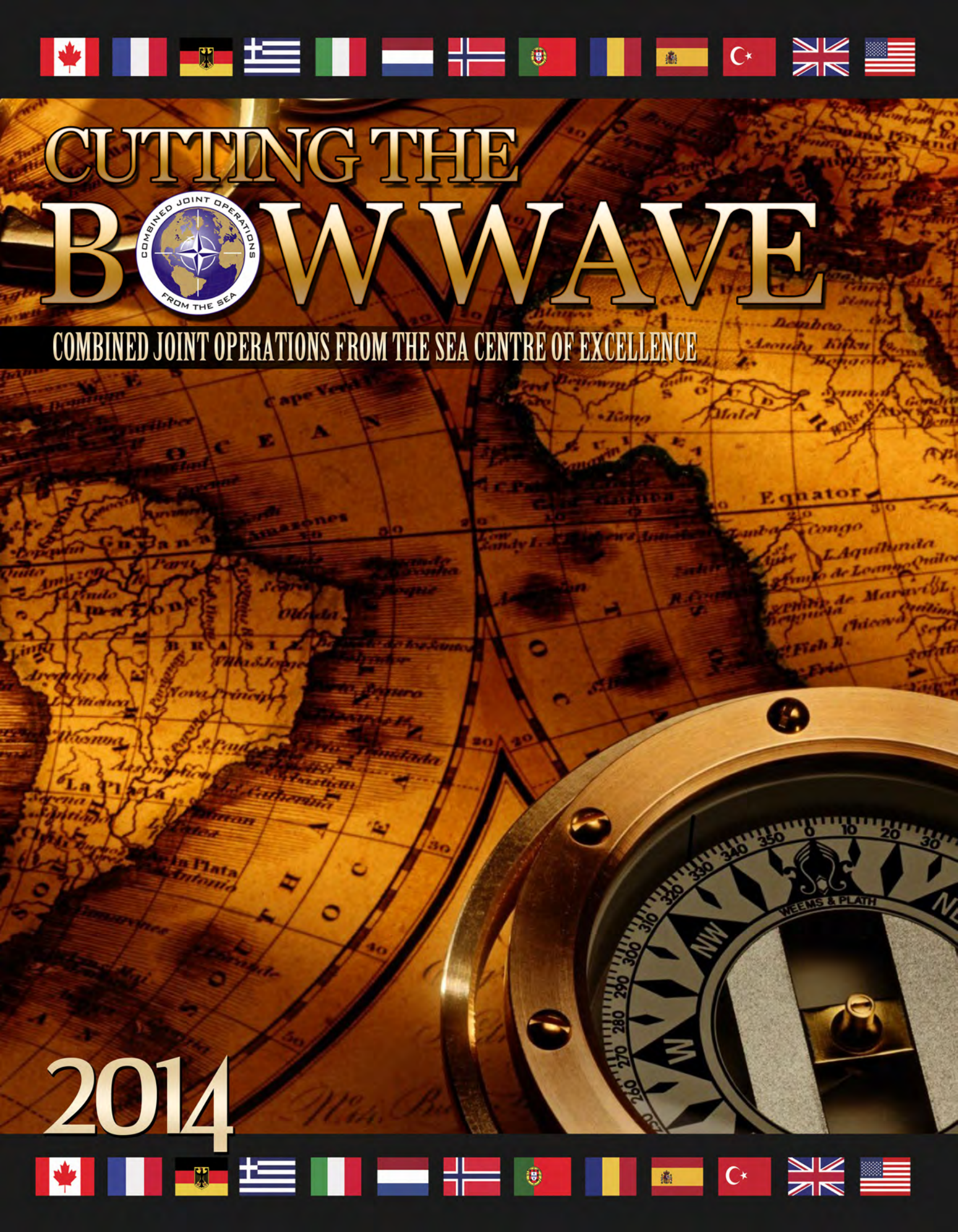

CUTTING THE
BOW WAVE
COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE
2014

CJOS Published Works

Cutting the Bow Wave 2013 (June 2013)
CJOS Author – CDR Patrick Nash, USA-N

This is a CJOS COE annual publication dealing with maritime security as well as all issues relating to and from the sea. Submissions were solicited and received globally from various organizations that have a specialized skill set in the maritime domain. Cutting the Bow Wave 2013's focus was the CJOS COE/COE CSW series of Maritime Security Conferences spanning from 2008 until 2012 and dealing with maritime security cooperation and awareness.

Future Use of Riverine Forces in Expeditionary Operations (February 2014)
CJOS Authors – LCol Gary Yuzichuk, CAN-A; WO2 Austin, GBR-RM

The Riverine concept paper aims to identify mission sets and key capabilities required of a Riverine Force, and propose a viable concept to FRMARFOR for the development of a riverine capability for expeditionary operations from within current force structures. The paper examined a select number of nations' riverine forces, reviewing their current doctrine, and defined the wide range of applicability, to include the fluvial and littoral environments in order to offer a realistic proposal. The concept is currently being reviewed by the requesting nation, with intent to circulate within the wider NATO Amphibious community for comment, which may lead to Doctrine change in the future.

Future Role of NATO in Global MSA (May 2014)
CJOS Author – CDR Carlos Couce Montenegro, ESP-N

In parallel with our MSA paper (see MSA Study Paper), CJOS COE was requested by ACT and ACO to perform an analysis of the potential future maritime security challenges. In tandem with relevant stakeholders, CJOS COE led the study and our conclusions were published by ACT and ACO to the maritime security community for review. The ideas and concepts offer a fresh look at MSA in a changing maritime security environment. After an ACT/ACO and community review, it is anticipated that ACT will initiate a new cycle of MSA conceptual development based on the conclusions.

Delivering Maritime Security in Global Partnership: Energy and Cyber Security Challenges in the Maritime Domain (May 2014)
CJOS Author - CDR Ricky McIver, USA-N

This paper considered the question of whether physical security is sufficient for ensuring freedom of navigation upon the high seas and prevention of a terrorist attack upon the nation's ports. The presence of war ships in the Arabian Gulf has prevented disruptions in the transfer of energy to the world's markets. However, this layer of physical protection may no longer be effective in preventing a disruption in the flow of energy. Technological changes have made it possible for state or non-state actors to exploit the cyber domain and circumvent the physical security that ensures the uninterrupted flow of energy.

Legal Questions Arising from Maritime Security Considerations in the Energy and Cyber Domains (June 2014)
CJOS Author – LCDR Kelly A. Mosteller, USA-N

This white paper was produced, in conjunction with CJOS COE's Maritime Cyber research, to identify key legal issues facing policymakers, military leaders, and maritime operators that arise from the overlap of energy and cyber interests in the maritime domain. It explores maritime security implications of recent developments in energy and cyber domains, but does not seek to be exhaustive in its treatment of the issues. The paper encourages information sharing among stakeholders, leading to the development of best practices in the maritime community.

CJOS Works in Progress

Maritime Situational Awareness (MSA) Study Paper
CJOS Authors – CDR Carlos Couce Montenegro, ESP-N; CDR Aytac Yavuz, TUR-N

CJOS COE, in coordination with COE CSW, is conducting an extensive MSA review in order to identify shortfalls within the information sharing environment of the maritime domain. Global MSA stakeholders were engaged to conduct an analysis and the MSA community was consulted to identify potential solutions or actions that could be taken to address the gaps. This is an ongoing project and the COEs are collaborating on a report that will summarize the results. The report will allow MSA practitioners and stakeholders to identify areas in which they can improve their MSA efforts..

Maritime Approach to Combined Operational Access (MACOA)
CJOS Author – CDR Patrick Cummings, USA-N

MACOA is a 12-nation concept collaboration to prepare for a combined operational access response, well before the actual response. MACOA does this by providing a framework for operational-level efforts to reduce the friction and risk inherent to operational access challenges. The framework describes three categories of activities, i.e. Building Understanding, Forming Partnerships, and Developing Scalable Forces. The framework starts well before there is a crisis, in the steady state i.e. Phase 0, and continue as a long term investment. These elements, when successfully combined over time foster a preventative stability as well as a preparatory responsiveness to operational access crises that is cohesive, coherent, and decisive. This concept provides the intellectual framework for the Maritime Approach to Combined Operational Access Practices Guide (MACOA PG). Concurrently, the MACOA concept is informing the implementation plan for the US CJCS's Joint Operational Access Concept (JOAC), as well as for several of US TRANSCOM's logistic development programs via the exercise TURBO TRANSITION (T2V5). Other nations participating in this concept development, e.g. Turkey, Norway, inter alia, are looking to adopt, incorporate, or reference MACOA within their national doctrine. NATO Joint Force Commands, U.S. Fleet Commanders, and U.S. Fleet Forces are other possible concept adopters.

MACOA Practices Guide (PG)
CJOS Author – CDR Patrick Cummings, USA-N

The MACOA PG is a menu of practical options for implementing the MACOA Concept, which is a concept designed to prepare for a combined operational access response, well before the actual response. It consists of various activities which foster building understanding, forming constructive partnerships, and developing scalable forces. These elements of the MACOA framework are prescribed to begin once a vital littoral area is identified (Phase 0) and continues persistently as a small-scale, enduring effort to prevent while concurrently preparing for an operational access crisis. MACOA PG is intended to help operational-level commanders and their staffs implement the MACOA concept. Fleet Commanders and CJTF commanders, along with their staffs, are the intended audiences for this document, although it is also a helpful companion to the MACOA concept, itself.

Alternate Command & Control Relationship & Staff Organization for Amphibious Operations EXTAC
CJOS Author – CDR Pedro Fonseca, PRT-M

The Alternate Command & Control Relationship and Staff Organization for Amphibious Operations document was developed considering intentions to downsize the size of military staffs and the most current technology available on modern amphibious platforms. In reality, this has already contributed to the current way of conducting operations and has changed the under lying assumptions for amphibious operations. The initial concept was included in the CJOS COE Programme of Work (POW) 2012 and the EXTAC is currentl being worked at the staff level in conjunction with the Royal Netherlands Maritime Warfare Centre.

CUTTING THE BOW WAVE 2014

DIRECTOR'S MESSAGE

MARITIME CYBER AND ENERGY SECURITY

MARITIME SECURITY

MARITIME ENABLERS

EXERCISES

ADDITIONAL SUBMISSIONS WILL BE INCLUDED IN THE ELECTRONIC VERSION POSTED ON THE CJOS COE WEB PAGE: WWW.CJOSCOE.ORG.

Future Employment of Corvettes in Confined and Shallow Waters – CDR Ingo Eilts, DEU-N. COE CSW

HUMINT in the Maritime Environment – Maj Alexandru Kis, ROU-A; Captain Pavel Istvanovicz, ROU-A. HCOE

Bold Alligator – CDR Pedro Fonseca, PRT-M. CJOS COE

Predators of the Deep: Hunter-Killer & Attack Submarines – Maj Tim Dunne, CD, MA, CAN-A (Ret).

Maritime Expeditionary Operations Conference 2013 (MEOC 2013) – Maj Andrew Cross, GBR-RM. STKFORNATO

STRIKFORNATO – Joint Headquarters, The Road to Joint Headquarters – Maj Andrew Cross, GBR-RM. STKFORNATO

Cyber Defense Modeling and Simulation Capability at the Network and Human Level – Mr. Edward Lundquist, USN (Ret). MCR Federal

Characterization and Analysis of Energy Security via Expert Reach Back Architectures in Maritime Interdiction – Dr. Alex Bordetsky, US NPGS; Dr. Dan Nussbaum, US NPGS; Dr. Silja Meyer-Nieberg, UNIBW; Mr. Goran Mihelcic, UNIBW; Prof. Dr. Stefan Pickl, UNIBW.

Publisher Note

Cutting the Bow Wave in an annual publication by Combined Joint Operations from the Sea Centre of Excellence, United States Fleet Forces Command, Bldg. 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 23511

Managing Editor:
CAPT Dermot Mulholland

Assistant Editor:
CDR John Mihelich

Assistant Editor:
CDR Russell Czack

Assistant Editor:
Colleen Hazlehurst

Magazine Printed & Designed By:
Strategic Marketing & Printing LLC
1.866.823.8699

Lori Ann Talens-*Owner*
Orrion Harris- *Graphic Designer*
Ina Mendoza- *Creative Director*

www.StrategicPrinter.com

MESSAGE FROM THE DIRECTOR

Vice Admiral Nora W. Tyson, USA-N
Director, Combined Joint Operations from the Sea Centre of Excellence
Norfolk, Va, USA

As I near the end of my first year as the Director, Combined Joint Operations from the Sea Centre of Excellence, I am extremely impressed by the quality of effort and research provided by CJOS COE, NATO, and our international partners.
The projects under the assigned 2014 Programme of Work initiated by CJOS this year aim to further increase the level of integration between NATO and our partner nations in the maritime domain. The past year, CJOS COE addressed challenges through multinational cooperation and coordination and explored opportunities in areas such as energy and cyber security, critical for developing a maritime strategy that charts the course for continued prosperity of Europe and the United States alike.

CJOS COE has also been busy this past year working on concept development for other Programme of Work items in the areas of Maritime Situational Awareness (MSA) and Joint Intelligence, Surveillance, and Reconnaissance (JISR). These projects are designed to highlight gaps in the current maritime situational awareness domain and identify areas where interoperability can be improved.

"The level of multinational cooperation and coordination we have achieved in areas such as energy and cyber security are critical to the continued prosperity of Europe and America alike."

Exercise BOLD ALLIGATOR 2014, an annual multinational amphibious landing exercise off the east coast of the United States is another high interest item for CJOS COE. BOLD ALLIGATOR 2014 is designed to increase US/Coalition operational confidence in the amphibious arena. The CJOS team is integrated into the planning committee and will assist US/Coalition forces in attaining the highest degree of interoperability and cooperation.

Admiral Michelle J. Howard *served as the Director of CJOS COE from August 2012 until July 2013. Under her leadership, CJOS COE produced the concept papers A Framework for Enhanced International Maritime Security Cooperation and Awareness and A Warfighting Concept for Littoral Sea Control Operations, and commenced an exhaustive study on the effects of cyber and energy security on the maritime domain. Her vision was instrumental in moving CJOS COE to the forefront of the maritime community. On July 1, 2014, ADM Howard became the first four star woman in US Naval history and she is currently serving as the Vice Chief of Naval Operations.*

CJOS has expanded its network by introducing research with US Fleet Forces Command, Old Dominion University, multiple national and international working groups around the world. As we continue the on-going study into the effects of cyber and energy security on the maritime domain, we plan to socialize our project findings and showcase the progress with key stakeholders at future events (workshops, working groups, webinars, etc). Last but not least, we are planning to develop a follow on project for continued research and a more in-depth study of ship vulnerabilities withinthis domain and against these threats.

CJOS Mission

Working in conjunction with the Commander, U.S. Fleet Forces, CJOS COE will provide a focus for the Sponsoring Nations and NATO in improving allied ability to conduct combined joint operations from the sea in order to ensure that current and emerging global security challenges can be successfully tackled.

CJOS Vision

To become the pre-eminent source of innovative specialist advice and recognized expertise on all multinational aspects of combined joint operations from the sea in support of the sponsoring nations, NATO, and other allies.

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

Having only just arrived in post, I would like to take this opportunity to firstly introduce myself, and express my thanks for the warm welcome I have received. Many thanks also to the many contributors to this edition of Bow Wave, which has significantly broadened the intellectual content of the document and I trust will be of interest to the joint readership.

CJOS COE's mission is: *'To provide a focus for the sponsoring nations and NATO to improve allied ability to conduct combined joint operations from the sea in order to ensure that current and emerging global security challenges can be successfully tackled'*. And as such there is much activity ongoing in the CJOS COE ranging from contributing to the strategic analysis of our future operating environment, researching the cyber vulnerabilities in our global supply chain to the more tactical issues of doctrine development and exercise support. This edition of Bow Wave will provide you with an inkling of our activity, whilst our website **(www.cjoscoe.org)** can provide more detail; for those requiring more please do not hesitate to make direct contact with myself or the staff: details of which are at the final page of this journal.

The maritime domain is presently at the forefront of many discussions on conceptual and doctrinal development; whether this is a result of refocusing post Afghanistan or whether because we have neglected to apply sufficient intellect during recent times is for debate. It is clear however that there is a renewed energy in discussing the utility of the maritime domain for operations; this, though is not just the preserve of maritime forces, it is part of the joint battle space, and therefore its utility must be exploited from a joint perspective.

Maritime Security has been, for several years now, a key work strand within our programme of work and stands out as a head mark activity for broad engagement across nations, agencies, industry and academia, and I see benefit in approaching other tasking in a similar manner – we are not the sole custodian of innovative thinking, and will not be the sole actor in the future battle space. An ongoing project on the 'Maritime Approach to Combined Operational Access (MACOA)' focusing on Phase 0 of a military campaign emphasises the need to take a holistic and comprehensive approach to operations. I believe there are many other opportunities to embrace industry and academia, and as we develop next year's programme of work I will be looking at the opportunities offered to pursue closer cooperation.

The demands on the CJOS COE continue to grow, which I am encouraged by, but to meet these growing demands, improved business practice and CIS are needed across our stakeholder and customer base, as well as more staff resources. As a NATO-accredited independent international organisation comprising staff from 13 nations, we would welcome additional member nations. Our vision is ambitious - *'Through a managed network with sponsoring nations, local US commands, academia and industry, to be the pre-eminent organisation within NATO developing maritime concepts and doctrine in a combined and joint maritime environment'* – but achievable. Our programme of work aims to be relevant to its principal customers and its output recognised as one of good quality; I would welcome feedback on whether we are achieving this objective.

Commodore S. J. Chick, CBE, *served as the Deputy Director of Combined Joint Operations from the Sea Centre of Excellence from April 2012 until June 2014. Under his leadership, CJOS COE made great strides with Joint Maritime Operations and Exercises, Maritime Security, and Interoperability. In the summer of 2013, he directed an exhaustive yearlong study on the effects of cyber and energy security on the maritime domain. Commodore Chick will retire from active service.*

He will serve as the trials master for the completion of England's newest aircraft carrier, HMS Queen Elizabeth. Following sea trials in 2016, he will take a position as the Harbour Master at Brightlingsea, Essex. All of us at CJOS wish Commodore Chick and his wife Catherine fair winds and following seas.

A View from the Reserves

CAPT Jeff Spivey, USA-NR
Commanding Officer, Naval Reserve Component Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)

Today's Navy is a trained and ready fighting force capable of deploying to any point on the globe with modern aircraft, ships, submarines, and combat systems which require core competencies from highly trained personnel tested by operational experience. Integral to the Navy's record of sustained readiness is integration of reserve forces to augment specific mission skill sets, retain key personnel, serve in mission-critical roles, and when called, deploy as an operational unit or an individual assignment. The result is a total force structure with enhanced combat readiness serving as a deployable fighting force.

There is no substitute for the unmatched combat capability of the Active Component, a trained and ready maritime force, continuously at sea. Those that serve in their nation's Navy bring a powerful combination of ability, grit, and sacrifice. Experience further refines their talents into a capable force. However, once those at sea return to shore; how does the Navy identify, recruit, and retain key personnel?

The Reserve Component (RC) offers a unique opportunity to retain personnel with operational experience as they continue to excel in their chosen professional fields. Those who train in logistics, medicine, law, information technology, aviation, business, and education, retain their core military skills while developing new skills in their civilian jobs. NR NATO CJOS COE is staffed with personnel from Naval Aviation, Surface Warfare, Submarine Warfare, Supply, Information Dominance, Human Resources, and Yeomen.

The forefront of CJOS COE's core mission set includes; Joint Interoperability, Joint Intelligence Surveillance-Reconnaissance (JISR), Maritime Security and Maritime Futures. Primary tasking is directed from USFF, while specific concept of operations and capability development assessments are requested by NATO Allied Command Transformation Capability Development.

Interoperability of Allied forces is a long-standing challenge dating back to when the first radio was invented. Today's modern combat information systems depict a near real-time common operating picture for certain military platforms, but transfer of information to Allied military platforms is difficult to manage. The challenge is to bring Allied forces into the construct via planning, communication and exercises. This work will be evaluated following BOLD ALIGATOR 2014. This exercise presents the opportunity to integrate coalition forces and develop improved interoperability through lessons identified. CJOS-COE will evaluate and present post-operational analysis of interoperability for participating coalition forces.

Intelligence, Surveillance, and Reconnaissance (ISR) collection is central to all military operations. Modernization of ISR capabilities is a critical requirement in the maritime domain. With satellites, radar, and inter-connected communication devices it may seem like the world is shrinking; however, the recent search for the lost Malaysian commercial airliner demonstrates that the world has remained the same, and just our technology-based perspective has changed. The question remains, what is the right mix of ISR platforms and can we get select cooperation to develop Joint ISR agreements with improved capabilities?

Maritime Security, as it relates to the defense of commercial shipping is more significant than pirates looking for a ransom or lost cargo. Commercial ships hijacked via cyber channels or commandeered via piracy with the intent to cause harm can block shipping routes, cripple the supply chain, and barricade military combatants. Anti-piracy is often the first thought that comes to mind when one considers NATO's role in maritime security. NATO has significantly reduced the threat to commercial shipping in regional hotspots around the world, all while conducting ISAF operations in Afghanistan.

Utilizing their experience in maritime law, commercial shipping, energy production, cyber vulnerabilities and other, RC members have provided excellent contributions and insight into these lines of work. The unique civil-military knowledge and expertise that NR CJOS COE offers continues to be a force multiplier for the Centre.

For more information about the US Naval Reserve, please visit www.navyreserve.com.
For information specifically about the NR CJOS COE component, visit
http://www.cjoscoe.org/leadership/nrcjoscoeco.html
or CAPT Spivey may be contacted at jeff.spivey@navy.mil.

NAVAL RESERVE

Delivering Maritime Security in Global Partnership: Energy and Cyber

Security Challenges in the Maritime Domain

CDR Ricky McIver
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

The presence of war ships in the Arabian Gulf has prevented disruptions in the transfer of energy to the world's markets. However, this layer of physical protection may no longer be effective in preventing a disruption in the flow of energy. Technological changes have made it possible for state or non-state actors to exploit the cyber-sphere and circumvent the physical security that ensures the uninterrupted flow of energy.

The world's economy depends on the availability of energy for transportation, communications, and security as well as healthly delivery systems. The primary energy source is crude oil, which is produced in large quantities for export in a limited number of countries.
The maritime domain is essential to supplying the world's energy needs given that one-third of oil and gas reserves are believed to lie offshore.

In addition, most oil transported around the world travels via the high seas with 2.6 billion tons of oil being transported by sea in 2008. Thus, the delivery and production of oil for trading to the world markets are dependent on the maritime domain. Since the 1970's, NATO has ensured the safety of offshore platforms, and tankers in the timely transportation of energy resources but increasingly, the presence of a physical force for providing security is being undermined via cyber attacks on energy production. To better understand the linkages between cyber security, energy supply and maritime security, let's take a brief look at the definition for energy security.

"...the next generation of terrorists will grow up in a digital world, with evermore powerful and easy-to-use hacking tools at their disposal."

Dorothy Denning
Is Cyber Terror Next?
November 01, 2001

A commonly accepted definition of energy security would be expressed in terms of supply and demand – that is the ability of a nation to satisfy its current and future energy needs. This premise is built on a nation's requirement to ensure a reliable source of energy to meet its economic needs. However, when examining the common area of maritime security, cyber security and energy security, it is useful to look more broadly at the definition of energy security to address the security (physical and cyber) of the exploitation, transportation and exploration elements. Of course, if the security of these elements cannot be assured, it could have an impact upon a nation's ability to satisfy its energy needs.

Warship escorting tanker in the Persian Gulf
Physical Security: not a thing of the past but not enough for the future.

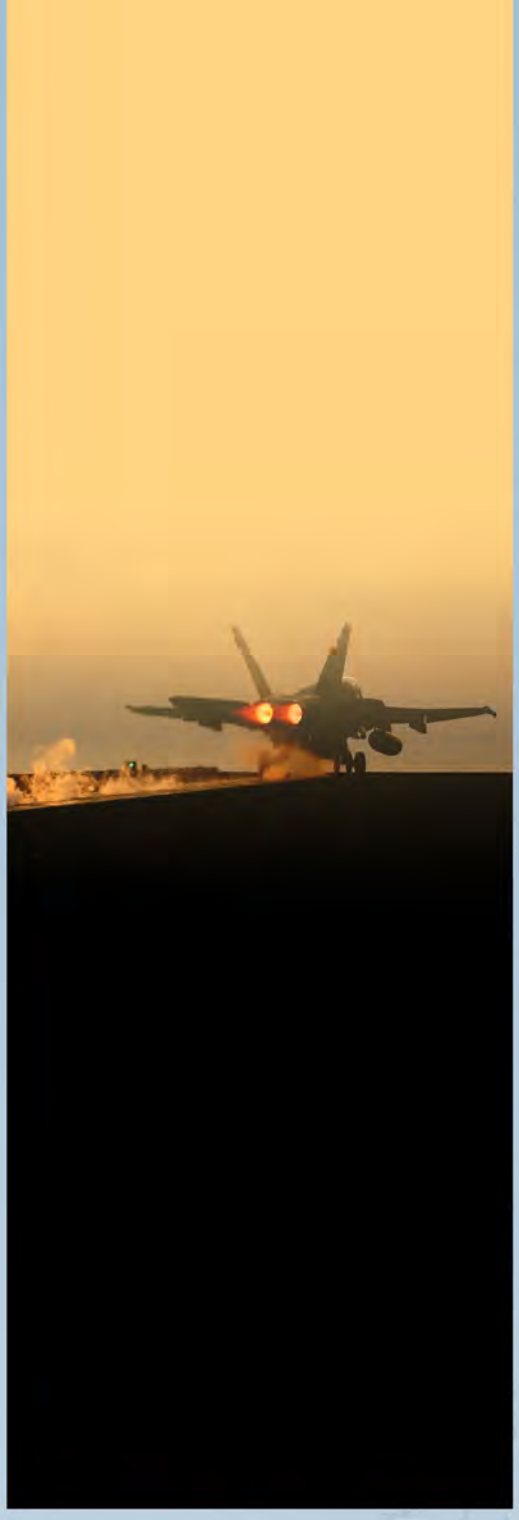
Loop Pumping Platform

In considering the energy aspects of the maritime domain, it could be interpreted that it includes those elements of energy security that are encompassed by the definition of the maritime domain:

"...all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."

It should be noted that, in some cases, the cyber vulnerabilities would not differ significantly between the maritime and land domains. However, in many other aspects, there could be definite differences on controls and security systems, particularly for sea-based exploration, exploitation and cargo systems, and, in virtually all cases, the impacts of, and reactions to, incidents would be more complex and difficult, thus demanding a potentially higher level of vigilance in their protection.

In addition to the maritime cyber vulnerabilities related to energy security, the maritime domain, in its own right, is vulnerable to cyber attack - commercially in the areas of cargo control, transfer and handling and management systems; and, in the public sector for information protection, management and exchange. Navigational systems and other marine management tools may also be at risk. Given the potential seriousness of the problems associated with reliance upon networks to gain efficiency in delivery schedules and reducing cost, one would expect that there would be a plan to tackle this problem. However, there has been little or no discussion or a definitive plan presented for addressing the issues.



Increasingly the maritime domain and energy sector has turned to technology to improve production, cost and reduce delivery schedules, eliminating the need for bulk storage.

These technological changes have opened the door to emerging threats and vulnerabilities as equipment has become accessible to outside entities. Today there are more than two billion Internet users and the number of cellular telephone subscriptions passed the five billion mark at the end of 2010, with nearly one in three people worldwide surfing the Internet.

In addition to increased use of the Internet, those organizations that support and defend the maritime and energy domains have increasingly exploited the Internet to improve efficiency and reduce operating costs. A large number of those industrial control systems not designed with cyber security in mind, have become interconnected with corporate computers and networks that expose them to a range of threats that have not been a major concern in the past.

Internet-facing systems provide the opportunity for minor to major disruptions to normal operations by anyone in the world. Such attacks can range from being an annoyance to being destructive in nature as was demonstrated by the "Stuxnet" attack and the "Aurora" demonstration.

It should also be noted that even if a system is not connected to the outside world, it can still be subject to a cyber attack introduced by other means such as a virus on a memory stick.

The increased availability of Internet access has given rise to 'hacktivism'. It is not uncommon to hear that cyber criminals have hacked a bank or stolen a business credit card database for political or social purposes. These individuals or groups are called hacktivists.

For example the group, "Anonymous" that took credit for the cyber-attacks on Saudi Aramco and others that threaten to attack energy producers around the world, often do so in the name of social activism.

