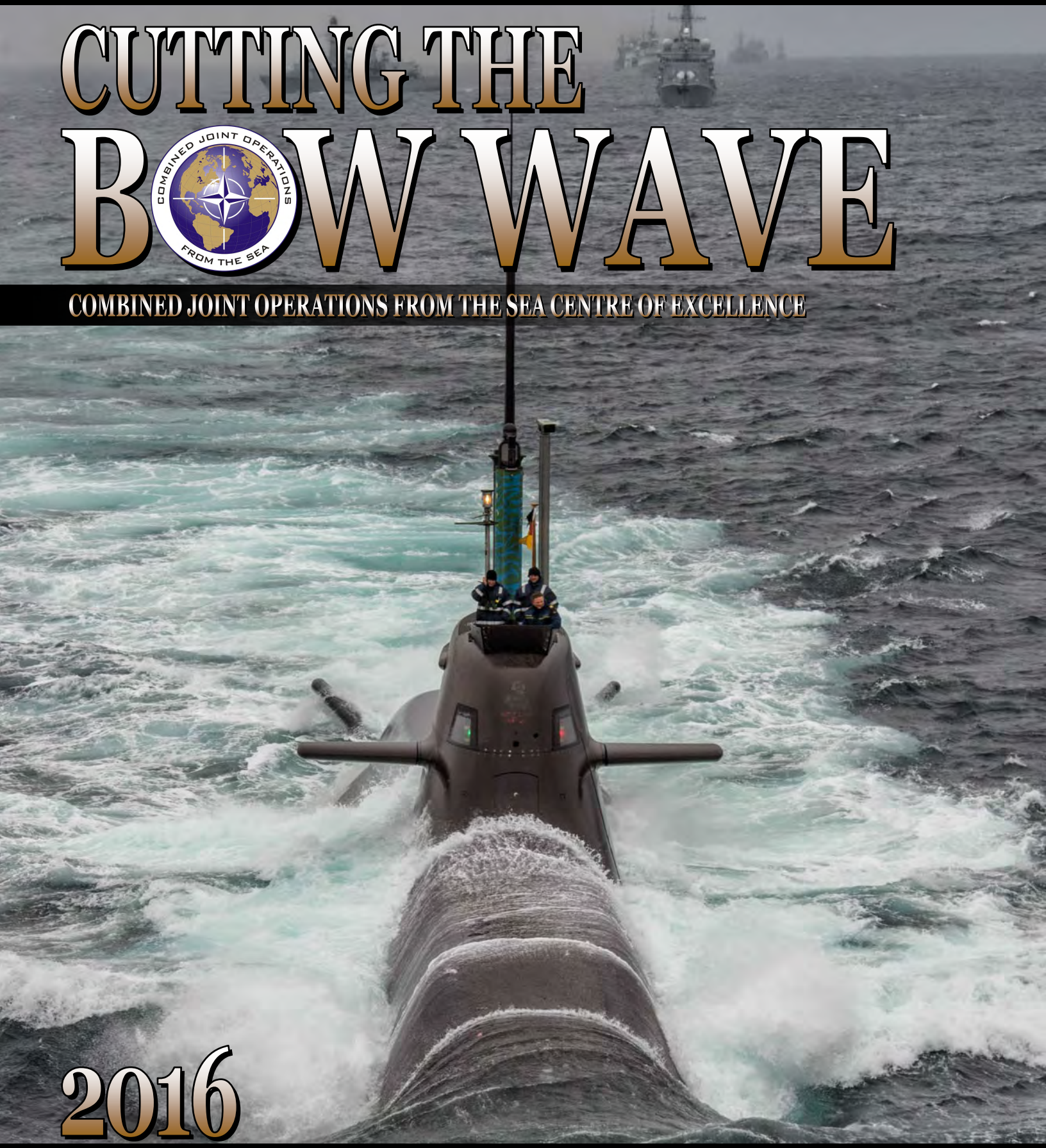
CUTTING THE BOW WAVE

COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE



2016

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: German submarine U33 (S183) and supporting units participating in Exercise DYNAMIC MONGOOSE 2015. 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

Assistant Managing Editor:
CDR Jonathan W. Sims, USA-N

USFF.CJOS.COE@NAVY.MIL

TABLE OF CONTENTS

NATO

United Kingdom HMS Ambush (S120) participating in NATO exercise JOINT WARRIOR 2015.

MESSAGE FROM THE DIRECTOR

Vice Admiral Richard P. Breckenridge, USN
Director, Combined Joint Operations from the Sea
Centre of Excellence (CJOS COE)
Norfolk, VA, USA

In September 2015, I took the helm as Director, CJOS COE from Vice Admiral Nora W. Tyson. I am honored to have the opportunity to lead such an outstanding organization as it strives to improve coalition operations in the maritime domain. I am extremely impressed by the products CJOS COE provides to our sponsoring nations, NATO entities and other valued customers. The COE's success is dependent upon our ability to leverage the vast array of subject matter experts within our staff. Each member's unique skills, from their respective country and service, has enabled CJOS to develop comprehensive solutions to complex problems and deliver a robust Program of Work.

Our ability to cultivate the integration of intellectual energy has allowed us to successfully spark innovation in joint maritime expeditionary operations, interoperability, naval doctrine and maritime security. One of our major achievements over the past year has been the work accomplished by the Interoperability Technical Advisory Group (ITAG). This CJOS-led initiative has pulled together stakeholders from across the coalition to identify technical, doctrinal and operational barriers to interoperability challenges in the maritime domain. These barriers are now being addressed across NATO and our partner nations, making CJOS COE a critical enabler of improved coalition operations.

I am very proud of the CJOS COE team and our accomplishments in 2015. I look forward to our continued success in 2016, advancing our efforts on transformation through sharing of best practices, strengthening existing partnerships and expanding our relationships. Furthermore, I expect CJOS COE to continue to play a key leadership role in developing solution-oriented ideas that will further improve global maritime security. ☸

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.

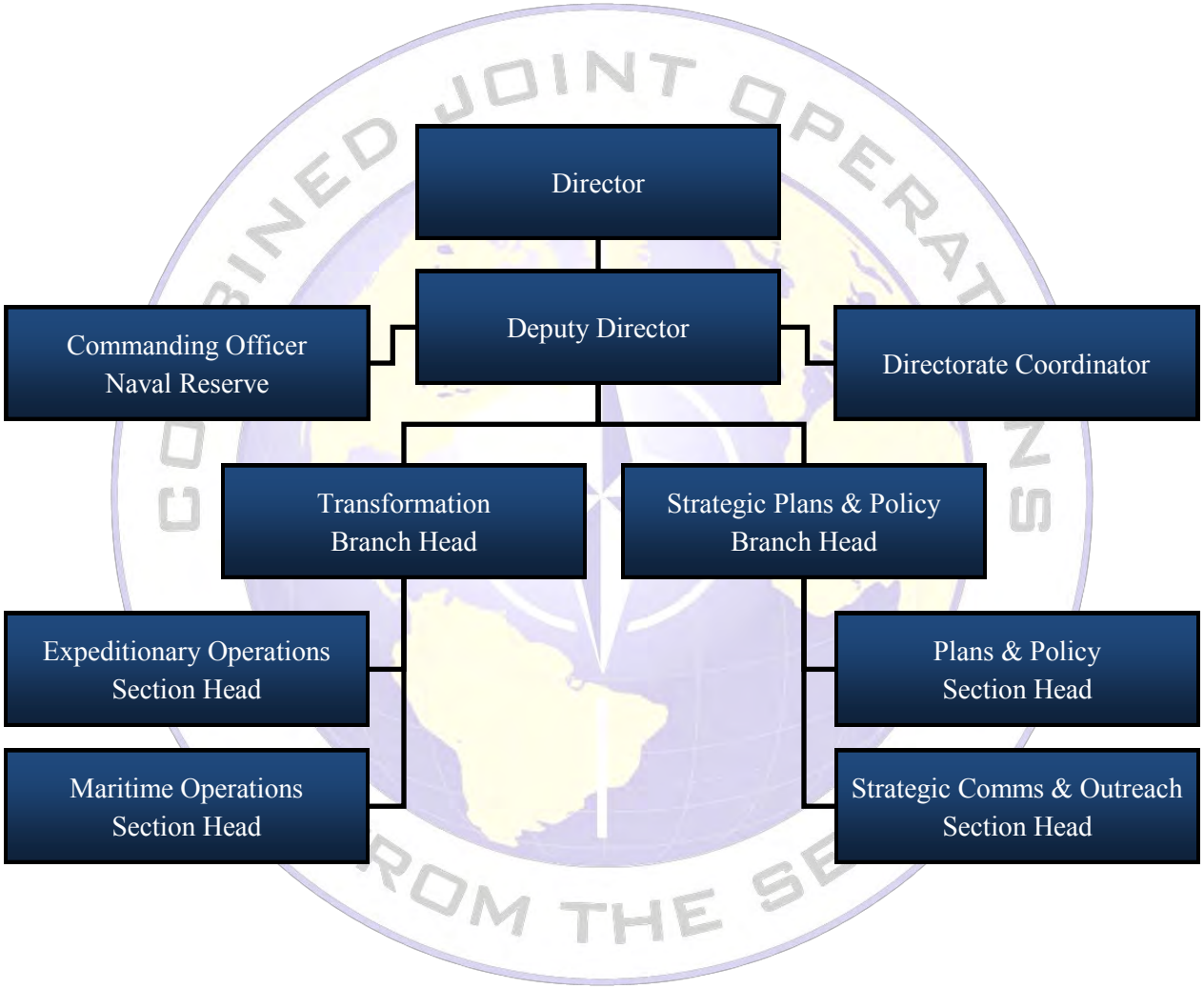
★ ★ ★

CJOS COE

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 20 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.



MESSAGE FROM THE DEPUTY DIRECTOR

Commodore Phillip J. Titterton, OBE, GBR-N
Deputy Director, Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

In this year's Bow Wave I hope you will observe a significant expansion of our contribution to the maritime domain and I look forward to our publication continuing to evolve to keep pace with interest from our coalition partners and stakeholders. Consequently, as I complete my first year as the Deputy Director, I would like to take an opportunity to reflect on everything CJOS has accomplished and offer a headmark to the future for our next challenges.

This year started with four CJOS personnel travelling to the MAROPS Working Group (WG) in Bergen, January 2015. The MAROPS WG is, I believe, our most important contribution to the output of NATO HQ. Extensive staff participation including our Transformation Branch Head, Captain Nannini, as Chairman of the Working Group and 3 staff officers as presenters allowed for excellent opportunities to contact relevant doctrine developers from NATO nations and MARCOM. CJOS demonstrated that we are a valuable asset to our member nations and to NATO to develop concepts and doctrine, be it nationally or as a custodian for NATO publication. We look forward to our continued participation in the future and the potential for future requests for support.

One of the projects presented at the MAROPS WG by CJOS was the Maritime Situational Awareness (MSA) project. CJOS COE and COE Confined and Shallow Waters (CSW) teamed together to improve information exchange among nations for a more secure maritime environment published in April 2015. To further enhance the effectiveness of Alliance maritime capabilities, including greater coordination between relevant international organizations, CJOS COE organised and facilitated an inaugural Roundtable meeting amongst Maritime Security Stakeholders held in Madrid, Spain. The Roundtable was successful in allowing stakeholders of various levels and ranks to speak frankly and directly about creating relationships between their organisations to improve MSA. We concluded the workshop with a discussion on next year's intentions and we are looking forward to hosting the second annual roundtable in Norfolk, VA in the Spring 2016.

Recently, CJOS COE completed the initial phase to develop interoperability between the US Navy and its Allies. The work was requested by Commander, U.S. Fleet Forces Command in March 2014. We found that Maritime warfighting effectiveness when the U.S. Navy is fighting in coalition is challenged by matters of U.S. policy, doctrine, geographic isolation, and mass. During more than a year of development by the Interoperability Technical Advisory Group (ITAG), Focus Area Teams conducted a gap and root cause analysis of the current state followed with concrete recommendations to improve doctrinal, training, and operational differences. After a successful meeting with Admiral Philip Davidson, Commander, U.S. Fleet Forces Command, he approved our recommended solution of adding 10 NATO Secret Wide Area Network (NSWAN) clients to the USFFC Maritime Operations Center (MOC) and to update the Lessons Learned instruction to improve sharing and emphasize a collaborative approach to resolving interoperability issues. More importantly, he further approved a recommendation to update the NATO Data Transfer System which is available to all U.S. Navy warships and

shore headquarters. Once this is achieved there will be a significant increase in classified interoperability between the U.S. Navy and the remainder of NATO. We were also directed to continue the ITAG's efforts by COM, and we are developing the implementation plan for the approved solutions.

Looking forward next year we plan to continue to push interoperability hard; particularly as the next live Exercise Bold Alligator approaches and the team will be heavily involved delivering the coalition aspects of this significant high-end US expeditionary exercise in 2017. We are also co-hosting two important conferences. Firstly, we will support C2 COE with a Maritime C2 conference here in Norfolk and this will be followed by a significant Maritime Expeditionary warfare conference with Strike Force NATO in July. Around all of this we will continue our commitment to the MAROPS WG, Urbanisation, MSA and many other NATO projects.

For me, CJOS COE has excelled beyond words in this past year. I could not have asked for a better team and the leadership from VADM Tyson as the Director was second to none. I now look forward to working with our new Director, VADM Richard Breckenridge who has recently assumed the position of Deputy Commander USFFC and Director CJOS. ☸

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 66). 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!

CJOS COE VISION

Working closely with partners and stakeholders from the international military, government and non-government agency, industry, and academic communities of interest, the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) will seek to optimize the efficient delivery of Maritime Effect.

CJOS COE MISSION

CJOS COE 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 effectively counter current and emerging global maritime security challenges.

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.

Regional Maritime Security Meeting 2016

26-27 April 2016
Norfolk, VA

CJOS COE is actively engaged in determining the ways and means to improve global Maritime Situational Awareness (MSA). To help cultivate this effort, CJOS COE is hosting an event that invites all key maritime security stakeholders. The purpose of this gathering is to determine the next steps in improving global MSA by fostering dialogue, sharing best practices, developing methodologies, and cultivating fruitful partnerships that will ultimately improve global MSA. The outcome of this monumental event will be briefed at COE CSW's Kiel Conference in June 2016. Together both events will further enhance international maritime security.

Visit www.CJOSCOE.org to reserve your seat !

CDR Ricardo Valdes, ESP-N
Email: usff.cjos.coe@navy.mil
Tel: +1 (757) 836-2442

IMPROVING MARITIME INTELLIGENCE SURVEILLANCE & RECONNAISSANCE

CDR Dimitrios Lymperakis, GRC-N
CJOS COE

U.S. Department of Defense

An operation center utilizing dynamic ISR resources.

Intelligence, Surveillance and Reconnaissance (ISR) functions are critical key elements that support a nation's defense capabilities, and consist of a diverse assortment of systems that acquire and process information for military commanders and national security decision-makers. The resources that feed or support ISR systems can range from human assists to orbiting satellites. However, the capabilities of ISR are limited to the effectiveness and efficiency of its synchronized and integrated collection systems that provide analytical products directly supporting the planning, preparation, and execution phase of an operation.

All kinds of platforms (land, sea, air and space assets) have important ISR roles in supporting operations. By massing ISR assets, all can contribute to Maritime intelligence and generation of the Recognized Maritime Picture (RMP). With the right combination and quantity of assets, an Operational Commander can be provided a clear and in-depth level of knowledge in support of current and future military operations. Hence, the Operational Commander will have the ability to plan effectively and respond intelligently to diverse and complex situations.

ISR is vital for all naval operations; it provides information and intelligence to decision-makers and action-takers, enabling them to make timely and accurate decisions. While surveillance and reconnaissance can answer the questions "what," "when" and "where", the combined elements from various intelligence sources and disciplines provide the answers to "how" and "why". By successfully merging these elements, ISR can be sustained over an extended area.

A variety of nations have a significant number of ISR capabilities. By applying these to NATO, the Alliance can establish a permanent ISR system that collectively provides information and intelligence to key decision-makers, helping them make well-informed, timely, and accurate decisions. ISR gathers data and information through projects such as NATO's Alliance Ground Surveillance (AGS) system or NATO AWACS aircraft, as well as a wide variety of national ISR assets from the land, air, maritime, and space domains. Both surveillance and reconnaissance includes visual and electronic observation (i.e. ground and maritime sensors, satellites, unmanned aircraft systems, etc.). Well trained personnel along with effective software tools can process and analyze the data, turning information into intelligence supporting different end-users.

In the Maritime domain, Maritime air – surface – subsurface units have ISR capabilities that can contribute to maritime intelligence and generation of the RMP and by extension, to a joint or coalition ISR picture. In the case of a multinational maritime force, the exponential expansion of ISR sensors has produced unprecedented volumes of ISR data which is straining Navy sea vessels' processing, storage, and dissemination infrastructure. Unlike rich shore-based infrastructures that can have a large physical footprint, most maritime vessels are hindered with a finite amount of floor space dedicate to ISR systems. This has resulted in an ongoing overhaul of Navy ISR systems, using cloud infrastructures and other technologies to consolidate systems, reduce replication of data and ease the burden on communication systems. The key to a commander's understanding of his battlespace is the back end of the tasking, collection, processing, exploitation, and dissemination process. The networks, automated processing, and people must be in place to turn vast amounts of raw data into information and knowledge. As the volume of data collected increases, it will continue to stress Navy networks and the 'task, collect, process, exploit, disseminate' infrastructure.

