Middle East.[2] This situation is nothing new for Europe.

In the aftermath of World War I, humanitarians like Fridtjof Nansen led the League of Nations' efforts to resettle people displaced by the fighting and ongoing famine in Russia. Bringing together the former combatants, Nansen developed new processes for resettling nearly 500,000 refugees to 30 different countries. Although Nansen's International Office of Refugees was disbanded with the outbreak of World War II, it was revitalized in 1950 as the United Nations High Commissioner for Refugees (UNHCR). Unfortunately, mass migrations triggered by warfare, famine, or political instability still challenge national coping capacities and are forecast to worsen in the future.

In 2009, the International Organization of Migration (IOM), the principal intergovernmental organization for migration, published "Migration, Environment and Climate Change: Assessing the Evidence," their seminal work on the subject. In it, they note that climate change impacts on the environment and governments could increase the number of migrants from between 25 million and 1 billion people by 2050.[3] Even managing only 200 million additional migrants, the most quoted estimate, will creates enormous challenges for the policy makers of tomorrow.[4] Luckily for the European nations, there is NATO to provide assistance and support.

"NATO's essential purpose is to safeguard the security and freedom of its members using both political and military means."

NATO's essential purpose is to safeguard the security and freedom of its members using both political and military means.[5] Politically, this means promoting democratic values and encouraging cooperation in security issues to build trust and prevent wars. When diplomatic efforts fail, NATO's role is to use its military capacity to undertake crisis-

management operations. Growing NATO expertise in disaster-relief operations and missions to protect populations against natural, technological, and humanitarian disasters positions the organizations to play a key security role as the climate change induced migrations increase.[6] And perhaps unbeknownst to many outsider observers, the United States military is working to rapidly develop their understanding of the impacts of climate change on national security.

In 2007, the Center for Naval Analyses (CNA) published their first study on "National Security and the Threat of Climate Change."[7] Putting together a Military Advisory Board of 11 three- and four-star admirals and generals, CNA asked the assembled leadership to explore the national security implications of the emerging climate science data. The conclusions of the report were that not only were the projected climate changes a serious threat to America's national security because of their ability to act as a threat multiplier for instability for unstable regions of the world, but they would also increase tensions in otherwise stable governments as well. The former senior military leaders recommended that the United States military take a leadership role in stabilizing climate change, build global partnerships to help less developed nations weather the impacts of climate change, and assess the impact of climate changes on U.S. military installations over the next 30 to 40 years.

Since that time, the United States military has increased research of the climate change impacts on national security starting with the 2010 Defense Science Board Task Force on Climate Change. Guidance for how to integrate climate change adaptation into military planning and operations quickly followed with the 2012 and 2014 Climate Change Adaptation Roadmaps (CCAR)[8] and 2016 DoD Directive 4715.21, Climate Change Adaptation and Resilience.[9] [10] These efforts were complemented by significant military investments in renewable energy to reduce the dependence on fossil fuels.

In 2014, the Government Accounting Office (GAO) published the GAO Report 14-446 highlighting the need for the Department of Defense to begin developing a deliberate plan for assessing future climate change impacts on the 555,000 U.S. military installations around the world.[11] Noting that the 28 million acres (113,000 km^2) included many coastal installations and training ranges that would be affected by sea level rise and droughts, the GAO report recommended developing a specific plan and milestones prioritizing the more than 700 coastal installations around the world.

It is clearly understood that in order for us to understand and estimate climate change and sea level rise, we must first understand the engine that drives these changes. A almost 15 years ago, the U.S. Oceans Commission recognized this fact and challenged the academic, government, and private sectors to work together to achieve integration across all observation platforms.

In 2013, President Obama, in his Climate Change Executive Order, challenged our nation to look at regional priorities and potential solutions by establishing pilot programs throughout the country. One such program was created in June 2014 and was introduced in the ON&T August 2014 Editorial. Scoped at two years, this program was organized and convened by Old Dominion University (ODU) to study an integrated whole of government/community approach to building coastal resiliency in the region called Hampton Roads. Named for an old British term meaning safe anchorage, this region includes 7 major municipalities, 17 jurisdictions, and a huge Federal presence that includes the largest Navy base in the world. In fact, approximately one of every two jobs in Hampton Roads is a Federal one. Coincidentally, it also has one of the largest natural harbors in the world.