To date, the attacks that have been launched by Anonymous have only caused minor interruptions; however, General Keith Alexander, Director of the National Security Agency, believes that their capacity for launching a wider attack is growing exponentially.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (US Department of Homeland Security) reported 198 cyber incidents in the United States during 2012, many of which occurred within the energy sector and ranged from the use of malware to sabotage systems, to phishing attacks for retrieving sensitive information. Cyber attacks within the energy sector have not been limited to the U.S. In 2012, Saudi Aramco was hit by one of the most disruptive cyber-attacks in recorded history and although this attack did not disrupt production, it did have an effect on delivery schedules. The virus that struck Aramco forced the company to shut-down its internal network, damaged over 30,000 computers while reducing communications to pen, paper and fax machine! Cyber attacks within the energy sector have gained increased attention since the attack on Saudi Aramco and Rasgas of Qatar. However, the energy sector is not alone in being attacked through cyber space; the interconnections between vessels that transport energy between ports are also at risk.

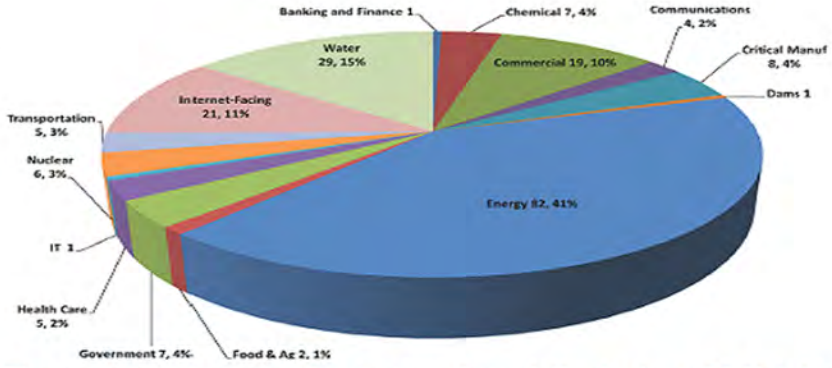
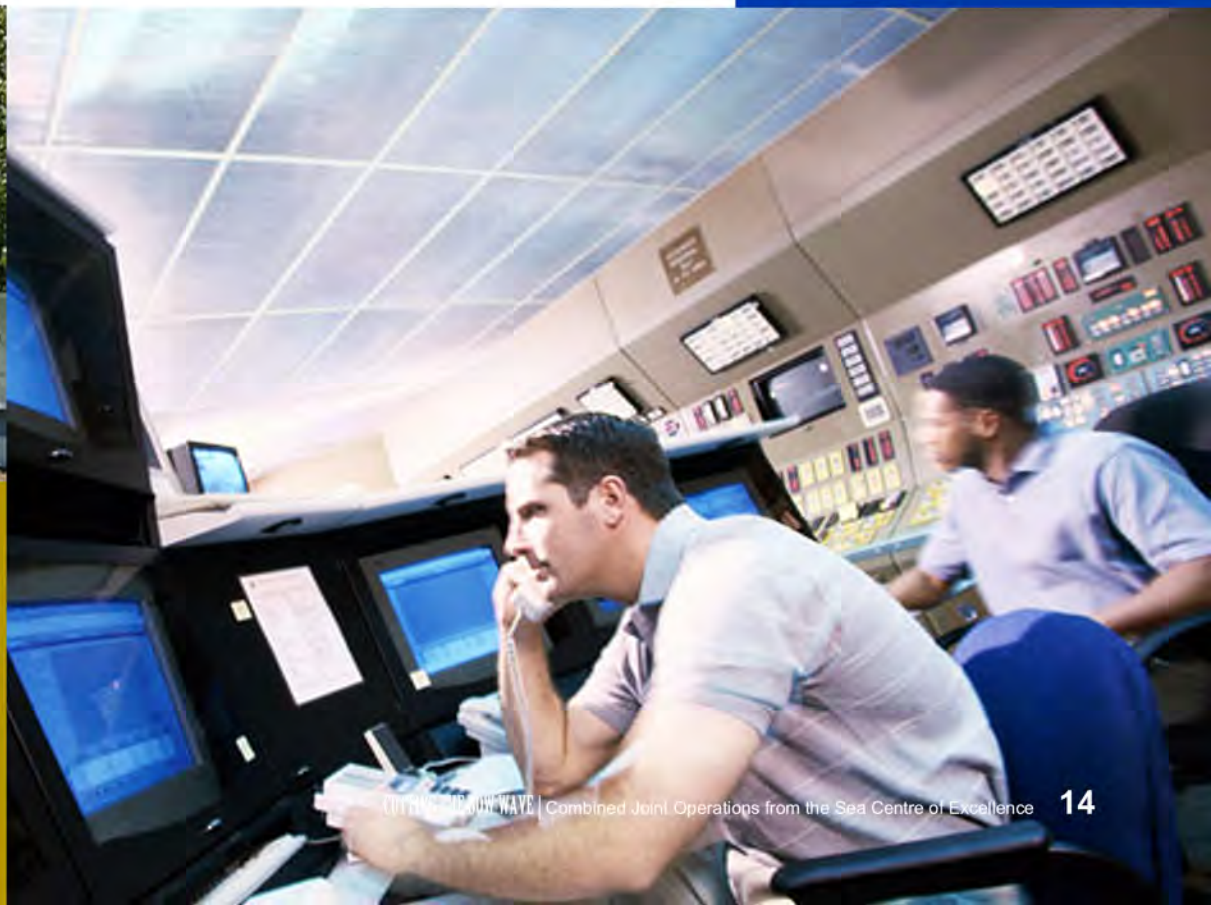


Figure 4. Incidents by Sector (+ Internet-Facing) – 198 Total in Fiscal Year 2012

*Fiscal year 2012 represents the time period of October 1, 2011–September 30, 2012

ICS-CERT's graph that depicts incidents by sector (+ Internet-facing) – 198 total in Fiscal Year 2012.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (US Department of Homeland Security)



Global Positioning System (GPS), the primary system that is used for navigation worldwide, is increasingly being threatened by jamming. A recent demonstration showed how a potential adversary could remotely take control of a vessel by manipulating its GPS. Under the guidance of SOLAS Chapter V, Regulation 19.2, all vessels of 300 gross tonnage are required to have installed and operational an automatic identification system (AIS). The usefulness of this system has led to some users integrating it with their navigational system, providing a common operation picture. It has been revealed that AIS is vulnerable to spoofing and manipulation, potentially affecting the safe passage of ships at sea.

Ports are also a vulnerability in the energy supply chain and, although, there have been no documented cyber attacks upon ports, this does not mean that ports are sufficiently protected or prepared to defend against a cyber attack. The European Network and Information Security Agency (ENISA) concluded in its report: "Analysis of Cyber Security Aspects in the Maritime Sector" that the awareness regarding cyber security aspects is either at a very low level or even non-existent in the maritime sector. A similar report was published by the Brookings Institute in 2013. This report found that for ports within the United States, cyber security awareness was on the same level as that in Europe.

Of the six ports studied, only one had conducted a cyber security vulnerability assessment and not a single one had a cyber incident response plan.

Moreover, of the $2.6 billion allocated to the U.S. Port Security Grant Program—created in the wake of 9/11 to fund new congressionally mandated security requirements at U.S. ports—to date, less than $6 million has been awarded for cyber security projects.

Although there has not been a successful cyber attack within the maritime domain, the potential for attack is both significant and increasing. The maritime domain, specifically ports, offers significant opportunity at a low risk to the aggressor. For example, Hurricane Sandy effectively shut down the Port of New York, creating energy shortages in New York and New Jersey. The New York harbor covers an area of 125 square miles in New York and New Jersey and accepts approximately 1.5 million barrels a day of oil from the U.S. and overseas. Considering the number of Internet facing systems and the significant vulnerabilities as highlighted in the ENSIA and Brookings Institute reports, a similar interruption in the energy supply could potentially be triggered by a cyber attack.

Given the unprecedented access and destruction that can be achieved via connected networks it is only a matter of when an attack will occur. Terrorists have taken notice that the slightest disruption in the energy supply chain can have a marked economic impact on world markets and that disruption could be caused by either a slowdown in production or the unexpected closure of a port. It is estimated that the impact of shutting down one or two ports could potentially cause more damage to the U.S. economy than the 9/11 attack. Terrorist groups also recognize the opportunity to disrupt the global economy by attacking oil supplies. In the past these attacks have been kinetic in nature - carried out by suicide bomber or by physical attack on oil pipelines. These attacks are costly in the terms of loss in human capital; it will not take an intelligent terrorist long to figure out that similar results can be obtained by waging a cyber attack on the energy sector and its supply chain. A sustained cyber attack within one of the major seaports has the potential to disrupt the flow of energy and give cover to its attacker.

Should a terrorist group decide to launch a cyber-attack, it is nearly impossible to determine with certainty the source of the attack. "Attribution – determining the source, location, and the identity of an attacker is extremely difficult for both technical and non-technical reasons." Unlike most weapons, cyber weapons do not come with markers to enable the determination of an attack origin. "Moreover, attackers enjoy a formidable advantage: anonymity. Smart hackers hide within the maze-like architecture of the Internet." Given the advantages and possible opportunities, it will not take someone that is determined on causing a ripple in the markets to turn to cyber.

The cyber vulnerabilities of the energy sector within the maritime domain are increasingly being exploited by state and non-state actors. While many naysayers will point to history and indicate that there has never been a cyber terror-based attack in the energy sector, we can also look at history to know that vulnerabilities present opportunities that are eventually exploited. It is only a matter of time before cyber terrorism takes its place within the maritime energy sector. Will we be prepared?

CJOS COE

Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) (www.cjoscoe.org) is an independent multinational, NATO-accredited organization charged with developing and promoting innovative maritime concepts and doctrine in order for NATO, sponsoring nations, Allies and other international partners and organizations to effectively counter current and emerging global security challenges.

CDR McIver is a Staff Officer with Combined Joint Operations from the Sea Centre of Excellence. For further information about our article, please contact us at cjoscoe@navy.mil.
For further information about the Programme of Work for CJOS COE, please see our web page at: www.cjoscoe.org.

INTERAGENCY COOPERATION FOR MARITIME SECURITY

CDR Mahmut Karagoz, TUR-N
Multinational Maritime Security Centre of Excellence (MARSEC COE)
Aksaz Naval Base, Marmaris/Mugla, Turkey

As we become more interdependent in the realities, needs and requirements of our economies, it is clear that availability and continuity in supply and demand is in the best interest of all nations. Considering the heavy burden and critical role of the maritime environment in this process, the sustainability of energy and trade is only possible by providing maritime security through international cooperation and keeping the sea lines of communication open. In this equation, maritime security is the common denominator of energy, trade, security and other maritime activities in the 21st century. In addition, the classical challenges, maritime boundaries and national interests, inherited from the 20th century, requires a multinational approach for potential solutions. Under these circumstances, formulating the problems of both centuries, by multinational and multi-agency parameters will be pivotal to start change, declaration of intent and mutual understanding of the agencies involved.

The organization to facilitate this initiative should be neutral, conform to international law, consider the interests of all parties, and work in scientific, transparent, patient and decisive method. Many International Organizations such as UN have made political level recommendations to safeguard the continuity of energy and trade. These policies are being implemented by nations through their national regulations. The cultural, systematic and language differences between the organizations and countries are also causing varied interpretations and implementations. A platform with a common understanding is needed to provide unity of doctrine and terminology in our fight against risks which are threatening maritime security. The solution lies in interagency cooperation. The idea of interagency cooperation is not new, but we are still struggling to formalize how to make it happen.

Maritime Security Related Global Initiatives with Interagency Cooperation

Piracy, armed robbery, WMD, maritime terrorism, smuggling and organized crime can be listed as some of the major risks in the context of regional and international security threats to the continuity of energy and trade. When maritime claims are included, defence and security issues get mixed and it becomes more difficult to decide which legal principles should be in force in such multi-faceted issues. In this complex structure, there are a number of security focused initiatives started by Unitied Nations-International Maritime Organization (UN-IMO), NATO, the European Union, regional bodies and some maritime nations. These initiatives/coordination mechanisms (or frameworks by their very nature) deal with interagency cooperation, in order to achieve effective use of maritme stakeholders' capabilities.

UN-IMO, the UN agency in the maritime domain for the safety and security, is getting more involved in maritime security via multinational approaches. These multilateral agreements include, the International Convention for the Safety of Life at Sea (SOLAS Convention) and in particular, the provisions of Chapter XI-2, and the International Ship and Port Facility Security Code (ISPS Code), Automatic Identification System (AIS), Global Maritime Distress and Safety System (GMDSS), Long-Range Identification and Tracking (LRIT), The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA), Djibouti Code of Conduct, and the Best Management Practice guidance. IMO is playing a critical role to orchestrate the efforts of international maritime community.

NATO's approach to interagency cooperation became clear following the 2008 Bucharest Summit1 with their development of the Comprehensive Approach Action Plan. The plan outlines how political, military and civilian instruments can contribute in a concerted effort, based on a shared sense of responsibility, transparency, and determination and taking into account their respective strengths, mandates and their decision-making autonomy. This is becoming increasingly more important as NATO operations shift from platform based to network operations. The Comprehensive Approach is a key enabler in most of NATO's current maritime security lines of work including: the Alliance Maritime Strategy (AMS), Mariritime Security Operations (MSO) and Maritime Sitauational Awareness (MSA) Concepts and Future Maritime Information Services (FMIS). Strong law enforcement involvement, information sharing and interagency cooperation are essential to these programs aimed at ensuring maritime security.

The European Union is also providing robust structures to establish an integrated, horizontal and cross-sector maritime policy, encompassing all aspects of our relationship with the seas and oceans. Some of these groups are the European Maritime Safety Agency (EMSA), European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (FRONTEX), the European Defence Agency (EDA), the European Fisheries Control Agency (EFCA), and the Common Information Sharing Environment (CISE).

There are also other international initiatives that contributed to maritime security; Proliferation Security Initiative (PSI), Container Security Initiative (CSI) Global Initiative to Combat Nuclear Terrorism (GICNT) and a Contact Group on Piracy off the Coast of Somalia (CGPCS), MARLO (Maritime Liaison Office), Maritime Security Centre – Horn of Africa (MSCHOA), Shared Awareness and Deconfliction (SHADE).

The common point in these initiatives is the significant maritime aspect as well as the political, military, social, economic, legal and technical considerations. These are complex problems which involve: flag state responsibilities, ownership of the cargo, nationality of the crews, coastal state regulations, and port state regulations. When we add maritime law issues to this equation, we are looking at a structure of multi-national, multi agency nature with multiple regulations. Knowledge management within such a structure requires a different mind set. It should be based on understanding of different cultures and disciplines but interconnected on a common platform. The focus of this platform is to fight the challenges against safe and secure navigation in order to provide the continuity of energy and trade. Under this structure/working environment, the maritime security stakeholders from the political, military, social, economic, legal and technical partners will be able to cooperate and share information to better manage the maritime environment.

National approachs to Interagency Cooperation for Maritime Security

Canada

The 2004 National Security Policy directed the establishment of Marine Security Operations Centres (MSOCs) as a way of strengthening marine security for Canadians and allies. Three MSOCs are in operation and though still in development, they presently collect and analyze vast amounts of information from the marine environment in order to identify security threats. The ongoing project implementation of these centres is led by the Department of National Defence (DND) for two coastal centres and by the Royal Canadian Mounted Police (RCMP) for the centre covering the Great Lakes and St-Lawrence Seaway. With staff representing DND, the RCMP, the Canada Border Services Agency, Transport Canada, the Department of Fisheries and Oceans (DFO) and the Canadian Coast Guard (CCG) the MSOCs are a unique example of multi-agency integration. Departmental mandates, lines of authority and communications structures are maintained by each agency within the MSOCs, while the unique information systems and expertise of each are combined to enhance the MSOCs' capacity to monitor Canadian territorial waters, and detect and assess security threats.

UK

In 2010, the government sought to provide "strengthened strategic oversight" by establishing the Maritime Security and Oversight Group (MSOG). The membership was comprised of "key representatives of core departments, agencies and the Cabinet Office, and is the senior-level decision making group for maritime issues." The MoD described the role of the group as providing "strategic oversight and direction of all cross-cutting maritime security issues and programmes, including aspects of maritime surveillance [and] is responsible for the Maritime Security vision, strategic objectives and risks, reviewing them as circumstances require, and allocating priorities in order to use a framework to drive and coordinate day-to-day policy on cross government programmes of work."

The 2010 SDSR acknowledged that no single department or body had the capacity or capability to deliver what is required to monitor the maritime environment and counter threats the UK faces both in territorial waters and internationally. The National Maritime Information Centre (NMIC) was established in Northwood on 1 April 2011 "to ensure information was disseminated, analysed and acted upon in a coordinated manner." NMIC brings together government departments and agencies with the responsibility for maritime safety, security and environment in one place and is accountable to the Home Office. Its intention is to develop a single picture of maritime activity similar to that used by air traffic controllers so that threats and risks can be recognised and countered as early as possible.

MARSEC COE Multinational Maritime Security Interagency Doctrine - MMSID

In December 2012, the Multinational Maritime Security Centre of Excellence (MARSEC COE) initiated a project called “Multinational Maritime Security Interagency Doctrine - MMSID.” This doctrine will involve the political, military, social, economic, legal and technical aspects of maritime security and consider national, regional and international level multi-agency characteristics and requirements. It will consist of three main parts: identifying the maritime risk areas, the means to deal with those risks and the generic governance structure to facilitate the interagency cooperation at national and international level. MARSEC COE is engaged with a broad spectrum of partners in this development, to include: academy, national/international organizations, COEs, private sector, military and civilian government agencies. Their contributions and support will be vital to capture the fundamentals of multinational interagency cooperation.

During the first Maritime Security Workshop organized by MARSEC COE in Marmaris, 14-16 November 2012, the requirements were identified. During the second Maritime Security Workshop in Istanbul, 7-9 October 2013, MARSEC COE began its development of the “Multi National Maritime Security Interagency Doctrine”. As the doctrine matures, it may provide a platform for the maritime security stakeholders from national and international agencies/organizations to interact and develop a new culture to work together. The critical point during development is not a “case-by-case” cooperation, but a “systematic- interconnected governance structure”.

Maritime Situational Awareness (MSA)

MSA is a major part of the MMSID and has very similar characteristics that require an international approach to achieve the required level of situational awareness in the maritime environment. There are a number of existing MSA initiatives around the world: **V-RMTC (Trans-Regional Maritime Network (T-RMN)), ReCAAP, OBSH-OMEGA, MARSUR, SUCBAS, MSSIS, CISE, OASIS, SISTRAM,** etc. These different MSA systems are designed for different purposes, capabilities and standards; therefore, causing information exchange and interoperability problems. The solution requires multinational cooperation that will provide a framework of working together and supportting each other towards the common goal of a safe and secure maritime environment.

The Way Ahead

The above listed examples in Maritime Secuirty and MSA related initiatives, albeit not the only ones, demonstrates the variety of organizations involved and the different goals and objectives for their specific area of concerns. Interagency collaboration is not just the key, but the only way to achieve effective maritime security. All these organizations should work in harmony to support and complement each other's work in a global solution. If this cooperation could be structured effectively, it may not require extra effort to support parallel activities, not to mention the benefits in awareness and access to information that would be available.

Working together is not an objective or a priority for individual organizations. They are focused on daily operations and sometimes completely miss the opportunity to benefit from another organization's work. The result is ineffective use of limited resources or deficiencies in core capabilities for maritime security. There are a number of best practices and successful models at the national or regional level but barriers which prevent interaction are still significant. Cooperation is a process - an evolution in the way of doing business. It will require training and education for military and civilian personnel, to include leadership and will be paramount to prepare the human factor and shape the environment.

MSSID is one of our many activities to accomplish this goal. We invite all the like-minded subject matter experts, nations and national/international organizations to joins us at the 3rd MARSEC COE Maritime Security Workshop, 21-23 October 2014. This workshop will be a milestone in our doctrine development. Our goals during this workshop are to finalize the scope and content of MMSID and determine the doctrine writing responsibilities among the volunteer participants. The finalized MSSID concept will be tested during MARSEC COE Multinational Exercise – 2015. It will comprise both TTX and LIVEX and will be conducted in the Eastern Mediterranean in the fall 2015. The IPC will be conducted on 24 October 2014, the MPC in March 2015 and the FPC in June/July 201511.

As our motto "***Working together for Maritime Security***" suggests, we will do everything in our capacity to promote and enhance martime security in our region and in the world.

MARSEC COE

CDR Karagoz is a Staff Officer with Maritime Security Centre of Excellence.
For further information about this article, please contact him at marseccoe.admin@dzkk.tsk.tr.
For further information on the Programme of Work for MARSEC COE,
please see their web page: www.dgmm.tsk.tr.

MARITIME DOMAIN, CYBER THREATS, ENERGY LOSSES?

Lt.Cdr.Murat Tuncer, TUR-N; 2-nd. Ltn. Heiki Jakson, EST-A
NATO Energy Security Centre of Excellence (ENSEC COE)
The General Jonas Zemaitis Military Academy, Vilnius, Lithuania

INTRODUCTION

Until the famous STUXNET malware was discovered, cyber threats to the energy infrastructure were not considered to be an important factor. Now, there are said to be two kinds of energy infrastructure companies: those that have been attacked and know about it and those that have been attacked but don't know about it. In other words, cyber-attacks on critical infrastructure and especially on information and communications technologies are a rapidly growing concern. There is a reason for the growing concern over cyber-attacks. A number of energy companies report "daily", "constant", or "frequent" attempted cyber-attacks on their facilities[1].

Despite the notion that the energy sector is the best cyber protected sector after IT and Banking, these attacks have added up to thousand per month per one utility. For the first half of 2013, the US Computer Emergency Readiness Team (CERT) reported about 111 major cyber-attacks on energy infrastructure, which counts for 53% of attacks in critical infrastructure. In comparison, the transportation (along with postal service) sector only reported 11 incidents, making 5% of total attacks on Critical Infrastructure. But it doesn't mean that this ratio will be true for very long – transport infrastructure and the maritime sector in particular (due to its rising strategic importance to the global trade and well-being of many states) may suddenly become targets for criminal offenders.

This short analysis starts with an overview of the rising importance of the maritime transport infrastructure. It also provides insights on the latest developments in the area of cyber security, paying the greatest attention to the latest cyber-attacks. The intention of this article is draw the parallel between energy infrastructure (already suffering from the cyber-attacks) and the maritime domain, which may be the next target. What best practices are applicable in order to avoid the damage from hackers who decide to attack maritime domain?

This article highlights some vulnerabilities that the authors feel are important to consider. Examples from Energy Infrastructure are used to provide a basis for concerns that the maritime sector is under threat from cyber-attack. In writing this article, a large number of public materials were reviewed, including research by Kaspersky and McAfee antivirus software companies, research done by U.S. and EU authorities, and articles by respected thinkers in the field such as Frank Umbach, Kevin Rosner, Lucian Constantin, Vytautas Butrimas, Audrius Bruzga and Arunas Molis.

I. IMPORTANCE OF LATEST DEVELOPMENTS IN MARITIME DOMAIN

It is not surprising when people from countries bordering the sea say that "oceans connect nations where land separates them." However, in the light of increasing seaborne trade, it takes on a new meaning. Over 50,000 merchant ships, transporting every kind of cargo internationally, not only "connect the nations," but also shape the major trade patterns that form the relations between nations. Two factors are used to support this statement. First, around 90% of world trade is carried by the international maritime industry. There is no other way to import and export goods on this scale in the modern world. Secondly, the proximity to raw materials and markets has become a factor that has shaped major trade patterns and shipping routes. As a consequence, coal transported from Australia, Southern Africa and North America influence those countries' and regions' relations with Europe and the Far East. The same may be said about grain that is being transported from North and South America to Asia, Africa and the Far East, iron ore shipped from South America and Australia to Europe and the Far East and oil sold from the Middle East, West Africa, South America and the Caribbean to Europe, North America and Asia. All in all, there is no doubt - global maritime trade allows for an enormous variety of resources to be widely accessible through quick and safe trade and has facilitated the increase of our planet's common wealth and/or influences the change in international relations[2].

Negative consequences to modernization are being observed as the maritime domain becomes increasingly important. Rising dependency on maritime transport reveals certain vulnerabilities that must be taken into account. For instance, maritime activities increasingly rely on so called "information and communications technologies" (later known as ICT) that optimize maritime operations such as navigation, propulsion, freight management, traffic control communications, etc. As a consequence, maritime vessels and ports and terminals depend on highly complex systems (like Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Long Range Identification and Tracking (LRIT) systems, Vessel Traffic Services (VTS), Maritime Situational Awareness Systems, or SCADA and other systems) which require adequate support and maintenance by maritime cyber defense systems. However, this is not always the case. The fast technological development and the struggle towards complete automation in the maritime sector were not followed by the proper parallel focus on the security features. As a consequence, maritime systems have become vulnerable to cyber-attacks and computer failures.

Like many other sectors, people responsible for security in the maritime domain are mostly dealing with physical risks and vulnerabilities. As disruptive impacts of cyber-attacks remains comparatively low, cyber security awareness remains also low. However, this might change soon since a majority of activities in the maritime field rely on sophisticated electronic and communication systems. These systems are equally vulnerable to accidental and purposeful infection. In other words, one doesn't have to be purposefully attacked. Malware can be easily spread online by someone downloading an infected email or connecting a virus-laden USB to a computer linked to operational controls.

Vulnerability of the ports was proven by drug smugglers in Port of Antwerp. After stealing the release codes from the computer system, they hid drugs inside legitimate shipments of other goods from South America. The precise location of the relevant containers, together with delivery locations, were identified and then changed in order to allow for the pick-up of the container before its real owner turned up at the port. Criminals simply hijacked the trucks carrying the containers after they left the port[4].

EXPOSURE OF CYBER-ATTACKS ON VARIOUS INFRASTRUCTURE OBJECTS

The problem with hackers and malware is nothing new. Cyber security specialists have been dealing with the question for decades. However, there is one aspect that becomes important today - the growing application of Industrial Control Systems (ICS) to the world's maritime transport systems which are increasingly finding themselves connected to internet for remote control purposes. When ICS was designed, the cyber security aspects were understood differently from those prevailing in the ICT world. Much more important factors were reliability and ease of access to the system to solve sudden problems. And what's more, the engineers who design the modern control systems are not the same who design the IT systems. This grey zone between the IT and the ICS solutions has led to the development of gaps in the ICS cybersecurity.

In 2010, a malware targeting ICS and sometimes called the first "Cyber Weapon" was discovered. Its name is STUXNET. This malware was designed to attack an object only when it reaches the predetermined target, leaving all other systems, intact. It changes the functioning of industrial systems, while displaying normal operations to the facility's personnel (as it appeared to happen for the Iranian uranium enrichment centrifuges). This malicious activity causes the system to destroy itself without the possibility to take adequate countermeasures. And this may happen even when the system is completely separated from internet. In the case of Iran, the system was most likely accessed by using a simple memory stick.

Since the discovery of STUXNET, many other related "Cyber Weapons" have emerged: DUQU, FLAME, RED OCTOBER, NIGHT DRAGON, to name a few. Even well protected and isolated ICS are being infected by malware due to the use of unprotected and infected computers, which are connected directly to critical systems for adjustments and maintenance. STUXNET related malware conducted espionage, gathered information from large number of systems and continued their attacks for years before discovery. Worthy of note is that malware activities are becoming coordinated. DUQU, for instance, is thought to be a reconnaissance-information gathering tool in order to facilitate future STUXNET-like attacks. As they are extremely complex malware, the adequate analysis of these worms might take many years[5]. This is enough time for cyber foes to gather information and facilitate new cyber-attacks in the future.

Cyber-attacks can also be organized through communication systems between the different remotely controlled objects in the system, or by communication and information services (servers) offered by communication companies, that don't always adequately value security. In other words, "smart grids" are not only helpful, but also vulnerable when not appropriately protected against hostile outside intentions. As the capability to control machinery from distance grows, so also does the possibility to exploit them. For instance, in Puerto Rico, hackers in 2009 changed the parameters in smart meters allowing users to use more electricity without paying. The potential loss in this case could reach 400 million dollars annually for the power company[6].

Not only do problems exist in the ICS but also in common IT systems. Windows, Office, and Internet Explorer are still extremely vulnerable to cyber-attacks. Though these attacks pose no threat to the functioning of ICS, they can cause panic and enormous material damage. Few examples of this sort are available from recent years. In 2012, the web page of the St. Petersburg's nuclear power plant was targeted. Information about "radioactive waste disposal" was distributed, causing panic among the nearby residents[7]. Also in 2012, the Saudi Aramco (the world's largest oil company) computer systems were cyber-attacked by a malware called Shamoon. It crippled 30,000 computers and caused disruptions in the corporate work of the company[8]. Again in 2012, the first confirmed cyber-attack against the European electrical grid operations took place via the German power utility 50Hertz. The attack lasted for 5 days and blocked the company's internet domains so that in the first hours, all e-mail and connectivity via the internet was blocked[9].