"The exponential expansion of ISR sensors has produced unprecedented volumes of ISR data which is straining Navy sea vessels' processing, storage, and dissemination infrastructure."

Lessons learned from recent NATO naval operations have revealed numerous shortfalls and deficiencies that need to be taken under serious consideration in order to improve Maritime ISR. By fully understanding NATO Maritime ISR capabilities and limitations and comparing them with existing NATO Maritime ISR requirements, maritime components may have the ability to overcome the challenge of defining key elements and identify the best practices that will effectively disseminate the data and collectively maintain the ISR in real-time. Moreover, this newfound understanding of Maritime ISR systems and requirements will provide an improved basis for prioritizing information and incorporating it into military planning and execution processes.

Utilizing new methodologies, like activity-based intelligence, is one approach to the navies' ISR data problems. The effort to make mounds of data more useful to warfighters might lead to the application of a number of methodologies and technologies including activity-based intelligence. Activity-based intelligence must seek to compare the current maritime situation with data garnered by persistent intelligence sensors informed by past experience to identify potential future threats. While things may look quiet and normal at sea, ships' teams can become overwhelmed by the deluge of available data, there are usually clues that could have pointed to a small boat attack or an encounter with a mine, and it is possible to alert operators when those clues appear.

Navy systems of today are indeed producing a lot more data than from decades ago. However, this data needs to be replicated and used across a much wider network. Creating effective workflows that reduce a lot of the heavy lifting for the operator may be key. Having a massive collection of real-time and near-real -time intelligence information available to operators as required, one can say that "intelligence collection to operational action" cycles have changed from days to hours and sometimes even to minutes and seconds. Navies are adopting technologies such as commercial

NATO

NATO's wide area surveillance Global Hawk unmanned aircraft is part of a broader system of systems solution designed to advance the Alliance's ISR needs during various missions. These missions include protecting ground troops and civilian populations, humanitarian assistance during natural disasters, crisis management, border control and maritime safety, and the fight against terrorism.

open source and standard data capabilities as an important part of their ISR data storage and processing strategy in order to empower the decision maker so that he can more effectively analyze intelligence data, prioritize and task ISR assets, and report mission status up and down the chain of command. This approach can effectively reduce the fog of war so that an adversary can be countered very quickly or a ship can be kept out of harm's way.

For example, the use of cloud technologies could be a solution which allows systems to migrate to a consolidated infrastructure and suggests the potential for ships within a single strike group to operate off a single instance of the cloud. There are commercial companies that are now working with navies to migrate legacy ISR applications to a future cloud environment, trying to over come the major obstacles to wider implementation, such as the difficulties associated with interaction between shipboard and shore-based environments. This task is made more difficult given the current reliability and connectivity issues related to bandwidth. Clouds are used to talking to each other but shipboard clouds will sometimes be forced to operate in isolation. Another key element will be the adherence of maritime ISR systems to a minimum set of standards. Without alliance-wide standards individual navies within the Alliance will naturally develop their own, thus undermining the desired interoperability required to fully exploit any future ISR structure. Doctrinal principles, definitions and standardized task lists should be the basis by which intelligence personnel effectively manage ISR processes across a multinational force.

Last but not least is the current budgetary climate, which has created a paradoxical situation vis-à-vis ISR: there is now an even greater urgency to build, within NATO, a modern, efficient, and robust ISR infrastructure that can handle more information with fewer personnel and at reduced cost, but at the same time there is a reluctance or inability to provide the necessary funding for navies to invest on newer, reliable and interoperable technologies to support future Allied Operations. ☸

CDR Dimitrios Lymperakis 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.

EXPANDING AFRICA'S INTEGRATED MARITIME STRATEGY

CDR Steinar Torset, NOR-N
CJOS COE

U.S. Navy

African and Indian Ocean militaries supporting CUTLASS EXPRESS 2015.

With an overall coastline of almost 40,000km, comprised of 34 states with coastlines varying from 37km (Democratic Republic of the Congo) to 3,025km (Somalia), the continent of Africa is greatly influenced by the maritime domain.[1] Over the past decades, losses of revenue from illegal activities in Africa's Maritime Domain are estimated to have exceeded hundreds of billions U.S. dollars, not to mention the loss in human lives.[2] Various forms of illegal trafficking, degradation of the marine environment, falling biodiversity, and aggravated effects of climate change are descriptions of the African maritime environment. However, with increased activity at sea, and an environment with growing instability and insecurity, Africa is actively working to improve its overall maritime domain awareness and security.

Understanding that the African continent has several major challenges to overcome and a long path ahead before they are resolved, we should appreciate the efforts necessary to establish an ambitious vision of having "an African Maritime Domain that positively contributes to socio-economic development, as well as increased national, regional and continental stability, through collaborative, concerted, cooperative, coordinated, coherent and trust-building multilayered efforts to build blocks of maritime sector activities in concert with improving

"In the complex security environment of the 21st century, militaries can advance national and collective security interests through basic ways: building partner capacity, which is our primary function; enabling allies and partners; and taking action."

- General David M. Rodriguez, Commander, U.S. Africa Command

U.S. Navy

Cameroon Navy boarding team supporting of Exercise OBANGAME EXPRESS 2012.

elements of maritime governance."[3] When we think about Africa, most of us will refer to the problems with piracy near the horn of Africa where maritime forces are playing an important role. Unfortunately, the challenges in Africa go far beyond the piracy threat in the Indian Ocean. The aim of this article is to describe some of the initiatives that exist and provide some understanding of the challenges that lay ahead.

Africa Partnership Station

Africa Partnership Station is a U.S. initiative incorporating several programs in different regions across the continent, such as the EXPRESS series exercises which focus on capacity building with selected partners in the region. The EXPRESS series is sponsored and facilitated by U.S. Africa Command (AFRICOM), and they are all designed to improve regional cooperation, maritime domain awareness (MDA), information-sharing practices, and tactical interdiction to improve the efforts to counter sea-based illicit activities. The series consists of four exercises focusing on different regions of the African continent:

PHOENIX EXPRESS: Focuses on the Northern African region.
SAHARAN EXPRESS: Aims to improve interoperability across West African nations.
CUTLASS EXPRESS: Designed to engage the East African nations.
OBANGAME EXPRESS: Emphasizes on improving maritime security in the Gulf of Guinea region.

OBANGAME EXPRESS, conducted by U.S. Naval Forces Africa, is an at-sea maritime exercise designed to improve cooperation among participating nations in order to increase maritime safety and security in the Gulf of Guinea. It focuses on maritime interdiction operations, as well as visit, board, search, and seizure techniques. The last exercise in this series was conducted in March 2015 and several nations, in addition to the regional maritime forces, participated.[4] For the first time this exercise was used to rehearse and test the new structure and procedures as laid down in the Yaounde Code of Conduct. The Yaounde Code of Conduct was signed in June 2013 after an initiative from the Economic Community of Central African States (ECCAS), the Economic Community of West African State (ECOWAS), and the Gulf of Guinea Commission (GGC). One of the main intentions is to "co-operate to the fullest possible extent in the repression of transnational organized crime in the maritime domain, maritime terrorism, Illegal, Unreported and Unregulated (IUU) fishing and other illegal activities at sea."[5] The code is modeled after the Djibouti Code of Conduct (2009), well known to those involved in combating piracy on Africa's East Coast and the Indian Ocean. OBANGAME 2015 demonstrated that there is still a long way to go as there are major challenges related to the sharing of information as well as severe technical limitations between the different stakeholders concerned with the maritime security of the region.[6]

In addition to the already well established EXPRESS series, in March 2015 the European Union (EU) adopted the Gulf of Guinea Action Plan 2015-2020.[7] This plan outlines support to the efforts of the region to address the challenges of maritime security and organized crime. It is intended that this plan will be coordinated with the ongoing efforts of ECOWAS, ECCAS and GGC; supporting the aim of the Yaounde Code of Conduct. This effort is also a part of the implementation of the overall EU Maritime Security Strategy (2014) and could become an important tool to support the region through an integrated 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.

U.S. Navy

Maritime forces from East Africa, South Africa, Europe, Indian Ocean nations and several international organizations concluded the fourth iteration of the multinational maritime Exercise CUTLASS EXPRESS 2015.

Africa's Integrated Maritime Strategy

Finally, and probably the most important development for the establishment of a lasting and well developed maritime security strategy in Africa, is an initiative of the African Union (AU) called 2050 Africa's Integrated Maritime Strategy (2050 AIM Strategy). This strategy was developed in collaboration with the International Maritime Organization and was formally adopted by the African Heads of State and Government in January 2014. The strategy was welcomed by the G7 Foreign Ministers in their Declaration on Maritime Security in March 2015.[8] It is assessed that the 2050 AIM Strategy represents a real effort to establish a regime for protection and sustainability for future exploitation of the AMD. It describes an overall and coherent plan that has a longstanding perspective and describes actions that will help to achieve the objective of the AU to enhance maritime viability for a prosperous Africa. However, as outlined below, there are challenges that must be overcome to make this a reality.

The 2050 AIM Strategy describes some of the challenges for the implementation of the desired objectives. First of all the strategy needs to be suitable. This means that sustainment of increased wealth creation from AMD positively contributes to environmental and socio-economic development, as well as increased national, regional and continental stability. Secondly, it needs to be acceptable. It must have the support and ownership of Member States, RECs/RMs, and it must be cost-effective in implementation.[9] The third challenge is that it needs to be feasible. The Plan of Action for implementation must clearly identify all resources, including funding requirements for execution within realistic time-frames. Finally the strategy needs to be compatible, meaning it must work within extant African and internationally agreed maritime instruments and legal frameworks.[10] An additional challenge that needs to be taken into account is that Africa is still struggling with severe corruption, and several of the countries involved are listed as the worst on Transparency's CPI (Corruption Perception Index).[11] The challenges related to corruption are acknowledged, and efforts are being made to deal with the problem. An example is the protocol on the fight against corruption established by ECOWAS. The protocol was signed in December 2001, but only 1 of the 15 states has so far ratified it. Hence, the protocol has not yet been implemented after almost 15 years.

The protocol has identified three major phases for the implementation of the 2050 AIM Strategy. The first phase aims to detail the goals of collaboration. This phase is ongoing and is scheduled to last until 2018. The objective of the next phase, out to 2031, is to establish a Combined Exclusive Maritime Zone of Africa, erect regional Maritime Operations Centres (MOCs) and to establish a Naval Component capacity within the framework of the African Standby Force. This will require significant capacity building and involvement from nations outside Africa. Finally, the last phase, from 2031 to 2050, is about realizing and synchronizing the positive effects from the previous phases.

There should be no doubt that the AU and the African maritime environment has a vision for the future of using the AMD to improve wealth and stability in the region. However, it is a very ambitious plan that could spark internal friction between the members. Mistrust between nations and potential national agendas may be a threat to an overall coordinated ability to establish a lasting and improved maritime security regime primarily driven by the African states themselves.

The Combined Joint Operations from the Sea Centre of Excellence has been heavily involved in the ongoing efforts to improve global Maritime Situational Awareness (MSA). The establishment of an African Maritime Strategy will be important to support this effort, and the integration of relevant African Maritime Security organizations will undoubtedly play a vital role in the future of global MSA.

Maritime Security has been a long-neglected issue on the African Security Agenda.[12] However, the focus on piracy has led to a renewed effort to improve maritime security cooperation in Africa. Initiatives like AFRICOM's Partnership Station and the EXPRESS series exercises, inclusion of African maritime security organizations in global work on Maritime Situational Awareness, and several initiatives by organizations like the EU will need to continue well into the future in order to ensure that the work required to achieve the goals, outlined in the 2050 AIM Strategy, can be achieved. After all, the more Africa is involved in the solutions, the better the chances for success. ☸

1. The CIA World Fact Book, 1 August 2015, https://www.cia.gov/library/publications/the-world-factbook/fields/2060.html
2. African Union, 2050 Africa's Integrated Maritime (AIM) Strategy, Version 1.0, (2012).
3. Ibid.
4. Corey Hensley, "Obangame Express 2015 Concludes in the Gulf of Guinea," United States Africa Command, 30 March 2015, http://www.africom.mil/newsroom/article/25316/obangame-express-2015-concludes-in-the-gulf-of-guinea.
5. "Code of Conduct Concerning the Repression of Piracy, Armed Robbery Against Ships, and Illicit Maritime Activity in West and Central Africa," Council on Foreign Relations, 25 June 2013, http://www.cfr.org/piracy/code-conduct-concerning-repression-piracy-armed-robbery-against-ships-illicit-maritime-activity-west-central-africa/p31200.
6. Dirk Steffen, "Obangame Express 2015: Two steps forward. One Step Back." Center for International Maritime Security, http://cimsec.org/obangame-express-2015-two-steps-forward-one-step-back/16227.
7. "Council Conclusions on the Gulf of Guinea Action Plan," European Council, 16 March 2015, http://www.consilium.europa.eu/en/press/press-releases/2015/03/16-council-conclusions-gulf-guinea-action-plan-2015-2020/
8. "G7 Foreign Ministers' Declartation on Martime Security in Lubeck," German Federal Foreign Office, 15 April 2015, http://www.auswaertiges-amt.de/EN/Infoservice/Presse/Meldungen/2015/150415_G7_Maritime_Security.html?nn=479796.
9. REC: Regional Economic Community. RM: Regional Mechanisms.
10. African Union, 2050 AIM Strategy, Version 1.0, (2012), p.14.
11. Samuel Mondays, "Corruption and State Instability in West Africa: An Examination of Policy Options," (2007), 3.
12. Christian Bueger, "Communities of Security Practice at Work? The Emerging African Maritime Security Regime," African Security, (2013), 297-316.

CDR Steinar Torset 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 Command and Control Centre of Excellence Seminar

5-7 July 2016 Norfolk, VA

The NATO Command and Control Centre of Excellence (C2 COE), supported by the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE), will present its annual 2016 seminar entitled "C2 in Future and Emerging Warfare - What are the Challenges for Coalitions and Alliances?" The intent of this year's seminar is to examine how C2 will evolve in the next 5 to 10 years given the fast pace of technology development and ever evolving and emerging threats. How and where will our adversaries fight in the future? What will be the consequence of worldwide urbanisation and the impact of advanced weaponry such as unmanned systems? Future conflicts will require cooperation between combined and joint military forces and civilian organisations. Therefore, we will approach this dynamic subject from the Civil, Maritime, Land and Air perspective to give seminar participants a comprehensive understanding of future C2 challenges of the future.

Visit www.CJOSCOE.org to reserve your seat at the seminar!

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

IMPROVING INTEROPERABILITY THROUGH THE CAMPAIGN PLAN FOR AMPHIBIOUS OPERATIONS TRAINING (CPAOT)

CDR Russell Czack, USA-N
CJOS COE

U.S. Marine Corps

U.S. and U.K. Marines conducting artillery training, BOLD ALLIGATOR 2012.

Taking a holistic approach to enhancing proficiency in naval amphibious mission essential tasks, the United States Fleet Forces Command (USFFC) and the Marine Forces Command (MARFORCOM) established the Campaign Plan for Amphibious Operations Training (CPAOT). The CPAOT uses a five-year cycle to provide opportunities to integrate the amphibious operations training plans of USFFC, MARFORCOM, Commander Pacific Fleet, Marine Forces Pacific, and allied and partner nations. The CPAOT plan utilizes live, synthetic, constructive, and tabletop exercises, combined with professional military education and leadership seminars, to achieve a continuum of training focused on readiness and interoperability of amphibious operations.

"Perhaps the most obvious observation, and the cause of arguably the largest interoperability issue, was the doctrinal differences in amphibious C2 structures."

BOLD ALLIGATOR Exercise Series

The cornerstone of the CPAOT, the BOLD ALLIGATOR (BA) exercise series, is aimed at accomplishing a set of strategic, operational, and tactical objectives, including building and maintaining interoperability between the U.S. Navy (USN), U.S. Marine Corps (USMC), and allied and partner nations across the range of military operations. With 19 nations participating in BOLD ALLIGATOR 2014 (BA14), the exercise has become one of the largest US-led multinational exercises focused on amphibious operations. The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) has played an instrumental role in supporting the USFFC Fleet / Joint Training Directorate, to ensure coalition partners' training objectives are integrated into BA exercise planning and execution phases. Additionally, in support of the Navy Warfare Development Command's (NWDC) Observation and Analysis

(O&A) Working Group, CJOS COE has led the collection of observations focused on interoperability by co-locating observers with units afloat and ashore throughout the exercise.

The CJOS COE O&A Team captured 53 observations throughout BA14, concerning intelligence, maneuver, fires, sustainment, force protection, safety, and command and control (C2). Perhaps the most obvious observation, and the cause of arguably the largest interoperability issue, was the doctrinal differences in amphibious C2 structures. The C2 structure utilized in BA14 applied U.S. doctrine, Joint Publication 3-02, Amphibious Operations, which establishes a single command known as the Commander Amphibious Force (CAF). The CAF C2 model differs from the Commander Amphibious Task Force (CATF) / Commander Landing Force (CLF) structure of NATO Allied Tactical Publication Eight, Doctrine for Amphibious Operations, which contributed to confusion on roles and reporting requirements. Additionally, the BA14 C2 structure for task organization, with a coalition partner task group separate from U.S. task groups, did not facilitate a full integration of forces within the exercise. A fully integrated staff and maneuver units across multiple partner nations would have allowed the coalition to train in a more realistic manner.

