

Issue 20
1st Issue 2020
ISSN: 2242-441X

nmiohc

*Maritime Interdiction Operations
Journal*

NATO MARITIME INTERDICTION OPERATIONAL
TRAINING CENTRE

Space-Based assets, Applications,
user importance and Cyber Vulnerability
in Maritime Operation

A Decade of Disruption:
Cyber in the Maritime Domain

Making Maritime Strategy Work -
A New Taxonomy

Littoral Operations at the Crossroads

Sea Control





NATO

Maritime Interdiction Operational Training Centre

11th NMIOTC ANNUAL CONFERENCE
**“Interagency and whole of society
solutions to maritime
security challenges”**
29th September

**4th NMIOTC CONFERENCE ON
CYBER SECURITY
IN MARITIME DOMAIN**
30th September to 1st October

CONTENTS



COMMANDANT'S EDITORIAL

4

Editorial by Panagiotis Papanikolaou
Commodore GRC (N)
Commandant NMIOTC

MARITIME SECURITY

6

Space-Based assets, Applications, User importance and Cyber Vulnerability in Maritime Operations
by Christopher Lavers & Fotios Moustakis

13

A Decade of Disruption: Cyber in the Maritime Domain
by Chris Parker & Dinos A. Kerigan-Kyrou

17

Making Maritime Strategy Work - A New Taxonomy
by Dr. Ian Ralby

22

Littoral Operations at the Crossroads
by Edward Lundquist

25

Sea Control
by Todd Bonnar

NMIOTC COURSES & ACTIVITIES

28

NMIOTC TRAINING

33

HIGH VISIBILITY EVENTS

39

MARITIME INTERDICTION OPERATIONS JOURNAL

Director

Commodore P. Papanikolaou GRC (N)
Commandant NMIOTC

Executive Director

Captain R. La Pira ITA (N)
Director of Training Support

Editor

Captain P. Batsos GRC (N)
Head of Transformation Section

Layout Production

Lieutenant JG I. Giannelis GRC (N)
Journal Assistant Editor

The views expressed in this issue reflect the opinions of the authors, and do not necessarily represent NMIOTC's or NATO's official positions.

All content is subject to Greek Copyright Legislation.
Pictures used from the web are not subject to copyright restrictions.

You may send your comments to:
batsosp@nmioct.nato.int



NMIOTC Commandant's Editorial

It is generally acknowledged that the maritime environment is characterized by complexity and diversity. By its very nature it offers abundant freedom to seafarers, being at the same time very vulnerable to activities threatening the security of Nations and the free flow of world commerce. Terrorist movements or support to them, human trafficking, piracy and the proliferation of Weapons of Mass Destruction are just few examples of illicit activities that may be conducted from or through the sea. Areas around the Globe such as the Middle East and North Africa (MENA) region for ex-

ample, are very sensitive in this aspect, combining both, high volume of sea traffic along with potential instability spots.

Global security challenges like those mentioned above, have led the Alliance to seek for enhanced capabilities, resulting in new training requirements. In the field of Maritime Interdiction Operations (MIOs), NATO Maritime Interdiction Operational Training Center responds to these requirements and since 2008 leads the effort throughout the Alliance and beyond, aiming to improve the capabilities of allied

and partner naval units in conducting interdiction operations, including interdiction at range to enable them to cope with a wide range of maritime security challenges at further out distances.

Considering the pandemic of the new Corona Virus Disease (COVID-19) and in the light of the measures taken by the Governments and international Organizations to fight the spreading of this virus, NATO Maritime Interdiction Operational Training Center has ceased all in-resident activities since Monday 16th of March 2020. In this

regard, the “11th NMIOTC Annual Conference” is also postponed and it is rescheduled to be held at our premises, Souda Bay of Crete, on Tuesday 29th of September 2020, followed by the “4th NMIOTC Conference on Cyber Security in Maritime Domain”, which will be held from Wednesday 30th of September to Thursday 1st of October 2020.

Following the termination of these unprecedented circumstances, we stand ready to welcome once again

allies and partners to our training programs and initiatives, in order to contribute to the combined effort of developing solutions and addressing current and emerging maritime security challenges. It goes without saying that our intention is to focus on the implementing preventive measures in order to protect our trainees, NMIOTC personnel and their families, as well as to stay vigilant and to act responsibly.