A final turbulent trend in this regard is that cyber diversions are becoming easier and easier to accomplish. Perpetrators of cyber-attacks do not have to be a cyber-expert in order to facilitate a destructive attack. Today, an ordinary person having access to internet and mediocre computer skills can execute a cyber-attack, even against ICS. There is even an internet search engine called Shodan that can be configured to locate ICS systems connected to internet. As many are unprotected, attackers don't even have to hack in! If they must hack the system because of protections that are installed, they can download malware attack tools from the internet. If that is not enough, companies exist (such as ReVuln) that specialize in finding ICS vulnerabilities and selling them to highest bidder. All in all, the situation requires some serious decisions to be made.

II. VULNERABILITIES IN THE MARITIME DOMAIN

Maritime security covers the protection of a state's land and maritime territory, infrastructure, economy, environment, and society from certain harmful acts occurring from the sea. These may include piracy and armed robbery, terrorism, illicit trafficking in drugs and weapons, human trafficking, illegal fishing and intentional and unlawful environmental damage. For a long time, there was hope by industry and among maritime security professionals that risks of cyber nature would not become relevant in the maritime domain. Today, it is evident that remoteness of ships from the land is not an obstacle anymore for criminals, terrorist groups or whoever intends to harm security and safety of ships, ports and related infrastructure.

The reason is that ports rely on computer networks as much as on human stevedores. Complex networked logistics management systems undergird the global flow of maritime commerce. These systems track maritime cargo from the time a container is stuffed by a merchant overseas until it reaches its final destination. They are so sophisticated, they have essentially done away with the warehouse. Today, goods are "stored in transit." Networked control systems are also often involved in the loading and unloading of these goods.

Modern gantry cranes and other systems use optical recognition and other technologies to locate, scan, and manage all facets of port terminal operations. Port facilities often leverage information from these same systems to comply with security requirements. Scanners and radio frequency identification devices (RFID) not only track cargo as it enters or exits ports, they also track the trucks, railcars, and drivers that operate these conveyances10. Many of these large complicated ports have oil and gas import terminals which are very vulnerable to any kind of the criminal attack on supporting ICT and ICS infrastructures. If damaged, it could cause great loss to the environment, economy and well-being of the state.

Thus, cyber security related issues are now an indispensable part of maritime security. Cyber-attacks in the form of malicious programs (viruses) or cyber espionage directed at the maritime domain (just as in energy domain) can cause far-reaching physical damage. Maritime vessels use digitized ICS such as Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Integrated Bridge Systems/Integrated Navigation Systems (IBS/INS), Automatic Radar Plotting Aids (ARPA) or the Global Maritime Distress Safety System (GMDSS) as only few examples.

Adequately supported and maintained, they are of great value. ECDIS replaces paper-based nautical charting by overlaying positioning information from global positioning system (GPS), and AIS on to electronic navigational charts (ENCs). ENCs are being upgraded periodically by using wireless internet connection or satellite communication. They are crucial for efficiency but at the same time it is possible to send these devices incorrect navigational data putting a ship in jeopardy. Compromising a vessel's security by transmitting fake data to the Maritime Situational Awareness (MSA) center may cause that ship to lose situational awareness. Or the real information may be used for wrongful purposes, including espionage, preparation to pirates' or hijackers' attacks.

In this context, it is worth noting that maritime situational awareness systems are being used not only by the commercial maritime industry but also in Naval Forces during the military operations like Ocean Shield and Atalanta in Gulf of Aden or Indian Ocean. Thus, information stolen from MSA systems or the intentional transmission of fake data could jeopardize naval forces.

Improper attention to cyber security issues and the absence of maritime cyber defence systems within the petroleum extraction industry could lead offshore oil rigs and platforms to become targets of cyber criminals.

They consist of interconnected systems running, monitoring and recording hundreds or thousands of calibrations each minute and may become targets of cyber criminals. These systems are just as complex as those found in any other industry and just as vulnerable. Therefore the real challenge is how to prevent the unwanted malicious software from affecting the offshore platform information and communication systems that have been left vulnerable until now. In this regard much like their onshore counterparts, work should be started to identify weaknesses and take a proactive stand against possible infections.

RECOMMENDATIONS: LEARNING FROM THE BEST PRACTICES IN THE ENERGY

The easiest way to ensure security in the cyber domain is by establishing a habit of "cyber hygiene" which helps to protect the system from 90 percent of the possible risks. This consists of having up to date software, suitable and correctly set malware protection, correctly set firewalls, personnel awareness on cyber-security, the secure separation of IT and ICS systems, ICS separation from internet, background checks on personnel and partners, and also control of hardware and software that the contractors maintaining the systems use. At the same time, adequate response to successful attacks must be applied. All attacks must be analyzed and reacted to by experts, in order to rebuild the system and avoid future breaches. This is best done by focusing attention on the "weak links" in the chain. Prevention is just as important. Plans for mitigation and recovery must be prepared in advance, back up's must be stored and the action to combat attacks must be practiced.

Cyber-attacks rarely target only one sector or one company. Information sharing among parties is essential in order to stop attacks and for gaining best practices to build a stronger defense. State institutions should trust private companies more by sharing information with them – and vice-versa. A concept of "Situational Awareness" could prove highly profitable on this matter, allowing fast and suitable information exchange and providing the party's with information relevant for their mission.

In talking about the maritime domain specifically, developing vulnerability assessments and cyber security requirements for maritime critical infrastructure (port and terminal facilities, ships, control and monitoring systems) could be a very useful starting point. Practical steps, which could improve cyber security in the maritime domain and as well as strengthen the security of offshore critical energy infrastructure, could be:

- Global maritime cybersecurity awareness should be expanded:
  - The International Maritime Organization (IMO) and other respective international organizations should come together to develop international maritime cybersecurity and cyber incident response standards.
  - The use of the Malware Information Sharing Platform (MISP) could increase the facilitation of information sharing on the technical characteristics of malware within a trusted community.
- Maritime Surveillance System (developed by Centre for Maritime Research and Experimentation - CMRE) that uses information from AIS (i.e. applies anomaly detection algorithms and filters to provide the NATO maritime surveillance community with information) should be reviewed and upgraded to consider cyber security risks.
- International Ship and Port Facility Security Code (ISPS Code), which includes a comprehensive set of measures for enhancing the security of ships and port facilities, should focus not only physical security, but also digital cyber-security risks.

[1] E. Markey, H. Waxman, Electric Grid Vulnerability – Industry Responses Reveal Security Gaps, May 2013
[2] Maritime Knowledge Centre "sharing maritime knowledge`` 6 March 2012
[3] ENISA, "Analysis Of Cyber Security Aspects In The Maritime Sector", November 2011
[4] http://www.marsecreview.com/2013/10/police-warning-after-drug-traffickers-cyber-attack/ Retrieved 26 January 2014
[5] Zetter, Kim (28 May 2012). "Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers". Wired. Archived from the original on 30 May 2012. Retrieved 10 February 2014
[6] http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/. Retrieved 10 February 2014
[7] V. Butrimas, A. Bruzga, "The Cyber Security Dimension of Critical Energy Infrastructure", per Concordiam (Volume 3, Issue 4) 2012
[8] http://www.nytimes.com/2012/08/27/technology/saudi-oil-producers-computers-restored-after-cyber-attack.html?_r=1 , retrieved 10 February 2014
[9] Frank Umbach, „Commercial Confidentialituy: An Opstacle to Effective Mitigation to Cyber Atacks on Critical Energy Infrastructures?", Energy Security Forum, 2013
[10] Commander Joseph Kramek, Center For 21st Century Security And Intelligence" The Critical Infrastructure Gap:U.S. Port Facilities and Cyber Vulnerabilities" Foreign Policy at Brookings, July 2013
[11] Maritime Reporter and Engineering News "Maritime Cyber Security", July 2012

ENSEC COE

Lt Cdr Tuncer and 2nd Ltn Jackson are Staff Officers with Energy Security Centre of Excellence. For further information on their article, please contact them at heiki.jakson@enseccoe.org.

For further information about the Programme of Work for ENSEC COE, please visit their web page at: www.enseccoe.org.

NATO CIMIC IN THE MARITIME ENVIRONMENT (NCME)

CDR Oliver Vanek, DEU-N
Civil-Military Cooperation Centre of Excellence (CCOE)
Enschede, Netherlands

Motivation

In analysing Civil-Military Cooperation (CIMIC) in the Maritime Environment it is necessary to look into maritime history. Naval expeditions in the period of European expansion, later colonisation and empire, were dependent on cooperation with foreign civilians, for the purpose of promoting trade, acquiring materials, or establishing supply bases. The skills required of the naval commander in order to complete these tasks were varied. In this complex environment, navies were not simply required to perform naval operations, but to simultaneously engage in the civil environment as commander, strategist, politician, diplomat, trade envoy and administrator. Performing these roles in an uncertain environment and without governmental oversight required navies to think strategically and apply the policies of the nation in foreign civilian contexts.

CIMIC in the Maritime Environment was taken into consideration in 2007 when the Chief of Staff Maritime Component Command Naples (MarCOM Naples), directed the development of a "Maritime CIMIC Concept" white paper. Joint Force Command Naples concurred with the development of the white paper and encouraged MarCOM Naples to further develop their maritime conceptual white paper. This effort resulted in creation of an Experiment Proposal for 2009. The scheduled 2009 "Maritime CIMIC Experiment" was delayed until 2010 as scheduling limitations prevented timely planning and execution in 2009. Concurrent with experiment rescheduling, the title of the experiment, "Maritime CIMIC Experiment", was changed to "CIMIC in the Maritime Environment Experiment (CMEE)." The CMEE has become an essential element of HQ SACT's civil military interaction campaign plan supporting the development of NATO's contribution to a Comprehensive Approach.

Given the new NATO Strategic Concept and the mission it implies, the requirement for interaction with civil authorities will certainly increase at all levels of command. Accordingly, the requirement for NATO maritime tactical staffs and units which are capable of conducting "civil military interaction" in the maritime environment will increase. The CMEE was a response to the request from a NATO operational maritime tactical staff to identify how CIMIC should be conducted in the maritime environment. The CMEE examined CIMIC doctrine; Tactics, Techniques and Procedures (TTPs), and the existing maritime doctrine.

According to the CMEE Final Experiment Report, maritime tactical staffs and units perform a myriad of CIMIC-like functions integrated into their everyday tasks which are embedded in maritime doctrine, but not recognized as distinct "CIMIC" tasks. Since these functions are not acknowledged as "CIMIC," they are not reported as "CIMIC" functions, and therefore the maritime tactical level and joint level CIMIC are disconnected. CIMIC functions are integrated throughout NATO maritime doctrine, Allied Tactical Publications, TTPs and other publications. At the Joint level, CIMIC is a unique function and formally recognized as such in NATO CIMIC doctrine and TTPs. However, the fundamental CIMIC functions (liaison, cooperation and coordination) are the same, regardless of the operating environment, but the specifics of their practical application may vary considerably across maritime and land domains. NATO maritime and land forces lack a general reciprocal awareness and knowledge of the CIMIC functions performed in each other's domain. Furthermore the CMEE Final Experimentation report states, NATO staffs do not fully recognize maritime force CIMIC capabilities. This may be attributed to a training deficit, but may also be due to peacetime establishment reductions and realignments.

CIMIC functions performed by NATO maritime forces in the maritime environment are not distinct from CIMIC functions performed by NATO land forces in a land environment. The actual conduct of CIMIC functions within NATO; however, is domain specific. The conduct of CIMIC functions in the maritime environment is integrated into everyday maritime tasks. However, in the land environment, the performance of CIMIC functions is conducted by a unique occupational group. Maritime forces collect a huge amount of civil related information and provide them to their respective higher command. This information is normally not fed into the civil picture at the joint level. This lack of reporting could impact the coherence of NATO's Strategic Communications objectives.

Comparison of Maritime Functions and NATO CIMIC

Pic 1. The head of NSC briefing an Admiral on an ongoing operation
(Photo from NSC webpage: http://www.shipping.nato.int/Pages/aboutus.aspx

The following two explicit examples illustrate the proximity of CIMIC functions performed by NATO maritime forces in the maritime environment, and CIMIC functions performed by NATO land forces in a land environment:

1. NATO Shipping Centre (NSC)

The NATO Shipping Centre is the primary point of contact between NATO and the international shipping community. Additionally, it is an advisor to merchant shipping regarding potential risks and possible interference with maritime operations. Their mission is to provide improved information exchange on merchant shipping matters, and facilitate increased voluntary co-operation between military commanders and commercial shipping operators. They collect and process merchant shipping information to develop a picture in areas of interest to support military operational requirements and advise the shipping as required of the evolving situation. The NSC is the primary point of contact for the exchange of merchant shipping information between NATO's military authorities and the international shipping community.

2. Naval Cooperation and Guidance for Shipping (NCAGS)

NCAGS is the provision of cooperation, guidance, advice and assistance to merchant shipping in support of the commander's mission and to enhance the safety and security of merchant ships. Maritime trade is a fundamental strategic interest to nations. Economic wealth depends on the ability to trade, which in turn depends upon freedom of navigation. The Alliance's capability for operations involving merchant shipping is NCAGS, with its associated tactics, techniques and procedures. Maritime operations frequently affect merchant shipping. Similarly, merchant shipping may impact, or be involved in, maritime operations. NCAGS is the interface with merchant shipping in support of the operational commander's mission. NCAGS enhances and contributes primarily to the following effects:

- Commander's freedom of manoeuvre.
- Commander's decision-making process.
- Effective and efficient commitment and use of military assets.
- Nations' economic well-being and international stability.
- Free flow of maritime trade in the area of operations.
- Merchant shipping's confidence in military operations.

NCAGS must be flexible and prepared to operate within a wide variety of command structures and operational environments. In a particular operation, the NCAGS response should be tailored to the scenario and coordinated with other warfare disciplines in order to deliver the desired effects.

The similarity between the Maritime Functions and NATO CIMIC becomes even more apparent if the definition of CIMIC and the CIMIC Core Functions are put side by side with these two functions:

Pic 2: NCAGS officer providing advice to merchant shipping officers
(Photo from navalforce.wordpress.com)

CIMIC Definition:

"CIMIC is the coordination and cooperation, in support of the mission, between the NATO Commander and civil actors, including national population and local authorities, as well as international, national and non-governmental organizations and agencies."

CCOE advocates fostered mutual understanding and the enhancement of the interoperability between maritime and land forces. These can be achieved best by identifying maritime procedures and reporting the execution of CIMIC functions to higher level commanders. Furthermore, the participation of maritime stakeholders in NATO CIMIC related activities, courses, events, publications, projects, and workshops as well as the awareness and understanding of NATO CIMIC doctrine, TTPs and doctrinal publications across maritime tactical staffs and units has to be increased.

CIMIC Core Functions:

1. Civil-Military Liaison

2. Support to the Force

3. Support to Civil Actors and their environment

Recommendations

Existing NATO CIMIC doctrine, TTPs and doctrinal publications have to be updated to reflect CIMIC functions performed in the maritime environment. Within the training and exercise landscape, a general maritime awareness of CIMIC functions has to be implemented. NATO CIMIC related exercises have to be broadened and enriched by maritime storylines to make the CIMIC personnel aware of the maritime environment. The updated doctrinal documents should cover tactical up to the lower operational levels. The same comes into consideration when considering TTPs. Existing TTPs are land-focused. This does not make them invalid, but of lesser use for the maritime community. Revision and adaptation would seem to be appropriate.

These recommendations lead directly to the development of a Standard Operator Profile for on-board personnel when it comes to CIMIC and comprehensiveness. It is much more than just the supply officer talking to the ship's agent. It should be designed by the appropriate organization but it should be understood across the maritime community as well as the joint level headquarters. Customized training and education at the tactical level is an issue that automatically raises the question of education and training at the senior and operational level. At this juncture, it is too early to be certain if there's a need for a Standard Operators Profile, as the two are compatible.

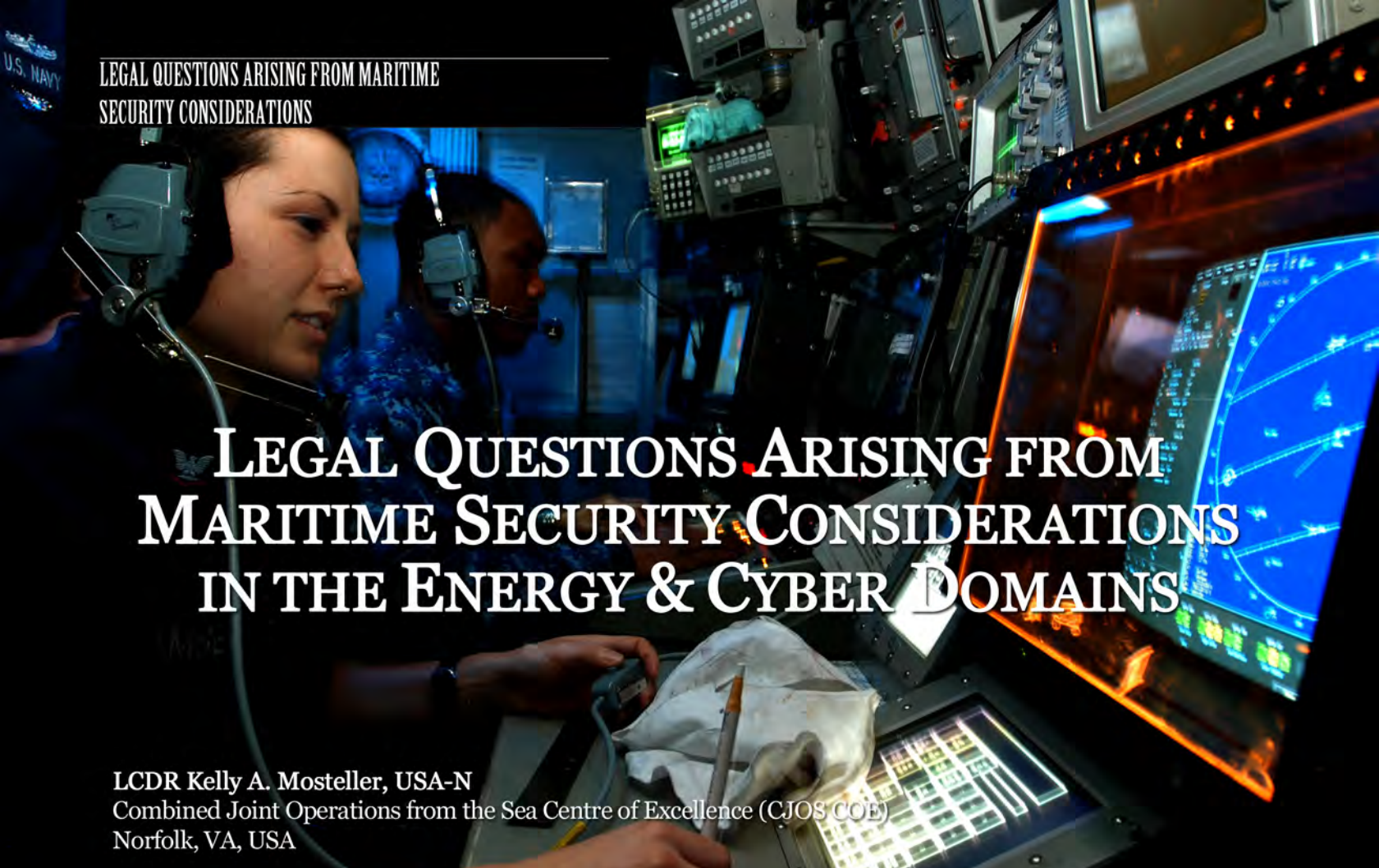
Conclusion

The operational environment is complex. A NATO response must therefore be integrated into a wider overall framework or a comprehensive approach. NATO's contribution to a comprehensive approach is the link to the civil environment with CIMIC as the military facilitator. This enables the operational commander to reach the desired end state by coordinating, synchronizing and de-conflicting military activities with civil actors, thus linking military operations with civil objectives. NCAGS is a contributor to the NATO comprehensive approach through its interface and liaison with merchant shipping civil actors. However, NCAGS is not shared across all strategic environments. Nonetheless, it is an example of CIMIC that requires capabilities, assets, knowledge, social and professional networks, techniques and interagency relations unique to the maritime domain. These activities require very specific knowledge, procedures and skills that can only be provided by naval personnel. In addition, NCME liaises with special and unique entities, which provide very special services to military and civil customers.

Similarities of CIMIC functions performed by NATO maritime forces in the maritime environment and CIMIC functions performed by NATO land forces in a land environment provide an excellent opportunity to continue the dialogue initiated by the CIMIC in the Maritime Environment Experiment (CMEE) in 2009. NCME is not just another outcome resulting from an experiment, but is being conducted throughout navies almost on a daily basis. CCOE sees itself as an advocate in the creation of a mutual understanding and enhancement of the interoperability between maritime and land forces.

CDR Vanek is a Staff Officer in the Concepts' Branch at the CCOE in Enschede, Netherlands.
For further information, he may be contacted at vanek.o@cimic-coe.org.
For further information about CCOE, please visit the CCOE web page at www.cimic-coe.org.

CIMIC COE



LEGAL QUESTIONS ARISING FROM MARITIME SECURITY CONSIDERATIONS IN THE ENERGY & CYBER DOMAINS

LCDR Kelly A. Mosteller, USA-N
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

Homeland Security

Introduction

Several news-worthy events this year have highlighted the intersections of the energy sector and the cyber domain with maritime security.

Maritime criminals in the Gulf of Guinea specifically target vessels carrying crude oil, impacting production costs and regional security. In October, it was revealed that cyber-attacks on the system controlling the location and movement of shipping containers had allowed criminals to smuggle tons of cocaine and heroin through the Port of Antwerp over a two-year period. Doomsday scenarios envision criminal or terrorist organizations taking control of a chemical tanker's e-navigation system and remotely piloting the ship for use as an instrument of destruction.

Despite certain drawbacks, the energy industry and cyber technologies can also enhance safety at sea and improve maritime security. Novel legal issues arise from the place where maritime security considerations overlap the energy sector and cyber domain, and these issues should be considered carefully by militaries, policy-makers, and intergovernmental bodies when crafting solutions to twenty-first century maritime security challenges.

Energy

The economic implications of the intersection of energy and maritime security are widely explored. Legal issues; however, continue to arise, and many remain unsettled. Some of these issues are definitional, and might be resolved through stakeholder conferences aimed at reaching consensus on the meaning or application of key terms. However, some legal issues arise from social or political deficiencies. Experts note the frequent coincidence of large natural resource stores and weak governance systems; this complicates the relationship between extractive companies and their host nations and muddies the legal waters when issues arise.

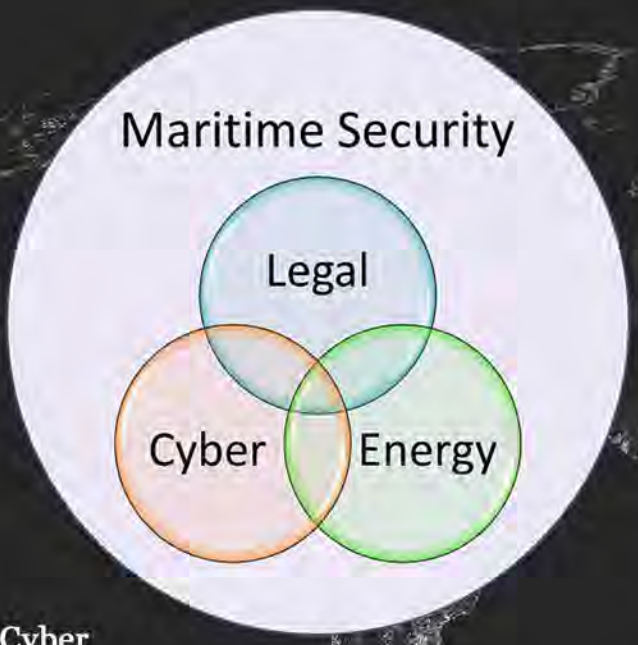
The extractive industry is often named as a catalyst of maritime security challenges in the Gulf of Guinea. Issues of resource distribution and disenfranchisement give rise to social unrest and crime that often spills over into the maritime domain. Data from the International Maritime Bureau indicates that maritime criminal organizations based in Nigeria specifically target vessels associated with the extractive industry: crude carriers are hijacked and their cargoes stolen, oil platforms require constant security to protect their crew and suppliers, and illegal bunkering is rampant throughout the Niger Delta.

Legal questions that arise from this situation revolve around definitions of piracy, jurisdiction over maritime crime, and the strength (or existence) of domestic laws governing maritime crime. International efforts to develop better means of bringing maritime criminals to justice, such as task forces to aid in the development of domestic laws and the establishment of the Regional Anti-Piracy Prosecution and Information Coordination Centre (RAPPICC) in the Seychelles, have met with some success, but these efforts and similar initiatives merit additional attention.

The environmental impacts of oil and gas extraction can contribute to threats against maritime security. Oil spills or leaks from extraction sites, and pollution from rigs or vessels have led some communities to resort to what they see as vigilante justice, particularly if the community was heavily dependent upon the maritime environment for their livelihoods. In these environments, the question of how communities can recover against extractive companies for damage caused to the living resources is often challenging, particularly in countries lacking effective legal institutions.

In regions where new offshore deposits of oil and natural gas have recently been discovered, countries may choose to commit a substantial portion of their maritime defense capabilities to protecting those lucrative assets. This leaves the rest of their maritime territory undefended from threats such as illegal fishing or pollution, or rendering an effective response impossible in the event of a maritime disaster such as a ferry sinking. This presents a legal and policy challenge regarding a government's duty to protect its people through effective legislation and regulation of public services like transportation and national resources like fish stocks.

Despite its role in exacerbating maritime insecurity, the energy sector could, and arguably does, contribute to greater maritime security, though this also raises some legal issues. Increased exploration of offshore formations results in a higher number of vessels and rigs in many areas. This can contribute to a greater awareness of what is taking place in the maritime domain, as well as greater importance being placed on maritime security. Indeed, discoveries of oil and gas offshore have contributed to a reduction in "sea blindness," or the lack of concern that many countries show for the issues affecting their territorial waters and exclusive economic zones, as these countries begin to recognize the lucrative resources under their waters and the need to protect those resources in order to reap the economic benefits.



Private armed security teams onboard vessels have been credited with the dramatic reduction in successful pirate attacks off the east coast of Africa. But the presence of these armed guards raises legal issues in regard to when a vessel is engaging in innocent passage. A vessel must be aware of the laws of each country whose waters it sails, as most countries restrict the presence of armed vessels in their territorial waters.

Many of the countries blessed with abundant energy resources are also burdened with ineffective governance institutions. Thus, when it comes to the intersection between the energy sector and maritime security, the legal issue that emerges most clearly is the need for international cooperation to strengthen the regulatory, legal, and law enforcement systems of oil-rich countries.

Cyber

The cyber domain both enhances maritime security and creates vulnerabilities in the maritime sector. Understandably, mariners want to be cautious about sharing information in order to protect themselves from potential exploitation, but national militaries and international bodies often seek greater information sharing as a means of enhancing the their maritime domain awareness (MDA) and developing a Recognized Maritime Picture (RMP). Balancing these interests has created new legal and policy questions.

The cyber domain facilitates information sharing that can contribute to maritime security. MDA systems can improve early warning capability for threats and response capability for disasters, improving the ability of national maritime authorities to secure their waters and maritime infrastructure. Digital and internet-based technology also enables the coordination of multinational forces in international waters.

Legal issues of privacy arise when discussing the type and extent of the information being shared, with whom the information is shared, and under what parameters it is shared. Ship and cargo tracking can be accomplished more easily in using digital technology, but issues of privacy and intellectual or commercial property arise in these realms also.

Despite the benefits cyber-based technologies can bring to maritime security, the prevalence of cyber-based control systems has also created some weaknesses in critical maritime areas. The Port of Antwerp, Belgium uncovered a drug smuggling operation that had been underway for approximately two years beginning in June, 2011. In October 2013, it was revealed that the smugglers were using hackers and other cyber-theft methods to redirect the containers in which the contraband was shipped, and steal them from the port. Legal issues may arise if a country's laws have not been updated or are not broad enough to encompass the cybercrime that can threaten the maritime infrastructure.

Always seeking greater efficiency, some shipping companies are turning to e-navigation. The International Association of Lighthouse Authorities (IALA) defined e-navigation as the "harmonised collection, integration, exchange, presentation and analysis of marine information onboard and ashore by electronic means to enhance berth to berth navigation and related services, for safety and security at sea and protection of the maritime environment." Some have raised concerns whether e-navigation opens control of ships to hackers, but a more important legal question may involve the apportioning of liability in the event that a ship relies on the e-navigation concept to its detriment.

The mandatory use of Automatic Identification System (AIS) raises legal issues as well. AIS allows other ships as well as coastal authorities to see information about the ship, including its identity, type, position, course, speed, navigational status, and other safety-related information. Many mariners, however, are concerned that using AIS can facilitate criminals and pirates targeting their vessel, and frequently turn AIS off when they are transiting through higher-risk waters. Failing to use AIS can open a vessel to civil penalties in certain countries.