While BA14 did reveal some new interoperability gaps, many of the observations were not new. In fact, almost one third of the observations can be seen in the O&A report from BA12. For example, the over reliance of U.S. units on the Secret Internet Protocol Router Network (SIPRNet), the U.S.-only network, made communication with coalition partners more challenging and gave operational partners the impression they were on the outside looking in. Any document or briefing slide which originated on SIPRNet had to go through the Foreign Disclosure Office (FDO) in order to determine releasability, or the ability to transfer the information onto the coalition information network based on classification. When the intended audience of these documents or slides includes coalition partners, this process causes an unnecessary delay in communication, not to mention an excessive workload for the often limited capacity of the FDO. By generating exercise documents and briefing slides on the coalition information network, also known as the Combined Enterprise Regional Information Exchange System (CENTRIXS), this interoperability deficiency could have been avoided.

U.S. Marine Corps

A Portuguese Marine provides security for Landing Craft Air Cushions during Exercise TRIDENT JUNCTURE 2015.

Closing the Interoperability Gap

Recognizing the importance of these observations from the BA exercise series, which highlight possible interoperability deficiencies or gaps between U.S. and

NATO

United Kingdom LCVPs (Landing Craft, Vehicle, Personnel) from HMS BULWARK on their way for an amphibious assault with a WILDCAT helicopter from HMS OCEAN for protection during NATO exercise TRIDENT JUNCTURE 2015.

coalition partners, USFFC and CJOS COE have established the Interoperability Technical Advisory Group (ITAG). The ITAG, structured around the focus areas of Doctrine and Lessons Learned, Operations, Capabilities and Experimentation, and Training, seeks to validate and determine the root causes of the gaps, recommend potential solutions, and develop Plans of Actions and Milestones to take remedial action. The ITAG consists of representatives from various stakeholders, including USFFC, MARFORCOM, NWDC, the Marine Corps Combat Development Command, Commander Naval Surface Forces Atlantic, Commander Naval Air Forces Atlantic, Carrier Strike Group Four, and Expeditionary Strike Group Two.

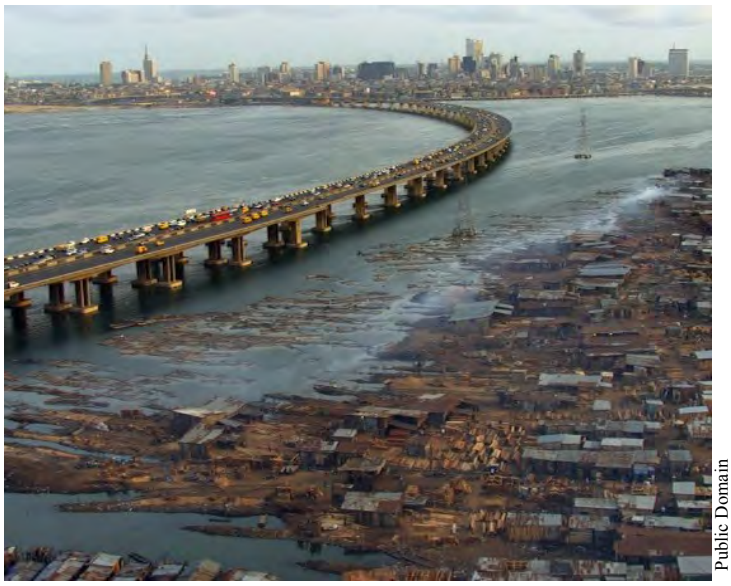
To close an interoperability gap, the ITAG must first determine the root cause. For example, in the case of U.S. reliance on SIPRNet, perhaps SIPRNet is used as the default system due to the lack of availability of CENTRIXS. Or, maybe U.S. Sailors are simply accustomed to using SIPRNet while conducting an exercise and must make a conscious effort to use CENTRIXS when operating with partners. Depending on the exact root cause, the solution may vary. If the root cause is determined to be an equipment shortage, then closing the gap will require an acquisition of additional capabilities. If the cause is related to a needed cultural shift, then the solution may be a policy change and training. Of course, the root cause may be a combination of both a capability shortage and a training deficiency.

Once a determination of root cause is made, and the approved solution is put in place, multinational exercises or events, such as those of the CPAOT, are the optimal method of assessing the impact of improvements made. As a member of the CPAOT working group, O&A lead for interoperability observations, and Co-Chair of the ITAG, CJOS COE is ideally placed to oversee and coordinate this iterative end-to-end process. The COE can ensure coalition partner training objectives are included in CPAOT events, can observe the events to assess the integration of U.S. and partner participants, and can work with U.S. stakeholders towards remedial actions aimed at closing interoperability gaps. ☸

CDR Russell Czack 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 OPERATIONS IN A FUTURE URBAN-CENTRIC ENVIRONMENT

LtCol Heiko Griesinger, GER-A
CJOS COE



Public Domain

A densely populated city with provisional floating settlements.

It is 2035 and NATO has been asked to support the city of Archaria– a coastal, fragile and loosely integrated city with around 7 million inhabitants.[1] Hit by a tsunami, many houses, especially in coastal slums, as well as parts of the port and airfields, are destroyed. Over 700,000 people have been killed, disease is spreading, and non-state actors control parts of the city.

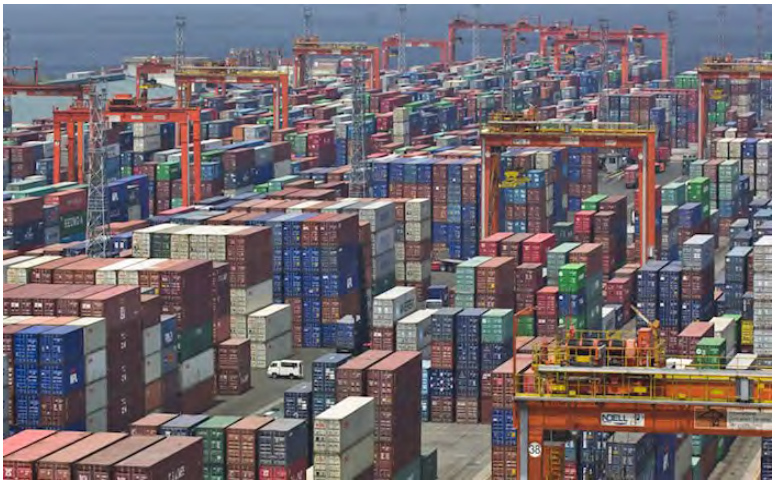
As the NATO Combined and Joint Task Force works to find appropriate entry points in order to deliver humanitarian aid, unidentified actors fire on approaching naval vessels with sophisticated weapon systems while fishing vessels block the port. Large Archarian diasporas in cities across NATO, organize demonstrations, with some turning violent and even escalating into attacks on governmental buildings. Politicians are already publicly discussing that they would like their nation's NATO contingent to leave the coalition force.

This is a fictitious scenario, but some trends suggest that NATO may have to cope with these types of challenges in the future. The Strategic Foresight Analysis and Framework for Future Alliance Operations have predicted that rapid global urbanization will be one of the most challenging future trends for NATO. Based on this critical trend analysis, NATO`s International Military Staff has implemented a task that will research the effects of rapid urbanization. The first key milestone of this project was a limited objective experiment, conducted in September 2015. The aim of the experiment was to bring together subject matter experts, civilian and military alike, to discuss the implications for NATO in the conduct of future military operations. The findings will later be incorporated into a conceptual study, led by Allied Command Transformation, with Combined Joint Operations from the Sea (CJOS) and Operations in Confined and Shallow Waters (CSW) Centers of Excellence providing maritime expertise in support.

"The sea has always been and will continue in the future to be critical for the livelihood of humanity, habitat, resources, and transport routes for up to 90 percent of intercontinental trade."

Globally, more people now live in urban areas

than in rural ones, with 54 percent of the world`s population residing in urban areas as of 2014. By 2050, 66 percent of the world`s population will be urban, with Africa and Asia urbanizing faster than other regions with nearly 90 percent of the global increase.[2] In addition, studies suggest that in some countries, especially in developing and fragile areas, there will be a youth bulge, leading to a demographic bomb if there is a high unemployment rate: "... because a large mass of frustrated youth is likely to become a potential source of social and political instability."[3]



Public Domain

Port of Long Beach, California experiencing severe congestion.

With 80 percent of the global population currently living within 100 kilometers of the coast, along with the majority of the world`s economic and political activity, including oil extraction, fishing, mining, banking and international trade, occurring in the littoral, the impact that continuing urbanization trends can have upon both the maritime environment and maritime operations becomes evident.[4] A basic assumption must be that, given the concentration of people and resources in this complex zone, there is a very high likelihood that this is where the bulk of military missions will occur in the future. Different aspects from a maritime perspective have to be considered when operating in that environment.[5]

Commodity & Information Flow

The sea has always been and will continue in the future to be critical for the livelihood of humanity, habitat, resources, and transport routes for up to 90 percent of intercontinental trade.[6] It is also clear however that the maritime domain will also be an arena for illegal activities. Both state and non-state actors will have access to the maritime domain, with an ability to impact connectivity, trade, and global prosperity. In other words, there are several key issues with which NATO will have to cope: Increased urbanization, as well as growth in the purchasing power of developing nations, will result in additional demands for energy and resources as well as an increase in shipping requirements due to the proximity to the coast. Interruption of maritime flows can cause major problems in the impacted urban area, so maritime security will be critical to ensure stability and connectivity of the world's markets and trade routes. Illicit transport of commodities will affect urban areas in different ways: population groups receiving goods, which are not delivered by legal means, leads to black markets and a system of shadow economy. Besides the positive effects, some goods – like weapons - can destabilize an entire region and undermine legitimate government control.

With an increase in automation and the introduction of autonomous systems, different actors can exploit the inherent vulnerabilities: The maritime cyber-threat is not only affecting military operations in this environment, but also commercial shipping. Automation has significantly reduced the number of crews needed, and while some argue the benefits and improved safety standards, others see increasing risks and vulnerabilities, especially with the availability of

better technology and the human resources with sophisticated technical skills common in urban areas, mainly with young people.

Ports, as key hubs for the commodity flow are a very important part of a city. With growing needs, ports will keep a key function within the global supply chain. Doctrine and handbooks on urban warfare consider ports as key terrain which is essential to be controlled, influenced and exploited. Ports are very unique but all are inextricably connected to, and dependent on infrastructure and activities both on and offshore. The increased automation of ports make them more vulnerable as they are exposed to a cyber-threats not previously seen.

Inland waterways see a growing importance in the future, connecting regions in the hinterland with international sea lanes. Some of these waterways are in urban areas or connected to them. Riverine operations in the urban environment face two key challenges: vulnerability from high-ground and limited or hampered accessibility due to barrages and dams or other artificial and natural obstacles.

Confined and/or shallow water (CSW) operations face a particularly challenging environment where the asymmetric threat is easily confused with the everyday activities of the region. Interdiction at range is a luxury, events typically unfold rapidly. Increased technology and the growing ease of access also produce future risks from autonomous systems such as drones, which could be used as flying, swimming, or submersible IED delivery mechanisms. With these new technologies, threats are less controllable and will be 360 degree, both kinetic and non-kinetic. As noted recently at a U.S. J-7 Futures Combinations Workshop: "In the future, we will not hunt IEDs. They will hunt us."[7]

Digital sea lanes today lack even basic protection. Considering the importance of these lines of communication for intercontinental digital traffic, there is a need to take this into account, especially since their main customers will be living in the cities of the future.[8] The population could be very sensitive, when for example their Internet access is shut down. The Arab Spring provides good examples for the anger and protests of the population after the regime purposely shut down Internet accessibility. Coastal shipping, illicit transport, all-domain automation, unlimited use of the electromagnetic spectrum and the spread of all kinds of communication means could create a crowded, cluttered and therefore "noisy" environment, imposing a myriad of challenges for conducting military operations.

"Digital sea lanes today lack even basic protection. Considering the importance of these lines of communication for intercontinental digital traffic, there is a need to take this into account, especially since their main customers will be living in the cities of the future."

Resources

Population growth is expected to strain global food resources, potentially leading to drastically increasing rates of malnutrition and starvation. Already current food supply demands and a continuous high level of illegal, unreported and unregulated fishing, has resulted in a situation where production from capture fisheries has leveled off and most of the main fishing areas have reached their maximum potential. It is likely that fish supplies from capture fisheries will not be able to meet this growing global

Public Domain (Anthony Ling, TSI)

Maritime platforms, such as floating islands, may be seen in growing numbers as overcrowding becomes more prevalent in urban cities and settlements.

demand for aquatic food. The U.N. Food and Agriculture Organization expects a huge increase in coastal food production based on fish farming and farming of aquatic plants.[9] This could lead to a significant problem when it comes to the use of coastal space for future maritime operations.

Offshore energy and mineral resources are means to satisfy the world`s growing hunger for energy, but the associated installations also present vulnerable and dangerous objects which can be exploited by different actors, with the potential of creating losses in life, property and significant environmental damages. In this aspect, NATO has to find out if it has the ability to protect these vital energy resources during coastal, urban related maritime operations.[10] Likewise industrial areas, clustered at the edge of coastal cities or coastal seabed based nuclear plants could pose significant hazards both to the population and the NATO force. The constriction of sea approaches to urban environments by these installations should also be considered.

As many of the world`s cities are on coastlines, the increasing dependence on coastal food production and energy systems might have important implications for future maritime operations, especially expeditionary ones.

Environmental Change

Although there are still significant uncertainties in projections of environmental change, there is a common view that coastal cities are particularly vulnerable to the long-term effects of global warming, such as sea-level rise, flooding, air pollution, and severe storms. Even if environmental changes do not worsen, the impact of such events would be significant due to the fact that more people will be affected.

A rise in sea level, for example, can have significant impacts in low-lying coastal areas. The magnitude of these sea-level change impacts will vary from place-to-place depending on topography, geology, natural land movements and any human activity which contributes to changes in water levels or sediment availability (e.g. subsidence due to ground water extraction). Despite these threats, few coastal cities have been assessed in terms of possible coastal impacts.[11] Humanitarian Assistance and Disaster Relief operations may not be core tasks of the Alliance, but are likely to be requested.

Coastal Habitat

As populations grow, cities will grow too. Littoral expert Dr. David Kilcullen predicts the "seamless city," a peri-urban space around the city that merges into "bands of urbanized terrain that extend hundreds of miles in coastal areas, cross national borders, and house many millions of people." The consequence is that access from the sea will be very difficult, even impossible, besides ports and rivers.[12]

In many countries, especially those in the

developing world, urbanization has been accompanied by increasing inequalities, growth of informal employment, expanding slums and informal settlements: large numbers of people are living in high risk areas such as creeks, river and canal beds, marshes, and even at sea on floating platforms, depending on the sea-level. If natural disasters hit a coastline, these vulnerable, often ungoverned spaces will be most affected. The informal structures and spaces may create conditions where people are forced to earn money by illicit activities, ranging from piracy to waterborne trafficking. These areas enable non-state-actors to "nest" in, protected by limited or non-existent government and security presence and therefor low situational awareness.[13]

With an ungoverned space comes weak health and physical infrastructure as well as uncertainty due to civil wars or general unrest, diseases will also be a major threat to the population and any military and civilian assistance force. With the relatively free and fast movement of goods and people in a coastal city, a lethal disease like the Ebola virus can easily hamper or even stop military operations, or at least force us to use different approaches.[14]

"The ability to establish and maintain sea control and to project power ashore as a result of various scenarios stemming from urbanization, will require NATO to effectively operationalize its maritime power strategy."

Another trend is the growth of artificial and floating islands, built on rivers and in the sea. This growing trend is the result of land becoming over-crowded by cities and settlements. Safety, prestige, and accessibility may be additional reasons why this alternative has become increasingly popular. Maritime platforms for recreational use might be seen in growing numbers and could be added obstacles and areas of concern for military operations.

Power, Influence, and Control

As always different actors will compete in this future maritime urban-centric environment for power, influence, and control; however the new paradigm is connectivity: being able to use global networks to disseminate and receive ideologies, weapons, drugs, revenues, and technical expertise while overcoming geographical isolation. This is affecting traditional power projection in a significant way, the U.S. naval strategy recently highlighted:

"…the proliferation of technologies that allow potential adversaries to threaten naval and air forces at greater ranges complicates our access to some maritime regions (anti access), as well as our ability to maneuver within those regions (area denial), including the littoral and landward access ….the free flow of goods and services can be impeded by state or non-state actors …." [15]

NATO will need to consider this issue as part of their own planning, because it suggests that operations in this environment will become even more susceptible to risk. Coastal cities, with their strategic location, population concentrations, transportation infrastructure, and above average income levels, have become important points of control for those seeking profit or support for their cause. All research suggests that the most prevalent future threats in this environment will come from non-state armed groups using irregular methods, avoiding direct confrontation, but being able to acquire highly sophisticated weapons. These groups can be very different and categorized by their aims: opposition groups, crime groups, militias, vigilantes and gangs, and also private security.[16] In some cases state actors will also use irregulars as their preferred instrument and weapon of choice, or use

asymmetric methods to minimize their footprint and avoid blame and counter-reaction. Using irregular or ambiguous warfare to mount attacks in NATO homelands is another option, especially if the adversary does not want to, or cannot directly oppose, the NATO force.[17] Diasporas of city-level immigrants could be used for this expansion of the littoral theatre.[18]

Private Security Companies provide guarding, protection of persons, escorting humanitarian aid and convoys, training and advising armed forces, operating complex weapon systems and intelligence gathering. As potentially armed non-state-actors they can be a relevant player with destabilizing potential.[19] In April this year, the G7 Foreign ministers acknowledged the use of Private Maritime Security Companies for sea-going vessels, including armed personnel in order to protect them against threats. It seems that this is a confession that states are no longer able to provide support and protection with their navies.[20]

With an increased competition for energy and resources, discussions to readdress international borders and economic exclusion zones will continue; further driving disputes over International Law of the Sea in its present form.