Lately, the Steering Committee of the European Security and

Defence College (ESDC), has decided to accept the application of the NATO Maritime Interdiction Operational Training Center to join the network of the ESDC as Accessing Associated Network Partner (ANP). NATO Maritime Interdiction Operational Training Center activities are of the interest for the ESDC and definitely a closer cooperation and collaboration with respect to maritime security issues and challenges, under the framework of NATO – EU joint declaration.

Panagiotis Papanikolaou
Commodore GRC (N)
Commandant NMIOTC



SPACE-BASED ASSETS, APPLICATIONS, USER IMPORTANCE AND CYBER VULNERABILITY IN MARITIME OPERATIONS

Christopher Lavers

Fotios Moustakis

*Dartmouth Centre for SeaPower and Strategy,
Britannia Royal Naval College*

Today we are reliant upon a growing number of space-based assets. Asymmetric hybrid threats towards space platform hardware, software, and data storage, may come from unexpected state and non-state actors, driven to deprive adversaries of such capabilities, requiring cooperative approaches to defend against, and combat effectively, damage to space-reliant data. To assess inherent space-related risks it is critical to evaluate existing and planned systems. Following previous analysis, the Dartmouth Centre for Seapower and Strategy (DCSS) has evaluated the current space-based market. This paper summarises 2019 findings from a wide range of participants. Our analysis includes: the importance of: persistency, all-weather, night and day capabilities, satellite image resolution, and other technical requirements. Hybrid threats, cyber warfare, GPS 'spoofing', jamming, la-

ser dazzling, and EMP are part of a new generation of threats becoming relevant with rapid exploitation of the space domain, in addition to space-weather impact. Space currently provides critical mission access for military tactical communications and other activities, and is an essential civilian element in social and economic life. The US Department of Homeland Security estimated that £1.6 trillion of US revenues in 2016 were derived from space-related data. According to the Royal Academy of Engineering Society we are already dangerously over-reliant on satellite radio navigation systems like GPS¹. Financial markets rely on globally synchronized time-stamp mechanisms to ensure fair trading. Signal failure or interference may potentially affect safety systems and other critical parts of the economy.

At DCSS we look at the key space-

based infrastructure planned for the coming decade, with a methodology developed for a prominent European Defence and Space customer, to inform discussion around proposed space systems. Space-based systems are at risk of sophisticated cyber-attack, and traditional methods. Here, we concentrate on user views of: Assets, Threats posed to current space-based systems, Capabilities, and Questionnaire Findings. Today, military and civilian national security rests upon geospatially-related economic data. Digitisation has transformed the way users conduct operations, creating new data products, often from multiple sources which only exist in cyberspace. Consequently the digital era affords opportunity for a growing number of existential threats to security, if the digital domain is compromised.

1. Asset Infrastructure

A wide range of global systems, on land, sea, air, and in space, are vulnerable to military or terrorist action, e.g. electromagnetic pulse (EMP), besides solar weather. These sources may affect more than just ECDIS and GPS. For unprepared space-systems operators, solar weather in its severest form can remove much of a ship's essential electrical infrastructure. Geomagnetic storms pose particular problems for space-based systems, such as GPS. When atmospheric transmission properties change unexpectedly, during storms, navigation fixes become inaccurate, and for short periods satellite signals may be lost completely. Protective measures against space weather are of vital importance to ESA, the EU, and the maritime community. Although GNSS has 3 critical segments: ground, space, and users, impact on space-based platforms directly impacts terrestrial users. Vessels are highly dependent on cyber-physical systems; navigation and control systems are vulnerable to solar weather and EMP. ECDIS, GNSS, and GPS system data provided by satellites for navigation and timing in turn feed ocean-going AIS, AIS compasses, GMDSS, besides other systems. Solar weather impact can be devastating, however deliberate targeting by EMP devices fitted to nanosatellites in the vicinity of critical space-based infrastructure could be as deadly, and if conducted in a coordinated manner, likely cause GPS and other networks to fail. Noise transmitted over GPS/GNSS frequencies raises levels to overload receiver circuitry, breaking signal lock; microwave or optical laser jamming can also deny, degrade or disrupt satellite performance.