Placing greater control of maritime assets -- whether containers, charts, or ships -- in the cyber domain demands commensurate increases in cyber security. In February 2013, President Obama signed an Executive Order assigning responsibility for critical infrastructure cybersecurity to various executive agencies. The order contemplated issues such as enforcement, intellectual property rights, and privacy concerns of affected parties. Significant milestones provided in the Order will be complete by May 2014, and it would be prudent for international maritime bodies to adopt best practices from the U.S. process to their own consideration of maritime cybersecurity issues.

Conclusion

Maritime security has long posed unique challenges to the national and international legal systems that seek to address it. New discoveries and the growing importance of offshore energy sources have added to the complexity of governance over these areas, and opened new geographic regions to maritime security threats. Rapid advances in cyber applications have helped to improve awareness of the maritime domain, but they have also created certain vulnerabilities in the maritime sector that could facilitate smuggling, terrorism, or attacks on a nations' critical infrastructure. The legal environment has not been able to keep pace with these changes in the maritime security environment, leaving gaps in the current international and national legal responses. National and international bodies must develop clear legal guidance so that those organizations charged with maintaining global maritime security can do so with the confidence that their enforcement actions will be in support of the law, not against it.

Sources:

- Bateman, Tom. "Police warning after drug traffickers' cyber-attack." BBC News, October 16, 2013. http://www.bbc.co.uk/news/world-europe-24539417 (accessed December 30, 2013).
- Executive Order 13636. "Improving Critical Infrastructure Cybersecurity." Federal Register 78, no. 33, 11737-11744. February 19, 2013.
- Fischer, Eric A. et al. The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress. CRS Report R42984. Washington, DC: Library of Congress, Congressional Research Service, November 8, 2013. https://www.fas.org/sgp/crs/misc/R42984.pdf (accessed December 30, 2013).
- International Association of Lighthouse Authorities. IALA Dictionary. http://www.iala-aism.org/wiki/dictionary/index.php/E-Navigation (accessed December 26, 2013).
- International Maritime Organization. "Automatic Identification Systems (AIS)." http://www.imo.org/OurWork/Safety/Navigation/Pages/AIS.aspx (accessed December 29, 2013).
- Kramek, Joseph. "The Critical Infrastructure Gap: U.S. Port Facilities and Cyber Vulnerabilities." Washington, DC: Brookings Institution, July 2013.
- North Atlantic Treaty Organization. "Energy security: a major factor in international security." September 9, 2013. http://www.nato.int/cps/en/natolive/news_102919.htm (accessed December 30, 2013).
- U.S. Department of Homeland Security, U.S. Coast Guard. "Cyber Security." http://www.uscg.mil/hq/cg5/cg544/cybersecurity.asp (accessed December 26, 2013).

CJOS COE NAVY RESERVE

LCDR Mosteller is a Reserve Staff Officer at CJOS COE in Norfolk, VA. For further information, she may be contacted at kelly.mosteller@navy.mil. For further information about CJOS COE, please see the CJOS COE web page at www.cjoscoe.org.

UPDATES:

Amphibious Operations Working Group (AMPHIOSWG), Allied Joint Operations Doctrine Working Group (AJODWG), & Alternate Command & Control Relationship & Staff Organization for Amphibious Operations (EXTAC) Maritime Operations Working Group (MAROPSWG)

CAPT Massimiliano Nannini, ITA-N
CDR Pedro Fonseca, PRT-M
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

Amphibious Operations Working Group - AMPHIOPSWG

The annual NATO Amphibious Operations Working Group (AMPHIOPSWG) was held in Brussels, Netherlands from July 8 through July 12, 2013 and was hosted by NATO HQ. This working group was established by the NATO Military Committee (MC) through the Maritime Standardization Board (MCMSB) and their focus is to develop standardization in numerous amphibious arenas in order to enhance NATO forces effectiveness and interoperability. The AMPHIOPSWG deals primarily in amphibious doctrine, techniques and training methods, equipment for use in amphibious operations, communications, operational intelligence, and command and control relationships. As an emerging authority on "Operations from the Sea", CJOS has participated in this working group since 2004, along with many NATO and partnering nations, strategic and operational military commands, Centres of Excellence, and numerous civil standardization development organizations.

Allied Joint Operations Doctrine Working Group - AJODWG

For the first time, CJOS COE joined NATO's Allied Joint Operations Doctrine Working Group (AJODWG) held in Amsterdam, Netherlands from the October 21-25, 2013 which was hosted by the Civil-Military Co-operation Centre of Excellence (CCOE). The AJOD was established by the Military Committee Joint Standardization Board (MCJSB), acting in its capacity as an MC Delegated Tasking Authority. Their primary mission is to enhance the interoperability of NATO forces while planning and conducting Joint Operations. This is accomplished through the provision of Allied Joint Doctrine and ensuring an emphasis on doctrine at the operational level. This includes development, review, and harmonization of Allied Joint Publications (AJP) as well as the formulation of related terminology. The AJODWG is attended by NATO and Partnership for Peace (PfP) nations, the International Military Staff (IMS), strategic commands, NATO subordinate commands and agencies that agree to participate.

Alternate Command & Control Relationship and Staff Organization for Amphibious Operations Extract from Tactical Publications (EXTAC)

In October 2012, CJOS COE, at the request of the Royal Netherlands Maritime Warfare Centre, produced a white paper titled "Alternate Command and Control Relationship and Staff Officer Organization for Amphibious Operations." This document was developed in consideration of today's economic climate and the need for reduced military staffs and describes some alternative staff organizational structures. During post-publication discussions with the Royal Netherlands Maritime Warfare Centre, it was decided to work on an EXTAC to this publication.

In order to provide dedicated manpower and effort for this study, the initial concept of the EXTAC was included in the CJOS COE Program of Work (POW) 2012. It focuses on improving the effectiveness of amphibious staffs and the optimization of C2 systems that assist in projecting and sustaining combat power ashore. By concentrating on staff effectiveness and C2 optimization, the concept concludes a diminished need for transfer of command. This allows the Commander Landing Force (CLF) to remain on board and reduce the number of augmenters and duplication of staff function for the two environments (sea and land). In reality, this has already contributed to today's way of conducting operations from the sea and has changed the underlying assumptions for amphibious operations by removing the need to set up facilities, equipment and additional personnel ashore. It minimizes the footprint and risk ashore, enhancing the land forces ability to conduct operations directly against a foe´s center of gravity simultaneously by air and sea.

Worldwide threats, from conventional to asymmetric, demand the use of active and agile organizational structures while maintaining a robust ability to develop complex plans and conduct a wide range of military amphibious missions. Developing and training to this structure and capability allows the effective use of smaller units in the execution of tactical, operational and strategic goals. Nonetheless, the decision of what is the appropriate command organization must be driven by the need to ensure flexibility and mobility in order to concentrate efforts and strike properly for mission accomplish.

The EXTAC exploits all available synergies to achieve a smaller, integrated command staff. Operating with a reorganized staff in a common command center will reduce resources and manpower requirements ashore. By utilizing a single C2 structure that is better suited for small scale operations, it can be an alternative to current doctrine, ATP-8(B) Volume I. The command authority will be capable of achieving a faster planning and decision cycle. In conjunction with the Royal Netherlands Maritime Warfare Centre, the EXTAC is currently being worked at the staff level.

Maritime Operations Working Group (MAROPSWG)

The Annual NATO MAROPSWG was held in Taranto (Italy) from JAN 21 to JAN 30 and hosted by the Italian Navy. The MAROPSWG was established by the Military Committee Maritime Standardization Board (MCMSB) to develop standardization in doctrine, tactics and tactical instructions and procedures in maritime operations in an effort to improve the effectiveness of NATO forces. The MAROPSWG is the largest MCMSB Working Group and is responsible for a wide range of tactical publications. It is attended by the majority of national Maritime Tactical Schools, mainly at the OF-5 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 to standardize Maritime Operations by NATO Forces to include, but not limited to, Submarine Warfare, Anti-Submarine Warfare, Above Water Warfare, Tactical Communications, and maritime Electronic and Acoustic Warfare.

Major progress was made this year on the development of AJP-3.1 and ATP-01(G) which are the two capstone publications for maritime operational and tactical level doctrine. Both of these major documents are anticipated to be ratified this coming year. Their completion will be a major success for this working group, and a testament to the dedicated work of the drafting teams and delegates.

CJOS COE

Captain Nannini and CDR Fonseca are stationed at Combined Joint Operations from the Sea Centre of Excellence. For further information about this article, please contact them at cjocoe@navy.mil.
For further information about the Programme of Work for CJOS COE, please visit our web page at: www.cjoscoe.org

The Increased Importance of Cyber Security and The Vulnerabilities Within The Maritime Domain.

Steps & Initiatives.

CDR Lucian Grigorescu, ROU-N
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

Since the terrorist attack on 9/11, governments around the world have invested millions to protect its critical infrastructure against attacks. Protection against physical attacks have significantly improved over the years, yet a critical portion of a nation's critical infrastructure remains vulnerable to an increasing threat, that of a cyber-attack. After "Titan Rain," a series of coordinated attacks on U.S. computer systems between 2003-2006, the second largest state-sponsored cyber-attack on the Estonian public and private sector in April 2007 raised global awareness of state-sponsored cyber-attacks. There are many cyber vulnerabilities within the maritimedomain. Governments and organizations have had initiatives to mitigate some risk associated with these vulnerabilities, but many steps need to be done and many aspects taken into considerations. Do we need a cyber-calamity or a 9/11 cyber incident within the maritime domain to raise the awareness and the importance of cyber security in the maritime arena?

The Arctic convoys of World War II were oceangoing convoys that sailed from the United Kingdom, Iceland, and North America to northern ports in the Soviet Union. There were 78 convoys between August 1941 and May 1945 that escorted 1400 merchant ships delivering essential supplies to the Soviet Union. The convoys were escorted by ships of the Royal Navy, Royal Canadian Navy, and the U.S. Navy, because at that time, the "enemy" was real and detectable. Nowadays, in the internet age, as more devices are connected online, the "enemy" is real, but often concealed and untraceable. As industries in the maritime and energy domains connect ships, containers and rigs to computer networks, they expose themselves to weaknesses that can be easily exploited. "Increasingly, the maritime domain and energy sector had turned to technology to improve production, cost and reduce delivery schedules," said CDR Ricky McIver in his article, Delivering Maritime Security in Global Partnership. "These technological changes have opened the door to emerging threats and vulnerabilities as equipment has become accessible to outside entities."

"When you look at the maritime industry, there's extremely limited evidence of systems having been breached," *compared to other sectors.*

"That suggests to us that they've not yet been found out."

Lars Jensen, founder of CyberKeel, a maritime cyber security firm, 2014

The prefix "cyber" is derived from a Greek adjective meaning skilled in steering or governing. The prefix is commonly used in computer, networking or electronic context to denote control. Thus, Cyber Security is associated with control of computers, networks and electronic security. Whether or not it can be agreed upon internationally, the definition of Cyber Security in the Maritime Domain, organizations realize the necessity to address maritime vulnerabilities and associated risks in a separate manner rather than incorporated or implied within Cyber Security in general (e.g. ENISA was one of the first organizations that hosted a workshop in Cyber Security focused on the maritime sector).

Maritime Security is about the protection and safety not only of the critical infrastructure that support services in the maritime domain, but also about securing the trading routes for transportation of energy (oil and gas) and essential and indispensable goods. In this new cyber era, it should be considered to include the security of the transfer and availability of information with the maritime domain. Any disruption in the supply chain may prove itself instrumental to the economy and population. Among the many means of disruption, the Cyber threat is growing and has been recognized as such by many stakeholders, governments and main actors from the private sector. In an era of sophisticated technologies and automation, the cyber threat is closer than it seems.

If we consider Integrated Navigations Systems (INS), Automatic Identification System (AIS), GPS, or the technologically sophisticated systems and products such as undersea production and processing systems, surface wellhead systems, high pressure fluid control equipment, and marine loading systems for the oil and gas industry, there is much evidence that vulnerabilities exist, as most of the systems are connected to cyber domain and exposed to cyber threats. There is also plenty of evidence to show that the average maritime company, vessels or facility is vulnerable to a cyber-attack. The likelihood that a terrorist will target a particular company, vessel or facility might be low, but not zero. It has been proven by the attacks on the destroyer USS Cole in Aden on October12, 2000, the supertanker Limburg of Yemen on October 6, 2002, and the supertanker M Star in the Strait of Hormuz on July 28, 2010.

Marine facilities have not been exempt from terrorism, with attacks on Ashod, Israel on March 13, 2004; the Iraqi Khawr al Amaya crude oil terminal on April 24, 2004; and the Karachi East Wharf in Pakistan on May 26, 2004. Terrorism has remain largely in the physical domain, but recently, a floating oil rig was shut down by cyber-attack which caused the platform to tilt out of safety standards. During another cyber incident, another oil rig was so riddled with computer malware that it took 19 days to make it seaworthy again. Somali pirates choose their targets by viewing navigational data online, prompting ships to either turn off their navigational devices, or fake the data so it looks like the ship is somewhere else.

Terrorism aside, there is a egocentric reason for hardening maritime assets against a cyber-attack. By taking such steps, it could be protected against such threats as spurious electronic signals, malicious activity, industrial espionage and criminal activities. Viruses and worms like Sasser, Stuxnet, Shamoon, and Duku are just a few examples of "tools" that can be used to collect information and disrupt normal business, affecting the supply chain and marine safety. In addition, we can consider the vulnerability of energy companies working in the maritime domain to cyber penetration. Destruction of the infrastructure may not be the main objective.

The goal is more likely to gain a competitive advantage by stealing intellectual property like oil/gas exploration findings to know where a company believes its resources to lie. This information could place some states in a better position to take advantage of their competition because there are states better positioned to act to overtake competitors because it steals other government and energy companies' secrets through an aggressive cyber campaign. Globally, it estimated that cyber-attacks against oil and gas infrastructure will cost energy companies close to $1.9 billion by 2018. The British government reckons cyber-attacks have already cost Great Britain oil and gas companies around 400 million pounds ($672 million) a year.

Forfeiture of advantage is a long term vulnerability that could be more devastating than the temporary shutdown of any infrastructure. On May 10, 1993, the US Coast Guard promulgated a new regulation by which the tankers equipped with an Integrated Navigation System (INS) could, under certain circumstances, use the INS with the auto pilot engaged while in the navigable waters of the United States.

Short-lived, the regulation was suspended on July 6, 1993 after a vessel utilizing its INS experienced a sudden, unintended, and drastic course change when the INS malfunctioned as a warship in the vicinity emitted a strong signal. Although the Coast Guard recognized that the use of INS with an autopilot offered the potential to improve navigation safety, adequate testing and evaluation of this technology had not been conducted. There is a growing threat to the ships, marine safety, security, and environmental protection from the over-reliance of electronics to accomplish operational tasks. Adopting appropriate cybersecurity measures will reduce those risks.

In the June 2003 edition of Maritime Reporter & Engineering News, an article was published entitled: "AIS – Panacea or Pandora's Box." When operating as intended, the Automatic Identification System (AIS) is an important navigational safety tool, particularly with respect to collision avoidance. Because of the way the transceiver is configured, much of the data being transmitted can be manipulated. Based on studies, the reliance on AIS as a maritime security tool has been questioned. Recently, it has been demonstrated that AIS signals can transmit false locations, incorrect course and speed, and ghost images.

In the September 2013 edition of the same magazine, another article was published entitled: "GPS Spoofing." It is now possible to spoof Global Positioning System (GPS) and other space-based positioning, navigation, and timing (PNT) services. As with AIS, these PNT services must incorporate an authentication system or adopt other measures to avoid accidental or intentional presentation or erroneous data. Work is currently underway to address these issues, but will likely make spoofing more difficult, but not impossible.

In March 2014, Marco Balduzzi, an anti-virus vendor for Trend Micro, showed that an attacker with a $100 VHF radio could exploit weaknesses in AIS. Mr. Balduzzi illustrated the ability to tamper with the data, impersonate a port authority and/or their communications with a ship, or effectively shut down communications between ships and ports. One can no longer inherently trust the AIS signals being received by the transceiver and displayed on the Electronic Chart Display and Information System (ECDIS). The system would benefit from revision to incorporate an authentication program.

There is also an important legal vulnerability. The rules of engagement in cyber warfare (defensive and offensive) are not only the legal partnerships between a government and its public but also with other nations. If there is no public-private business partnership, real national cyber defense is an illusion, and if there is no international convention allowing defensive and offensive actions, all countries are vulnerable regardless of their domestic cyber capabilities. Similarly, when applied within the maritime domain, it is and it will continue to be difficult to pursue the perpetrators of cyber-incidents in territorial waters, and even more challenging in international waters.

There are some steps that have been taken to mitigate and manage the cybersecurity risks. The US National Institute for Standards and Technology (NIST) has developed a Preliminary Cyber security Frameworkiii. The objective is to encourage organizations to consider cybersecurity risk as a priority similar to financial, safety, and operational risk, while factoring in larger systemic risks inherent to critical infrastructure.

In 2011, ENISA has published the first EU report ever on cyber security challenges in the Maritime Sector. This principal analysis highlights essential key insights, as well as existing initiatives, as a baseline for cyber security. High-level recommendations are given to address these risks, one of most important being that the International Maritime Organization together with the UE Commission and the Member States should align international and EU policies in this sector.

The US Department of Homeland Security has established a Cybersecurity Training & Exercises Websitev to assist organizations in becoming familiar with and staying current on cybersecurity threats and available countermeasures. Of more relevance to the maritime community is the US Coast Guard cybersecurity site accessible through Homeport. The site provides access to a variety of background documents and links to other cyber-related websites and members are provided with recommendations and activities to help them to maintain awareness of cybersecurity issues. Also, the Coast Guard has included cybersecurity issues in its various Area Maritime Security Plans.

The Software Engineering Institute (SEI) sponsored by the U. S. Department of Defense had many initiatives that helped government and industry organizations to develop and sustain software systems that are enduring and innovative. They published annual and research reports with interesting findings about maritime management in the arena of cyber security, cyber resilience and global information-grid survivability. SEI's host, Carnegie Mellon University (CMU), a global research university that is rated among the best for its programs in computer science and engineering has organized seminars and published reports about building cyber capability to meet Navy's maritime challenges; cyber readiness with a focus on maritime combatants; cyber threat information on transportation systems; maritime GPS traces; and, resilient C2 in contested cyber environments.

Steps should be taken by members of the maritime community to enhance their cybersecurity. If we consider critical infrastructure within the maritime domain, the ships are the maritime connection of infrastructure. In June 2014, the U.S. Government Accountability Office (GAO) produced a report to the Chairman of the Committee on Commerce, Science and Transportation because the actions taken to address cybersecurity in the maritime port environment have been limited. The report emphasized the "Needs to better address Port Cybersecurity."

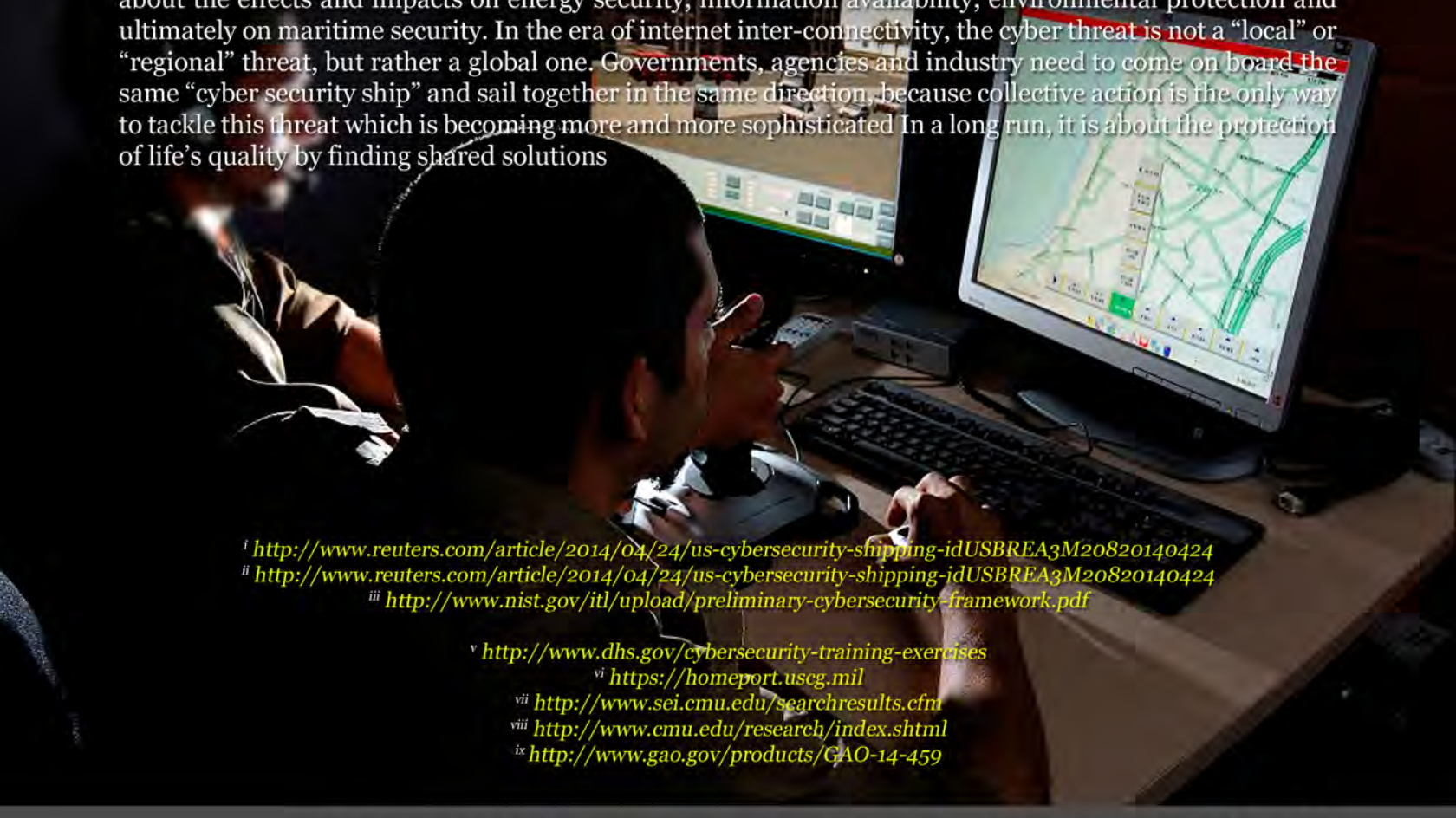
Probably, the most important step is greater international information sharing (specifically ethics and policies) on cyber probes, attacks and incidents, so that companies and governments achieve a higher level of awareness and can then take steps to prevent similar attacks from happening across the entire maritime domain. While some action is being taken today, it is mainly voluntary and many companies keep their vulnerabilities veiled because they don't want the public or their clients to lose trust in their capabilities.

Another important aspect is the "consequence management." How does the maritime industry deal with major cyber-attacks that might lead to electronic and physical damage?
The main focus is not only environmental damage, but perhaps more to the point, what kind of planning should be in place to ensure that there are back-up systems, failsafe systems, or alternative ways to support the maritime industry operations when parts of the system are under attack? These topics could be interesting aspects to further explore.

What does the future hold? How long it will take to demonstrate the wireless ship hacking?
British engineering company Rolls-Royce has been working on hardware and software systems designed to turn the giant cargo ships into semi or fully autonomous robots. The company says that these drone ships would be safer and more efficient than manned ships, but the shipping industry although interested, is not ready for unmanned ships. Rolls-Royce is creating a prototype of a virtual reality display system which would give a captain 360-degree views from this virtual bridge. The captain can move from virtual bridge to virtual bridge, theoretically overseeing the control of many different ships at once through remote supervised autonomy. From a cyber-threat perspective the remote supervised autonomy will bring more vulnerability that can be exploited for other reasons than supervision.

There are many aspects that demonstrate the equal importance of securing critical infrastructure of the maritime sector, the freedom of information flow and the movement of vital goods. These aspects should and will become areas of concern and a priority for the main actors within the maritime domain.

The concern is not only about preventing cyber-attacks on maritime "cyber targets," but most importantly about the effects and impacts on energy security, information availability, environmental protection and ultimately on maritime security. In the era of internet inter-connectivity, the cyber threat is not a "local" or "regional" threat, but rather a global one. Governments, agencies and industry need to come on board the same "cyber security ship" and sail together in the same direction, because collective action is the only way to tackle this threat which is becoming more and more sophisticated In a long run, it is about the protection of life's quality by finding shared solutions



[i] *http://www.reuters.com/article/2014/04/24/us-cybersecurity-shipping-idUSBREA3M20820140424*
[ii] *http://www.reuters.com/article/2014/04/24/us-cybersecurity-shipping-idUSBREA3M20820140424*
[iii] *http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf*

[v] *http://www.dhs.gov/cybersecurity-training-exercises*
[vi] *https://homeport.uscg.mil*
[vii] *http://www.sei.cmu.edu/searchresults.cfm*
[viii] *http://www.cmu.edu/research/index.shtml*
[ix] *http://www.gao.gov/products/GAO-14-459*

CDR Grigorescu is a Staff Officer with Combined Joint Operations from the Sea Centre of Excellence. For further information about this article, please contact him at Lucian.grigorescu.ro@navy.mil. For further information about the Programme of Work for CJOS COE, please see our web page at: www.cjoscoe.org.

CJOS COE

A New Dimension of War: C2 in Cyberspace

Captain Brian Chamberlain (US Marine Corps) & Lieutenant Darryl Diptee (US Navy)
US Fleet Forces Command, N6
Norfolk, VA, USA

Introduction

Information Dominance seeks to deliver an operational advantage through information technology (IT) while denying those capabilities to the adversary. Our networks are not merely applications and infrastructure that enable the delivery of information; rather, IT has been elevated to a critical resource needed to achieve the operational advantage. In kinetic wars the occupied space is a focal point for attack as it enables the delivery of valuable resources, making the ability to immediately and effectively respond to attack extremely critical. Similarly, the virtual space has become a focal point for attack thereby transforming cyberspace into a virtual battleground. Similar to the physical battlefield, a commander must have command and control (C2) of the cyber Area of Responsibility (AOR). Our collective military knowledge base is saturated with C2 strategies and best practices for traditional kinetic wars; but with cyberspace being our newest battlefield, how can C2 strategies of traditional kinetic wars be implemented in response to cyber attacks on the network infrastructure? Written from an operational purview, this article identifies the challenges of performing C2 in a war where the battlefield is the network itself and translates the tenets of C2 for kinetic war to this new battlefield. Embracing this new paradigm is demanding, but not doing so risks degrading maritime, national, and global stability.

Fundamentals of Command and Control (C2)

The foundation of C2 as we know it today is heavily focused on traditional kinetic warfare; however, the cyber adversary represents a new type of invisible actor with the ability to traverse across continents at the speed of light causing significant network destruction and/or degradation with a click of a mouse. Cyberspace has expanded the traditional battlefield adding a new dimension where time tested kinetic C2 strategies have yet to be properly translated into effective cyber defense. The fundamentals of C2 cover ten primary areas, six of which will be the focus of this article: clearly defined authority, information management, communication, timely decision making, coordination mechanisms, and battle rhythm discipline.

These established kinetic C2 strategies require suitable interpretation to master the art of war in cyberspace as this modern battleground poses serious challenges that must be addressed to achieve effective C2 within the cyber AOR. The following sections detail the fundamentals of C2 and translate those fundamentals with respect to the cyber realm.

Clearly Defined Authority

The first tenet of C2 is the authorities, roles and relationships between commands. The foundation of C2 is built upon a unity of command through the designation of a commander with the necessary authority to accomplish mission objectives via an uncomplicated chain of command.

In the cyber realm, however, one of the greatest challenges is identifying a single individual who has clear authority within the cyber AOR. While the Chief Information Officer (CIO) is the most senior executive responsible for information technology and the network infrastructure, many CIOs lack proper authority to direct IT implementation without organizational approval. Moreover the CIO often is unable to gain organizational support as the complexity of the cyber is often grossly misunderstood.

Certified and qualified CIOs should have the clearly defined authority that is commensurate with the responsibility of protecting the cyber AOR. However, the CIO's execution of successful cyber warfare and defense begins with positive organizational culture that avoids finger pointing and focuses on problem solving. The manifestation of a problem may have deeper root causes, so non-IT organizational leaders should remain open-minded and supportive of the CIO's efforts. If CIOs aren't empowered to a level of authority proportionate to the task of commanding the cyber battlefield, then there will be a lack of leadership.

Information Management

Information management enhances a decision maker's ability to make timely decisions despite the chaos and uncertainty of war. Proper information management seeks to make available pertinent information to the right person at the right time through established systems and procedures in order to generate the best possible outcome. Such outcomes are often facilitated through a Common Operational Picture (COP) which displays areas of responsibility, friendly and enemy forces, while aiding the commander with identifying points of friction.