Conclusion

Urbanization as such does not necessarily imply a higher risk of instability. However, taking into consideration that most of the population growth will happen in the developing world, it is not unlikely that urbanization in under-governed and fragile areas will lead to situations where NATO may have to conduct some form of security or defense operations. The ability to establish and maintain sea control and to project power ashore as a result of various scenarios stemming from urbanization, will require NATO to effectively operationalize its maritime power strategy.

Current and future planning and execution of maritime operations, or joint operations in the maritime domain, will have to focus on difficult littoral areas where state and non-state actors will be operating with different capabilities and under different rules. While "blue water" operations may still occur, current trends such as the emergence of powerful non-state actors, urbanization in coastal regions and increasing connectivity of huge parts of the population suggest that combined and joint operations in the littorals, and most likely within confined and shallow waters environments will be prominent in future NATO operations.

A lot of focus regarding challenges related to urbanization has primarily looked into the complex potential scenarios related to the land and air domains. With the start of NATO´s urbanization project and CJOS`s participation, it was clear that this is a field of effort which requires a long term focus. A project of this nature would be incomplete without examining the effects and implications of urbanization on operations in the maritime domain. CJOS COE, as a maritime-focused think tank and facilitating organization has started early gathering experts from different international and multi-disciplinary entities to look at all aspects of this future challenge. In February 2015, CJOS COE organized and conducted a workshop, bringing together a Maritime Urbanization Community of Interest (MUCOI); comprised of academia, commercial shipping industry, law-enforcement and military stakeholders.

MUCOI continues to exchange papers, ideas and products. David Kilcullen has suggested in the conclusions of his NATO Urbanization research papers that a network like this is necessary, to keep up with developments in the littorals, catch the latest trends and turn them into military realities. Moreover, CJOS COE will continue to identify, outline and address the myriad of maritime challenges associated with future urbanization, helping to ensure NATO is better prepared when called upon to conduct maritime operations in a future urban-centric environment. ☸

1. A term used by the U.S. Army to describe cities which have decentralized, informal systems, poor quality infrastructure and unregulated flow capacity: Chief of Staff of the Army, Strategic Studies Group, Megacities and the United States Army: Preparing for a Complex and Uncertain Future, 2014.
2. United Nations, "United Nations World Urbanization Prospects," (2014), 1.
3. Justin Yifu Lin, "Youth Bulge: A Demographic Dividend or a Demographic Bomb in Developing Countries?" 5 January 2012, http://blogs.worldbank.org/developmenttalk/youth-bulge-a-demographic-dividend-or-a-demographic-bomb-in-developing-countries.
4. U.S. Department of Defense, U.S. Joint Publications JP 2-01.3, 16 June 2009, II-49.
5. Systematic approach adopted from maritime security challenges in Borchert, Heiko, Maritime Security at Risk, Trends, Future Threat Vectors, and Capability Requirements, Lucerne, 2014.
6. G7 Foreign Minister's Declaration on Maritime Security, Luebeck, 15 April 2015.
7. T.X. Hammes, noted at a Futures Combination Workshop, hosted by the Joint Chiefs of Staff Directorate for Joint Force Development (J-7) and the Hopkins Applied Physics Laboratory, 5-8 May 2015.
8. Robert Martinage, "Under the Sea – the Vulnerability of the Commons, Foreign Affairs," Foreign Affairs, Volume 94, Number1, 2015, 117-126.
9. Food and Agriculture Organization of the United Nations, "State of World Aquaculture," http://www.fao.org/fishery/topic/13540/en.
10. Working group meeting protocol, Scenario-based meeting on "the protection of energy infrastructure in the maritime domain", NATO HQ, Brussels, 20 April 2015 and http://ensec.org/index.php?option=com_content&view=article&id=453:protecting-offshore-oil-and-gas-installations-security-threats-and-countervailing-measures&catid=137:issue-content&Itemid=422.
11. Keynotes from an environmental expert on trends, MUCOI-WS, Hampton, February 2015.
12. David Kilcullen, "Out of the Mountains, The Coming Age of the Urban Guerilla," (London: Oxford University Press, 2013).
13. Ibid.
14. United Nations Development Group, "Socio-Economic Impact of Ebola Virus Disease in West African Countries," (February 2015), iii.
15. A Cooperative Strategy for 21st Century Seapower, (March 2015), 8.
16. Armed Non-State Actors: Current Trends & Future Challenges, (DCAF & Geneva Call, 2015), 16.
17. "Ambiguous warfare is a term that has no proper definition and has been used within the U.S. Government circles since at least the 1980s. Generally speaking, the term applies in situations in which a state or non-state belligerent actor deploys troops or proxies in a deceptive and confusing manner – with the intent of achieving political and military effects while obscuring the belligerent ´s direct participation"
18. Kilcullen, David, "The Conduct of Future Operations in the Urban Littoral, and its Implications for NATO," (March 2015).
19. Dirk Steffen, "Troubled Waters? The Use of the Nigerian Navy and Police in Private Maritime Security Roles," 1 July 2014, http://cimsec.org/troubled-waters-use-nigerian-navy-police-private-maritime-security-roles/11918.
20. G7 Foreign Minister's Declaration on Maritime Security, Luebeck, 15 April 2015.

LtCol Heiko Griesinger 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.

COUNTERING IMPROVISED EXPLOSIVE DEVICES IN THE MARITIME ENVIRONMENT

CDR Luis Constante, PRT-N
CJOS COE

U.S. Navy

USS COLE returning home after its attack in Aden Harbor, Yemen in 2000.

In recent decades, Coalition Partners have fought in numerous battles across the globe in areas such as Iraq and Afghanistan. Undoubtedly these battles have fostered an invisible enemy that has entrenched themselves within frightened populations. This anonymity has allowed even an unsophisticated enemy to maximize their use of Improvised Explosives Devices (IED) targeting adversary military forces, facilities, and innocent civilians. The effectiveness of these tactics can be readily seen in the high IED-related casualty rates in Iraq – 46%, and Afghanistan – 35%.[1]

> **"If we consider how dependent most nations are with their maritime resource assets … one can see the wide spectrum of maritime target opportunities available to a perpetrator."**

Unfortunately the threat of IEDs is not completely land-centric and has become increasingly prominent in other domains such as the maritime environment. There are devastating examples of how Sailors and Marines, ships and sea platforms have been targeted by IEDs in the maritime environment. One of the most iconic tragedies of this type of threat was the terrorist bombing of the U.S. Navy guided-missile destroyer USS COLE on 12 October 2000. This terrorist act utilized IEDs, causing the death of 17 sailors, severely injuring another 39, and rendering the ship non-operational for 14 months.

When compared with the number of land based IED attacks, maritime incidents may appear negligible. However, the maritime domain is the backbone of many societies; providing commerce, transportation, security, and food. As a result, this maritime dependency creates an enticing target for adversaries to exploit. One motive is to create a perilous environment where a single IED event would be enough to receive a disproportionate amount of worldwide media attention.

IED Defined

IEDs are bombs that are normally constructed and deployed with unorthodox methods not commonly practiced by conventional militaries. However, these

makeshift devices may be constructed with conventional military explosives and detonating mechanisms. With the appropriate level of knowledge and skill, an aggressor can fabricate an IED with remnant artillery rounds or chemical products to achieve their desired bomb blast. The basic composition of an IED consists of a main charge, a switch, an initiator, a power supply, and a container.

The only limiting factor for the deployment and detonation of an IED is the aggressor's imagination. All IED configurations can be detonated from a remote location, using a wire or wireless connection or any option within the electromagnetic spectrum. They can be activated by the victims through an imaginative proximity trigger mechanism, and lastly by a suicide normally making use of a suicide vest, known as Suicide Bomber Improvised Explosive Device.

Public Domain

IED threats are not solely limited to land terrain, the maritime domain can be just as acceptable to an IED threat.

The IED in the Maritime Environment

Non-state actors tend to seek highly visible targets such as government and military facilities, public transportation, and troop movements; capitalizing on events and places which could possibly receive vast media coverage instilling fear and distress across the globe. These heinous acts of devastation are continuously seen in the "Land Environment." If we consider how dependent most nations are with their maritime resource assets, which represent 90% of worldwide trade, one can see the wide spectrum of maritime target opportunities available to a perpetrator. Major harbors receiving and dispatching not only millions of cargo tons every day, but also thousands of people travelling in cruise ships; oil and gas sea platforms which significantly support the global economy; and from a strategic perspective, geographical sea lane choke points. Indeed we have witnessed various types of delivery methods primarily seen in the land environment; however this methodology has seamlessly translated over into the maritime domain. The following is a list of IED delivery mechanisms demonstrated in the maritime environment:

- Ships/Skiffs: can be hijacked, and used against a major target ranging from a cruise liner to a port.
- Fast Attack Crafts: A small agile boat that can minimize reaction time and deliver a considerable payload to a navy ship or a coastal military facility
- Submersible Vessels: Already seen in the drug traffic also with a considerable payload and discreet presence capable of targeting with a tremendous surprise effect any maritime platform from military to commercial
- Divers / Swimmers / Swimmer Delivery Vehicles: limited payload but hard to detect specially by commercial vessels
- Improvised Maritime Mine: Like an IED on the side of a road it can be laid on a maritime corridor waiting for the best target of opportunity.

Success in addressing this IED threat in the maritime environment will require more expertise and

further development of a comprehensive measure that will adequately counter this ongoing danger. A vast range of subject matter experts crossing various fields such as explosive ordinance and disposal, oceanography, combat diving, developmental engineers, and naval architecture and sailing will be needed. Consequently, acquiring this expertise and resources will require a great financial investment to further develop viable maritime IED countermeasures.

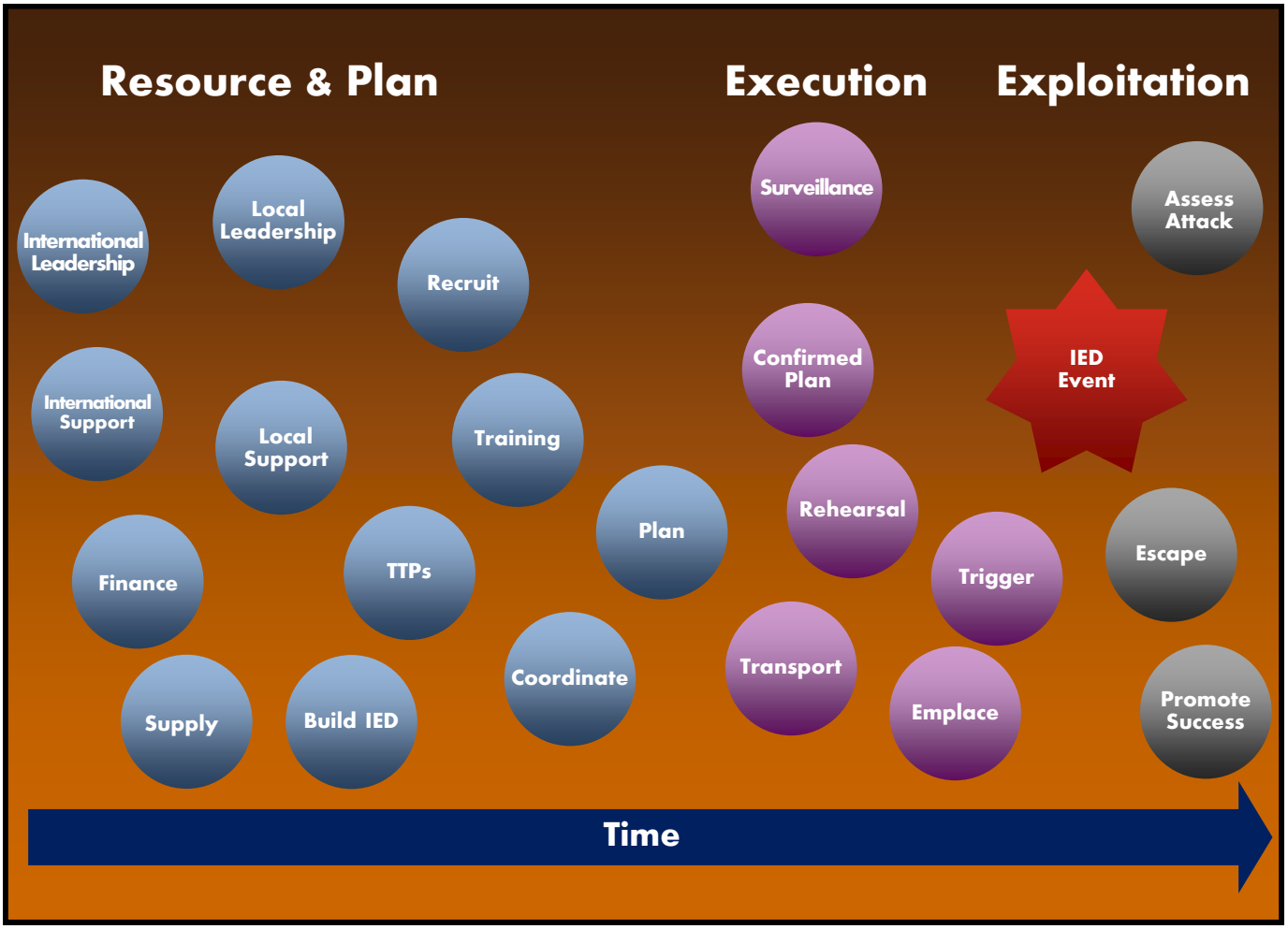


Figure 1. The IED System

How can we stop an IED?

Based on the years of operational experience in Iraq and Afghanistan, many studies have been developed by NATO and contributing Nations on effectively countering IED attacks. These studies are condensed on AJP-3.15, and show us that every IED event has a series of procedures prior to its execution known as IED System. This System is divided in three phases: Resource and Plan, Execution, and Exploitation (see Figure 1).

In order to properly stop an attack, the importance of identifying and understanding the different phases and tasks is critical. To the common individual the easiest method of identifying tasks would be transport and emplace. Many of the lifesaving decisions and brave actions taken to successfully disrupt past IED attempts were based on the identifiers illustrated in the IED System. In the maritime environment implement-

ing the IED System can be more of a challenge because some of these tasks or identifiers may not be as apparent as in the land environment. Hence, the opportunity to disrupt the process in its earlier stages may become difficult to identify and counter.

Every military operation needs to understand the IED System, and to consistently address it in their efforts. In order to Counter the IED System the response must be organized in three main pillars: Prepare the Force, Defeat the Device, and Attack the Network (see Figure 2). Countering a maritime IED will initially require the forces to become acquainted with the threat. This force must be prepared to properly utilize its tactics, techniques, and procedures (TTPs). IED experts with their specific equipment and resources will defeat the devices and protect not only the force but also the littoral populations and maritime infrastructures. Only time with the appropriate intelligence collection plan for a given campaign will provide the knowledge needed to understand an IED System, and "Attack the Networks" by preventing and pursuing those who manage them.

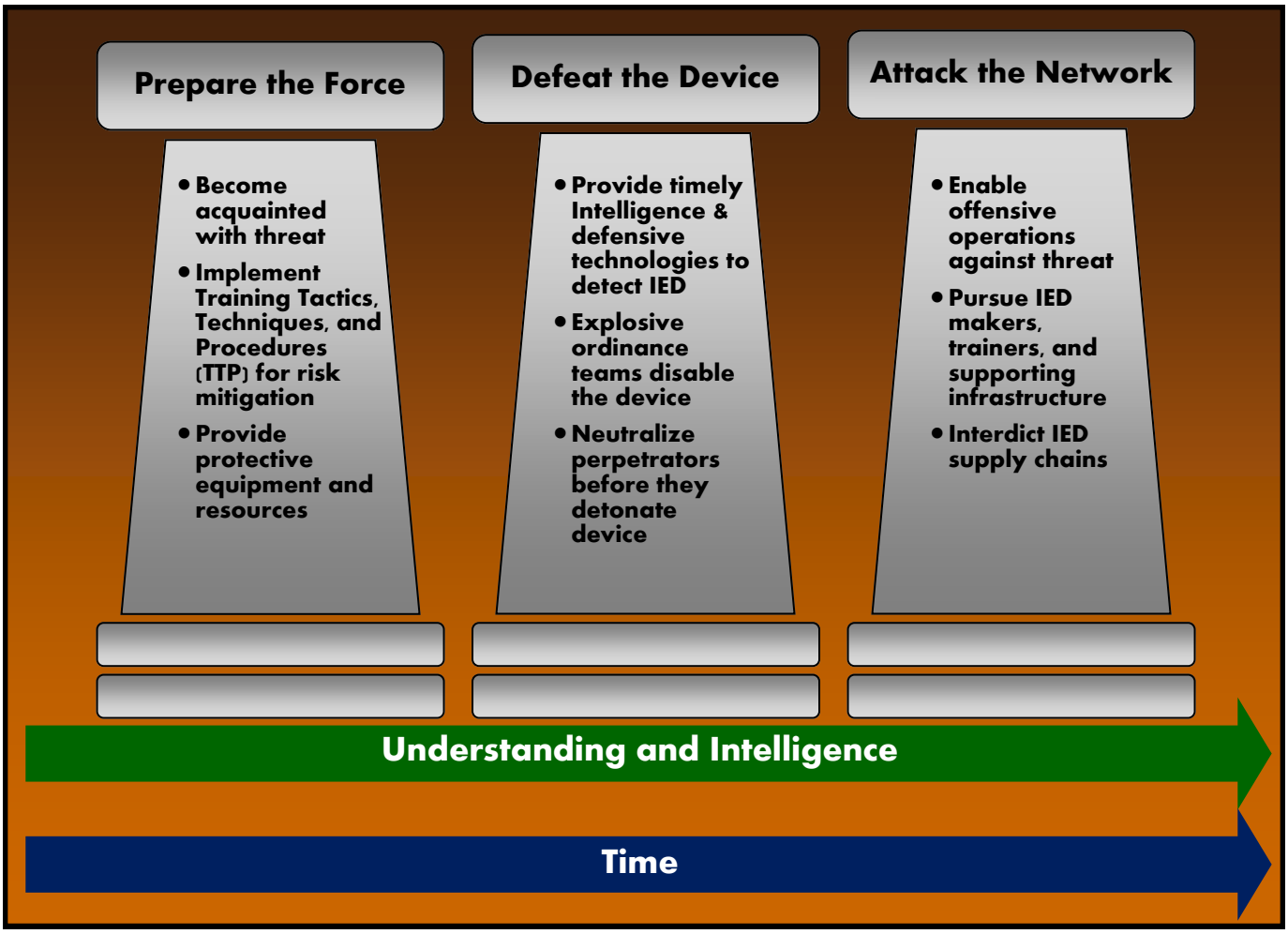


Figure 2. The three pillars of countering IED systems.