Over the past two years, this integrated regional approach has looked at building coastal resiliency through mitigation and strategic adaption processes in a unity of effort involving over 400 volunteers from all echelons of government, citizen groups, private sector, and focused research from both ODU and The College of William and Mary. The focus has been on both national security and economic impacts to our maritime industry. Interdependencies were studied from legal, infrastructure (private and public), public health, citizen engagement, economic impacts, and science perspectives. Ultimately, this approach is intended to lead to a realignment of federal and non-

federal programs that could exemplify a whole of government/community methodology that other regions could use. Certainly, this approach would lead to a more efficient use of tax dollars to address a challenge all societies must address at some point.

In Hampton Roads, the research community lead by ODU research has identified three key reasons why sea level rise and recurrent flooding is threatening local communities:

- Global warming causing ice melt and an increase in storm severity and frequency
- Slowing of the Gulf Stream
- Land Subsidence

Thus, one clear priority for this two-year effort going forward is the need to build a regional network to properly monitor both sea level rise and the regional challenge of land subsidence caused by years of drawing from below-ground water tables. This network is needed to identify the changes occurring within the region and offshore so that the various interdependencies in both the water cycle and ocean-based phenomenology can be properly measured and studied to improve our ability to model and predict future changes.

To understand and predict future sea level rise, we must observe the oceans better by enhancing the existing ocean observing systems and making the research efforts operational. Clearly, this must be accomplished on a global scale. The Marine Technology Society (MTS), an international organization, provides a forum through which the latest technology and its relevance in this arena is disseminated worldwide. Ocean observing systems, like research vessels and far-ranging sea gliders, represent operational assets with scope and reach that frequently transcend international borders. Cooperation among neighboring maritime nations is essential to the success of operational oceanography on this scale. MTS works closely with the United Nations Intergovernmental Oceanographic Commission (IOC) to assure its stakeholders from government, academia, and private sector industry are afforded the opportunity to be engaged in this global activity.

Both the regional and global challenges are among those addressed in this edition. Clearly integrated ocean observing must remain a priority to address societal needs today and into our future. The health and welfare of our future generations are depending on it. ☸

1. A. Barnard and K. Shoumali, "Image of Drowned Syrian, Aylan Kurdi, 3, Brings Migrant Crisis Into Focus," *N.Y. Times*, http://www.nytimes.com/2015/09/04/world/europe/syria-boy-drowning.html.

2. "Migrant crisis: Migration to Europe explained in seven charts," *BBC News*, http://www.bbc.com/news/world-europe-34131911 .

3. "Migration, Environment and Climate Change: Assessing the Evidence," International Organization for Migration (IOM), http://publications.iom.int/system/files/pdf/migration_and_environment.pdf.

4. Syria Regional Refugee Response Inter-agency Information Sharing Portal, UNHCR, http://data.unhcr.org/syrianrefugees/regional.php.

5. NATO, http://www.nato.int/nato-welcome/index.html#basic .

6. "Operations and Missions: Past and Present," NATO, http://www.nato.int/cps/en/natolive/topics_52060.htm.

7. "National Security and Assured U.S. Electrical Power," CNA, https://www.cna.org/mab/reports.

8. "DoD 2014 Climate Change Adaptation Roadmap," U.S. DoD, http://www.acq.osd.mil/eie/Downloads/CCARprint_wForward_e.pdf.

9. "DoD Releases Climate Change Adaptation Roadmap in Support of Sustainability Planning," SERDP-ESTCP, https://www.serdp-estcp.org/News-and-Events/News-Announcements/Program-News/DoD-releases-Climate-Change-Adaptation-Roadmap-in-support-of-sustainability-planning.

10. "DoD Directive 4715.21 Climate Change Adaptation and Resilience," U.S. Department of Defense, http://www.defense.gov/Portals/1/Documents/pubs/471521p.pdf.

11. Brian J. Lepore , "Climate Change Adaptation: DOD Can Improve Infrastructure Planning and Processes to Better Account for Potential Impacts," U.S. GAO, http://www.gao.gov/products/GAO-14-446.

Ray F. Toll is the Director of Coastal Resilience Research at Old Dominion University and President of the Marine Technology Society, and Gregg Nakano is a student at the University of Hawai'i Manoa. For further information contact rtoll@odu.edu.

CJOS COE ANNUAL REPORT

CAPT Dermot Mulholland, CAN-N
CAPT Massimiliano Nannini, ITA-N
CJOS COE

Source: NATO

NATO Submarine Exercise DYNAMIC MANTA .