Much data exists about individual networks; however, it remains challenging to refine this data into useful information that would assist a network executive in making timely decisions. An automated data collection process is necessary to pull, sift, sort, process, and push this data to a centralized location with a comprehensive display. This cyber COP would paint a clear picture allowing a commander to see what the cyber AOR looks like, who is responsible for portions of the network, and quickly identify any points of friction during a cyber attack. Just as it is critical to maintain fidelity on the distribution of forces in kinetic wars, it is also critical to know exactly what systems comprise the network. Without a cyber Common Operational Picture that updates in near real time, network defense will be performed blindly.

Communication

A commander must communicate commander's intent and the mission statement to subordinates. Doing so incorporates the purpose of the operation, method of execution and the intended end-state. This conveys the central idea without specifying how the mission should be accomplished enabling decentralized execution by subordinate commanders. The mission statement specifies the essential task(s) and purpose of the mission, and the required actions and reasons for execution. This promotes initiative throughout the chain of command by empowering those closest to the point of friction to take decisive action.

There is no difference in cyber operations, where unfortunately, there lacks a common cyber lexicon. Currently there is disparity in definitions across cyber organizations where simple words like: "protect", "attack" and "defend" may have different meanings. While it remains difficult to effectively conduct cyber operations without a common language that all organizations clearly understand, it is impossible to accomplish the commander's intent without a commonly understood operational task.

Timely Decision Making

Commander's intent and mission statement accelerate the decision making cycle. The operational advantage is gained by those who are more expeditious at assembling information and taking decisive action. In doing so the adversary is placed in a reactive position and is unable to set the terms for a decisive engagement. Timely decision making is not guaranteed by the aforementioned alone, but hinges on a decision making model that steers the commander toward a decision. This decision making model should remain dynamic to meet the changing landscape of the battlefield.

Having a decision making model is essential in cyber where the time-space gap is significantly narrowed leaving less time to react. Moreover, predicting adversarial activity can be extremely difficult and obtaining intelligence on future cyber attacks remains challenging as they can be designed, built and tested in complete isolation. When a breach of the network occurs this should trigger the assembly of a Crisis Action Team (CAT) that uses a decision making model tailored to the threat. Each stakeholder of the CAT should have clearly defined roles that contributes to the recovery. Simply disconnecting from the network while a deliberate course of action is developed is not sufficient. Once a threat has breached the network it will continue to degrade the network until removed.

Coordination Mechanisms

Effective C2 is further complicated when introducing joint and coalition partners. Organizational, cultural and language barriers are only a few of the obstacles that hinder synergistic interaction and integration. Implementing proper coordination mechanisms such as agreements and memoranda of understanding help fuse alliance members into a single cohesive force; however, pieces of paper alone are not enough to assimilate previously segmented forces into an organized faction. True interoperability requires levels of trust, understanding, and practicality that can only be obtained by the tacit exchange of knowledge between participants as is typically achieved via liaison exchange programs, joint exercises, integrated staffing, and maintaining multinational environments.

As one traverses the network it is quickly realized how many different organizations contribute to its infrastructure. Depending on configurations and other factors, it is possible for data packets to reach space satellites en route to a destination less than a mile away from the sender. Cyberspace has eliminated physical boundaries and to a great extent, organizational and national ones as well. Adversaries no longer have to cross oceans, mountains or valleys; they can be at your virtual doorstep by simply traversing the global network infrastructures. Therefore, implementing coordination mechanisms across organizations are now more critical than ever. As the mutual dependence for defending physical borders increases, so to will there be a need to mutually defend partner networks. An organization can only be well protected if all members of the alliance work in harmony to protect each other.

Battle Rhythm Discipline

A daily agenda of meetings, reporting requirements, briefs, etc. make up the typical battle rhythm and is a key component to the decision making process. The battle rhythm should not be laden with excessive meetings, briefings, or travel regardless of mission objective. A healthy command and control posture maintains a battle rhythm that perpetuates the decision making cycle and allows sufficient time to plan, effectively collaborate, and properly execute. Battle rhythm discipline rests in two areas; first, the battle rhythm must serve as an enabler for decision making. Second, stakeholders must strictly adhere to the timeline set by the battle rhythm and make relevant contributions.

When the CAT is activated, stakeholders should be within immediate reach and know what information is required to be gathered and briefed to organizational executives. Expectations outlined prior to an attack instill a sense of responsibility and accountability in those responsible for the network's recovery. This can be primarily achieved through realistic cyber attack simulations that exercise the CATs response. Responses to "real world" network attacks will closely correlate with the manner in which training occurs. Training for an impending cyber attack should be the standard, and not merely using attacks as an opportunity to train. Without a healthy battle rhythm, unit cohesion and unity of effort deteriorates.

Translating Kinetic C2 into Cyber

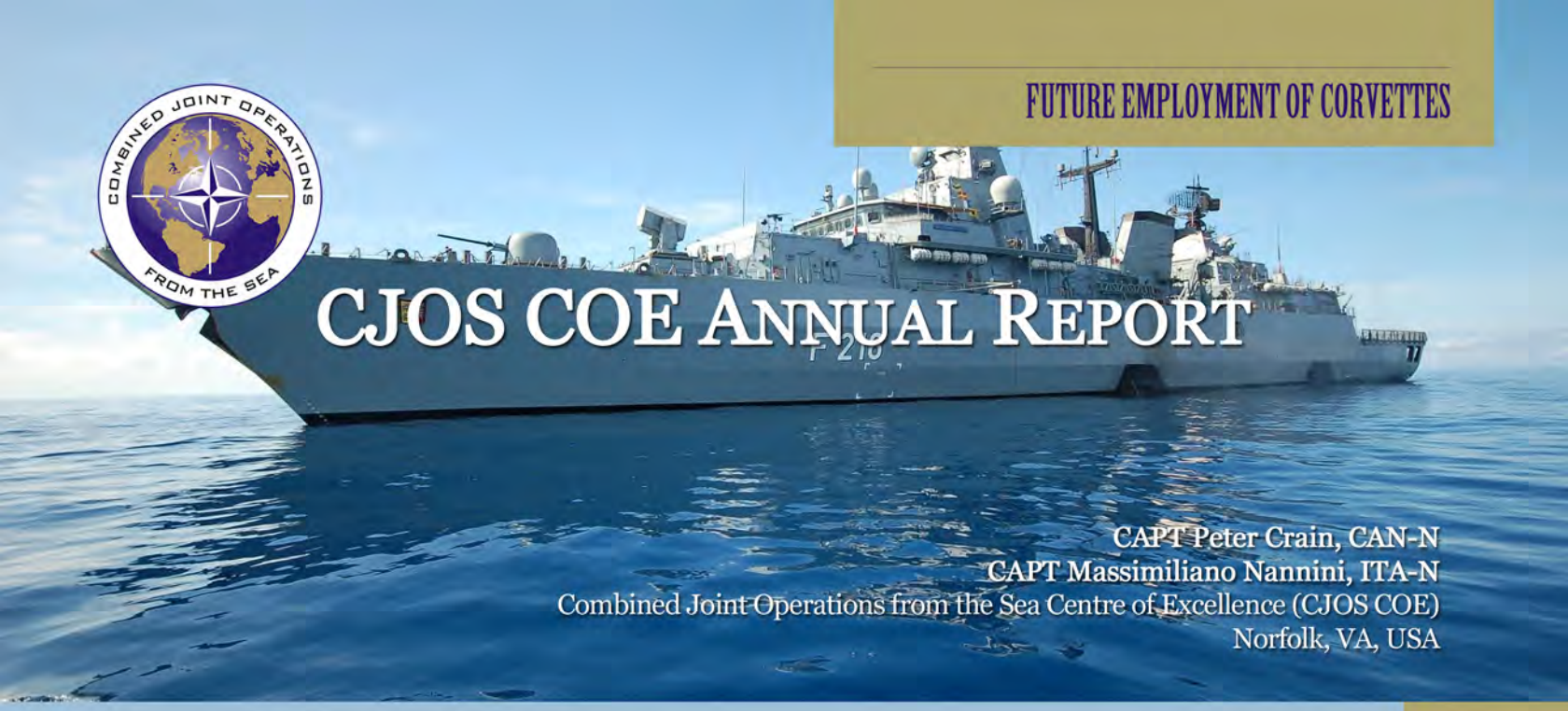
Dissemination of information at the strategic, operational and tactical levels of war is reliant on global networks, making it a critical vulnerability that is extremely appealing for an adversarial focus of attack. Cyber attacks are both cost effective and relatively safe for the belligerent. Furthermore, the enemy can hide behind international boundaries with little threat of physical retaliation as the definition of what constitutes a cyber act of war is not yet clearly defined. Thus this new battlefield should be commanded with a philosophy of C2 that is consistent with the environment.

The commander of the cyber AOR should be a CIO with requisite authority that is commensurate with their level of responsibility and one who understands the complexities of computer networking and cyber defense; in effect aligning positional responsibilities and personnel capabilities. A competent CIO can skillfully identify threats and what information is necessary for effective decision making. This should be facilitated by an automated system that creates a common operational picture depicting a logical topology of the network and captures pertinent information. A CIO also needs a common cyber lexicon to facilitate unambiguous tasking to subordinates as this is essential for decentralized control and to work towards a common objective. When the enemy attacks, a decision making model will expedite response times in an already time-compressed environment and bring together all stakeholders responsible for disaster recovery. Stakeholders maintain a healthy defensive posture by adhering to a unique battle rhythm that is tailored from routine defense to a network breach. Defense should not be an isolated effort but transcend across geographical, organizational, and governmental boundaries and demands cooperation from a local to global scale.

National and global security hinges on the ability to maintain fault-tolerant and secure lines of communication. This includes the communication that exists between all systems that commanders of the kinetic wars use to meet strategic objectives. It's not enough to build taller and thicker cyber defense walls.
If the philosophy of cyber C2 doesn't adapt to the threat of the environment then the adversary will gain time to further develop network exploits. There remains a critical need to modify cyber C2 philosophies as current methods leave us vulnerable to adversarial cyber attacks that may negatively affect national and global stability.

USFFC

Captain Chamberlain and LT Diptee are Staff Officers in the N6 Directorate at United States Fleet Forces Command. For further information about this article, they can be contacted at brain.m.chamberlain@navy.mil and darryl.diptee@navy.mil respectively. For further information about USFF Command, please visit their web page at: www.cffc.navy.mil.



CJOS COE Annual Report

CAPT Peter Crain, CAN-N
CAPT Massimiliano Nannini, ITA-N
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

2013-2014 Programme of Work

CJOS COE's Programme of Work was centered on five areas or broad themes: Maritime Futures; Maritime Security; Interoperability; Maritime and Joint Operations; and, Strategic Communications. This year has seen CJOS continue some of the projects from last year including Maritime Situational Awareness, Interoperability and Joint Sea-basing while introducing new projects such as Maritime Cyber Security Study and Maritime ISR. Staples of the CJOS Programme of Work, supporting key exercises such as Bold Alligator and the NATO Trident series, have continued to be supported, as having key engagements in the NATO working groups including chairmanship of the Maritime Operations Working Group.

The Maritime Futures theme allowed CJOS to maintain a forward-looking focus on future challenges that will affect the maritime. Key projects in 2014 included supporting the Future Framework for Alliance Operations development and participation in the US-led Multi-national Capability Development Campaign.

Multi-national Capability Development Campaign (MCDC)

The MCDC is a US-led project with 20 partner nations and representation from NATO and the EU. Following on from the highly successfully Multi-national Experiment (MNE) series, the MCDC operates on a two year cycle in which an over-arching theme is identified and supporting focus areas are proposed and developed by sub-groups of interested and subject matter experts from the MCDC stable of partners. CJOS has co-led, with the US Marine Corps, a focus area on Maritime Approach Combined Operational Access (MACOA) and participated in a second, ACT-led focus area on Combined Operations From the Sea Through the Littoral.

MACOA: The MACOA focus area examines the challenge of preparing for assured access to the maritime areas in time of need by the persistent application of a series of activists prior to the eruption of a crisis. These activities have both a preparative and preventative effect in that they may positively influence a region to prevent crisis while also serving to obtain a better understanding for the region and thus prepare forces for potential intervention in time of crisis. The MACOA project will deliver a concept and a practice (activity) guide by end 2014.

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, in turn, informs 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.

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 situational 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. The Maritime Situational Awareness Study will be published by the end of 2014.

Future of Maritime Situational Awareness

CJOS published a brief report that examined the future maritime situational awareness environment. This report looked at trends and drivers, challenges and opportunities and then proposed some actions that could be taken to prepare for potential future challenges in the maritime environment.

Maritime Security

CJOS has continued its work in Maritime Security, engaging in collective projects to improve information sharing on a global basis in addition to looking at future influences on MSA. One of the primary efforts for CJOS this year was to do a preliminary study into cyber security in the maritime domain.

Maritime Cyber Security Study (MCSS)

CJOS conducted an eighteen month examination of cyber security challenges in the maritime environment. The study looked at cyber security vulnerabilities in the maritime portions of the energy supply chain; in containerized cargo management in-port and at-sea; and, in ships' systems to include navigation and ship control systems. Phase one of this study, currently in the final stages of research, will result in a report being issued in the Fall of 2014.

U. S. Navy OPTASK IM

CJOS-COE is collaborating with the U.S. Fleet Forces Command Fleet Capabilities, Requirements, Concepts and Experimentation Directorate to conduct a comprehensive review of the Navy-Wide Operational Task (OPTASK) messages. Warfare and functional mission areas covered in the OPTASKs serve to establish fleet interoperability standards associated with Joint and Navy doctrine as well as Tactics, Techniques and Procedures. CJOS-COE review focus areas include: message format standardization, content currency, consolidation of material and release to Allied/coalition partners. The review OPTASK messages will continue throughout the year and is expected to complete with the review of OPTASK Information Management/Knowledge Management (IM/KM) in September 2014.

Multi-national 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.

Maritime 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 from 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.

Support to JALLC

COJS-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 review in support of their Programme of Work.

Exercise TRIDENT JUNCTURE 2014

Exercise TRIDENT JUNCTURE 14 (TRJE 14) is an operational level headquarters training exercise designed to practice coordination between NATO Command Structure (NCS) and NATO Force Structure (NFS) that will be conducted as part of the evaluation and certification process for Allied Joint Force Command-Naples (JFC-Naples). CJOS-COE will provide a subject matter expert with Political Advisor (POLAD) expertise to facilitate review and certification throughout the planning and execution phases of the exercise. Planned in two phases, SHAPE will conduct two TRJE14 Evaluation Seminars to prepare participants and the exercise includes a Crisis Response Planning Phase in June 2014 with the subsequent Execution Phase scheduled in November 2014.

To view CJOS COE's Programme of Work; seek additional information; or to request CJOS COE support, please contact us at usff.cjos.coe@navy.mil

CENTRES OF EXCELLENCE FACT SHEET

- A COE is a nationally or multi-nationally sponsored entity, which offers recognised expertise and experience to the benefit of the Alliance, especially in support of transformation.

- A COE is not part of the NATO command structure, but forms part of the wider framework supporting NATO Command Authority.

- COEs support transformation through Education and Training; Analysis of Operations and Lessons Learned; Concept Development and Experimentation; and, Doctrine Development and Standards.

- There are 20 NATO accredited COEs:

  - Joint Air Power Competence Centre (JAPCC / DEU) – www.japcc.de
  - Defence Against Terrorism (DAT / TUR) – www.coedat.nato.int
  - Naval Mine Warfare (NMW / BEL) – www.eguermin.org/coe/coe.asp
  - Combined Joint Operations from the Sea (CJOS / USA) – www.cjoscoe.org
  - Civil Military Cooperation (CIMIC / NLD) – www.cimic-coe.org
  - Cold Weather Operations (CWO / NOR) – http://mil.no/education-training/coe-cwo/Pages/coe-cwo.aspx
  - Joint Chemical, Biological, Radiological & Nuclear Defence COE (JCBRN / CZE) – http://jcbrncoe.cz/joomla
  - Air Operations Analysis and Simulation Centre (CASPOA / FRA) – www.caspoa.org/
  - Command & Control COE (C2 / NLD) – http://c2coe.org/
  - Cooperative Cyber Defense COE (CCD / EST) – www.ccdcoe.org/
  - Operations in Confined and Shallow Waters COE (CSW / DEU) – www.coecsw.org/
  - Military Engineering COE (MILENG / DEU) – http://milengcoe.org/Pages/default.aspx
  - Military Medicine (MILMED / HUN) – www.coemed.hu/coemed/index.php
  - Human Intelligence COE (HUMINT / ROU) – www.natohcoe.org/en/home/
  - Counter – Improvised Explosive Devices COE (C-IED / ESP) – www.coec-ied.es/
  - Explosive Ordnance Disposal COE (EOD / SVK) – https://www.eodcoe.org
  - Modeling and Simulation COE (M&S / ITA) – https://www.modelling-simulation-systems-autonomous-capabilities.org
  - Energy Security COE (ENCOE / LIT) – http://enseccoe.org/
  - Multinational Centre of Excellence for Mountain Warfare (MN COEMW/SLO) – www.slovenskavojska.si/en/structure/genneral-staff-commands and-units/doctrine-development-educational-and-training-command/mountain-school/
  - Military Police Centre of Excellence (MPCOE/ POL) – www.mpcoe.org/

(All web sites are unclassified)

- The NATO point of contact for COEs is ACT's Transformation Network Branch - https://transnet.act.nato.int/WISE/TNB

NAME	POSITION	Email/TELEPHONE# Email Suffix: @navy.mil 757-836-xxxx DSN 836-xxxx

STAFF HEADQUARTERS

VADM Nora Tyson, USA-N	Director	Not for Publication 5201
CDRE Phillip J. Titterton, GBR-N	Deputy Director	Not for Publication 2465
CDR David Hazlehurst, USA-N	Fiscal Officer	david.k.hazlehurst 2457
LT , Clarissa Butler, USA-N	Flag Aide	clarissa.butler 2452
LT Colette LaCompte, USA-N	Administrative Coordinator	colette.lacompte 2611
YNC (EXW/AW) Shonka Houston, USA-N	Administrative Assistant	shonka.houston 2453
IT1 (IDW/SW/AW) Ana Moyer, USA-N	IT Support	ana.moyer 2467

TRANSFORMATION OPERATIONS BRANCH

CAPT Massimiliano Nannini, ITA-N	Transformation Operations Branch Head	massimiliano.nann.it 2449
CDR Fabrice Berthelot, FRA-N	Expeditionary Operations Section Head	fabrice.berthelot.fr 2446
CDR Luis Constante, PRT-M	EO SO	luis.constante.po 2444
CDR Gerrit Wiegman, NLD-N	EO SO	gerrit.wiegman.nl 2443
CDR Dimitrios Lymperakis, GRC-N	Maritime Operations Section Head	dimitrios.lympera.gr 2448
CDR Russel Czack, USA-N	MO SO	russell.czack 2441
WO2 Trevor Austin, GBR-RM	MO SO	trevor.austin.uk 2960
CDR John Mihelich, USA-N	MO SO	john.l.mihelich 2445

STRATEGIC PLANS AND POLICY BRANCH

CAPT Dermot Mulholland, CAN-N	Strategic Plans and Policy Branch Head	dermot.mulholland.ca 2450
CDR Steinar Torset, NOR-N	Strategy and Policy Analysis Section Head	steinar.torset.no 2440
CDR Aytac Yavuz, TUR-N	SPA SO	aytac.yavuz.tu 2466
CDR Marvin W. Carlin, USA-N	SPA SO	marvin.carlin 2462
LTC Heiko Griesinger, DEU-A	SPA SO	heiko.griesinger.gm 2464
CDR Carlos CouceMontenegro, ESP-N	SPA SO	josecarlos.coucem.sp 2442
CDR Ricky McIver, USA-N	Strategic Communications and Outreach Section Head	ricky.mciver 2461
CDR Patrick (Tater) Nash, USA-N	SCNO SO	patrick.nash 2463
CDR Lucian Grigorescu, ROM-N	SCNO SO	lucian.grigorescu.ro 2451

Mailing Address:
1562 Mitscher Ave. STE 250
Norfolk, VA 23551-2487

For more information about Combined Joint Operations from the Sea Centre of Excellence (CJOS COE), our Programme of Work, activities and projects, please visit www.cjoscoe.org.

CJOS COE

Our Contributors

CCOE
Civil-Military Cooperation
Centre of Excellence

der Bundeswehr
Universität München

MCR
CRITICAL THINKING.
SOLUTIONS DELIVERED.

Transforming Allied Maritime Potenial Into Reality

CUTTING THE BOW WAVE

COMBINED JOINT OPERATIONS FROM THE SEA CENTRE OF EXCELLENCE

ADDITIONAL SUBMISSIONS

2014

Future Employment of Corvettes in Confined and Shallow Waters

CDR Ingo Eilts, DEU-N
Centre of Excellence Confined and Shallow Waters (COE CSW)
Kiel, Germany

Within the last two decades the world's political situation has changed considerably. Whereas the focus has traditionally been focused on conflict between the two major opposing alliances at the beginning of the 1990s it has shifted toward regional conflicts, possibly having a wider global effect.

Over the last several decades, the role of maritime forces has also changed significantly. During the Cold War era, the basic function of naval forces was to fight or prevent war. The combatants were designed to deter and attack a clearly recognizable enemy with an emphasis on the sea lines of communication. Although NATO showed its presence throughout the world, its Area of Operation (AO) was focused on the Atlantic Ocean and its surrounding bodies of water such as the Mediterranean, the English Channel and the North Sea.

Along with the change to the global political situation, the likeliness of a war between major industrial nations has significantly diminished. Nonetheless, the threats to our sea lines of communications have not been lessened. Although the perils are not as clearly recognisable as in the past, the effect to our economy and welfare still remains significant.

Taking a closer look at navies around the world, we can see that their composition has altered. In the Mediterranean, where home bases are situated close by, Fast Patrol Boats (FPB) still remain an essential element of the navies providing surface warfare capabilities. The number of FPBs in Northern Europe has been reduced significantly. Instead, a variety of corvette-type ships have been commissioned, ranging from Offshore and Oceangoing Patrol Vessels (OPV) to multi-role combat ships with increased operating range and endurance.

NATO's **defence and deterrence** remain the core functions of the Alliance. Although this is not the most likely scenario at present, the Alliance must remain prepared for a major conflict. Despite the requirement for capabilities in the "classic" warfare areas, NATO will continue to be committed to 'preventing crises, managing conflicts and stabilizing post-conflict situations'. To comply with NATO demands for defence and deterrence, a warship must nowadays be able to deploy worldwide at strategic distance, out of reach of homeland support. As a forward logistic site may not necessarily be within close range of the AO, all means of advancing technology must be taken into consideration to extend the ship's endurance. In order to credibly meet the requirements of defence and deterrence, a surface warfare combatant must be capable of conducting at least one major warfare area at full scale. To enhance flexibility and the operational potential, major warships should be capable of supporting at least another warfare area. In the light of decreasing defence budgets and an increasing number of operations other-than-war, the character of corvettes is anticipated to change in the future. While the strengths of the crews are likely to be further reduced, an increase in capabilities can be expected at the same time.

Anti-Surface Warfare (ASuW)

Surface warfare has always been the most prominent role for smaller surface combatants. Patrol assets made up of fast patrol boats and corvettes form a major part of many navies operating in confined and shallow waters environments. Small and fast surface combatants are often the first ship to be procured by any state which is building up its navy. Armed with small to medium calibre guns, torpedoes and/or ship-to-ship missiles, they are capable of engaging both surface warships and merchant traffic. Navies lacking the resources to acquire larger vessels may either procuring new FPBs or purchasing FPBs formerly used by those navies which are now introducing OPVs or corvettes. These very capable surface combatants pose a serious threat to all maritime operations.

Anti-Submarine Warfare (ASW)

Although submarines are certainly no less dangerous than surface combatants (they do not pose the main threat in today's operations). It is assessed that this will not significantly change in future because submarines require intensive resources and are challenging to employ and maintain. As such, not every navy is capable of operating this complex platform. However, a small number of less sophisticated submarines can significantly impact naval operations if unaccounted. Conventional submarines are hard to detect and it's difficult to counter the risk to the naval and merchant ships operating in the area. Capable of delivering naval mines; launching torpedoes or missiles; gathering intelligence off foreign coasts; and, able to deploy Special Operating Forces (SOF) teams, they effect any operation in the littorals. As NATO prepares for high-intensity conflicts, navies must be prepared to conduct anti-submarine operations. Confined and shallow waters provide difficult conditions through which to locate and counter any underwater threats. Hence ASW requires a specific set of sensors and effectors.

Anti-Air Warfare (AAW)

Air assets, whether attack or surveillance aircraft or missiles, constitute an imminent threat to any surface vehicle. Employed in confined and shallow waters, the task of building a recognized air picture to allow for early warning and ample time for protective measures is a very challenging task indeed. Despite today's sensor capabilities to discriminate slow and stationary targets from fast moving objects, the timely acquisition of air targets in this dense radar environment remains a crucial problem. For self-defence reasons, the basic requirements of AAW must be met. Increasing radar range and capability will increase survivability and allow for a more effective AAW posture at the same time.

Land Ground Force Support

As almost all conflicts arise ashore and after all other means have conspired to shape the operation, eventually the conflict will have to be resolved with forces on the ground. At a strategic distance away from a home base, these forces have to be supported by a wide variety of means. This could range from logistic support and provision of C2 infrastructure, up to and including naval fire support. Naval forces may be utilized to provide a base for support and ensure the security of the sea lines of communications.

As a result, the support of land forces in joint operations comes increasingly into the focus of naval operations. Effective naval gun fire support typically demands large-calibre ammunition. Classically this will start at 127mm which is too large for small corvette-size ships. Guns of smaller calibre like 76mm, the standard on the majority of modern warships, generate no useful effect on land-based targets. However, today, naval gun fire support can be accomplished by a variety of surface missiles. The greatest consideration for their use is the ability for target acquisition and discrimination: either by its own means or third party targeting in order to achieve effective long range effects on the target.

Mine Warfare (MW)

Naval mines are an inexpensive means to deny an opponent freedom of navigation. They are easily deployed by nearly all vessels and have been the weapon of choice for less capable navies. Since the end of World War II, more ships have been sunk or severely damaged by naval mines than by any other weapon and there is no indication that this might change in the future. Subject to very restrictive requirements with respect to signature reduction and shock resistance, operations in support of Mine Countermeasures (MCM) seem to be limited. While dedicated MCM vehicles are slow with less endurance, the need for support in a maritime task force is estimated to be high.

Crisis Management & Maritime Security

For crisis management and maritime security operations, the main tasks performed are maritime interdiction operations and embargo operations. Being capable of performing or supporting boarding operations is vital to these operations. As a consequence, vessels for such tasks must be able to host specialized boarding teams or recruit boarding teams from the ship's crew.

In a crisis, it may also be necessary to evacuate non-combatants. Vessels should be able to enter port and berth without external harbour support. The vessels must be capable of alternative means for quick access to ports and facilities in order to support the transportation of non-combatant personnel. Also, the ability to embark, house and provide critical care to refugees has become a standard. Similar to Non Combatant Evacuation Operations (NEO), it may be necessary to provide humanitarian aid or disaster relief in the aftermath of events.

Law Enforcement

Although legal restrictions could apply to some countries, a corvette may be requested to conduct or support coast guard and law enforcement operations. Today, very few operations are based on conflicts between nations involving regular combatants. They now involve the challenges which follow failed states that have become the breeding grounds for terrorist and criminal groups. These groups are typically the opponents now.

Piracy has caused a severe impact to commercial traffic. Anti-piracy operations and protection of shipping have become increasingly important. Only naval vessels have proven capable of providing the required surveillance and countering capabilities at a distance off shore. As many coast guards do not have the endurance nor the war fighting power of navies, naval assets are being employed in support of law enforcement operations such as countering narcotics and human trafficking.

Conclusion

Corvette-size warships which are capable of operating in a high-threat environment must also be able to conduct conflict prevention and crisis management operations, which may include, but not be limited to, the following specific missions and tasks:

- Humanitarian relief operations;
- Support for multinational responses to natural disasters;
- Protection of maritime infrastructure;
- Protection of shipping;
- Ensuring freedom of navigation;
- Embargo control;
- Non-combatant evacuation operations;
- Policing (law enforcement) operations (piracy, trafficking in drugs, people, weapons, technology, and other contrabands);
- Defence against terrorists attacks.

As regional crises are expected to be the most likely conflicts in the future, Crisis Management and Conflict Prevention will continue to be the focus of maritime security operations and could grow in importance. Although combat operations are the least likely situation, navies must be able to operate in such a scenario.