Preparing a Campaign from the Sea

Expeditionary Operations and Sea Basing are very common terms within NATO's recent work and experimentation. To reach and sustain 'from-the-sea' objectives ashore, Naval Forces, and especially the

ship-shore connectors, will expose themselves, to the already mentioned unconventional threats in the Littoral environment. To face these challenges the forces must improve their capability to fight against the IED System, by addressing the above mentioned 3 pillars. To succeed on that absolute need for efficiency, three Centres of Excellence, including the Combined Joint Operations from the Sea, are developing new concepts in these three areas.

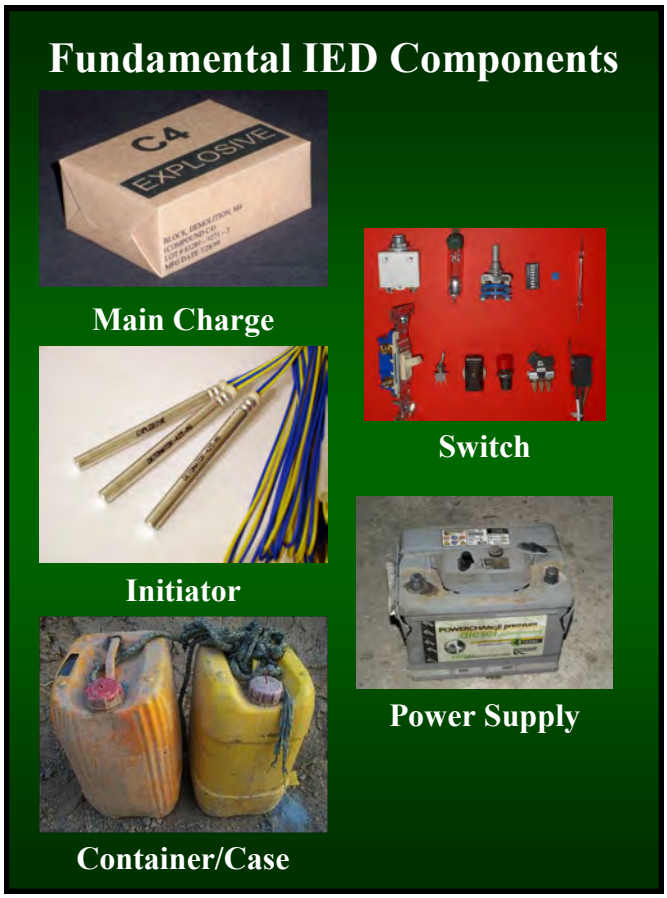


Figure 1. The 5 fundamental components of an IED.

Based on a formal request for support from NATO Allied Maritime Command (MARCOM), CJOS is currently developing the "Preparation of the Force" pillar. A great deal of effort will be required with planning, training, and ensuring the pillars properly support each other.

Per the Allied Joint Publication 3.15, Preparation of the Force has four main areas specific to the maritime environment:

- Set of support measures and activities
  - Activities within the Naval Force (planning ,training, and assembly)
  - External activities (liaison with government and non-government agencies)
- Understanding the Operational Environment
  - Operational analysis
  - Dissemination of Standard Operational Procedures
  - Deployment of Force Protection
  - Interact and secure population
- Environment IED System Threat
  - Tridimensional above and below surface
  - Type of device and control
- Mitigate the threat
  - Vulnerability and risk assessment
  - Risk management
  - Response and recovery

CJOS is a committed agency in a global effort to develop methods for countering IEDs in the Maritime Environment. Only a joint effort, with shared lessons learned and actionable intelligence will create the necessary awareness for naval forces to fight this global threat, and safely bring back home the men and women, Sailors and Marines that risk their lives every day. ☸

1. Based on an 11 November 2010 report released by the Center for Strategic and International Studies: "IED Metrics for Iraq: June 2003 – September 2010" and "IED Metrics for Afghanistan: January 2004 – September 2010."

CDR Luis Constante 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.

COUNTERING HYBRID WARFARE

CAPT Marv Carlin, USA-N
CJOS COE

NATO

NATO Wales Summit of 2014 addressing hybrid warfare.

There seems to be many names for it whether you call it new-generation, unconventional, asymmetric, indirect, ambiguous, irregular, guerrilla, or even possibly 'hybrid'. Regardless, although there are numerous names for it, everyone seems to know it when they see it. Of course we are referring to the recent popularity of the term 'hybrid warfare' stemming from the NATO Wales Summit of 2014. The recent events in the Crimea and Ukraine, the rise of ISIS/ISIL in Syria and Iraq, and continuing counter-piracy efforts around the world have caused NATO partners to reevaluate the hybrid threat. NATO now faces its toughest challenge since the fall of the Berlin Wall to understand and counter the 'hybrid threat'.

"We can no longer overlook our own vulnerabilities or underestimate the imaginations of our antagonists."
- LtCol Frank G. Hoffman, USMCR(Ret.)

As part of the Multinational Capability Development Campaign (MCDC) for 2015-2016, led by the United States and composed of 22 Nations and Intergovernmental Organizations, the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) has joined the efforts of the Norwegian-led team for the 'Countering Hybrid Warfare' project. Along with the 8 other nations of MCDC, the effort is also setting up a community of global partners with the goal of building and strengthening multinational interoperability and collaboration. There is no shortage of intellectual thought on hybrid warfare or any of 'also known aliases.' As a NATO-accredited Centre of Excellence, CJOS COE hopes to bring an often overlooked maritime component to the already large body of work that exists for land-based hybrid warfare thinking.

The specific problem statement was:

"Our understanding of hybrid warfare is underdeveloped and hampers our ability to deter, mitigate and counter the challenges posed by this threat."

By reading this statement, there are academics

and military theorists that might say the opposite is true and that hybrid warfare definitions are overdeveloped, over-thought, and muddled, but what can be said are that efforts to deter, mitigate, and counter these threats are lacking.

The Idea

"Nation-state adversaries are adapting to counter U.S. and allied advantages, blending advanced weapon systems and non-kinetic effects with operational and tactical ambiguity. This new "hybrid warfare" observed in Crimea and elsewhere means that crises may erupt with little warning and from unknown or unanticipated approaches."

- Admiral Philip S. Davidson,
Commander, U.S. Fleet Forces Command

Approaching and engaging a type of warfare means that your forces have some sort of foundational understanding of the enemies' operating concept and that the character of war is recognized. As stated by Admiral Davidson in his Commanders Guidance: Fleet '15 Vision, there has been a proliferation of threats around the globe that appear to blur the lines of conventional warfare. A fusion of efforts that blend the irregular with the regular threats appear to be the new norm rather than open conflict.

The genesis of this project understood that there is no common analytical framework to understanding Hybrid Warfare. It is seen that to address the challenge there must be a starting point to create a basis for understanding. This effort must be done prior to creating planning methods or decision-making matrices. The understanding of the enemy is key to this effort. Prior to effective engagement in countering hybrid warfare, the enemies' organization, operations, and tools/instruments of warfare must be analyzed. After that work, efforts to deter, mitigate, and counter the hybrid threat can then be developed.

Part of the difficulty is that numerous definitions and lexicons exist and disagreements occur simply due to the vernacular. Thus, due to problems with vocabulary, our approaches to the threat become difficult because of the inability to shape the warfare across multinational entities. In the end, we may all possibly be referring to the same concept, but the language seems to interfere.

How do we get there?

Previous efforts have used a model of examining prior conflicts and current events to assist in describing hybrid warfare. Other articles use those same conflicts to shape completely different thoughts and concepts. This project plans to develop a Concept Map to analyze hybrid warfare in a different way. Essentially, creating a baseline of all academic thought on the topic and then moving out from that basis of knowledge.

The Concept Map will entail an extensive literature review of hybrid warfare, analyzing existing theories, concepts, and doctrines. Along with a literature review, this will also encompass looking at historical case studies and interviews with experts in the field. Workshops and seminars will be used to gather these resources to assist the methodology. A culminating effort may include experimentation or red-teaming.

The construction of the Concept Map involves three distinct areas. The first step is to examine the vocabulary and determine how terms are used when talking about this type of warfare. Figuring out the common constructs and established differences in conflicting theories is what appears to hamper any effort to counter hybrid warfare. Theoretically, this would become the launching pad for any future efforts to combat hybrid warfare. Second, the Concept Map provides a means to identify gaps in previous concepts. With those gaps identified, the project will examine how to seam those areas where academic rigor appears to be lacking. Third, and most importantly, cooperation with current efforts in counter-

ing hybrid warfare are vital to fighting it in the future. This research must work closely with academia and other entities such as NATO- Allied Command for Transformation (NATO-ACT), that are also working to solve this threat. There are numerous parallel efforts on-going in this field and this project intends to engage and leverage those other efforts.

From the Concept Map, the analytical framework is developed with the intention to shape future efforts for operational planning to counter a Hybrid Warfare strategy. This framework should also assist in the determination of capabilities and capacities to counter a hybrid threat existing within a given nation or alliance. Again, it is only through understanding the threat that an alliance or nation can begin thinking of countering it effectively.

The Future

The future appears to be that hybrid warfare is the preferred method of modern conflict. It may be the precursor to larger scale conflicts, but in the hands of adaptable challengers, the methods and the results give the impression that they work. The enemy is highly adaptable and ready to exploit weaknesses. This brand of warfare challenges NATO methods of operational planning and the way their forces are organized. In the end, this must also spur a change in approach and prioritization of assets to combat the modern threat. Given the track history of thought on hybrid warfare, this will be no easy effort. However, while nations and entities around the world continue to chip away at NATO interests, it is imperative that hybrid warfare be comprehensively addressed. ☸

U.S. Department of Defense

In 2014, USS THEODORE ROOSEVELT launches a rolling airframe missile in the Atlantic Ocean. The test focused on its combat readiness and its ability to defend against anti-ship cruise missiles and other asymmetric threats.

CAPT Marv Carlin 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 PLANNING FOR THE FUTURE

CDR Steinar Torset, NOR-N
CJOS COE

NATO

Militaries conducting maneuvering exercise, DYNAMIC MONGOOSE 2015.

NATO has been put under pressure lately, and the focus is very much switching from Crisis Response and Cooperative Security to Collective Defense.[1] All of the three core tasks are of course important to NATO, but it still remains important for NATO to be able to look into the future in order to prepare the alliance for future challenges. This work is an important part of the continuous transformation effort led by NATO through their HQ Allied Command Transformation (ACT). The Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) is participating in the work of looking into the future focusing on the maritime and littoral aspects of future operations in a joint context.

When NATO governments are trying to deal with several crises, including Russia's aggression in Ukraine, the activities of Islamic State of Syria (ISIS) and the mass migration in the Mediterranean Sea region, it can sometimes be hard to stay focused on the long term (i.e. 25 years) required for effective military preparation. CJOS COE has been participating in projects that are specifically looking into the future in order to describe evolving maritime elements in the maritime domain which will contribute to the military implications for the alliance, and by that inform the NATO Defense Planning Process (NDPP) for future capability requirements.

Strategic Foresight Analysis (SFA)

Every four years NATO produces an analysis describing the most up-to-date trends that might influence the future security environment of the alliance. As NATO's area of interest is growing the analysis is for all practical purposes a global assessment of the future. The latest report was issued in 2013, and this report describes a number of trends that might impact the ability for NATO to conduct operations in the maritime domain. The report is written in close cooperation and with substantial contributions from national think tanks and academia. The report is describing the future by using 5 different themes (see Figure 1):

- Political: Examines the shift of global power and political structures. It defines what is called 'The Polycentric World' meaning the world is going to become interconnected and there will likely be a development where non-state actors play a more influential role .

- Human: Covers the aspects of changing demographics and urbanization .

- Technology Development: Describes the acceleration of technology development and the increased access to technology in the future.

- Economics and Resources: Explains how the world will face challenges related to energy, food, water and other natural resources essential to sustain all aspects of what we today regard as daily and normal activities.

- Environmental: Addresses climate change and its possible implications.

In 2015 an interim report was initiated to review the identified trends and to describe potential new trends that have emerged; the main SFA report will be delivered by ACT in 2017.

Framework for Future Alliance Operations

The aim of Framework for Future Alliance Operations (FFOA) is to identify security implications aligned and prioritized with the core tasks and describe potential ways for conducting the core tasks which may have military implications in the long-term (out to 2030). The starting point for FFAO is the SFA report and the project has so far identified "Instability Situations", "Strategic Military Perspectives" and "Military Implications".

Instability Situations

Based on the trends described in SFA, the work continued with describing what was called "Instability Situations". Instability Situations describe possible instances of conflict where NATO could become engaged in the future. They provide a background against which to develop perspectives on conflict that may drive future military and other requirements. The Instability Situations cover a broad spectrum of crisis and conflict that NATO could face in 2030, from the low end consisting of large-scale disasters (either natural or man-made), disruptive impacts of migration, political and economic attacks, or assaults on critical infrastructure, to the high end of state-versus- state warfare. The spectrum of potential opponents that NATO may encounter includes non-state actors working alone or in collaboration and coordination with states or other non-state actors.[2] Some 50 different situations were identified as possessing the potential for future instability and/or creating a potential for increased security risks for the alliance. It became clear that there was a requirement to reduce the number of different instability scenarios, and they were merged and consolidated into 10 comprehensive instability situations.

One example of an Instability Situation is classified as the 'Shift of Global Power'. This describes how the rebalance of power from the west to other regions might present political and economic challenges to NATO members in the future. Another example is 'Urbanization' which is actually a result of several trends such as continuous population growth, migration and an increasingly connected world. The urbanization trend also indicates that the majority of urban growth will take place in coastal regions. This points to the possibility of a crowded, complex, and littoral future operating environment for NATO.

"NATO's focus is transitioning from Crisis Response and Cooperative Security to Collective Defense."

Strategic Military Perspectives

The instability scenarios outlined above were next put into a military context through the establishment

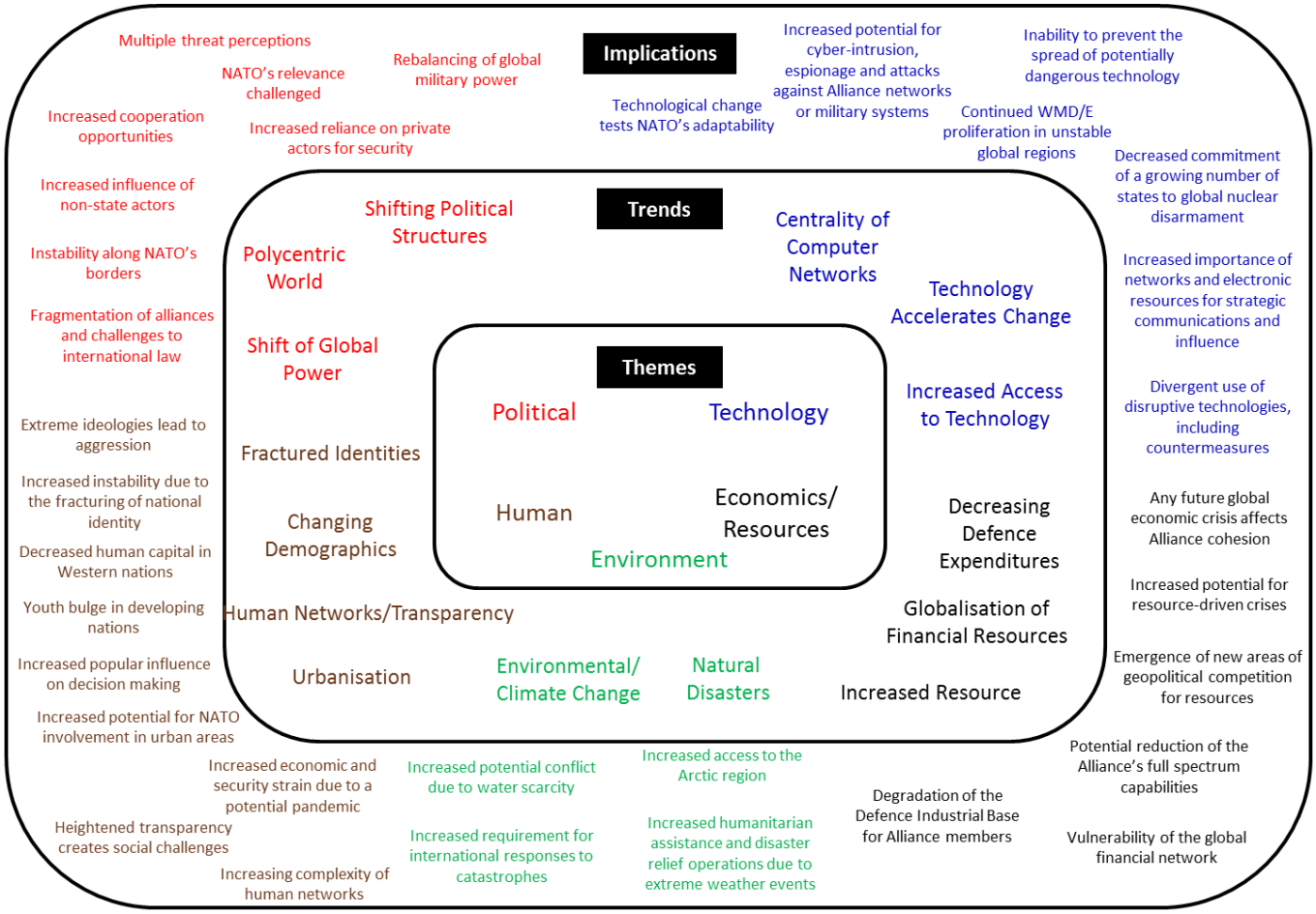


Figure 1. The connection between themes, trends and implications (NATO ACT)

of Strategic Military Perspectives (SMP). The SMPs are Bi-SC military guiding principles that aims to inform long-term NATO defense planning, specifically NDPP Political Guidance.