2 Overview of Digital Maritime Surveillance Technology

Digital maritime surveillance today is cyber-space representation of what is happening over, on and under the physical domain of the sea surface and coastal areas, from various data

products, to detect potential activities impacting security, safety, and economy of the environment. Maritime surveillance aims to understand, prevent, and manage actions and events that impact maritime safety, security, search and rescue, accident or disaster response, fisheries control, marine pollution, border control, general law enforcement, and defence, as well as economic interests. Such differing tasks require deployment of various assets such as ships, submarines, aircraft, helicopters, communications, UAVs, the sea-bed, and space-based capabilities. Information is collected at various levels using these assets, including satellites (covering a wide domain); maritime patrol aircraft or ships (at a more precise level); with UAVs and helicopters (over specific target areas).

Space technologies have supported the maritime community for over 30 years. Now these technologies benefit the community through enhanced navigation accuracy, GNSS (PNT), and marine environmental monitoring and surveillance (ESA, 2008)². Surveillance at sea poses unique challenges: detection of small targets; large areas to survey; with constantly moving or changing targets and backgrounds. Maritime surveillance technology is a proven decisive factor in naval warfare and national security, and is a force multiplier for successful operations. Advancing technologies play an increasing role in monitoring surveillance, with modern surveillance relying on radar, and electro-optical solutions: notably night vision or thermal imagery. Recently Synthetic Aperture Radar (SAR) and Inverse SAR (ISAR) have entered the stage, providing opportunities in several critical areas for Military or Civil authorities, enhanced situational sea safety, and potential economic savings to Fleet managers. Reduced space-based capabilities in these areas will significantly affect the ability to conduct maritime operations.

2.1 Space-based capabilities

Military requirements for detailed satellite imagery globally, 24/7/365, is driving satellite providers to reassess how they conduct business. The primary solution today is imaging radar, which operates under cover of darkness and in challenging battlefield or environmental conditions. The military market is significant, yet potential for civil exploitation is larger, with governmental and pan-governmental users (e.g. the EU's Copernicus programme) looking to provide detailed large-area views rapidly to end users. There are over 30 proposed satellite radar sensors, many of which will be realised. Key space-based capabilities include:

2.1.1 Synthetic Aperture Radar (SAR)

Satellite-based SAR is used widely in maritime surveillance due to its ability of achieving high resolution in both range and azimuth directions³. Unlike optical imagery, SAR is unaffected by time of day, or meteorological conditions, meaning data acquisition can be made any time of day or night and independent of cloud coverage. When SAR satellite imagery is combined with Automatic Identification System (AIS) data in synergistic products, they provide a powerful tool for maritime surveillance, as AIS data can identify ships which SAR imagery detects, whilst SAR imagery detects ships which may not cooperate with AIS⁴.

2.1.2 AIS

AIS, an automatic tracking system used on ships and by Vessel Traffic Services, identifies and locate vessels by electronically exchanging data with nearby ships. It is used extensively in the maritime world with vessel AIS transponders using GPS receivers to collect vessel position and movement details. Maritime security and tracking are important AIS applications, with 250,000+ ships now broadcasting on AIS, allowing terrestrial detection up to 50km away. Due to earth curvature restrictions information is only

available around coastal zones or on a ship-to-ship basis. One company Nano Satisfi is looking at LEO nanosatellite fleets to provide vessel positions without costly uplinks. Nanosatellites, typically 1-10kg in mass, are a recent maritime satellite solution, developed at low cost, and in numbers for threat resilience, but without the capabilities of traditional systems, previously only affordable by wealthy nations. These offer emerging countries and actors the ability to deploy spacecraft rapidly from development to launch. Nanosatellites can operate in co-operative ways, providing increased loss resistance, as well as being harder to target than existing maritime drones. Satellites solve this problem, whereby a ship's identity is recorded and decoded by satellite and sent to ground stations for further processing and distribution⁵. Known as S-AIS, it significantly increases the number of potential vessels within a satellite's footprint. Since the mid-2000s companies have detected AIS transmissions with satellite-based receivers. ExactEarth and Spire, alongside government programs, have deployed AIS receivers on satellites.

2.2.3 Applications of Maritime Surveillance Technology

The potential applications of maritime surveillance technology include:

ISR- Intelligence, Surveillance and Reconnaissance encompasses multiple activities which relate to planning and operation of systems which support current and future military operations. Land, sea, air and space-based platforms have critical ISR roles in supporting operations.