References:

NATO 2020: Assured Security; Dynamic Engagement

The Alliance Maritime Strategy, dated, 3 February 2010

"Strategic Concept For the Defence and Security of the Members of the North Atlantic Treaty Organisation", Active Engagement, Modern Defence, 19 Nov. 2010

Driven by budget constraints, "all-round-fitted-for" ship design may not be a realistic option and could impose restrictions on ship design. Warfare areas and associated capabilities have contradicting needs and further constrain design freedom. For example, naval mine warfare requires acoustic and magnetic signature reduction as well as high manoeuvrability with little or no speed. On the other hand, surface warfare requires high-speed and the ability to operate organic small boats and aircraft such as helicopters or drones. Differing warfare conditions lead to different hull requirements and propulsion configurations. Aiming to address multiple warfare capabilities inevitably will result in a compromise which could limit the capabilities in each warfare area. Due to limited weapons' storage and limitation of crew size, a corvette's capabilities are less than optimal, but regardless of the mission, a set of minimally required capabilities will be required on all corvettes as they will be mandatory for survivability and required for operating in almost any foreseeable scenario. However, interests and priorities differ based on current events and secondary missions could be neglected or assigned to other units. When one mission is favoured over others, it is likely that the remaining mission requirements will be downscaled. Most likely, the crew manning will be reduced while operating increasingly complex systems to carry out a wider variety of duties.

If technology does not assist with computer-assisted decision making applications, the variety of duties will include an increased requirement for individual education and training. Or alternatively, with each change of role, the operators will have to be exchanged accordingly. In addition to specially trained personnel for different roles, extra staff and teams would be required for temporarily embarked modules. As a result, more team training will be required to achieve operational readiness for a larger variety of roles being encompassed on board a vessel.

Therefore, it is recommended to focus corvettes on one major warfare area. Surface warfare operations are deemed the most favourable as they best suit the envisioned tasks of operations other than war. Additionally, a secondary role should be included to augment the operational value but not have negative effects on the primary capability.

COE CSW

CDR Ingo Eilts is a Staff Officer at COE CSW in Kiel, Germany. For further information he may be contacted at ai1@coecsw.org.

For further information about COE CSW, pleased see the COE CSW web page at www.coecsw.org.

HUMINT IN THE MARITIME ENVIRONMENT

Major Alexandru Kis, ROU-A
Captain Pavel Istvanovicz, ROU-A
Human Intelligence Centre of Excellence (HCOE)
Oradea, Romania

The relevance of HUMINT in the maritime environment

Emerging security challenges necessitate new methods of employment and operations for military forces. Current and future asymmetric or non-conventional security threats and geographical features of NATO areas of interest lead to a requirement for a stronger emphasis on maritime power within the joint operations environment. Naval forces must evolve to act decisively within a complex maritime spectrum (fig. 1) where, in addition to traditional missions, naval forces are increasingly involved in counter-piracy, defence against terrorism, and humanitarian assistance missions. In this complex maritime environment with these emerging missions, a more detailed understanding of human motivations and human networking in the Area of Intelligence Interest is required.

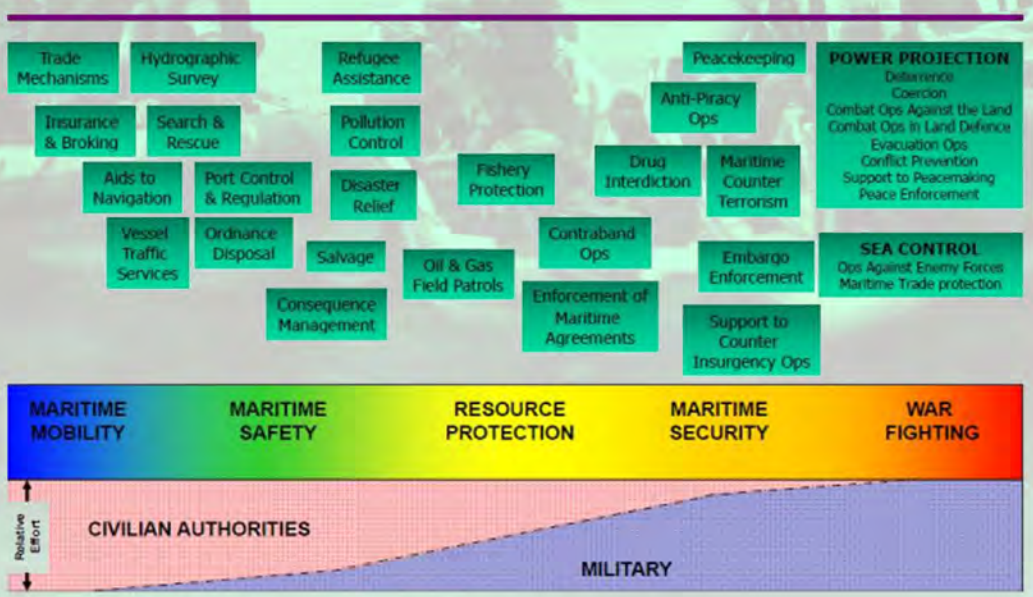


Figure 1:
Today's Maritime Spectrum
(Source: VADM Andreas KRAUSE, NATO Operations & their contribution to Maritime Security challenges, briefing at 2012 COE CJOS/CSW Conference on Maritime Security)

The fusion of all-source intelligence data produces the Common Operational Picture (COP), which is derived from surveillance, reconnaissance, signals intelligence (SIGINT), human intelligence (HUMINT), imagery intelligence (IMINT), and measurement and signature intelligence (MASINT). These intelligence products are processed for fusion, analysis, and distribution of data/information to provide a comprehensive, continuous, and accurate intelligence picture to the Joint Force Commander. In a joint operation, maritime intelligence collection efforts contribute to the development of the Recognized Maritime Picture, which is integrated into the COP.

The maritime environment offers unique opportunities for HUMINT collection activities. Doctrinal references generally describe the HUMINT function as a stand-alone building block of Intelligence. In practice though, this function may be combined to leverage synergies within the collection management function and to facilitate integration of HUMINT information into overall intelligence analysis efforts. NATO defines HUMINT as "a category of intelligence derived from information collected and provided by human sources". Humans are therefore seen both as sources and collectors, and the term human intelligence can be used to mean all forms of intelligence gathered by humans, from direct reconnaissance and observation to the use of recruited agents. Naval units and task forces collect information through the exploitation of organic, attached or supporting intelligence assets to detect, locate, identify and track adversary as well as friendly or neutral naval units and forces. While some NATO nations have traditionally used HUMINT elements for these purposes, other NATO nations are only now assessing the relevance and efficacy of HUMINT collection by naval forces in the maritime environment. Commanders require actionable intelligence from the HUMINT community to supplement technical collection to fully comprehend adversary intent as well as pertinent features of the operational environment. Although technical collection disciplines prevalent in naval forces meet many of the Commander's Critical

---

[2] *The Common Operational Picture (COP) is a snapshot in time of friendly, neutral and adversary forces and of the Battlespace environment;*

[3] *The RMP is a non-real time geographic presentation of processed all-source contact and planning data, known at a given time, of surface, subsurface, amphibious and maritime air units, forces and operations in a designated area of interest, compiled by an asigned RMP manager. The RMP is in accordance with requirements from operational directives and tasking to support decision makers in the conduct of C2 of maritime forces and operations. The RMP is neither a tactical plot nor a real-time display. ATP 2(B)*

[4] *The maritime environment offers several opportunities for military vessels' crews to interact with people – fishermen, traders, crews of commercial ships, coast guard, custom authorities, offshore enterprises (on maritime platforms), harbour administration personnel – all of them potential sources able to provide data and information of intelligence interest.*

[5] *AAP-6 (2013) – NATO glossary of terms and definitions (English and French);*

Information Requirements, they cannot always provide reliable evidence of intentions, deliberation and decisions, plans, research and development goals and strategies, doctrine, leadership, political or military relationships, weapons systems, physical and cultural infrastructure, morale and medical conditions, and relationship among individuals and organizations interacting with the mission. HUMINT offers insights into the mentality, perceptions, and attitudes of a wide range of players and penetrates human networks specific to insurgent/terrorist/piracy activities, as well as the customary life of a community.

Within the framework of a joint operation, HUMINT collection can provide answers to a series of Priority Intelligence Requirements in direct support of a joint forces operating offshore or in coastal waters or using services provided by coastal or harbour facilities such as supplies and maintenance. Coordination and mutual awareness between land-based HUMINT capabilities and naval intelligence could facilitate appropriate management of specific Intelligence Requirements and enhance the collection effort. In this respect, HUMINT is able to spot specific warnings and indicators not available to other sensors. From this perspective, HUMINT is unique because it is especially useful in recognizing the context within which decisions are made and in assessing the likelihood of various activities and courses of action.

Aspects of HUMINT collection within maritime operations

According to AJP 3.1, maritime operations include a series of specific missions and tasks that, alongside actions carried out to protect national security interests in the maritime environment during peacetime, involve, direct interaction between crews and other actors in the Area of Operation (opponent forces, civilians, refugees, persons in distress and other categories of persons, as well as a comprehensive list of institutional entities - organisations, associations and agencies - operating in this environment). At the operational and tactical level, intelligence collection can be achieved through conduct of Maritime Interdiction Operations (MIO) that can enable HUMINT and document exploitation, along with other, mostly technical, intelligence surveillance reconnaissance (ISR) assets.MIO are normally restricted to interception and, if necessary, vessel boarding to verify, redirect, or impound cargo as required to support economic or military sanctions. There are two objectives of Maritime Interdiction:

a. Primary - to determine if a vessel is in compliance with or in violation of the stated reason for interdiction.

b. Secondary - to gather intelligence about the vessel's itinerary and future intentions or about military and shipping activity in and around an embargoed nation's port.

6 AJP 3.1 Allied Joint Maritime Operations, April 2004.

7 STANAG 1040 – ATP 2(B), Volume I. Naval Cooperation and Guidance for Shipping (NCAGS) Manual, May 2004;

Both objectives can be supported by the subset of HUMINT collection called Force Collection Activity. To take advantage of routine and necessary personal interactions, key members of the deployed naval force must be made aware of relevant information requirements then respond to those requirements by reporting their own observations of local conditions as well as identifying individuals of intelligence interest for further exploitation by HUMINT specialists.

Supplementary to maritime intelligence collection, HUMINT can provide detailed information and intelligence on the interior of buildings and facilities for harbour assessments, and vessels' cargo, shipments, technical features of weaponry and assets used by opposing forces, as well as their techniques, tactics, and procedures, and other data of value.

Additionally, HUMINT can cross cue technical ISR sensors to potential targets, in support of the broader targeting process. In this context, HUMINT support is used throughout the joint targeting process and primarily supports three phases:

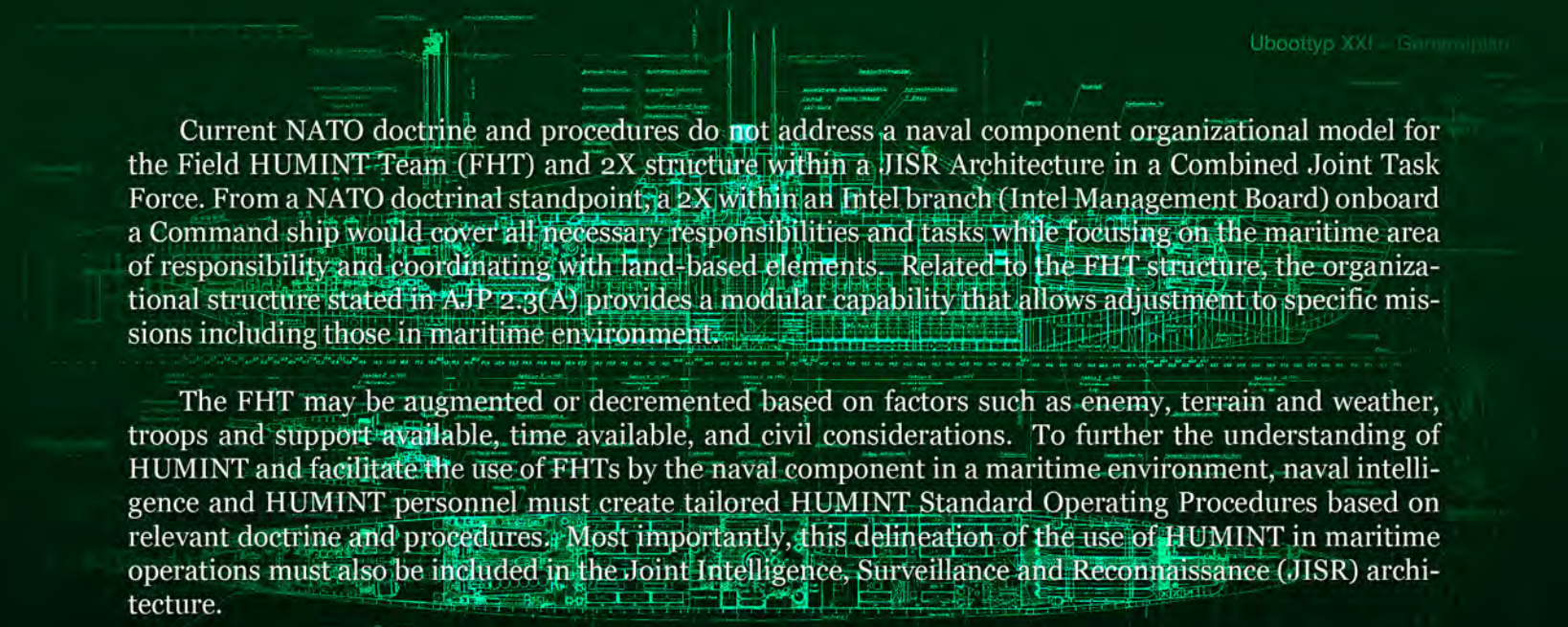
(1) Target Development, Validation, Nomination & Prioritisation,
(2) Mission Planning and Execution, and
(3) Combat Assessment/Measurement of Effectiveness.

Close cooperation between naval targeting entities and the appropriate 2X staff is necessary to ensure that intelligence requirements for joint targeting will be met.
In addition to incorporating targeting-related intelligence requirements into the Intelligence Collection Plan, more information about and involvement in current targeting priorities and focus areas would allow 2X staff to provide more comprehensive and target-oriented intelligence.

Challenges for the HUMINT capability in the maritime environment

As is necessary for the employment of any collection asset in a Combined Joint Operation, legal aspects related to international and national legislation, operational limitations and caveats, and status of forces must be considered for the employment of HUMINT. Subsequently, the contribution and impact of HUMINT collection to a Combined Joint Operation is dependent on the type, mandate, and nature of the operation; the composition and size of the force; characteristics of the operational environment; the adversary; the likelihood of encountering potential sources
(e.g. areas where captured personnel or refugees are expected) or assessments of direct interactions with humans.

[8] *The staff element responsible for coordination, deconfliction and management of HUMINT, CI and, to a lesser extent, Security (Sy) within a JOA and is subordinate to the CJ2; according to AJP -2.3 (A), Annex A;*



Current NATO doctrine and procedures do not address a naval component organizational model for the Field HUMINT Team (FHT) and 2X structure within a JISR Architecture in a Combined Joint Task Force. From a NATO doctrinal standpoint, a 2X within an Intel branch (Intel Management Board) onboard a Command ship would cover all necessary responsibilities and tasks while focusing on the maritime area of responsibility and coordinating with land-based elements. Related to the FHT structure, the organizational structure stated in AJP 2.3(A) provides a modular capability that allows adjustment to specific missions including those in maritime environment.

The FHT may be augmented or decremented based on factors such as enemy, terrain and weather, troops and support available, time available, and civil considerations. To further the understanding of HUMINT and facilitate the use of FHTs by the naval component in a maritime environment, naval intelligence and HUMINT personnel must create tailored HUMINT Standard Operating Procedures based on relevant doctrine and procedures. Most importantly, this delineation of the use of HUMINT in maritime operations must also be included in the Joint Intelligence, Surveillance and Reconnaissance (JISR) architecture.

Another challenge for HUMINT in the maritime environment is linguistic support. Commercial shipping crews are frequently multinational comprising individuals from an unlimited combination of nations using innumerable languages while the residents of the coastal areas may be speakers of different dialects and variations of a national language. Even though a FHT may have organic or attached interpreters, to be effective in a maritime environment, an FHT may need to be augmented with appropriately trained and vetted interpreters in a variety of languages.

To make full use of naval component HUMINT reporting, naval personnel should load standardised HUMINT reports into the automated intelligence systems that are part of the intelligence reporting architecture, part of a coherent JISR structure, as annotated in the Operations Plan. Each element must be aware of its function within the architecture to ensure that information is disseminated expeditiously, to the right place, and in the right format.

Training and education of naval forces leadership and intelligence and operations personnel would improve knowledge and understanding and integration of HUMINT capabilities. Additionally, HUMINT training could be improved through the insight of naval personnel in the development of realistic scenarios and operating constraints. To fully integrate a HUMINT into the maritime intelligence collection capability then integrate that with land and air forces HUMINT, education and training across the NATO enterprise is needed.

---

[9] *According to AJP-2.3 (A), Allied Joint Doctrine for human intelligence, June 2013, para. 0219;*
[10] *Joint Intelligence, Surveillance and Reconnaissance (JISR);*

Conclusion

As maritime operations become more complex and cover a wider range of mission types, HUMINT can make an increasingly valuable contribution. HUMINT reporting can stand on its own as actionable intelligence; it can be used to cross-cue or tip other sensors; it can corroborate or refute other reporting; it can be used for the collection of biometric data. The full development of a HUMINT collection capability in the maritime environment is a necessary and important process which could ultimately lead to not only more robust intelligence collection by naval forces, but a more robust joint intelligence collection capability in a Combined Joint Operation.

The NATO HUMINT Centre of Excellence (HCOE) fully supports the development of a tailored HUMINT organization in NATO naval forces as well as increased education for current HUMINT operators, analysts and other intelligence personnel to better understand the maritime environment and better incorporate it into the JISR architecture. To that end, the HCOE, with the generous support of Netherlands Defence Intelligence and Security Institute, NATO Combined Joint Operations from the Sea Centre of Excellence (CJOS), and experts from Canada, Belgium, Germany, and the USA, has attempted to open a discussion through its study, HUMINT Support to Maritime Operations. The study will be made available in 2014 to NATO stakeholders under the aegis of NATO HUMINT Working Group.

Major Kis and Captain Istvanovicz are Staff Officers at Human Intelligence Centre of Excellence. For further information about their article, please contact them at pavel.istvanovicz@natohcoe.org. For further information about the Programme of Work for HCOE, please see their web page: www.natohcoe.org.

HUMINT COE

Bibliography:

1. *STANAG 1040 - ATP 2(B), Volume I, Naval Cooperation and Guidance for Shipping (NCAGS) Manual, May 2004.*
2. *AAP-6 (2013) – NATO glossary of terms and definitions (English and French).*
3. *MC-0582 NATO JISR Concept, May 2013.*
4. *NSA (JOINT)0788(2008)/2537 – STANAG 2537 JINT (Edition 2) – Allied Joint Doctrine for Human Intelligence (HUMINT) – AJP-2.3 (A), 06 June 2013.*
5. *AJP 3.1 Allied Joint Maritime Operations, April 2004.*
6. *VADM Andreas KRAUSE (Deputy Commander HQ MC Naples), NATO Operations & their contribution to Maritime Security challenges, briefing at 2012 COE CJOS/CSW Conference on Maritime Security.*
7. *HCOE & CJOS, HUMINT support to Maritime Operations (draft study), November 2013.*

"The Helsinki workshop allowed the nations to come together with a better understanding of each other's needs and find a common ground on which to build on. It also allowed new participants to come in with a fresh perspective and offer novel concepts to analyze. It served as a forum to exchange ideas, allowing the cyber experts to educate the data farming community and vice versa. If we can have capable cyber subject matter experts educate our models, we will have a more powerful analysis toolset. At the same time, cyber subject matter experts learned the data farming tools and processes and how it can be applied to address operational cyber defense problems. This offered a glimpse of a currently unavailable higher level cyber defense modeling and simulation capability, where the concern is not at the IP packet and port level, but at the network and human level

"Cyber is a complex adaptive warfare domain," Schwierz said. "To understand the relations and interrelations is the purpose of Data Farming. With Data Farming, we try to answer questions, not only to pinpoint solutions, but to understand relations and interrelations, dependencies and interdependencies and provide a variety of possible progressions in complex systems in a short time."

Gary Horne, PhD, a research scientist with MCR Federal in McLean, Va., who originated the data farming concept and who co-chairs MSG-124 said, "The workshop in Finland had productive collaborations of people working in five different teams consisting of both data farming analysts and subject matter experts from a variety of nations giving diverse perspectives. This kind of collaboration allows for important progress on questions important to NATO and to the advancement of data farming capability."

MCR FEDERAL

Mr. Lundquist and PhD Horne are Principal Science Writers/Research Scientist at MCR Federal. For further information on this article, they may be contacted at lundquist989@cs.com and ghorne@mcri.com respectively. For further information about MCR Federal, please visit their web page at: www.mcri.com.

BOLD ALLIGATOR

CDR Pedro Fonseco, PRT-M
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, Va, USA

The Bold Alligator exercise series is an annual multi-national-U.S. Navy/U.S. Marine Corps hosted amphibious assault exercise event. Beginning in 2011, it has alternated between live and synthetic formats. The 2012 exercise format was live. The 2013 exercise format was a synthetic, scenario- driven exercise which was designed to revitalize the integration and training of staffs in their ability to conduct large scale amphibious operations. The 2013 Bold Alligator exercise was an excellent opportunity to strengthen the proficiency of the Navy/Marine Corps amphibious capabilities with coalition participants. It enhanced the interoperability and exchanging experience. Coalition participants included representatives from Brazil, Canada, Italy, Mexico, France, Italy, the Netherlands, Portugal, Spain, Great Britain and STKFORNATO. However, due to global fiscal challenges, individual coalition units were not able to participate in the exercise. Within the exercise planning staff, this has highlighted a need for a synthetic or constructive training solution that incorporates the integration of coalition synthetic units to reflect real life operations.

Amphibious capabilities are essential in the modern world. Allied amphibious forces can be called upon to act worldwide and must be ready to operate in an anti- access/area denial (A2AD) environment. They will be required to conduct opposed forced entry operations, sea control and power projection. Realistic exercises such as Bold Alligator are essential to rehearse this complex form of warfare; particularly during the transition of forces from sea to land. It requires a clear chain of command and a strong relationship between the Commander Amphibious Task Force (CATF) and the Commander Landing Force (CLF).

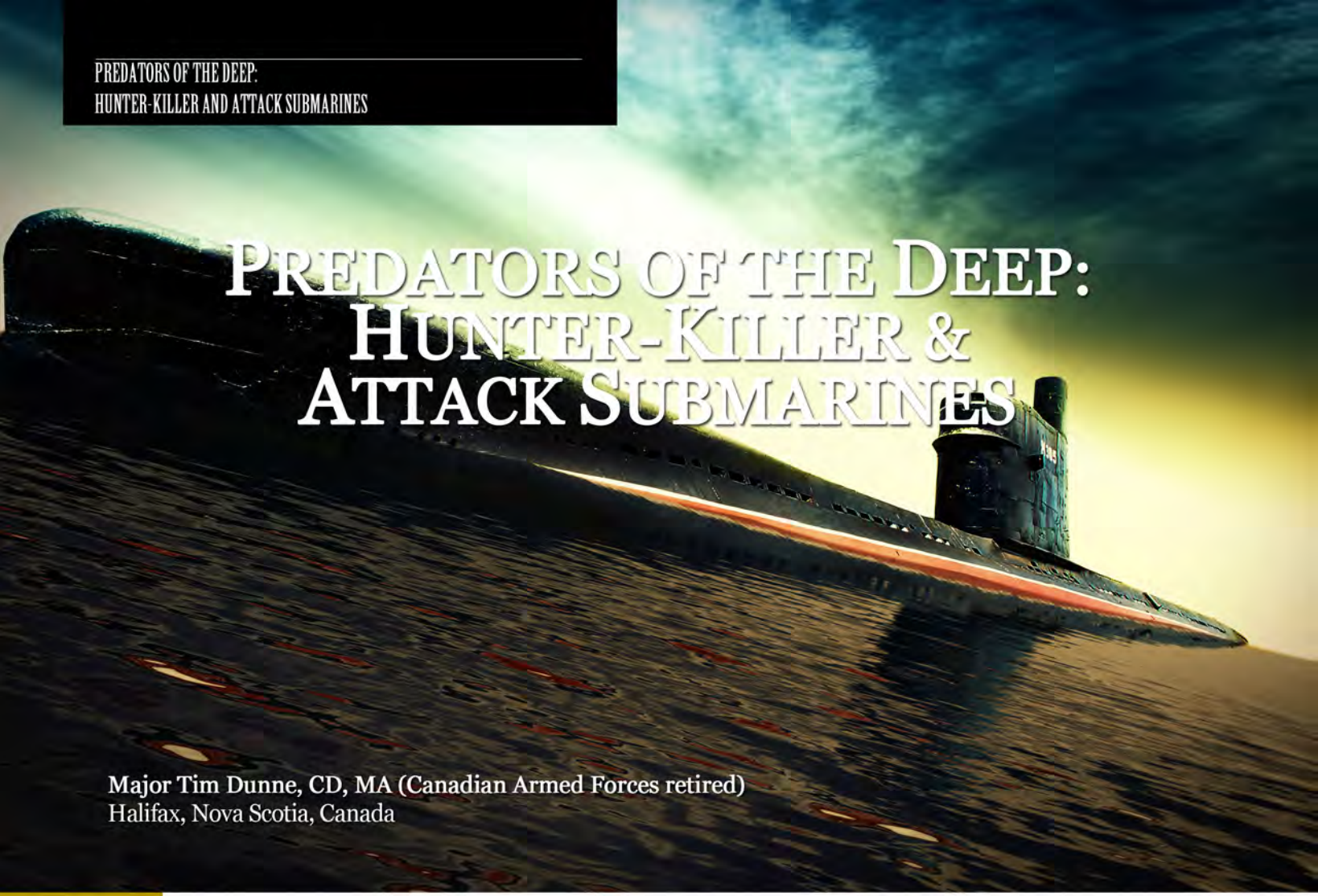
As a USFFC partner, CJOS was involved in all aspects of Bold Alligator 2013 which placed them in a unique position to capture observations and analysis from a coalition perspective and simultaneously collect data to support their Program of Work (POW). They were codified and included in the Bold Alligator Lessons Investigated/Lessons Learned Final Report. CJOS personnel were able to use this information to support and develop items in the Programme of Work, specifically Joint SeaBasing concept, Riverine concept and Alternative C2 Structure for Amphibious Operations.

The goals of Exercise Bold Alligator 2014 are to maximize the combined nature of the exercise with the lead nation, and to incorporate realistic and challenging aspects of combined operations. During Bold Alligator 2014, CJOS is participating as part of the "Exercise Coalition Syndicate" team. From this strategic position, they are able to provide support to the international engagement and identification of coalition training objectives. This ensures that the training objectives are incorporated into the exercise for maximum possible interoperability. A continuous commitment to meet exercise training objectives will ensure Bold Alligator 2014 builds on the success of previous exercises and will increase interoperability among all stakeholders.

CDR Fonseca is a Staff Officer with Combined Joint Operations from the Sea Centre of Excellence. For further information about this article, please contact him at pedro.fonseca.po@navy.mil. For further information about the Programme of Work for CJOS COE, please visit our web page: www.cjoscoe.org.

CJOS COE

PREDATORS OF THE DEEP: HUNTER-KILLER & ATTACK SUBMARINES



Major Tim Dunne, CD, MA (Canadian Armed Forces retired)
Halifax, Nova Scotia, Canada

Submarines have been panned, penned and punned since 1580 when English innkeeper William Bourne wrote that "a Ship or a Boate may goe under the water unto the bottome, and so come up again at your pleasure." He envisaged a vessel with leather chambers that could be drawn inwards to flood and outwards to expel the water. Dutchman Cornelius Drebbel may have been the first to develop a working model when he demonstrated his "submarine" in 1623. The enclosed rowboat with near-neutral buoyancy submerged through forward momentum, making a submerged transit down the Thames River at a depth of about 4.5 metres (15 feet). The English King, James I, purportedly witnessed the event.

The concept of the submersible underwent numerous tests, prototypes and designs until American David Bushnell's "Turtle" became the first submarine to attack an enemy ship during the American Revolution. His version was designed to submerge and surface by a valve that pumped water into and out of a bilge tank below the deck. Movement was by two hand-operated propellers, one to move forward and the other to move vertically. Intended to be towed into the vicinity of the attack, it carried 91 kg (200 pounds) of lead ballast that could be released to increase buoyancy and had a speed about five km/hour (three miles/hour). The vessel was operated by one person and contained enough air for about thirty minutes. In the early morning of 7 September 1776, Sergeant Ezra Lee navigated the Turtle toward a British warship, believed to be HMS Eagle, in New York harbour and attempted to drill into the hull to attach a 60 kg (150 pounds) gunpowder charge. He failed and was spotted by a British lookout, but escaped.