CJOS activities are guided by a programme of work approved by the sponsoring nations based upon the requests received by NATO, the 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 programme of work based upon their alignment to CJOS interests and those of the sponsoring nations and NATO. The 2016-2017 CJOS Programme of Work is summarized below:

Meteorological and Oceanographic (METOC) Support to NATO Operations

CJOS COE assisting NATO ACT in ensuring specialist fields receive best support in accordance with international METOC principles. Review exercises and operations to develop new METOC products. In addition, CJOS COE will review doctrine to ensure compliance and coherence across all domains.

Maritime C2 Programme (NATO TRITON Project)

Project TRITON, NATO's Future Maritime Information Services, is due to replace NATO's current maritime C2 capabilities. CJOS COE will be conducting an operational analysis for the use of TRITON as the main Maritime C2 capability. The analysis will provide a Concept of Operations (CONOPS) document which will provide NATO Allied Command Transformation (ACT), Supreme Headquarters Allied Powers Europe (SHAPE) and Allied Maritime Command (MARCOM) a review of TRITON's operational capabilities and the effectiveness of its new C2 architecture for static and afloat commands.

Multinational Capability Development Campaign (MCDC)

The Multinational Capability Development Campaign (MCDC) series is the follow-on to the Multinational Experiment (MNE) series initiated by United States Joint Forces Command in 2001. The first cycle started in 2013 and was designed to develop and introduce new capabilities to enhance the coalition force's operational effectiveness in joint, interagency, multinational, and coalition operations. While it maintains the foundational blocks that made the MNE series successful, MCDC incorporates significant changes in scope, mission, and governance that improve responsiveness, agility, and relevance.

CJOS COE participates as key contributor and observer in three focus areas: Countering Hybrid Warfare, Countering Unmanned Autonomous Systems, and Joint and Combined Operations in and from Confined Waters. The MCDC 2015-2016 cycle topic is "Building and Maintaining Regional Security"; multinational and coalition partners having the ability to successfully plan and execute globally integrated efforts to build and maintain regional security. These partners must employ a comprehensive approach in areas where they have mutually direct and indirect national interests to prevent, deter, mitigate or respond to destabilizing events and activities.

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 presented CUSFFC with nine interoperability gaps focused on MOC coalition operations, doctrinal differences, and increased coalition training in the FRTP. The ITAG will now develop PoA&M to track the progress of recommended solutions to ensure the desired end-state is achieved.

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 mis0sion 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

CJOS will deliver a NATO Conceptual Study on Urbanization to the NATO Military Authorities in accordance with IMSM-0543-2014 dated 28 November 2014. The concept examines the impact of NATO military operations based on the potential crises and consequences of urbanization between now and 2035. This study will be linked to the NATO Defense Planning Process, Strategic Foresight Analysis, and Framework for Future Alliance Operations (FFAO) where urbanization is one of the key topic areas. In September 2016, CJOS will provide subject matter experts to support the Urbanization Experiment that will be conducted at the Modeling and Simulation (M&S) COE, Italy.

E-3A 'Sentry' Airborne Warning & Control Systems (AWACS) Follow-on

NATO operates a fleet of Boeing E-3A 'Sentry' Airborne Warning & Control System (AWACS) aircraft, which provides the Alliance with near real-time airborne command and control (C2), air and maritime surveillance and battle-space management capability. CJOS will provide input and advice to the NMA in accordance with IMSW-0028-2015 dated 30 January 2015 on the future requirements for any follow-on to the E -3A AWACS capabilities; more generically an Air Command and Control/Battle Management and Surveillance Capability for the 2035+ timeframe. Several products are expected and the COEs are expected to contribute studies on viable conceptual solutions.

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 will provide assistance to JALLC in conducting analysis reviews in support of their Programme of Work.

NATO Integrated Air and Missile Defense C2 Architecture

The Allied Joint Publication (AJP-3.3.1) inadequately describes the coordination and synchronization required between Joint Force Air Component (JFAC)/Air Defense Component (ADC) and surface forces that are responsible for fires within a designated Area of Operation (AOO); maintaining control of air and missile defense forces (i.e. surface forces retaining Operational Control (OPCON) and Tactical Control (TACON), and with naval Ballistic Missile Defense (BMD) forces, AEGIS ashore). Similarly, AJP-3.3.1 briefly describes the establishment of air defense regions and sectors to enhance decentralized control.

Support to Capability Requirement Review 2016 Planning Process

CJOS will provide Subject Matter Experts (SMEs) for the planning phases of the Capability Requirement Review (CRR16). This effort will contribute in identifying NATO/Allies capabilities, and discovering shortfalls preventing the fulfillment of NATO Level of Ambition (LoA).