Piracy- The worldwide threat of terrorism and piracy in international waters is high and the need for solutions is paramount⁶. For piracy surveillance, and recent terrorist attacks on Saudi shipping (2018), satellite-based vessel detection can integrate with conventional data streams to extend surveillance information to Coastguard, police, naval, intelligence services, customs

and border guards. Satellite imagery gives a unique overview of what happens around a hijacked ship, and can monitor movements of mother ships and smaller craft swarms. A Copernicus-funded project supported the Italian Coast Guard tracking the oil tanker Caylyn Savina, pirated in the Indian Ocean in 2011, using COSMO-SkyMed constellation satellite imagery⁷. Data collected is now effective in preventing attacks before they happen. Denial of satellite imaging will hamper such operations. It is likely satellite ship monitoring will tackle illegal immigration as imagery resolution improves.

Pollution and Oil Spill

Surveillance- Oil slicks are visible in SAR imagery as dark areas. Most oil slicks are caused by ships emptying bilges before entering port⁸. A satellite image can capture over 100,000km² of sea surface at once; an efficient way to check for oil spills. Satellite-based optical with SAR are of special relevance for oil spill detection, providing high-resolution all weather, day and night, wide-area coverage. CleanSeaNet, an European satellite-based oil spill and vessel detection service, uses SAR images from polar orbiting satellites. CleanSeaNet identifies and traces oil pollution on the sea surface from ships and offshore installations, and monitors accidental oil pollution at sea during emergencies⁹. Sentinel 1 is a satellite-based SAR system that supports operational oil spill monitoring and vessel detection and tracking in Europe⁹. Disrupted data reception may limit effective early response.

Ice Monitoring- Satellite-platform SAR data is valuable in monitoring seasonal or permanent ocean ice-cover in the Arctic, Baltic Sea, Bohai Sea, or Sea of Okhotsk. SAR images provide sea ice condition operational mapping for marine traffic or offshore operations. Sea ice cover change over recent years provides an indication of global warming, and is expected to strongly impact the Arctic environment¹⁰. The Copernicus Marine

Environment Monitoring Service (CMEMS) provides operational forecasts for sea ice to support Northern Sea ship routing, and search and rescue activities. The Sentinel-1A satellite allows frequent revisits (from daily). Satellite products are available (within 3 hours) to CMEMS operators who produce daily ice charts, iceberg density maps and maps of sea ice drift and deformation¹¹. Infrequent data updates may increase collision risk.

Illegal Fishing- Illegal Unrecorded Unregulated (IUU) fishing has depleted fisheries to critical levels, yet IUU fishing persists as authorities cannot survey all seas simultaneously to stop it and protect marine species worldwide. London Economics (2015)¹² reported 1 in 5 fish are taken illegally from the oceans, costing the global economy an estimated £15.2Bbn p.a. Fishing vessel behaviour monitoring is critical to tackle this problem. In the UK, a prototype Information Analysis Platform was developed to analyse fishing vessel behaviour, and can potentially use freely available satellite data from providers such as NovaSAR, Sentinel-1, or CubeSats, and data used by Defra, the Fisheries Departments and other authorities to inform of illegal fishing in UK waters¹³. Satellite imaging operates independently of AIS, but if satellite-based AIS and imaging reception are disrupted illegal fishing may go undetected.

Search and Rescue- Maritime surveillance technologies support search and rescue missions, detecting distressed vessels or missing aircraft or ships. Recent maritime operations have significantly changed priorities, providing a more effective approach to mass rescue operations highlighted by the Mediterranean crisis, and development of new search and rescue technology. Errors or outages in GPS information may hamper successful rescue of those in distress.

Illegal Trading of Goods- Maritime security threats include illicit activities, e.g. transport of migrants, smuggling goods, or drug trafficking.

In the EU large amounts of cigarettes and tobacco are smuggled from China at an estimated cost to the EU economy of 10bn Euros p.a., whilst drug smugglers use containerised sea transport as a simple, convenient and cost effective mode of transport¹⁴. NovaSAR is a constellation of 4 SAR satellites which once fully developed, will operate in all weather conditions, day and night. The UK allocated £21M to assist in development and launch of the first satellite in 2018. The Maritime Analysis and Operations Centre –Narcotics (MAOC-N), based in Lisbon, is an EU initiative involving 7 countries. The Centre uses integrated vessel information to monitor and track suspect vessels in the Atlantic and Mediterranean¹⁵.