An array of vessel shapes, designs and capabilities were adapted into a variety of prototypes until the submarine reached its early stage of maturity in the beginning of the 20th century. On the eve of the First World War, Great Britain had the largest submarine fleet with 74 in service and 31 under construction; France had 62 in service with nine under construction; Russia had 48; Germany 28 in service and 17 under construction; and the United States had 31 in service and 17 under construction. Prior to WW1, the United States focused its submarine fleet on coastal defence. It was Germany's First World War U-boat that influenced the design of follow-on submarines, with its streamlined hull allowing faster running. In 1943 Germany began to add double-tube snorkels to their submarines. Based on the design of Dutch submarines captured during Germany's occupation of the Netherlands, one tube took air to the engine and the other vented exhaust gases and foul air from the diesel engines.

The United States launched the first nuclear powered boat, the USS Nautilus, which first sailed on 21 January 1954. This began the process of replacing all USN diesel-electric boats with nuclear-powered submarines. Installing a nuclear power system exponentially increased range and manoeuvrability, and radically altered naval strategy and tactics. Nautilus was the first submarine to sail under the Arctic ice, reaching the North Pole on 3 August 1958, an impossible feat for the conventionally-propelled boats of that time.

Submarines are variously called "boats", a shortened form of the original name, "submarine boats".

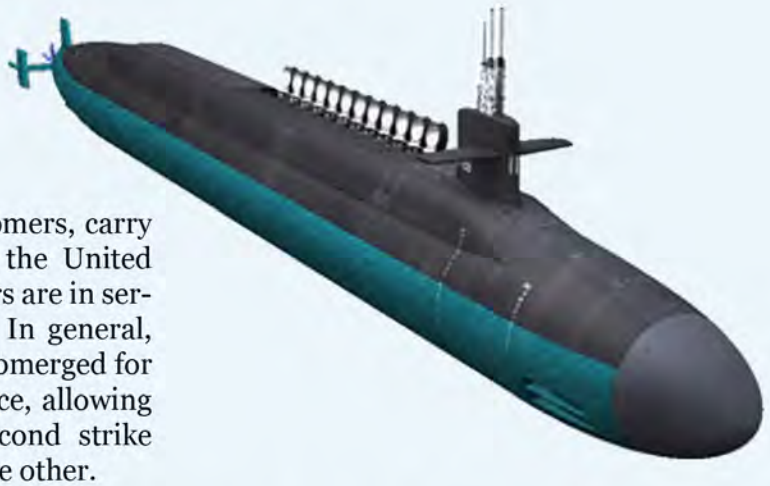
First World War

On 5 June 1914, British Admiral Percy Scott wrote to The Times, "As the motor has driven the horse from the road, so will the submarine drive the battleships from the sea." The press and the Admiralty described Scott as suffering from "an attack of midsummer madness" and that his vision was nothing more than "a fantastic dream." Three weeks later, on 28 June, the Serbian anarchist Gavrilo Princip assassinated Archduke Franz Ferdinand of Austria, heir to the Austro-Hungarian monarchy, and his wife Sophie, Duchess of Hohenberg. This started the tumble of dominoes of declarations of war by the European powers that ended the Concert of Europe and began the First World War.

One month later, on 28 July, Austria-Hungary declared war on Serbia and within days Germany declared war on France and Belgium, provoking Britain's declaration of war on Germany. By 14 August the land war began and on 28 August the Royal Navy attacked German ships in the Battle of Heligoland Bight, the first naval battle of the war. Eight days later, on 5 September, the German submarine U-21 torpedoed and sank the British cruiser HMS Pathfinder. The following week, the British submarine HMS E-9 sank the German light cruiser SMS Hela with two torpedoes. The submarine war escalated with the U-17 stopping and searching the British 866-ton merchant ship SS Glitra on her way to Stavanger, Norway. The crew was ordered into lifeboats and the Glitra scuttled. On 26 October, the same submarine torpedoed the French ferry SS Amiral Ganteaume in the straits of Dover.

The exploitation of the oceanic sub-surface began 100 years ago with those initial operational deployments of submarines during the First World War, changing the nature of naval warfare forever. Since then, surface invisibility allows a submarine to operate close to and even within an adversary's naval force, to avoid perimeter defences, observe without being seen and attack with near invulnerability. From its earliest military operations during the First World War, the submarine could invisibly observe or engage the enemy vessels and escape in the resulting chaos.

What Do Submarines do?



Naval submarines fall into two basic types.

The ballistic missile submarine, nicknamed boomers, carry intercontinental ballistic missiles (ICBM). While the United States and Russia dominate, smaller fleets of boomers are in service with Great Britain, France, China and India. In general, these strategic submarines are loners and remain submerged for long periods using the oceans to mask their presence, allowing them to launch their missiles as an effective second strike weapon in the event of a strategic attack of one on the other.

The hunter-killer, or attack, submarines are tactical vessels specifically designed to use the oceans for stealth as they patrol to protect allied shipping and warships, to conduct their various missions and, when necessary, to attack and sink an adversary's submarines and ships. They can carry a variety of munitions, including their principal weapon, the torpedo, but some can also launch naval cruise missiles and use guns.

"Attack" normally denotes nuclear-powered and "hunter-killer" is the term applied to diesel-electric (conventionally powered); however, the two terms can be used interchangeably. While nuclear-powered submarines can remain submerged almost indefinitely, new innovations in air-independent propulsion (AIP) promise to allow conventional boats to remain submerged for longer periods. Submarines, even the older and noisier that have fewer protection technologies, can be surprisingly effective in a number of tactical and operational roles.

Intelligence, surveillance and reconnaissance (ISR):

A submarine can remain in a specific location for extended periods and covertly trail other submarines and surface ships. Multiple sensors allow monitoring of surface and sub-surface activity to investigate if the activities of the vessels under observation pose a threat or a danger. It is both a "force multiplier", providing early detection of suspicious or threatening activities and events; and a "force enabler", giving pinpoint directions for over-the-horizon forces to engage otherwise unseen targets, and directing land and constabulary forces toward adversarial or illegal personnel landings. Simply put, they alone can conduct extended operations in areas and circumstances inaccessible to other platforms or systems to support both military and anti-criminal objectives.

For example, at a time when the global fisheries biomass is critically stressed, the submarine's capacity to remain on station and observe the practices of foreign fishing fleets is critical. Visible observation changes the behaviour of those being observed, but a submarine can observe unseen and monitor the fishing operations and when necessary, either intervene or call on over-the-horizon enforcement officials to address illegal behaviour.

Submarines can enter an area prior to a conflict and conduct a range of ISR activities, gain an understanding of the geospatial features of an operational area, the patterns, doctrine, tactics and capabilities of an enemy and remain on station until hostilities have ceased.

Power projection, in the naval context, is a nation's capability to employ defensive or coercive force beyond its own littoral waters to meet a threat or to influence activities or events in other areas, and can employ defence, deterrence and diplomacy. In its military form, it can involve various profiles of force, from implied to lethal.

In general, submarines can launch torpedoes or submarine launched cruise missiles (SLCM) through vertical launch silos or their torpedo tubes. The U.S. Navy's Ohio class nuclear submarines are converted ICBM strategic boats that can launch up to 144 Tomahawk cruise missiles from their modified vertical SLCM tubes (silos). The Royal Navy's Astute class and the U.S. Navy's Los Angeles class nuclear submarines can launch SLCMs through their torpedo tubes. The U.S. Navy is replacing the Los Angeles class with the **Virginia class** nuclear-powered fast attack submarines. Designed for a wide array of missions in both open-ocean and littoral missions, they can carry a payload of Tomahawk cruise missiles, an undersea unmanned vehicle and, potentially, conventional medium range ballistic missiles. The Virginia class has a number of futuristic systems and features that contribute to its stealth, effectiveness and resiliency.

Power projection leads to sea control, the freedom to use a maritime area and to deny its use to an adversary, including the airspace above (air defence) and the undersea to the seabed below (waterspace management). This allows a navy to protect sea lanes of communication and deny access to the enemy ships, submarines and aircraft, and to prevent mine-laying in areas of particular interest or concern.

Sea control is essential for maritime nations whose trade and sovereignty depend on safe and secure use of the high seas. The U.S. Navy speaks of the "70-80-90 paradigm," 70 per cent of the world's surface is covered by water, 80 per cent of the world's population lives within 100 miles (160 km) of a coastline and 90 per cent of the world's commerce travels on the oceans. Ocean transport satisfies a vast majority of commercial and strategic shipping requirements. Submarines are critical sea control platforms with anti-submarine warfare and anti-surface capabilities.

They proved to be major threats to sea transportation and in both world wars. The German U-20 attacked and sank Cunard's ocean liner RMS Lusitania on 7 May 1915, as she secretly carried munitions to Britain for the war. She sank in 18 minutes, 18 km (11 miles) off County Cork, Ireland, killing 1,198, and 761 surviving. This was a major factor in the United States entering the war against Germany. During the Second World War, German U-boats preyed on ships crossing the Atlantic to the United Kingdom to bring vital supplies to the British population and the allied forces preparing for D-Day. In the Pacific theatre, USN submarines sank over 5.5 million tons of Japanese shipping.

Sea control establishes the environment for more direct effort in relation to the land. Maritime forces can shape, influence and control the environment, as well as deliver combat forces ashore, working in concert with maritime power projection.

Sea Denial is a critical component of sea control and is used by navies against merchant and naval shipping. Deploying a submarine into an area of operations dramatically changes how opposing naval forces conduct their operations. Locating a submerged boat can divert ships, aircraft and other submarines from other missions, and consume incredible quantities of resources, making its search and pursuit a strategic decision.

The Second World War's Battle of the Atlantic, the war's longest battle, lasted virtually the entirety of the war, from 1939 to 1945, some 2,075 days. Allied naval and air forces conducted more than 100 convoy battles and 1,000 single ship engagements against the submarines and warships of the German and Italian navies. As many as 125 merchant ships were at sea at any one time. Escorted and guarded by allied warships, merchant vessels carried more than 180 million tonnes of cargo to Europe, essential to the war effort. Germany's effort to block allied shipping came at a huge cost for both sides 3,500 merchant ships and 175 warships were lost, and 783 U-boats were sunk.

During the Falklands War Britain deployed one aircraft carrier, 11 destroyers, five nuclear submarines, one diesel-electric submarine and 25 helicopters to anti-submarine warfare. They depleted all their sonobuoys and anti-submarine weapons, and asked the United States to replenish the British inventory, all against one small Argentinean diesel-electric boat, the ARA San Luis.

In 2004, the two-day search for an old and noisy Chinese Han class nuclear submarine in Japanese waters required an entire US Navy P-3 Orion maritime patrol aircraft squadron, Japanese Defence Force P-3s, a number of nuclear submarines and surface ships and a T-AGO surveillance ship with towed sonar.

In response to the 5 April 1986 fatal bombing of Berlin's popular "La Belle" nightclub, the U.S. launched Operation El Dorado Canyon, U.S. air strikes against Libya ten days later. Modern US Navy submarines deployed into the area during the pre-strike and post-strike positioning of the U.S. Sixth Fleet and caused Colonel Muammar Qaddafi to keep Libya's fleet of six Soviet-built diesel submarines in port.

Operational stealth: Submarines excel at non-conventional military operations: covert mining; clandestine mine reconnaissance; precise placement of maritime mines for maximum effect; and stealthy insertion and extraction of Special Forces. In short, modern submarines are multi-mission platforms, fitted with specialised suites of equipment and particular operational characteristics that enable them to operate covertly when required.

When it operates below the sea surface, it is immersed in a naturally hostile environment that favours counter-detection sensors. A submarine remains virtually invisible to all but the most capable anti-submarine forces. The significance of a submarine's operational stealth grows as countries develop their own national ocean surveillance systems, which build a wide-area maritime picture for using space, airborne, surface, sub-surface and land-based systems. Operating without being detected is a fundamental capability to the submarine's military effectiveness. In times of political tension or crisis, the boat's covert nature provides a hidden and potentially lethal asset that can exacerbate or escalate the political scenario without notice.

In 1977, the Argentinean government was pressing the British government to pass over control of the Falkland Islands. The British did not want to complicate the negotiations by visibly deploying forces, but wanted to be prepared in case Argentina seized the islands. A task force of two frigates and one submarine deployed but only the submarine was permitted into the immediate vicinity of the islands. The frigates remained more than 1,000 miles away. The Royal Navy submarine deployed into the region without the Argentineans being aware of the deployment, allowing the British government to employ the submarine's full range of ISR and combat capabilities or recall the boat as circumstances dictated.

The element of surprise is an option in the commanding officer's arsenal of operational alternatives, if and when he or she decides to reveal the boat's presence to the enemy. During the Falklands War, the Argentine submarine, ASA San Luis, operated in the main areas of the British task force during the 36-day patrol, at some times firing shots against the British fleet. There was no effective counter attack. The British fired more than 150 weapons without a hit, and Britain was considered NATO's anti-submarine warfare specialist at the time.

Operational endurance: Among the submarine's most important attributes is its ability to linger, submerged, silent and invisible, for relatively long periods, periodically raising the periscope and snorkel. During their times on-station, they can observe and develop their intentions to address tactical and operational situations.

US Navy attack submarines, all of which are nuclear powered, usually deploy for 90 days and can remain on station and submerged for 60 days or more. Australian Collins class are said to be designed for 70 day patrols. Small conventional submarines, such as Pakistan's Agosta 90B air independent propulsion (AIP) submarines have an endurance of 60 days; Germany's Type 214s and French Scorpenes can deploy for 50 days or more; Argentina's San Luis, a German Type 209 submarine, could remain deployed for 60 days before needing refuelling and resupply. Canada's Victoria class boats have a patrol endurance of 56 days.

Freedom of Movement, derived from stealth and endurance, is the ability to covertly move with relative impunity and to access any chosen area within the area of operations, including those closed to surface vessels or aircraft. It can shift positions within the area of operations as the operational and tactical situation changes and while submerged, and are generally unaffected by rough seas and poor weather.

Flexibility: Stealth, secrecy and silence are their advantages. The submarine has a wide range of sensor and communications equipment, effectors and an ability to operate covertly and independently across the full spectrum of maritime operations. A force commander can task a submarine with a number of different mission types as the strategic, operational or tactical situation changes. At the operational level, a submarine might arrive in an area to insert Special Forces, conduct intelligence, surveillance and reconnaissance assignments, maritime mine-laying operations, launch cruise missiles against land-based targets, and engage enemy shipping and submarines with torpedoes and anti-ship missiles. Hunter-killer and attack submarines can carry torpedoes against ships and other submarines, and cruise missiles against land targets up to 1,000 miles away.

In recent times, submarines have shifted away from absolute lethality in their payloads to allow greater flexibility and relevance in lower level conflicts. The flexible range of activity and weapons against an enemy force at tactical and theatre levels allows the commander to monitor, harass, engage and destroy maritime targets with virtual impunity.

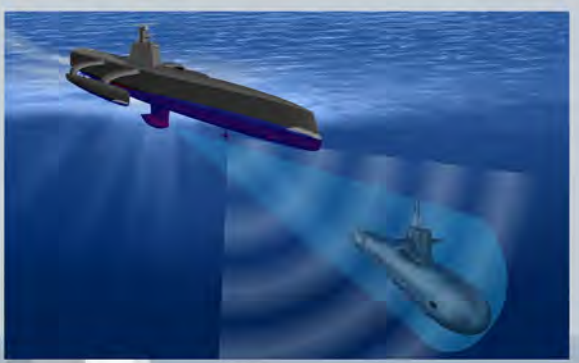
New Technologies

The enhanced technologies being integrated and retrofitted into submarines are giving these vessels a variety of futuristic characteristics.

Air independent propulsion-equipped submarines have significant operational advantages over both conventional diesel-electric engines and nuclear powered submarines. These systems allow submarines to stay submerged far longer than their diesel-electric counterparts, which must either surface more frequently or ascend to snorkel for air, revealing their positions. They also run much more silently than nuclear-powered submarines, which continuously pump coolant through their nuclear reactors, generating noise that can betray their presence. Sweden's Gotland class diesel-electric submarines, designed and built by the Kockums shipyard, are the first to have Stirling engine air-independent propulsion systems, which extends their underwater endurance from a few days to weeks.

The USN Virginia class submarines are designed for the full spectrum of blue-water and littoral missions. Twin AN/BVS-1 telescoping photonics masts replace the traditional periscope, eliminating the periscope tube that protrudes from the steel pressure hull, increasing watertight integrity and limiting risks of water leakage in the event of damage. The photonics mast exchanges the mechanical, line-of-sight periscope with high-resolution cameras, light-intensification and infrared sensors, an infrared laser rangefinder, and an integrated electronic support measures array. Information from these sensors is carried through fibre optic data lines to the control center with visual data displayed wirelessly on LCD monitors. The boat uses pump-jet BAE Systems propulsors that reduce cavitation and are quieter than traditional bladed propellers, a fibre optic fly by wire ship control system and an updated AN/BSY-1 integrated combat system by General Dynamics AIS (previously Raytheon).

According to news media reports, the Royal Navy's HMS Ambush, Britain's newest Astute class nuclear powered attack submarine, has a sensor package that can "hear" vessels 4,800 kilometres (3,000 miles) away, carries 38 Tomahawk cruise missiles, and can travel up to 800 km (500 miles) per day. In 2020, Singapore will operate the Indo-Pacific's most advanced non-nuclear powered submarines. Thyssen, the German shipbuilder, has been contracted to construct two Type 218G U-boats that will maintain Singapore's submarine fleet's interoperability with western navies.



China is dramatically expanding its fleet of nuclear and conventionally-powered hunter-killer submarines in quality and quantity. Russian news media reports the development of a fifth-generation submarine class, which may be made available to China. The Kalina-class will feature a made-in-Russia air-independent propulsion (AIP) system to be developed by 2017 with the first boat fitted with the system by 2018.

Japan, South Korea, Vietnam, Indonesia, Australia, the Philippines and Pakistan all maintain programs that will start, modernize or expand their submarine fleets. South Korea has already purchased German submarines. Small countries which do not have the resource base, the economy or the capacity for large, expeditionary naval fleets can be expected to respond to China's increasing capabilities by expanding their submarine fleets.

Today, modern submarines can deny access and can hunt almost with impunity. With 40 nations employing more than 400 boats of all types, the need for these specialized vessels will grow with the development of technologically sophisticated weapons, and information and detection systems. Future adversaries will have more access to relatively inexpensive, high-tech systems, such as space-based surveillance and targeting systems, quiet diesel-electric submarines, low-cost maritime mines, information warfare tools, tactical ballistic missiles, cruise missiles and weapons of mass destruction.

A submarine's operational survivability will certainly be affected by emerging weapon systems, which will be employed defensively by submarines against surface ships and anti-submarine helicopters, and by ships and helicopters against submarines. A non-nuclear electro-magnetic pulse generator and high intensity microwave weapons could affect or destroy microcircuits, computers, radar, sonar, communication and other critical electronic systems. Thermo-baric weapons, explosives that generate an intense, high-temperature explosion and blast wave, are under development. Hoist-able mast-mounted guns are presently under development.

Current submarines are generally invulnerable to such weapons, and their lethality will be enhanced with the integration of wire-guided missiles, such as IDAS or AIM 9X, which will be integrated into German and U.S. submarines to eliminate anti-submarine helicopters.

Narco-submarines

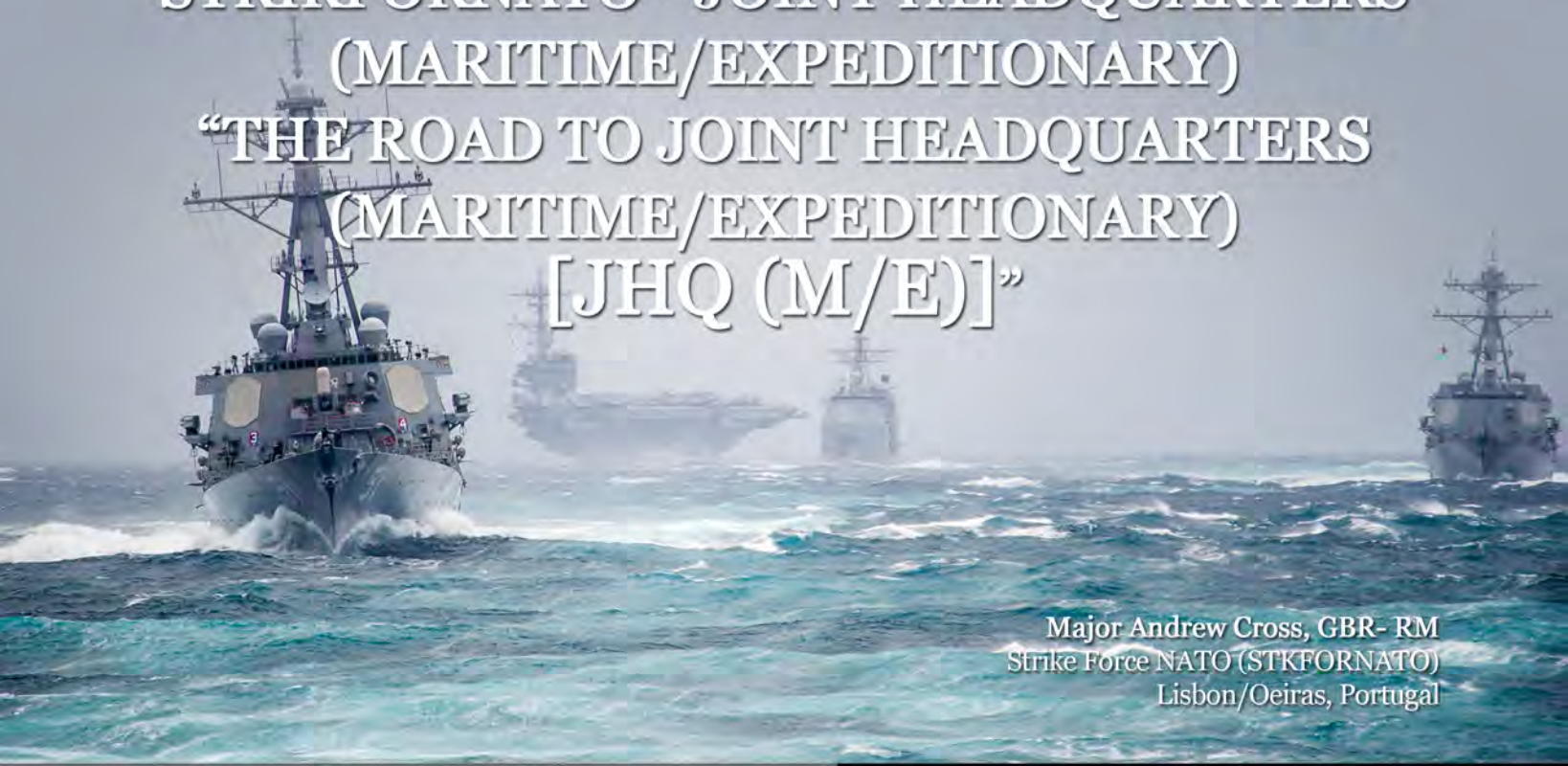
But future adversaries may not all be nation-states. Columbian drug cartels have developed special-purpose submarines, in one case, a camouflaged boat 22.5 metres (74-feet) long with twin propellers and a five-foot conning tower. The ocean-going, self-propelled "narco-submarines" are built by drug traffickers to smuggle cocaine from Colombia to Mexico, and which is then brought overland into the United States. First detected in 1993, the early vessels were semi-submersibles and could not dive. Most of the vessel was submerged with only the cockpit and the exhaust pipes visible above water. Newer narco-submarines are fully submersible, designed specifically to be difficult to detect visually or by radar, sonar and infrared systems. Moving up to 330 tonnes of cocaine per year, they cost up to two million dollars each to construct. But, they can move enough cocaine in a single trip to bring in more than $100 million in profits.

Conclusion

Submarines contribute to all areas of maritime operations, including warfare, sea control, sea denial and maritime power projection. Many are equipped to conduct land strike operations to take out enemy command and control, enemy air control capabilities, conduct mine countermeasures operations and traditional anti-shipping and anti-submarine operations, and to support blue force operations ashore. Simply stated, modern diesel-electric submarines with a full complement of sensors, a weapons package that includes torpedoes, submarine launched cruise missiles, anti-ship and anti-air missiles, a hoist-able, mast-mounted gun and air independent propulsion are the best effective defence against similarly-equipped adversary submarines. They are an essential component in a nation's naval fleet mix.

Tim Dunne is a retired Canadian military officer and is currently a Nova Scotia-based military affairs writer and analyst. He can be contacted for comment at tdunne@dunnecom.ca

STRIKFORNATO - JOINT HEADQUARTERS (MARITIME/EXPEDITIONARY) "THE ROAD TO JOINT HEADQUARTERS (MARITIME/EXPEDITIONARY) [JHQ (M/E)]"



Major Andrew Cross, GBR- RM
Strike Force NATO (STKFORNATO)
Lisbon/Oeiras, Portugal

Since the 2010 Lisbon Summit, NATO has been committed to reforming the NATO Command Structure (NCS), placing a greater reliance on the NATO Force Structure (NFS). In accordance with the NATO Joint Command and Control (JC2C) Capability Model, NFS Headquarters would command at the operational level, delivering capable and credible forces in the event of any potential future crisis. The JC2C capability model, and more specifically, the Joint Headquarters (Maritime/Expeditionary) [JHQ (M/E)] employment model is therefore designed to be responsive while building upon realistic force packaging constraints and achievable readiness criteria, utilising the advantages of Smart Defence and the guiding principles of the NATO Connected Forces Initiatives.

The JHQ (M/E) employment model is designed to exploit the advantages of sea-basing and to minimise the military footprint ashore. The range of military tasks that might be executed under this Command and Control (C2) construct spans from humanitarian and peace support operations to conventional, theatre-entry and full spectrum warfighting. The C2 node may have a short to medium-term focus, or may contribute to a single phase of a broader campaign plan. Potential missions may include:

- Humanitarian Aid/ Disaster Relief;
- Security Operations (Littorals / Harbours);
- Protection of critical infrastructure;
- Demonstrative Force Package;
- Non-Combative Evacuation Operations (NEO);
- Peace Support Operations;
- Contribute to the Preservation of Territorial Integrity;
- Initial maritime entry operations to set conditions for follow-on forces; and
- Embargo or other Maritime Security Operations

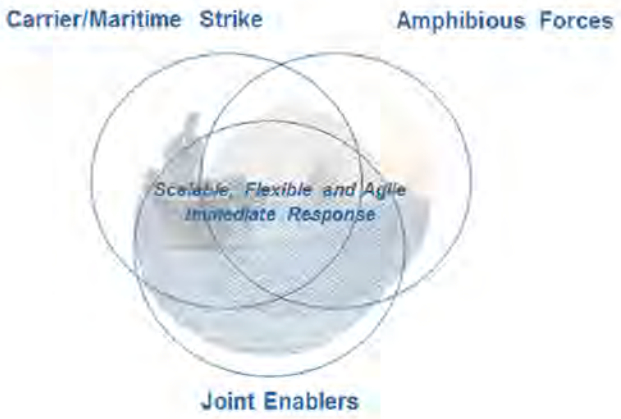
In addition to the examples of smaller scale and less complex operations, JHQ (M/E) forces may also utilise the advantages of operating within the maritime/littoral environment potentially in support of Major Joint Operations commanded at the Military Strategic or more traditional NCS Operational Joint Force Command levels. Also conceivable is an operation involving large scale follow-on land forces that may involve a transfer to another tailored JHQ (Land) or Joint Force Command.

The defining principles of MEO are founded upon a predominantly maritime force, maximising the advantages of the sea space and supported by the other domains, to enable rapid response, flexibility, adaptability, interoperability, deployability and the ability to operate in remote theatres. While not limited to, MEO consists of conducting operations in the littorals, ashore and afloat, from self-sustaining, deployed maritime assets. The key advantage of this force package is in fulfilling a wide range of mission sets with a minimal military footprint ashore.

Considering STRIKFORNATO's long-standing expertise and experience in strike and amphibious operations within NATO, SHAPE looked to the Command to assume the first role as JHQ (M/E) and to deliver an initial entry capability by July 2014. This tasking required STRIKFORNATO to be capable of delivering a tailored headquarters designed to rapidly support a broad range of tasks utilizing the freedoms and advantages the sea space provides. Specifically, the JHQ (M/E) is intended to command and execute a Maritime Expeditionary Operation (MEO) as defined in Allied Command Operations (ACO) Directive, AD 080-098, Volume V:

"Maritime Expeditionary Operations comprise NATO's ability to project maritime forces at up to strategic distance that can deliver decisive joint effect from the sea on land, at sea, in the air, space and cyberspace, with little or no host nation support. This immediate response capability is built on rapidly deployable and interoperable maritime forces including sea-based strike, initial entry and amphibious assets, sustained by embedded logistics and communications. It provides an agile and flexible Allied response across the full range of the crisis spectrum."