Military Implications

The final and important outcome of the FFAO process is to inform the long term planning process that can provide guidelines to capability requirements for potential future operations in NATO. Initially the plan was to identify implications for each specific domain (maritime, air, land, etc). However, since several of the implications are common for all domains, ACT chose to identify the implications and describe the capability requirements based on the Capability Hierarchy Framework. This framework describes the requirements for all aspects of future capabilities related to establish, prepare, project, engage, sustain and protect NATO forces in order to create a sufficient and effective presence at the right time and with the right forces. It will still provide useful input to the long term process of transformation, but it will inevitably be more complicated and challenging to derive the 'So Whats?' for the different and specific domains. Following the trends, the next operating scenario for NATO could be in an urban, coastal and hybrid conflict. This will challenge capability requirement and future planning, as they will have to balance this against a reinforced focus on collective defense within the Alliance.

An example of a military implication would be an increased use of the coastal zones for aquatic food pro-

NATO

Exercise DYNAMIC MONGOOSE: French Maritime Patrol Aircraft ATL2 in Sola air base (Norway).

duction essential to feed a growing population. This could have an impact on NATO's ability to conduct expeditionary and littoral operations in such a zone. The military implication would be that NATO might need to consider alternate ship-shore connectors when conducting expeditionary and amphibious operations where it may not be possible to operate across the beach.

Conclusion

In order to remain relevant as a military alliance, NATO needs to have a certain understanding of the future security environment and the SFA and FFAO processes help to shape this understanding. The SFA and FFAO are not processes which consider whether NATO should or should not get involved in any specific scenarios, but they will describe what NATO can expect of the future and what requirements NATO needs to meet to enable the effective conduct of operations in this future environment.

CJOS COE will continue to contribute to this work by providing subject matter expertise in the different aspects of maritime operations as part of the overall military implications for the different scenarios developed in the SFA/FFAO process. ☸

1. NATO's core tasks as described in the Strategic Concept of 2010.
2. ACT Workshop Final Report, 12 June 2014, http://www.act.nato.int/images/stories/events/2012/fc_ipr/final_report_ffao_ws5.pdf.

CDR Steinar Torset 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.

FOLLOWING THE MULTI-NATIONAL CAPABILITY DEVELOPMENT CAMPAIGN

CDR Gerrit Wiegman, NLD-N
CJOS COE

NATO

Portuguese, British, and U.S. marines perform exercise storming a beach.

The Multinational Capability Development Campaign (MCDC) is a follow-on initiative to the Multinational Experiments (MNE) initiated by United States Joint Forces Command in 2001. The first cycle started in 2013 and supported military forces by improving their operational effectiveness in joint, interagency, multinational, and coalition operations. While the MCDC campaign maintains the core ideas of the MNE series, it has significant changes in scope improving relevance.

"MCDC 2015-2016 further investigates the capabilities required to plan and execute globally integrated operations across geographic, national, and organizational boundaries."

The theme of MCDC 2013-2014 was Combined Operational Access. The campaign addressed the Operational Access challenge by focusing on the versatile, agile capabilities required to project combined forces into an operational area with sufficient freedom of action to accomplish their mission. Recognizing that the military instrument of power should never be wielded alone, MCDC 2013-2014 addressed planning and coordinating the employment of all relevant instruments of national, multinational and international power in the operational environment. It concentrated on enabling forces and other capabilities from different nations to swiftly combine for employment in an orderly, efficient and integrated manner with little to no modification or conversion required. The specific problem sets addressed by the MCDC 2013-2014 program of work were categorized into seven distinct Focus Areas (FA) proposed and led by one or more of the contributing partners.[1]

CJOS COE participated as key contributor in two of these FAs: Combined Operations from the Sea Through the Littoral (COSTL) and Maritime Approach to Combined Operational Access

(MACOA). Within these two FAs, opportunities and challenges were explored covering by joint, multinational or coalition operations being conducted from the sea.

The COSTL study was based on the NATO Joint Sea Based Operations (NJSBO) Concept. At the time of this study this concept was still in draft form; it was approved in March 2015. The idea of NJSBO is to project sustained joint effects across a wide spectrum of the Alliance's operations from a base physically located at sea. A major conclusion from the analysis was that a sea base can bring operational and logistic efficiencies to an operation under specific circumstances, such as the lack of host nation support. This was seen as the strongest advantage of COSTL. Fulfilling warehouse requirements and providing an operational base to conduct and sustain joint, multinational, or coalition operations ashore. This is what sets COSTL operations apart from conventional expeditionary or amphibious maritime operations. A second major conclusion was that a sea base offers better protection of operational assets from direct threats to the extent that the necessary local maritime control and air superiority can be ensured. It must still be kept in mind that threats (e.g. mines, submarines, small boats, artillery/mortar fires, other symmetric or asymmetric threats, etc.) must be evaluated as a COSTL operation . COSTL offers options in support of military missions but implementation will not come without costs since most individual nations lack specific COSTL capabilities and those that do have such capabilities generally lack them in any substantial numbers. The team further concluded that at present it is more realistic to focus on existing capabilities rather than the procurement of costly new platforms; in other words, focusing on the organization of existing capabilities, headquarters and forces as a whole. Detailed recommendations focus on sharing existing capabilities. The joint, multinational or coalition nature of COSTL missions dictate that success can only be achieved by drawing together all the recommendations of this study. Gaps in any of these areas will adversely impact the ability of COSTL to function effectively and efficiently. The conclusions of the study form the foundation for the implementation plan of the NJSBO concept. This implementation plan is currently under development.

NATO

Polish Naval Special Forces Unit GROM participating in NATO exercise TRIDENT JUNCTURE 2015.

The second MCDC focus area in which CJOS had a leading role was MACOA. The Maritime Approach to Combined Operational Access Concept and Practices Guide is designed to assist nations, their military forces, and most importantly, military commanders, in reducing the friction and mission risk incurred when nations quickly combine to project military forces into the littoral. To do this, MACOA presents a proactive approach offering a common framework of eight discrete practices. The MACOA Practices Guide is organized in three parts. Part 1 describes the concept, scope, challenges, and framework of the MACOA project. It is critical to understand and internalize the unique littoral environment, the inherent dangers of operating in this environment, and how this document is structured to most effectively apply the concepts presented in MACOA to the littoral environment. Part 2 of the MACOA Operational Implementation describes how a

NATO

Allied forces practice amphibious assault near Ustka, northern Poland during BALTOPS 2015.

commander with littoral operational responsibility could apply MACOA to assist in designing and directing steady-state maritime operations. Part 3 consists of eight specific MACOA practices to apply the concept. While not a distinct checklist, the MACOA practices are supported by numerous examples and five related case studies. The practices detail specific considerations and applications a commander should utilize to shape, execute, and assess their operational approach in their littoral area of responsibility.

The theme of the MCDC 2015-2016 is the Interoperability for Future Combined Joint Operations. While the MCDC 2013-2014 campaign was focused on developing the capabilities required to project combined forces into an operational area with sufficient freedom of action to accomplish their mission, MCDC 2015-2016 further investigates the capabilities required to plan and execute globally integrated operations across geographic, national, and organizational boundaries. The campaign focus is on building and maintaining regional security. In fact, multinational and coalition partners must have the capability to successfully plan and execute globally integrated efforts to build and maintain regional security, using a global comprehensive approach in those areas where they have mutual direct and indirect national interest, to prevent, deter, mitigate or respond to destabilizing events and activities. The specific problem sets addressed by the MCDC 2015-2016 program of work is categorized into ten distinct FAs.[2]

CJOS COE is participating as a key contributor and observer in three FAs: Countering Hybrid Warfare, Countering Unmanned Autonomous Systems and Joint, and Combined Operations in and from Confined Waters. The campaign has started and is expected to deliver results at the end of 2016. ☸

1. Multinational Capability Development Campaign 2013-2014, Program of Work.
2. Multinational Capability Development Campaign 2015-2016, Program of Work.

CDR Gerrit Wiegman 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.

EVOLVING MARITIME CYBERSECURITY

CDR Jonathan W. Sims, USA-N
LCDR William T. Rimmer, USA-N
CJOS COE

CCICADA

Illustration of a sophistically integrated ship's bridge system.

Despite the attention generated by the media's coverage of cybersecurity attacks ranging from the private pictures of celebrities, details of philanderers, and the great troves of personally identifiable information (PII) pulled from government data warehouses, there remains the over cast of persistent as well as devastating cyber threats that receive remarkably little or no media attention. Although these hazards are not commonly exposed, they have the ability to present significant harm to civil infrastructure, public safety, national security, and economic stability. The vulnerability of networked and automated platforms in the maritime environment represents one such understudied and underestimated area of concern.

According to U.S. intelligence officials, the newest oil rigs, some of which cost upwards of $1 billion, employ cutting-edge robotics technology, but the software that controls a rig's basic functions is often antiquated.[1] Unfortunately, many maritime systems utilize decades old supervisory control and data acquisition (SCADA) software; coded in an era of which information security was nonexistent or a complete afterthought. Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) has taken notice of this grave danger by assembling an international coalition of academia, industry, government and military organizations to better understand and spread awareness of this impending threat within the maritime domain.

Cyber and the Maritime Domain

Over the last few decades, maritime organizations initiated great strides in securing networking capabilities between vessels and oceanic platforms in an effort to achieve optimum maritime territory awareness. Conversely, there is growing concern that the required modernization efforts now expose maritime stakeholders to significant attacks via cyberspace conduits. Automated and integrated operating systems network communication and port operations to improve efficiency and strategy. Consequently, this intricate hierarchal classification of systems presents hackers with a tantalizing target. Often, maritime regulations and policies focus primarily on the physical aspects of security and safety, and fall short of protecting the weaknesses allotted to the cyber element. Policy makers have become more cognizant of the maritime cyber threat and are working to create or improve policies that better address malicious hazards. The Maritime

Transportation Security Act of 2002 (MTSA) (Pub.L. 107–295) is an Act of Congress enacted by the 107th United States Congress to address port and waterway security.[2] It was signed into law by President George W. Bush on November 25, 2002. It was designed to require the design and implementation of quality security plans for ports; mandated improvements in screening seaport personnel; increase international collaboration on port security, and improve cyber maritime domain awareness. The MTSA (2002) evolved into an international effort spurring collaboration between ports and policy makers securing vast improvements in the physical safekeeping of the waterways. However, what is not addressed in the document is the invisible and intangible threat of cyberspace. Absent is a detailed plan of emphasis to strengthen the technological pathways necessary to evade cyber terrorism.

"Technological advancements have provided hackers a means of using cyberspace to infiltrate and take over control systems of modern maritime vessels and seaports."

It is evident that there is pressure to remain in step with the lightning fast evolution of technology, even at sea. The motivation to network mission essential vessels underway through technologies such as the Global Positioning System (GPS), modern automation, and wireless data communications offers nation states unimagined data centric awareness of the trade and traffic just off their shores as well as the origins of goods heading into their ports. Modern automation and statistical computerized systems radically increases the throughput and efficiencies of ports as well as reducing the manpower and personnel required aboard merchant ships. Yet, maritime networking and automation technologies equally increase the risk of susceptibility of an infrastructure attack capable of impacting guidance modules and providing access to top secret strategic plans. In short, maintaining modernized networks alongside antiquated capabilities deliver hackers a means to infiltrate and hijack the control systems of modern seafaring vessels.

For example, in June of 2013, students from the University of Texas built a briefcase sized device to wirelessly hijack the GPS input connected to a yacht's navigation system. The wireless device allowed the students the ability to "ghost" drive the ship through several turns and onto a path mapped several hundred yards off the course of its intended track. The attack relied on remotely spoofing thus instead of jamming the GPS signal, no alarms sounded and the ships electronic chart falsely logged a straight path. The device operated under similar principles to demonstrate Iran's claim to have taken control of an American drone in 2011 after it entered Iranian airspace from its eastern border with Afghanistan. Today, Iran has claimed it managed to reverse-engineer the devices cyber capabilities and that they are able to subsequently produce a line of unmanned aircraft. During the Black Hat Information Security conference in 2013, a company demonstrated the proficiency to hack the controls of an oil rig remotely cycling the pumps to force a severe pipeline rupture. Earlier this year, Reuters University reported a cyber-intrusion that disabled a floating oil rig and caused it to critically heel to one side.[3] While attacks to this end have been either limited in scope, confined to demonstrations, or unidentified maritime stakeholders must accept and address the reality of unidentified motives and focused plots to infiltrate, incapacitate, and win wars through virtual means.

The threat extends far beyond the happenings

summarily exposed and described. The realization and awareness of this particular threat is being recognized through a growing list of articles and reports by Senior War Command & Staff Colleges, the U.S. Government Accountability Office (GAO), trade press and other reputable sources. Many of these documented sources highlight the potential of disruptions to defense and commerce that encompass significant breaches such as problematic delays to scuttled ships and environmental catastrophes. A GAO report from June 2014, titled "Department of Homeland Security (DHS) needs to better address Port Cybersecurity", highlights the lack of attention paid to the cybersecurity of port facilities and shipping infrastructure. The DHS agreed with the GAO's recommendations for both the U.S. Coast Guard and Federal Emergency Management Agency to better assess and prepare for cyber based threats to maritime stakeholders. Academic journals and media outlets are also raising concerns about the extent of the threat.[4] A recent Naval War College Review article devoted to cyber conflict in the maritime domain stressed "cyberspace favors the offensive military capabilities of adversaries and enhances their potentially destabilizing effects on the nature and level of interstate conflict in the coming years."[5] Virtual risks within the maritime domain impact critical infrastructures that must be evaluated and analyzed for resistance to such threats. Essentially, it is time to reexamine the urgencies and techniques for safeguarding against strategic terrorism and improve international cyber resilience.

NATO

Abundant amounts of energy resources, such as oil and liquefied natural gas, are produced offshore and transported by sea. Plagued with the risks of terrorist attacks, piracy, and natural disasters, there is growing concern about the potential consequences of cyber-attacks against this maritime infrastructure.

Identifying Risk

When discussing information security risk analysis, many security practitioners present the following formula: Risk = Threats x Vulnerabilities x Impact. A compelling concept, risk fluctuates according to variations of time, nature of threats, and instances of vulnerabilities. Concurrently, risk must be assessed periodically based on changes in the environment.[6] CJOS COE does not intend to use this formula as a mathematical approach, but rather use threat, vulnerability and impact as concepts; that, within the context of performance and interaction, can be examined to determine the probability of a potential outcome. In the world of cyber-terrorism numerous possibilities exist that are intermingled with virtual contamination of sophisticated systems onboard a ship. A formal analysis of a risky action needs to take into account the urgency of the scenario, outcomes, and mitigation of such an adverse action. CJOS COE believes that this approach is relevant to their study of virtual entities impacting strategic cyber capabilities that are adept at disrupting communications and transmissions at sea.

Cybersecurity in the maritime domain is both complex and heavily populated with constituents who share the responsibility for security between many different national and international agencies and groups as well as commercial, public and private entities. Hence, an effective maritime cybersecurity (MCS) plan must holistically include a mosaic of various stakeholders, interest, regulations, and governance to succeed. As time persists, entities solely mitigating and addressing cyber threats have become increasingly

antiquated and ineffective; more cooperative and collaborative measures must be identified.

In the context of cybersecurity, technical resiliency entails the capability of a maritime vessel to continue operations at the height of a disruptive event and physically displaying the capacity to return to normal operations once the event has been addressed. Ensuring effective technical resiliency against a maritime cyber-attack entails a proactive approach that includes the following actions:

- Remain abreast of current and potentially repetitive international maritime cyber-attack themes and targets.
- Identify and secure personnel equipped with the technical expertise onboard vessels to immediately identify and thwart virtual crime attempts.
- Identifying critical mission-supported information and technology assets .
- Implementing controls to protect such assets from harm.
- Implementing controls to sustain the ability of those assets to operate under stress and recover from disruptive events.