COE Strategic Foresight Analysis

COEs will be requested to support development of the Strategic Foresight Analysis (SFA) 2017 report. The SFA writing process is expected to start in the second half of 2016. Final product will be developed in 2017 and will be available to the public. COEs will be asked to provide research papers in their respective areas related with the existing SFA and emerging trends. The centres will be invited to attend two to three SFA workshops and provide comments on draft documents.

Framework for Future Alliance Operations (FFAO)

The FFAO builds upon and interprets the outcomes of the Strategic Foresight Analysis (SFA) that was completed and published by Allied Command Transformation (ACT) in late 2013. Where the SFA identified key trends and drivers that could influence the future security environment, the FFAO extracts the military implications of those inputs and facilities a forecast of how those implications may need to be addressed by NATO forces in the future. This effort will continue to inform the NATO Defence Planning Process, allowing long-lead capabilities to be identified, and potentially, scheduled for acquisition. CJOS has contributed to both the SFA and FFAO development by providing subject matter expertise, advice and drafting/editing services.

TRIDENT Exercise Series

Exercises TRIDENT JUNCTURE (TRJE), TRIDENT JAVELIN (TRJN), and TRIDENT JAGUAR (TRJR) are operational level headquarters training exercises designed to practice coordination between NATO Command Structure (NCS) and NATO Force Structure (NFS) that will be conducted as part of the evaluation and certification process for Allied Joint Force Command – Naples (JFC-Naples). CJOS COE will provide a subject matter expert to support the maritime element of the exercise.

Maritime Intelligence, Surveillance, and Reconnaissance (ISR) Improvement

The Joint Intelligence, Surveillance, and Reconnaissance (JISR) branch of Allied Command Transformation (ACT) has been focused on Maritime ISR processes and capabilities to support NATO maritime future operations. Much of the observation and analysis has been on the International Security Assistance Force (ISAF). Over the recent past, maritime operations have received less attention and the lessons learned may not be incorporated into the ISR processes and capabilities to support maritime operations. As a Programme of Work item requested form ACT, CJOS COE is reviewing operational reporting, lessons learned and after action reports from NATO Operations such as Operation Unified Protector (OUP) and Operation Active Endeavor (OAE) in order to determine maritime ISR shortfalls. CJOS COE work in this area has led to the development of a MISR publication currently in the drafting process.

Counter-Improvised Explosive Device in Maritime Environment

CJOS is providing support investigating Improvised Explosive Device (IED) threats and countermeasures in the maritime domain. For CJOS, 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)

The outcome of the Maritime Security Regimes Round Table 2016 event was a series of findings and recommendations (F&R), based on an analysis of key points and recurring themes. F&R are included in the final product for all participants: the Report of Proceedings. F&R are the starting point to CJOS moving forward to identify the key stakeholders, develop an engagement matrix and identify what information exchange requirements and protocols should be established for the purpose of building MSA. CJOS COE examines problems in the maritime domain and suggest solutions.

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.

Joint Battlespace Management

Develop Joint Battle Space Management procedure which will adapt to joint procedures in order to ensure adaptive means and measures that enable the dynamic synchronization of activities in the coastal environment

During several exercises it has turned out to be a challenge to ensure 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. There are existing systems used within major land operations, primarily synchronizing campaigns with land and air forces. However, in the maritime domain, and in a coastal and littoral environment it seems to be a lack of a well-functioning Battlespace Management tool as well as a common understanding of the importance of both inter and intra component coordination and synchronization. Battlespace Management in the maritime domain is often understood as water space management, but this is dealing with just one part of the battlespace volume.

Maritime Cyber Security

While Cyber Security has been recognized as an important concern all over the world, Cyber Security in the maritime domain has become a growing topic and being discussed by more and more organizations. The possibility of a cyber-attack being directed towards a maritime operation is very likely, and the impact of that attack could be catastrophic. Hence, cyber risks within the maritime domain need to be analyzed and evaluated to create a cultural awareness, to reexamine the priorities and method for safeguarding maritime critical infrastructure and improve the cyber resilience within the Maritime Domain. Due to its potential consequences, continued cooperation and collaboration among different stakeholders, military and academia are a necessity to tackle those risks. CJOS is working in cooperation with various stakeholders, military, and academia to identify measures that will significantly increase the resilience of 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)

The Amphibious Operations Working Group addresses standardization objective areas within their four Panels: Operations, Publications, Communications, and Information Exchange Requirements Panel. Together,

their 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. Staffs from NATO nations and organizations deliver proposals for military standardization, including tactics, tactical instructions and procedures for employment of Amphibious Forces In response to NATO strategy, the group is also focusing on Non-Article V Operations. As an independent, multinational source of innovative advice and expertise on all aspects of maritime operations, CJOS COE is responsible with developing and promoting maritime concepts and doctrine is a natural and active element of the AWG.