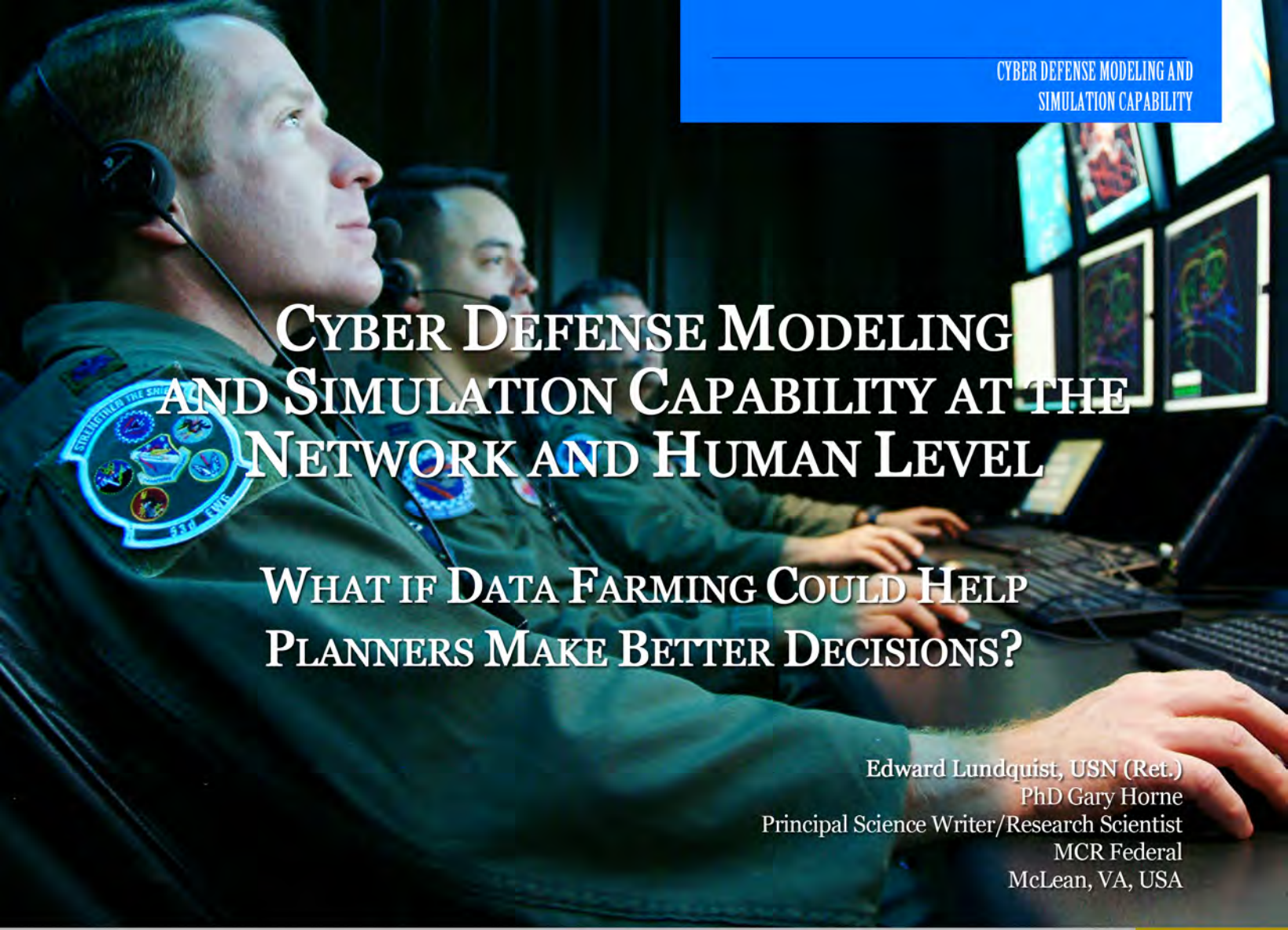
The inaugural STRIKFORNATO Maritime Expeditionary Operations Conference (MEOC) in May 2013 provided NATO with an opportunity to come together and provide much of the intellectual rigor that supported the development of the first iteration of the future JHQ (M/E) Concept of Operations (CONOPS), which was completed in early 2014.



This past May, STRIKFORNATO, supported by Allied Command Operations (ACO), Allied Command Transformation (ACT) and the Joint Warfare Centre (JWC), engaged in the preparation and execution of Exercise TRIDENT JAGUAR 2014, a high intensity, full spectrum and complex Command Post Exercise specifically designed for STRIKFORNATO to deploy and command a significant NATO joint force as an operational level JHQ (M/E). The exercise validated STRIKFORNATO's capability to deploy at very short notice and to deliver an immediate and positive NATO response in the event of a crisis. The outcomes and lessons from TRIDENT JAGUAR will provide analytical evidence that will further enhance the JHQ (M/E) CONOPS, provide others who might fulfil this role with valuable insight into the challenges and best practices of a JHQ (M/E) and further validate the Alliance and NFS JC2C Capability Models post transformation.

Major Cross is a Staff Officer at Strike Forces NATO. For further information about this article, please contact him at a.cross@sfn.nato.int. For further information about the Programme of Work for STKFORNATO, please visit their web page at: www.sfn.nato.into.

STKFORNATO



CYBER DEFENSE MODELING AND SIMULATION CAPABILITY AT THE NETWORK AND HUMAN LEVEL

WHAT IF DATA FARMING COULD HELP PLANNERS MAKE BETTER DECISIONS?

Edward Lundquist, USN (Ret.)
PhD Gary Horne
Principal Science Writer/Research Scientist
MCR Federal
McLean, VA, USA

Data Farming is a way to conduct operational analysis and visualization through modeling and simulation, high performance computing, build scenarios, and explore new options for decision makers. The methodologies permit planners and decision makers to ask the "what if?" questions to determine the probabilities of various outcomes.

When representatives from Germany, Sweden, Canada, Turkey, and the United States gathered at the National Defense University in Helsinki, Finland in January 2014 for the International What-If? Workshop 27 (IWW 27), they examined Humanitarian Assistance Modeling, Cyber Defense Planning, Operational Defensive Planning, and validation of the data farming methodologies. This workshop was conducted in conjunction with the NATO Modeling and Simulation Work Group 124 (MSC 124) which met concurrently at the Finnish Defense College. MSG 124 followed the very successful MSG 088 which completed its work in 2013.

"IWW 27 tested the system and allowed us to train officers attending the Finnish Defense College to use models efficiently," said Maj. Esa Lappi, head of the Information Technology Division at the Finnish Defense Forces Research Agency and the host for the week. "The international cooperation opened the eyes of our students to see things in a new and different way." "Data farming is a clearly stated process," Lappi said. "The design of the experiments can save a huge amount of calculation and analysis time, and provide for better visualization of results. One example, Lappi said, is artillery optimization during an operation. "We examined the effectiveness of fire while avoiding collateral damage. We could also show some worse courses of action. We could explore the parameter space using the trained process, and bring experts and the modelers closer together to provide better quality studies and outputs."

Santiago Balestrini Robinson, PhD, a research engineer with the Georgia Tech Research Institute in Atlanta said the defense university students, who are all serving officers, are especially helpful in discussing scenarios. “They know what would really be going on in an operational military context.” But, Lappi said, there’s room for improving the workshops. “We spend a lot of time defining parameters and designing experiments. Maybe running actual simulations during the workshop would make it more interesting.”

A special team of gifted and talented high school students from the Päivölä School of mathematics, Tarttila, Finland, also participated by investigating the impact of climate change on military humanitarian assistance and disaster relief.

Scoping the problem

“The workshop is very useful for scoping the problem,” said Klaus-Peter Schwierz, PhD, an operations research scientist from Germany. “We can see what is of common interest among the nations. You get a new perspective.”

Data farming combines various disciplines of modeling and simulation; rapid scenario prototyping; design of experiments; high performance computing and visualization of results in a collaborative way. Data farming can provide a more rigorous, traceable and therefore defensible process for decision makers. It is more rigorous because it is generally based on quantitative analysis. It is traceable because there is a logical process for conducting the analyses, inferring information and the associated decisions. Balestrini Robinson said these two characteristics make it defensible in the sense that when someone asks "why did you select this option?" you can state with confidence that "this option performed better than these other options we considered in these conditions", and if someone says "why didn't you pick my option?" you can show that option (if it was considered) did not perform well in certain conditions.

“We are using data farming to help decision makers understand the tradeoffs between network architectures and cyber defense measures (both the ways and means available in terms of technology and processes), under a variety of uncertain conditions. We are exploring hundreds and thousands (ideally we want to explore hundreds of thousands or millions of potential scenarios) to understand the value of the different alternatives. If there is a question about the analysis, you can dig deeper and trace it down to the lowest level of abstraction. It is all there – there’s no hiding behind fuzzy concepts or expert opinion,” Balestrini Robinson said.

In Finland, the process was applied to cyber to help decision makers understand the tradeoffs between network architectures and cyber defense measures under a variety of uncertain conditions. “We found that cyber is not a well understood problem. To some people it is one thing, and to others it is something different. We are finding that by formalizing the analysis we are performing, we are forcing the experts to agree on basic concepts associated with cyber defense. For example: How does it impact operations? What can we expect to be able to do or have done to us? How do we measure success? Or the enemy's success? What phenomena should we be concerned with when we are modeling an operational cyber defense scenario? Most of these answers are not clear cut, they have to be discovered and refined. We understand the problem as we formulate and test various alternatives and potential solutions. The data farming process is ideal in helping us navigate that iterative process in a rigorous and collaborative manner,” Balestrini Robinson said.

CHARACTERIZATION AND ANALYSIS OF ENERGY SECURITY VIA EXPERT REACH BACK ARCHITECTURES IN MARITIME INTERDICTION

Dr. Alex Bordetsky, Professor, CENETIX, Naval Postgraduate School, Monterey, CA
Dr. Dan Nussbaum, Professor, Naval Postgraduate School, Monterey, CA
Dr. Silja Meyer-Nieberg, Fakultät fur Informatik, Universität der Bundeswehr, München, Germany
Goran Mihelcic, Fakultät fur Informatik, Universität der Bundeswehr, München, Germany
Prof. Dr. Stefan Pickl, Fakultät fur Informatik, Universität der Bundeswehr, München, Germany

ABSTRACT

In this contribution, we pose the question: In which way can specific expert reach back experiences be integrated into the design, optimization, and cost-benefit analysis of critical infrastructure energy systems. Our aim is to strengthen the resilience, survivability, and affordability of critical infrastructures via such an experimental framework by using modern reach back conceptions and expertise. First, we will present the unique Center for Network Innovation and Experimentation (CENETIX). Next, we will introduce expert reach back as a key element of CENETIX and the challenge of analyzing critical infrastructure energy systems. COMTESSA, a competence center and branch of CENETIX, is a study in operational research which focuses on awareness, analysis, control, and optimization of complex systems. COMTESSA develops a management cockpit for such complex analysis: Cost-Benefit Analysis (CBA) and Foresight Analysis Techniques will be part of that cockpit. Its architecture will allow us to include cloud computing aspects. This new approach will be integrated and tested within the CENETIX environment as part of a modern reach back strategy to strengthen maritime energy security.

1. Center for Network Innovation and Experimentation (CENETIX)

Society depends decisively on the availability of infrastructures such as energy, telecommunication, transportation, banking and finance, health care, and governmental and public administration. Even selective disruption of one of these infrastructures may result in disruptions of governmental, industrial, or public functions. Therefore, vulnerability of infrastructures offers spectacular leverage for natural disasters, as well as criminal actions. Threats and risks are part of technological, economical, and societal development. Increasing complexity of our critical infrastructures exacerbates consequences of natural and/or man-made disasters. Primary and cascading effects of increasing dependencies and interdependencies of our technological and societal systems require intelligent simulation and optimization techniques in the area of industrial informatics and comprehensive safety and security management. There is a need to analyze and forecast such threats via a new kind of experiment:

The Naval Postgraduate School (NPS), Center for Network Innovation and Experimentation (CENETIX), was founded in 2004. It soon became nationally and internationally recognized for excellence in applied research studies of emerging networking and collaboration frontiers. CENETIX provides students and faculty with opportunities for interdisciplinary study of agile socio-technological adaptive mobile networks, network-controlled unmanned vehicles, sensors, network decision support, and situational awareness architectures.

CENETIX integrates and manages a unique student-operated NPS Tactical Networking and MIO Test Bed. Together with international partners, CENETIX integrates and operates a globally distributed test bed environment for the study of tactical self-organizing networks and network-enabled operations. The project work at CENETIX involves cooperation with researchers and students from National Laboratories and major universities, including Lawrence Livermore National Laboratory, the Army Research Laboratory, MIT, Johns Hopkins University, Carnegie Mellon University, the University of Alabama at Huntsville, the University of the Bundeswehr at Munich (COMTESSA), the NATO Maritime Interdictions Operations Training Center at Souda Bay, the Defense Science and Technology Agency of Singapore, and Salzburg Research. A strong group of industry partners supports CENETIX team work on TNT and MIO experiments. Industry and academic partners are available at the CENETIX website: http://cenetix.nps.edu.

The CENETIX team of faculty and students produces unique case-studies, innovative agile adaptive networking solutions, and new operational concepts for emerging network-centric operations. From the scholarly standpoint, the research at CENETIX is a vehicle for generating new concepts and theories. As a field model of emerging complex relationships between networked humans and machines in a tactical ad hoc mobile environment, the TNT test bed allows the NPS team and partners to explore feasibility and major operational constraints associated with those relationships, and to identify critical elements of emerging tactical networking frontiers.

EXPERT REACHBACK AS KEY ELEMENT OF CENETIX – COMPLEX COLLABORATION AND DATA SHARING

CENETIX is actively contributing to the NPS mission by conducting a series of unique experimental studies leading to a better understanding of collaboration and global data sharing in the interagency and coalition environments. The phenomenon of expert reach back and its application to real-time support for Maritime Interdiction Operations missions (which is a great challenge, especially in the energy domain) has been at the center of CENETIX team research. The experimental and concept development research at CENETIX is conducted in close partnership with the NPS CRUSER, CORE Lab, SEED, and Littoral Operations Center programs. In this contribution, we pose the question: In which way can specific expert reach back experiences be integrated into the design, optimization, and cost-benefit analysis of critical infrastructure energy systems. Our aim is to strengthen the resilience, survivability, and affordability of critical infrastructures via such an experimental framework by using modern reach back conceptions and expertise. Before presenting a specific analytic framework of a management cockpit, we introduce the general idea of a cost-benefit analysis (CBA).

2. Analytic Tools for Critical Infrastructure Energy Systems

Energy Security is the set of conditions in which energy is able to fulfill the demands placed on it by the society and economy. Critical infrastructures are those that are essential to a nation's economy and security. These infrastructures are interdependent, as one can understand, for example, by considering fuel and electric infrastructures.

In the national security arena, there is a fundamental interest in developing decision support mechanisms for use in evaluating alternative courses of action (COA) that strengthen the resilience, survivability, and affordability of critical infrastructures. "What Is the Definition of Energy Security?"

- In Energy Rush: Shale Production and U.S. National Security, by Elizabeth Rosenberg (Report of the Unconventional Energy and U.S. National Security Task Force), published in February 2014, energy security is defined as "...reliable access to sufficient, affordable energy supplies to fuel economic growth."

- Prof G. Bahgat, of the US National Defense University, and the author of many energy-related publications, including Energy Security: An Interdisciplinary Approach (2011, ISBN-13: 978-0470689042), defines energy security as "the uninterrupted availability of energy sources at an affordable price with little environmental footprint."

To address these questions we introduce the idea of a Cost-Benefit Analysis (CBA) as an important analytical tool for choosing among alternative COAs to strengthen the resilience, survivability, and affordability of critical infrastructures, especially energy critical infrastructures. We note the important fact that every CBA rests on a cost estimate and its underlying set of assumptions.
We introduce the idea of a "fully burdened cost of energy" as part of the Life Cycle Costs (LCC) in support of a properly done cost estimate to support a complete and useful CBA. Because all sectors of society and the economy rely on energy, disruptions to energy have important consequences across the full spectrum of organizations, populations, and systems.

CBA as a Systematic Approach for a Management Cockpit

A CBA can be defined as a "systematic approach to choosing the best method of allocating scarce resources to a given objective." A CBA is an important analytical tool for making choices among several COA) as in, for example, comparing different ways to make a critical infrastructure more resilient (which is a central task of an expert reach back architecture). An important tenet of CBA is that the costs considered when comparing the different COAs must address the LCC or sometimes called "Whole Life Costs".

This principle is equally valid in developing cost estimates for Critical Infrastructure Energy Systems, but only recently has the concept of Fully Burdened Cost of Energy (FBCE) been introduced into CBAs. The FBCE calculation includes expenditures for the basic fuel purchase and expenses (including depreciation) related to the fuel's transportation, storage, distribution, and any provisions required to protect it. Even though fuel costs account for only two to three percent of the overall US Defense expenditures, the FBCE concept is important for several reasons:

- Fuel costs represent a large portion of the total LCC of aircraft and non-nuclear ships.
- Energy delivery is characterized by "it takes energy to deliver energy," and therefore, energy use is subject to large multipliers and co-factors, which are, in turn, functions of the delivery assets, infrastructure, manpower, and security considerations of the fuel to end user (the burdens that make up the FBCE).
- There are significant logistical burdens and operational constraints associated with the delivery of energy.

Foresight Analysis as Decision Support Tool
Despite forecasting tools, which are based on neural network theory, machine learning as well as graph analytic methods will be integrated. The management cockpit should support within CENETIX the monitoring, diagnosis, and process optimization within critical infrastructure energy systems. CENETIX offers the opportunity to test specific tasks in order to analyze the performance of certain network structures.

3. Properties of the Management Cockpit: Integrating Energy Expert Knowledge into Expert Reach Back Conceptions

The vision of COMTESSA is to create a management cockpit as part of a decision support tool to analyze such energy security issues. COMTESSA develops a decision support tool for the simulation and optimization of certain complex supply networks. As mentioned before, modern methods like computational intelligence, evolutionary algorithms, system dynamics, and data farming are embedded to master such complex networks. Through modern command and control systems, this knowledge will be integrated into expert reach back systems. The innovative sensor networks, network control, and reach back architectures of CENETIX will support an adaptive information and smart management system for energy security.

4. Integrating Cloud Computing Services into CENETIX

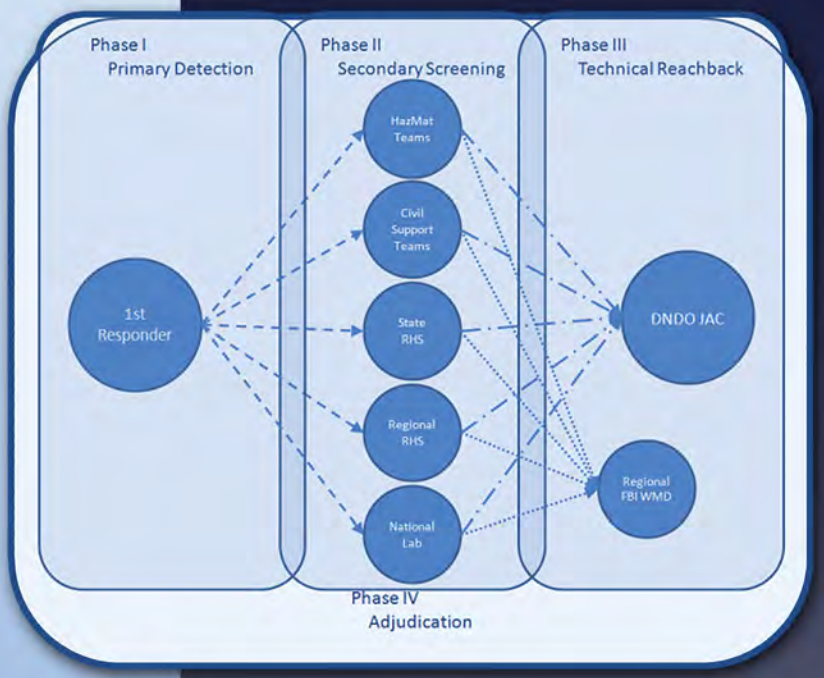
Actual questions of energy are more and more connected with cloud computing aspects. Despite that, the Cloud Computing services are entering the world of tactical networking. According to CDR James Mills (Mills, 2011), the new area of tactical networking, cloudlets, is shaping up:

"Cloudlets are small, portable appliance-like devices akin to a 'data center in a box' and include an embedded compute cluster, wireless access point and battery or alternate source power (e.g., solar, wind, etc.). Cloudlets offer the benefit of offloading computation from mobile devices, reduce latency of mobile devices by being in close proximity to the user's device, and offload data relay costs to the larger cloud/network from the mobile device".

If we study the CENETIX experiments, the reader may observe findings and prototypes of emerging tactical networking services, which we were able to identify based on unique experimental studies of tactical networking. The future findings would be helpful in structuring tactical cloud services for the variety of manned-unmanned sensor networking applications. An immediate delivery of unique expert knowledge to support front line operator actions becomes an interesting new tactical networking paradigm in which social and information networking comprise a unified system of tactical knowledge services. The recent analysis of expert-operator collaboration, conducted by Nissen and Bordetsky and based on results of the Maritime Interdiction Operations (MIO) experiments, illustrates the profound relationship between expert reach back and team tacit knowledge emergence (Nissen and Bordetsky, 2011). The following is a field experimentation example of reach back services in which such geographically-distributed experts collaborate with boarding officers in real time as the detection and interdiction of the target takes place, assisting in adjudicating the level of threat and providing most critical information.

5. Outlook: Expert Reach Back Prototype for Maritime Energy

A series of MIO experiments conducted from 2007-2013 focused on interagency collaboration during the cargo vessel search and identification of nuclear radiation threat. The experimentation team observed how the emergency response network is "flattening" itself trying to execute the required expert reach back process by means of end-to-end networking and collaboration. These findings represent a good illustration of finding new paths in the knowledge flow transfer, analytic challenges and foresight tasks ... a management cockpit which reflects these aspects might be a new step towards an expert reach back prototype for maritime energy.



6. Summary: Energy Efficiency and Performance for Critical Energy Infrastructure Networks

The expert reach back services represent another interesting phenomenon: This type of tactical service could be viewed as a foundation for Tactical Knowledge or "Tactical Memory Cloud." Such a cloud would allow live expert knowledge to be immediately shared with tactical manned-unmanned nodes on the move, so that frontline operators can become the remote situational sensors available to a "collective brain" of experts. In turn, the experts could give back the fastest learning experience to the operators. This aspect is especially for distributed energy networks and an interesting aspect which should be analyzed in the future.

Network-based cloud computing is rapidly expanding as an alternative to conventional office-based computing. We focus on the development of dynamic resource provisioning and allocation algorithms that consider the synergy between various data center infrastructures (such as the hardware, power units, cooling, software, and critical energy infrastructure networks), and holistically work to boost data center energy efficiency and performance.

LITERATURE

Bordetsky, A. (2012), Patterns of Tactical Networking Services, in: Anil Aggarwal (Ed.) Cloud Computing Service and Deployment Model: Layers and Management, IGI.

UNIBW

Prof. Dr. Pickl may be contacted through the Universität der Bundeswehr web page at: www.unibw.de/startseite/index_en.htm.

MARITIME EXPEDITIONARY OPERATIONS CONFERENCE 2013 (MEOC 2013)

"THE FUTURE OF MARITIME EXPEDITIONARY OPERATIONS (MEO) IN A CHANGING WORLD"

Major Andrew Cross, GBR-RM
Strike Force NATO (STKFORNATO)
Lisbon/Oeiras, Portugal

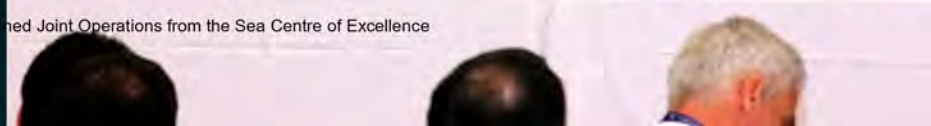
Naval Striking and Support Forces NATO (STRIKFORNATO) hosted the inaugural Maritime Expeditionary Operations Conference (MEOC) in Lisbon, Portugal on the 28th and 29th of May 2013. Over 200 senior NATO officers, including more than 60 Flag/General Officers and subject matter experts came together to have a frank, honest and open debate on current and emerging issues facing NATO since it committed to the direction of the Lisbon Summit 2010 and transformed the NATO Command Structure. The discussion, focused on the recently published Allied Command Operations (ACO) definition of MEO and the opportunities and challenges a NATO Force Structure Joint Headquarters Maritime/Expeditionary [JHQ (M/E)] might face, provided several key findings and conclusions.

STRIKFORNATO is the foremost Carrier Strike and Amphibious expert within the NATO Force Structure and as such was charged by ACO with leading the way ahead on MEO and JHQ (M/E) development. STRIKFORNATO, in collaboration with the Combined Joint Operations from the Sea, Centre of Excellence (CJOS COE), NATO's Maritime Command (MARCOM) and other NATO Commands and experts, developed five pre-MEOC 'food for thought' papers in order to focus and stimulate the debate. The ideas presented in these papers were presented in seven Flag and General Officer panels over the two-day event. Topics discussed included:

- Evolving MEO: From Requirement to Employment;
- Future Challenges and Requirements in Strike and Amphibious Warfare;
- Joint Initiatives Enabling MEO;
- Expeditionary Operations beyond the Land/Sea Border: Delivering Amphibious Capability at Strategic Distance;
- Supporting MEO: Command and Control Capabilities including Logistics and Communication;
- MEO: The Evolution of Training, Exercises, and Experimentation; and
- MEO: The Way Forward for Force Packaging and Capability Development.

Panel 3: Joint Initiatives enabling MEO: Lieutenant General Friefric Ploeger, Deputy Commander AIRCOM, Lieutenant General Frederick Hodges, Commander LANDCOM and Air Chief Marshal Sir Stuart Peach, UK Vice Chief of the Defence Staff.

ned Joint Operations from the Sea Centre of Excellence



Of the discussion topics, Force preparation, training and exercising of a JHQ (M/E) to command any potential MEO, drew considerable attention and provided the following key findings. Close cooperation and coordination between ACO and Allied Command Transformation (ACT) is required to ensure that the right capabilities are identified. A well-trained and suitably generated force is also an essential requirement. National commands will need to support these levels of readiness and work towards better exercise coordination to maximize resource efficiency; an increasing challenge in a time of fiscal constraint. Utilizing the Connected Forces Initiative (CFI) as a roadmap, ACT and MARCOM, working closely with the national commands, must work to enhance this synergy, developing exercises (CPX and LIVEX) that meet the diverse challenges facing the maritime community, and to ensure experimentation, lessons learned, doctrine and conceptual development support these exercises and training. A greater use of synthetic exercises scoped to enhance scale, evaluate interoperability and force complexity, should also be investigated.

With respect to Command and Control (C2) for MEO and JHQ (M/E), there was conference consensus that capabilities, vice complex hierarchies, are more important and relevant to delivery of future desired effects. Simplicity through familiarity, and interoperability through realistic exercising support this intent; particularly relevant when commanding complex modern-day operations requiring rapid synchronisation of a wide-range of joint enablers. Furthermore, the nature of 'componency' to support a JHQ (M/E) needs to be re-evaluated in order to support a command functionally operating at both the operational and tactical levels. On its path to certification as NATO's first JHQ (M/E), STRIKFORNATO, supported by ACT, began this evaluation during Exercise TRIDENT JAGUAR 2014, conducted this past May. Lessons will be incorporated in a comprehensive CONOPS presented in due course.

"MEOC is current, useful and delivers on behalf of the future Maritime Enterprise."

- Vice Admiral Frank Pandolfe
USN, COM STRIKFORNATO, MEOC 2013

Transparency and cohesiveness of effort resonated as themes throughout the conference. Openness and collective resolution to address emerging issues will prove critical to closing the gap between the realities of present day resource restrictions and the Alliance's requirement to meet the multitude of possible security threats. The ability to work together in a coordinated effort will help to ensure the right resources are allocated, at the right level, to deliver the right skill sets to execute the full range of missions NATO could face in the near to long-term future. The MEOC clearly demonstrated the willingness within NATO to cooperate and be transparent across commands and traditional environmental domains. Ongoing work within ACT and CJOS COE, in collaboration with MARCOM and STRIKFORNATO, will continue to foster conceptual work within the Maritime Enterprise to assure the Alliance's success.

STKFORNATO

For more information about MEOC 2013 products and details on MEOC 2014, scheduled to take place in December 2014, please contact STRIKFORNATO[1]
Public Affairs Office: sfnpao@gmail.com or your CJOS COE contact.

Our Contributors

CCOE
Civil-Military Cooperation
Centre of Excellence

der Bundeswehr
Universität München

MCR
CRITICAL THINKING.
SOLUTIONS DELIVERED.

Transforming Allied Maritime Potenial Into Reality