Developing processes to maintain and repeatedly carry out protection and sustainment activities.
Researching and evaluating measures to drive and determine best practices.

Conclusion

The concerns of protecting platforms and infrastructure within the maritime domain from cyber-attacks have been an afterthought by many operational commanders. Many navies, as well as public and private maritime entities, lack strong resiliency mechanisms. This is partly due to the fact that these maritime actors are primarily private or public enterprises, and information sharing among this group is limited due to privacy concerns and additional top secret proprietary issues. In addition, there is tension between technological progress to increase performance and the closing of ever-emerging new gaps opening the sea to cyber- vulnerabilities. It is CJOS COE's intent to find common ground and develop amiable means to foster a maritime industry culture of increased awareness – cooperation and collaboration among different stakeholders, military, and academia. In a competitive global landscape, maritime facilities must also protect sensitive business information and proprietary data. These efforts are critical not only to the maritime industry, but also to the industry's stakeholders in the U.S. Department of Homeland Security (DHS)and Department of Defense.[7] The outcome of the study aims to lead to further exploration towards better understanding of cybersecurity (including cyber defense and cyber warfare), information sharing, legislative initiatives, shared capabilities, and ultimately greater synergy, all with regard to the improving sustainability of virtual capabilities within the maritime domain. ☸

1. Richard Sale, "Beating an advanced persistent threat." 1 May 2013, http://www.oedigital.com/technology/safety-security/item/3165-beating-an-advanced-persistent-threat?tmpl=component&print=1.
2. Greg Jaffe & Thomas Erdbrink, "Iran says it downed U.S. stealth drone: Pentagon acknowledges aircraft downing," 4 December 2011, The Washington Post,.
3. David Dickman, "Reducing cyber risk: Marine transportation system cybersecurity standards, liability protection, and cyber insurance." (U.S. Coast Guard Proceedings, Winter 2014-2015).
4. U.S. Government Accountability Office (GAO), "Maritime Critical Infrastructure Protection: DHS Needs to Better Address Port Cybersecurity," (GAO-14-459, 2014).
5. Peter Dombrowski & Chris Demchak, "Cyber War, Cybered Conflict, and the Maritime Domain," (Naval War College Review, 2014), http://www.thefreelibrary.com/Cyber+war,+cybered+conflict,+and+the+maritime+domain.-a0366344681.
6. GAO, "Information Security Risk Assessment: GAO Practices of Leading Organizations," (GAO-AIMD-00-33, 1999).
7. Thad Odderstol, "C-Cubed: Increasing Cyber Resilience, Awareness, and Managing Risk," (Proceedings, Winter 2014-2015).

CDR Jonathan W. Sims and LCDR William T. Rimmer are staff officers at CJOS COE in Norfolk, Va. For further information on this subject, they may be contacted at usff.cjos.coe@navy.mil.

IMPROVING INTEROPERABLE COMMUNICATIONS

WO2 Trevor R. Austin, GBR-RM
CJOS COE

NATO

Spanish Navy participating in NATO group passing exercise (PASSEX).

Multinational Operations represent a unique challenge to today's maritime forces in establishing effective support for Command and Control (C2). Dramatic and far-reaching changes in doctrine, organizations, and most of all technology are altering the conduct of modern warfare. These ongoing changes are revolutionizing the information that a commander has available to maintain their situational awareness, make decisions, and coordinate the application of forces across the full spectrum of warfighting. In support of this maritime multinational effort, the United States Department of Defense (DoD) has developed the Mission Partner Environment (MPE), a concept that will provide communication interoperability with NATO's Future Mission Networking (FMN). The intent of this future concept is to ensure reliable and interoperable communication persists with other NATO members and supporting mission partners.

"The intent of this future concept is to ensure reliable and interoperable communication persists with other NATO members and supporting mission partners."

Future Mission Networking and Mission Partner Environment Concepts

The FMN concept builds upon the operational experiences and lessons learned from the Afghan Mission Network (AMN). During the 2009 troop surge in support of Operation Enduring Freedom, the predominant use of Secret Internet Protocol Router Network (SIPRNet) by U.S. Forces in Afghanistan constrained the Commanders' ability to combine and/or tailor Allied and Coalition forces to realize their full warfighting potential with combating the insurgency. The inability to speak with immediacy to all mission partners inhibited the commanders' ability (at all levels) to rapidly direct International Security Assistance Force (ISAF) forces in Afghanistan, thereby increasing risk of failure for the mission and

undermine effective interoperability of coalition forces. The need to reduce this risk and increase the overall effectiveness of the coalition task forces spurred the development of the AMN. The AMN is the federation of several networks linked to a NATO-Core mission network, complying with NATO security and information assurance (IA) policies; at its height (circa May 2011) there were over 48 NATO and mission partner nations successfully operating on the AMN. The FMN framework is neither 'Future', nor just a 'Network'; it is a "Framework" that is intended to influence the policy, transport, systems, tools and applications; this along with a concept of operations and agreed upon Joining, Membership and Exiting Instruction (JMEI), between mission partner nations and U.S. COCOMs. The FMN capability provides the means for commanders to effectively share their intent, communicate mission orders, and empower decentralized execution when operating with mission partners. The evolution from "need to know" to "need to share" was a critical lesson learned from Operation ENDURING FREEDOM. This fundamental tenet of the FMN concept will definitely be expected to reflect the MPE architecture. What was realized in the AMN, and conceptualized in the FMN, has morphed into the MPE, this being the U.S. implementation of FMN concept, but still viable.

NATO

A sailor of German Navy frigate HAMBURG is visually sending a message in Morse Code via spotlight during Exercise TRIDENT JUNCTURE 2015.

MPE Alignment with the Joint Information Environment

The MPE and the Joint Information Environment (JIE) are separate, but closely related Information Technology (IT) environments. The JIE will provide the infrastructure and services used by all U.S. MPE users and some external mission partners (U.S. Federal Government/Agency). JIE contributes to MPE by administering a computing environment supported by enterprise services, and a single security architecture (SSA) providing global cyber situational awareness for the entire consolidated DOD network. MPE users access JIE capabilities and services through a number of data centers and processing nodes; this flexibility and agility of JIE provides the ability to establish distinct and separate mission networks with multiple mission partner sets within a specific theater or when globally dispersed.

The MPE of today are characterized by multiple permanent or semi-permanent (Enduring) network enclaves as well as short-term (Episodic) configura-

tions, which tend to be more ad-hoc in nature. Each enduring enclave typically operates at a particular classification level (e.g. SECRET/REL) with a group of mission partners specified by a bi-lateral or multi-lateral information sharing agreement supporting a U.S. Combatant Commanders' individual or overall mission requirements. Each enclave provides its own infrastructure, services, or capabilities based on the needs of the mission or the individual enclave itself. Episodic examples of the MPE are often conducted at the Unclassified security level with infrastructure and services provided by the partners themselves, examples of this are the All Partners Access Network (APAN) which has been used for a number of Humanitarian Assistance and Disaster Relief (HA/DR) missions. There are several other examples of services being set up to support a mission requirement One such example is MERCURY. This service currently supports the European Union's Counter Piracy Mission off the Horn of Africa. Although this arrangement has been in effect for several years, it is still episodic in nature as it supports a mission not a function. Conversely, the Combined Enterprise Regional Information Exchange System (CENTRIXS) is an example of an enduring maritime system that entails an array of communication enclaves that continuously support steadfast and transient U.S. COCOMs globally.

CENTRIXS-Maritime

Today, many Navies' are having to operate a plethora of IT systems in order to allow them to collaborate in a multinational or coalition maritime task group. Both MPE and FMN concepts are designed to streamline these requirements. However, the challenge to the maritime community is to take these concepts (which are inherently LAND centric and static in nature) and make them work in the mobile tactical environment that naval forces operate today. CENTRIXS-Maritime (CENTRIXS-M) and its many enclaves are supporting current maritime operations worldwide that allow maritime coalitions to operate on a single information-sharing domain. This U.S. led network is continually adapting to meet the new requirements and challenges of not only the network, but more importantly the Coalition that these networks support. At the heart of this debate are the nations that conduct interoperable communications with CENTRIXS. These communities of interest come together bi-annually to discuss the current problems and issues at the Multinational Maritime Information Services Interoperability (M2I2) Board. M2I2 is the single coalition maritime Information Warfare working group focused on improving interoperability and collaboration in the CENTRIXS and Collaboration at Sea (CAS) arenas. The conference is a bi-annual event hosted in turn by those countries with a significant vested interest in current, and the more importantly the future, development of network architecture. Conference attendees include representatives from the U.S. numbered fleets, U.S. agencies which maintain CENTRIXS, and 25 plus nations that utilise CENTRIXS at a significant level. Representatives from NATO Supreme Headquarters Allied Powers Europe (SHAPE) J6 and NATO Communications and Information Agency (NCIA) also attend the event.

The MPE and FMN concepts federate networks to allow a 'seamless' passage of information, which in turn enables the Commander to exercise command and control across a multinational task force. The future of CENTRIXS-M and its requirement to support the ever evolving needs of the 'coalition' is still under debate. Despite the uncertainty, M2I2 is at the center of this debate ensuring that the MPE and FMN concept is being realized in the Maritime domain; ensuring future communication remains interoperable between all NATO members and mission partners. ☸

WO2 Trevor R. Austin is a staff officer at CJOS COE in Norfolk, Va. For further information on this subject, he may be contacted at

LEVERAGING UNDERSEA AUTONOMY FOR NATO: ALLIES MUST WORK TOGETHER TO AVOID FRACTION

Dr. Heiko Borchert
Daniel Mahon
Tim Kraemer

U.S. Navy

Autonomous maritime vehicle conducting undersea maneuvers.

In the 21st century NATO will operate in a different undersea domain. What used to be a rather benign environment will become increasingly crowded and contested. Among others this broad trend results from power projection in a new geostrategic environment, toughening competition for offshore resource exploitation and strategic maritime transport corridors as well as the proliferation of technology, which enables the deployment of different types of sensors that will make the undersea domain more permeable.

"Autonomy describes the degree to which tasks can be delegated between men and machines and among machines."

As a consequence, undersea autonomy is as much a driver for change in the undersea domain as it is a result of the developments changing it. If NATO nations want to benefit from the advent of undersea autonomy they need to understand the respective risks and opportunities. In particular, they will have to come up with a common understanding of how to operate autonomously in the undersea domain in order to avoid friction between the US as the current thought leader on undersea autonomy and the remaining Allies.

Undersea Autonomy is Different

Autonomy describes the degree to which tasks can be delegated between men and machines and among machines. Autonomy is not only about technology, but foremost about concepts, culture, and mindsets. Trust binds all of these elements together. As Armed Forces around the world have been using systems with different levels of autonomy for quite some time, it is tempting to assume that operational experience gained ashore or in the airspace could easily be transferred to another domain. This, however, risks ignoring the essential drivers and characteristics of naval operations in the undersea domain.

At first sight, the undersea domain seems the most challenging environment for the use of autonomous systems. The unstable physical characteristics (e.g., salinity of water, changing water temperature, water currents, reflections from seabed or surface resulting in multipaths) render certain tasks such as

communication and data transmission much more difficult than in other domains. While these specifics might reveal the limitations of today's technology, they should not be construed as fundamental show-stoppers. Rather, the undersea domain might be the place where autonomy could come to fruition faster than elsewhere. Why?

- All human ignorance about the oceans is astonishing. This might explain why the subject of undersea autonomy is attracting scientists in large numbers. The more scientific research is seen to be leveraging undersea autonomy in the advance of mankind's knowledge about the oceans, the more the respective technology is seen as an enabler for human progress. This creates a positive branding for undersea autonomy and paves the way for a better understanding of the benefits offered by autonomous undersea systems.

- Undersea traffic differs from air traffic, as there is – apart from very specific NATO/PfP regulations on water space management – no undersea traffic management regime. As a consequence regime discussion needs to start from scratch and can thereby find innovative ways to take into account the specifics of traditional and autonomous assets as well as the contribution of autonomy and automation for water space management.

- The C2 paradigm of the subsea forces is different from that in other domains. Subsea commands are at ease with delegating tasks to assets that neither need constant monitoring nor control as this might be detrimental to their operational success. Thus, the subsea culture seems more palatable to fully embracing the principle of mission command, which provides an optimal starting point for the use of autonomous systems.

- Opposition against weaponized remotely piloted aerial systems mainly stems from resistance against a certain type of waging war. Despite some countries considering the option, weaponizing autonomous undersea systems to use them in a similar way is not on the table these days. This removes a key stumbling block for public acceptance.

Key Benefits of Undersea Autonomy: Think Beyond the "3Ds"

Today's debate about autonomous systems centers around the "3D" paradigm suggesting that autonomous systems are useful because the can conduct "dull, dirty, and dangerous" missions. Reference to the "3D" paradigm is understandable: By portraying autonomy as life sustaining it might be easier for humans to accept it. However, the problem is that the "3D" paradigm is only focusing on risk avoidance. This is important, but neglects the true potential of autonomous technology. There is thus an urgent need to bring to the forefront the broader spectrum of benefits resulting from undersea autonomy:

- Greater flexibility. Autonomous systems are not just another means of transportation. Rather they should be seen as smart agents that can be tasked to accomplish different missions. Future forces blending manned units with assistive autonomous agents will provide political and military decision-makers with a greater number of options. In addition, greater flexibility provides for improved adaptability as forces will have more options to react to changes in their surrounding operational environment.

- Greater scalability. In today's undersea domain, the provision of effects is either "1" (e.g., fire a

Atlas Elektronik

Autonomous Undersea Vehicle, SeaCat, conducting maneuvers in the North Sea.

torpedo) or "0" (e.g., refrain from firing a torpedo). In the future autonomous systems and smart payloads could provide for graded effects such as disabling other undersea platforms, tracking and tracing enemy submarines and thus depriving them of their stealth advantage, or enabling undersea fencing to enforce sea control by electronic countermeasures. In doing so, autonomy supports the subsea forces' adherence to the principle of proportionality.

- Broaden mission spectrum. Autonomous systems can open up new opportunities to get closer to adversarial targets without being noticed. In addition, autonomous systems can provide advanced loitering and endurance capabilities thereby improving the "coping" power of subsea forces in attrition scenarios.

- Enable new ways to overwhelm adversarial forces. In combination with cheap expendable assets, autonomy will promote swarming as a new warfighting regime. Swarms would leverage all of the above benefits and provide armed forces with disruptive operational advantages in the fields of range and persistence, daring, mass, coordination and intelligence as well as speed and thus operational tempo.

Autonomy à l'americaine Will Be a Tough Race for Allies

As with many other military innovations, the US is currently leading the development of concepts and technologies for autonomous undersea systems. This poses challenges for NATO. For the US technological superiority is key to maintain political leadership. This leads Washington to perceive all challenges through a technological lens that is hard to share even for its most ardent Allies thus fuelling the risk of decoupling from Allies. This is also the case today with regard to undersea autonomy.

Overall, the U.S. drive for autonomous undersea systems is one response to the adversarial anti-access area denial (A2AD) postures that could limit future US power projection. Although Allies might share the need to push back adversarial encroachment upon the freedom of navigation at sea, not all will buy into the specific A2AD requirements. In a sense, the current debate about the need to nullify adversarial A2AD resembles the intra-Alliance discussion about the need to shift from territorial defense to international intervention and crisis management at the beginning of the 1990s. The lesson for the US should be to make the argument in favor of undersea autonomy broad enough for all Allies to have a stake in it.

In addition, US subsea forces face unique challenges resulting from the shrinking of the fleet whereas China's subsea fleet is growing. This opens the risk of capability gaps. The very specific capability requirements resulting from this development give room for ideas like the Large Displacement Unmanned Undersea Vehicle (LDUUV). The LDUUV perfectly fits into the US preference for "multi-capability big size" platforms. The risk is that LDUUV's are likely to extend today's problems related to technical complexity, maintenance, and costs from manned to autonomous

systems thereby deepening existing lock-in effects.

Conclusion: Getting Allies Back In

In the future, NATO will require a greater number of more capable and diversified autonomous undersea assets. For this reason NATO nations should work on a family of autonomous undersea systems that blend with more traditional subsea assets. This approach would leverage the strengths of all Allies and would provide opportunities for each partner to carve out a tailored role that reflects individual levels of ambition, undersea capability requirements as well as undersea industrial ambitions and capacities. For autonomy to boost Allied undersea capabilities, NATO should do the following:

- Re-animate the 2009 concept on "Maritime Unmanned Systems in NATO" since Allied operational experience has matured. This helps recalibrating the mission set to focus on more realistic tasks. Allied partners should welcome this step and bring in their own conceptual ideas on the use of undersea autonomy thereby helping the Alliance to tap into its broad pool of multinational experience.

- With four Centres of Excellence directly engaged in the maritime domain the Alliance has enough intellectual horsepower to develop and align concepts for underwater autonomy. In doing so, it will be important to hook up on conceptual work being done at other places such as SHAPE's a future Anti-Submarine Warfare roadmap, swarming concepts envisioned by the Joint Air Power Competence Center (JAPCC), and the cyber expertise at the Cooperative Cyber Defence Center of Excellence. Reaching out to the Centre for Maritime Research and Experimentation (CMRE) builds a bridge to experiment with different ideas on undersea autonomy.

- Undersea autonomy will depend on the contribution of innovative scientific and commercial players residing outside the traditional defense-industrial complex. The NATO Industry Forum could tap into this community by giving it a voice and bring innovation in from the outside. To this purpose joining forces with the European Defence Agency, that also maintains an Unmanned Maritime Systems program, would be most useful.