Maritime UAS Operational Concept

CJOS COE provides subject matter expertise to ACT's Capabilities Development Branch in the drafting of an operational concept that will address specific maritime UAS countermeasures. CJOS COE will also participate in the subsequent testing, experimentation, and modeling required to validate this concept. Additionally CJOS COE is working with MARCOM to develop Joint ISR doctrine to address the integration of UAS into NATO's battlespace management.

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.

Exercise BOLD ALLIGATOR 2017

CJOS COE is providing subject matter expertise and coordinates with US Fleet Forces Command on behalf of NATO for the inclusion of Allied navies in BOLD ALLIGATOR 2017. This exercise will be the largest live amphibious exercise in history with ships, aircraft and personnel from across the Alliance. Commander, Striking and Support Forces NATO will act as the Maritime Component Commander for the exercise and has employed CJOS COE as their Executive Agent to liaison with the US Navy in preparation for the exercise. As such CJOS COE staff members have been involved in the scripting of the exercise and will serve as observers and analysts for the exercise itself.

Future Aspects of Sea Control

Anti-Access Area Denial (A2/AD) tactics challenge NATO's ability to conduct maritime operations throughout its AOR. CJOS COE in conjunction with the US Navy is working to develop new tactics to defeat maritime A2/AD threats across the spectrum of warfare. This entails the development of experimental tactics that cover joint integration of land/sea air power, employment of unmanned systems, and information operations in addition to the traditional aspects of war at sea such as ASW and SUW. CJOS COE is producing a 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

In 2011 CJOS COE produced an interoperability handbook designed to facilitate operations between Allied navies. In the intervening years the dynamic changes in technology and the nature of warfare itself have made much of the original handbook obsolete. Through its existing work on interoperability CJOS COE is in the process of updating the interoperability handbook in concert with US Fleet Forces command as it updates the

Source: U.S. Navy

Republic of Korea Navy Captain waves to the Republic of Korea Navy destroyer Seoae Ryu Seong-Ryong (DDG 993) as it arrives at Joint Base Pearl Harbor-Hickam to participate in the Rim of the Pacific 2014 exercise. Twenty-three nations, including NATO ally and partner nations, participated in the month-long exercise.

OPORD 2000. One outcome of the Interoperability Technical Advisory Group is that many parts of the new OPORD 2000 will be published as releasable to NATO. These portions of the OPORD along with the update Interoperability Handbook will be designed for tactical level watchstanders on ships and in various Maritime Operations Centers to standardize procedures and make it easier for Allied navies to operate together across the spectrum of warfare.

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 Organisation 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. ☸

CAPT Massimiliano Nannini 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 24 NATO accredited COEs:

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

CJOS COE REQUEST FOR SUPPORT
(Continued from page 5, "*How We Are Tasked*")

Originator:

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

Point of Contact/Subject Mater 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 Richard Breckenridge, USA-N	Director	2997
CDRE Phillip Titterton, GBR-N	Deputy Director	2452
CDR David Hazlehurst, USA-N	Fiscal Officer	2457
LT Clarissa Butler, USA-N	Flag Aide	2452
CDR Jeffrey Betz, 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
CAPT Marv Carlin, USA-N	SPA SO	2462
CDR Geir Arne Hestvik, NOR-N	SPA SO	2440
CDR Aytac Yavuz, TUR-N	SPA SO	2466
CDR Ricardo Valdes, ESP-N	SPA SO	2442
CDR Michael DeWalt, USA-N	Strategic Communications and Outreach Section Head	2461
CDR Jonathan Sims, USA-N	SCNO SO	2463
CDR Ovidiu Portase, ROU-N	SCNO SO	2451
ITCS Stephen Wheeler, USA-N	SCNO SO	2467
TRANSFORMATION OPERATIONS BRANCH		
CAPT Massimiliano Nannini, ITA-N	Transformation Operations Branch Head	2449
CDR Gwenegan Le Bourhis, FRA-N	Expeditionary Operations Section Head	2446
CDR Luis Constante, PRT-M	EO SO	2444
CDR William Hawthorne, USA-N	EO SO	2429
CDR Pavlos Angelopoulos, GRC-N	Maritime Operations Section Head	2448
CDR Russell Czack, USA-N	MO SO	2454
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