- NATO nations would be well advised to consider how autonomy will affect adversarial action in the undersea domain. The Counter-Unmanned Autonomous Systems project, which is part of the 2015-2016 Multinational Capability Development Campaign, provides a good opportunity to do so. In looking at adversarial benefits, NATO's red teaming will need to keep an eye on the cross-domain nature of autonomy and the disruptive impact of innovation stemming from commercial breakthroughs. ❁

1. James Jay Carafano, Autonomous Military Technology: Opportunities and Challenges for Policy and Law (Washington, DC: Heritage Foundation, 2014).
2. For more on this, see: Paul Scharre, Robotics on the Battlefield Part II: The Coming Swarm (Washington, DC: Center for New American Security, 2014).
3. Statement by RADM Richard P. Breckenridge and RADM David C. Johnson, Program Executive Office Submarines, before the House Armed Services Committee, Subcommittee on Seapower, 12 September 2013.

Dr. Heiko Borchert is proprietor of Borchert Consulting & Research AG, a strategic affairs consultancy, CDR (ret.) Daniel Mahon is a Naval Analyst with ThyssenKrupp Marine Systems, and Tim Kraemer is Head of Unmanned Systems with ATLAS Elektronik.

COUNTER UNMANNED AUTONOMOUS SYSTEMS (CUAxS)

LtCol Luca Bertonati, ITA-AF
CJOS COE

U.S. Navy

Unmanned helicopter prepares to land on littoral combat ship, USS FREEDOM.

The CJOS COE is actively supporting the Multinational Capability Development Campaign (MCDC) project on Counter Unmanned Autonomous Systems (CUAxS, where the "x" stands for the three domains: ground, air, sea). A total of fourteen Nations are contributing to the project with NATO ACT leading. The project is working on the development of an overarching CUAxS concept to explore the potential threats to military and civilian personnel, leadership and facilities and implementing protection and countermeasure solutions. Within the scope of this project, the team will also conduct a study exploring the evolving technology and future operation implications of UAxS in four domains (ground, air, sea and C3IS), explore policy recommendations on priority areas for both future capability implementation and integration with existing assets; develop policy recommendations on priority areas for both future capability implementation and integration with existing assets. Particular attention will be paid to CUAxS systems and related countermeasures capable of contributing to joint, multinational or coalition operations in a range of areas including strategy, operational concepts, interoperability, and capability development.

The CUAxS study examining evolving technology and future operations implications will also attempt to improve the understanding over the development and use of unmanned autonomous systems by military friendly and opposing forces. Over the past decade, unmanned systems have proven their value in military operations. Unmanned systems are evolving rapidly and the introduction of autonomous capabilities is expected to be the next step in the progression of development. Such systems, in state and non-state actor's hands, may have a critical impact on defense and security, and may become central to modern warfare. It is vital to understand the risk and potential threat posed by UAxS to military, civilian leadership and facilities to

"Over the past decade, unmanned systems have proven their value in military operations."

develop a concept leading to the future implementation of relevant and effective countermeasures. From a military perspective, UAxS are increasingly becoming part of joint, multinational, and coalition operations and can be used by state and non-state actors in a defensive or offensive across the entire spectrum of operations. The major objectives that the project will undertake is to develop viable, credible and reliable solutions:

Objective 0: Formalize UAxS definitions and characterization.

Objective 1: Understand how the existing military operational environment will be changed by the application of UAxS.

Objective 2: Understand how to counter adversary UAxS and protect friendly UAxS.

Objective 3: Identify the best practices related to legal and technical implementation of new UAxS systems and technology.

Objective 4: Conduct policy review on priority areas for both future capability implementation and integration with existing and future assets.

Future joint, multinational, or coalition forces will be expected to conduct operations using UAxS in an unconstrained, interoperable, and effective manner. They will need to protect these systems against exploitation and attack and also to counter adversaries' UAxS to allow the multinational force commander to project military force in globally integrated operations, and sustain it, in the face of armed opposition by increasingly capable enemies.

The approach used in the project provides a blended set of activities, all focused on contributing to the accumulation of knowledge and validity regarding the utility of the solution product under examination.

U.S. Navy

An X-47B Unmanned Combat Air System (UCAS) demonstrator aircraft is transported on an aircraft elevator aboard the aircraft carrier USS HARRY S. TRUMAN.

The design and analytical framework addresses a compromise between an adequate degree of analytical rigor at an acceptable degree of cost required to discover, assess and evaluate the CUAxS solution set with an understanding and acceptance that the ratio of rigor to resources are directly proportional. The proposed solutions will be a combination of four products delivered at the end of the CUAxS project:

Product 1: Study Report: UAxS in the Future – Evolving Technology, Operational Implications and Opportunities

Drawing from the project work strands, this study will integrate findings and describe the use of existing, emerging, and future UAxS to understand the military implications and opportunities for strategy, capability planning, force protection, and the conduct of

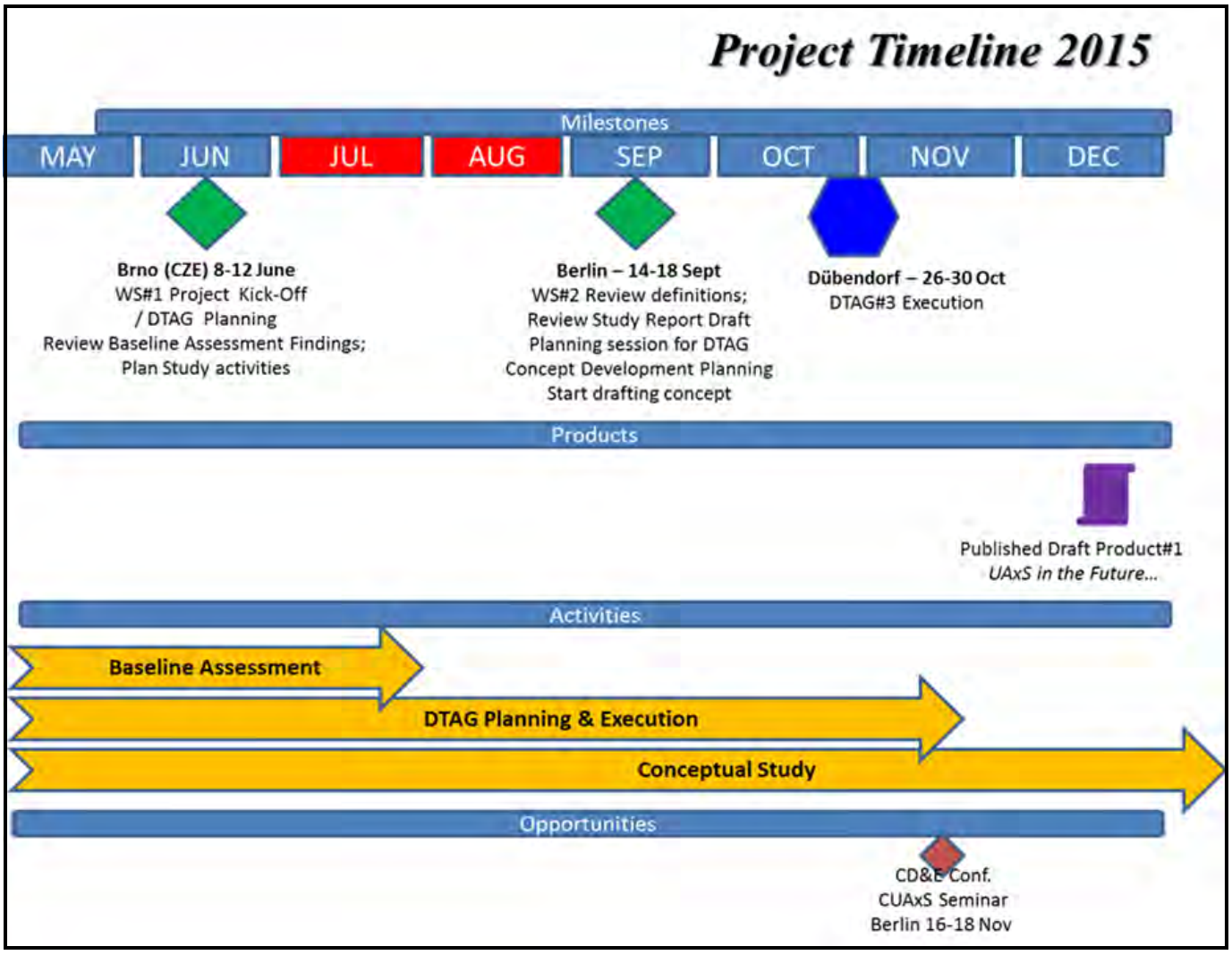


Figure 1. Project Timeline 2015

operations.

Product 2: Future Operational Concept on Counter-UAxS (DOTMPLFI)

This concept will recommend an implementation path for future CUAxS capability, integration and interoperability with current and future capabilities, and provide a baseline for helping the Nations address capability gaps. Furthermore, the concept will address all related DOTMLPFI domains and the embedded studies will focus on information concerning available, emerging, and/or required CUAxS technologies. The studies will incorporate a system architecture perspective, showing how the proposed concept could lead to the implementation of a CUAxS materiel solution, and how that solution would exist and be integrated in a typical military operating environment.

Product 3: Review of National Practices of New Technology / System Review and National Policy and Legal Regulations

This study will review national practices of new technology / system review and national policy and legal regulations. Additionally, the study will investigate processes that determine safety, reliability, legal and performance thresholds, and how they impact interoperability in joint, multinational or

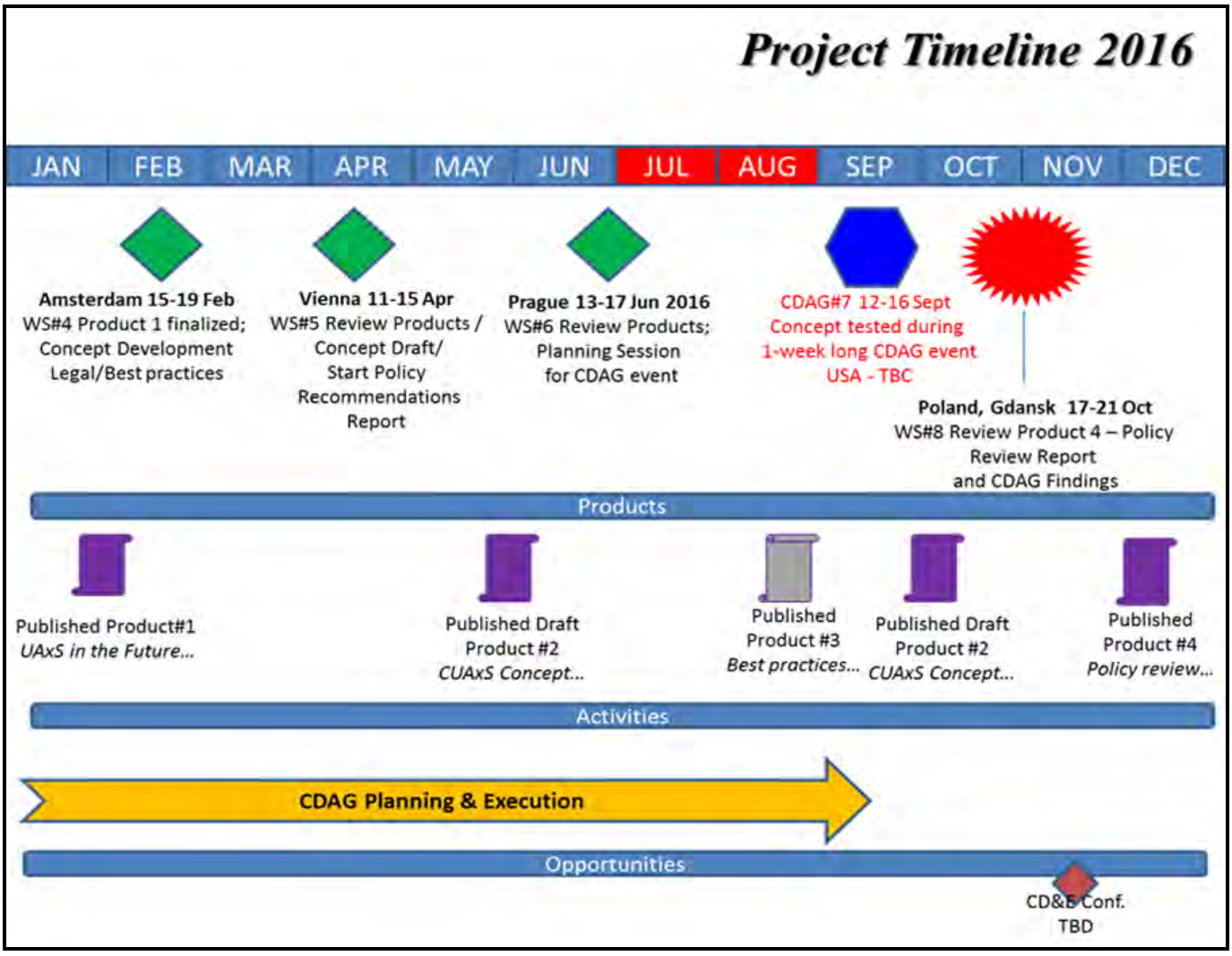


Figure 2. Project Timeline 2016

coalition operations.

Product 4: Policy Review of Priority Areas for Both Future Capability Implementation and Integration with Existing Assets

Results of this review will be presented in an integrated summary report, which will identify key issues and gaps surrounding counter-UAxS to inform senior defense policy-makers.

The Focus of CJOS COE

The CJOS COE is focusing its activities in the following areas: assessing the future UAxS operating environment, integrating operational concepts, doctrine and capabilities, improving interoperability and standardization and providing maritime expeditionary expertise. The CUAxS project, in line with CJOS COE scope and intent, represents one of the priority efforts to improve military effectiveness and interoperability with NATO assets, forces and capabilities. ☸

LtCol Luca Bertonati 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

German submarine U33 off the coast of Norway.

2015-2016 PROGRAMME OF WORK

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 2015-2016 CJOS Programme of Work is summarized below:

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 mission activities would enhance the effectiveness of future operations and inform FMN implementation. As a result, this document called for the Military Committee to task the strategic commands to produce a NATO Mission Thread Capstone Concept. This concept paper, developed in response to that tasking, is the result of significant analysis and several years of internal discussion within various NATO communities.

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

NATO Urbanization Concept

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. Unfortunately the publication doesn't significantly identify how and why they are created; what they are; and their roles and responsibilities.

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.

Exercise TRIDENT JUNCTURE 2016

Exercise TRIDENT JUNCTURE 16 (TRJE16) is an operational level headquarters training exercise designed to practice coordination between NATO Command Structure (NCS) and NATO Force Structure (NFS); 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. Along with surveying participating commands and personnel and analyzing future capability requirements, this study will allow CJOS COE to make recommendations for improvements to NATO Maritime ISR.

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)

CJOS, in cooperation with the Centre of Excellence for Operations in Confined and Shallow Waters (COE CSW) and the Turkish national Maritime Security Centre of Excellence (MARSEC), has undertaken a detailed study to examine how maritime situation awareness information sharing could be improved between entities on a global basis. This study was conducted through a gap analysis and then the assembly of potential solutions/best practices that could be used to address the gaps. Based on EXTAC 790 and lessons learned from Operation OCEAN SHIELD (OOS) and OAE, the COEs will make efforts to revise the MSA Doctrine.

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 has been 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.

NATO

Exercise TRIDENT JUNCTURE 2015, NATO's largest maritime exercise involving 36,000 personnel from more than 30 Allied and Partner Nations.

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 maritime operations, CJOS COE is responsible with developing and promoting maritime concepts and doctrine is a natural and active element of the AWG. ☸

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, Doctrine Development and Standards. ☸

There are 21 NATO accredited COEs:

NATO Accredited COE

In Accreditation Process

CENTRE OF EXCELLENCE WEBSITE LINKS

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)
www.cimic-coe.org

Cold Weather Operations (CWO/NOR)
https://forsvaret.no/en/education-and-training/coe-cwo

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

Air Operations Analysis and 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 and 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 (ENCOE/LIT)
http://enseccoe.org

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

NATO

Canadian HMCS HALIFAX and HMCS GOOSE BAY participating in NATO exercise TRIDENT JUNCTURE 2015.

CJOS COE REQUEST FOR SUPPORT

(Continued from page 7, "*How We Are Tasked*")

Originator:

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

Point of Contact/Subject 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
LCDR Jeffrey Betz, USA-N	Directorate Coordinator	2611
YNC Shonka Houston, USA-N	Admin Assistant	2453
IT1 Ana Moyer, USA-N	IT Support	2467
	STRATEGIC PLANS AND POLICY BRANCH	
CAPT Dermot Mulholland, CAN-N	Strategic Plans and Policy Branch Head	2450
CDR Steinar Torset, NOR-N	Strategy and Policy Analysis Section Head	2440
CDR Aytac Yavuz, TUR-N	SPA SO	2466
CAPT Marv Carlin, USA-N	SPA SO	2462
LTC Heiko Griesinger, DEU-A	SPA SO	2464
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
	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 Gerrit Wiegman, NLD-N	EO SO	2443
CDR Dimitrios Lymperakis, GRC-N	Maritime Operations Section Head	2448
CDR Russell Czack, USA-N	MO SO	2454
WO2 Trevor Austin, GBR-RM	MO SO	2960
CDR John Mihelich, USA-N	MO SO	2445

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

CJOS COE

OUR CONTRIBUTORS

der Bundeswehr
Universität München

TRANSFORMING ALLIED MARITIME POTENTIAL INTO REALITY