Other threats, satellite imaging and RF detection may assist include:

Anti-Terrorism Activities- Ships and seaports may be used to facilitate terrorist activities in different ways including: using ships as 'bombs'; and weapons trafficking. Operation Sea Guardian (OSG) is a maritime surveillance operation led by NATO's naval forces which patrol the Mediterranean and monitor shipping to help detect, defer and protect against terrorist activity. The operation evolved following terror attacks against the USA (Sept. 2001.)

Port and Off-Shore Security- refers to the defence, law and treaty enforcement, and counterterrorism activities that fall within the port and maritime domain, including protecting seaports and harbours by monitoring facilities, storage areas and container depots. Current systems operate by scanning and observing all land and maritime zones for unauthorised activities continuously. If intruders are observed, the systems continue with identification and tracking of the intruders and direction of security forces¹⁶.

Autonomous Boat Navigation- Rolls-Royce began developing unmanned technology

in 2013 and expects by 2025 there will be satellite remote controlled unmanned coastal vessels, and ocean-going ships by 2035. GPS reception disruption and consequent AIS output for unmanned vessels, will have a significant impact.

Land-based Applications- Surveillance can gather information to support maritime-based activities, and provide benefits in observing and supporting land-based activities in the littoral environment. Applications include: Agriculture, Forestry, Risk Management and Disaster Monitoring, where satellites monitor areas affected by disasters e.g. flooding, tsunami, critical for timely disaster relief efforts, allowing for rapid response to priority areas captured in images.

3. Threats

Good cyber-security at organisational and personal level is essential if threats to space-based GPS, AIS, and other data are to be neutralised effectively. The size of geospatial vectors in raster and point cloud data make them obvious targets for computer-based-learning algorithms. The importance placed on GPS, and AIS by end users is clear. Subversive space-based attacks on GPS-satellite platforms will likely attempt exploitation by new methods as well as traditional attacks. Likely attack routes include: jamming, EMP devices, direct satellite destruction (bomb or kinetic device), or laser-based weapons. Anti-satellite (ASAT) demonstrations prove kinetic capabilities; a recent Indian ASAT test took place at an altitude low enough that debris burned up in the atmosphere¹⁷⁻¹⁸. Kinetic systems create permanent and irreversible space asset destruction, whilst electronic and cyber provide temporary disruption and damage to space systems. Some states are moving away from expensive consumable direct-ascent missiles to affordable and available long lasting electronic and cyber methods that impact space assets. In addition co-orbital satellite

systems (COSAT) are satellites placed on similar orbits directed to intercept or interfere with other adjacent satellites through close orbital rendezvous operations. Threats may also be provided from high altitude pseudo-satellite platforms.

GPS jamming or spoofing of a satellite may prevent ephemeris ground station updates. A small space jammer can disrupt the satellites GPS signal reception as effectively as a small terrestrial GPS jammer can disrupt proximity receivers. Protocol-specific attacks [RF] or 'messing with in-built commands.' attack systems through flaws in data protocols, and Software-specific attacks [SW] or 'messing with the data'. Implementation threats exploit vulnerabilities in service provider systems, attacking collection and vessel information visualisation. Ground station update authentication must ensure transmitters are genuine, and time-stamped. Integrity tampering is vital so valid data checks are required, e.g. is geographical information correct? Data location must be cross-checked across data sources. Fake reports or numerous false GMDSS satellite alarms may be broadcast, triggering satellite response. Spoofing 'hijacks' a satellite's command and control, and feeding it false data is a known means of disruption, available to the US since 2004. We must build protection for critical space-based infrastructure, covering space, maritime and terrestrial systems, for military and civil operations. At present the main protection means from solar weather is increased warning time. However, co-ordinated attacks from nanosatellite threats may happen without warning. Satellite swarms may provide some protection against sudden catastrophic system loss, but 'hunter-killer' nanosatellites armed with EMP generators may degrade systems overall. Hardening all space-based systems to military grade EMP protection is unfeasible, nor affordable. Early examples of Chinese scientists 'blinding' optical satellites with ground-based laser guns (2005),

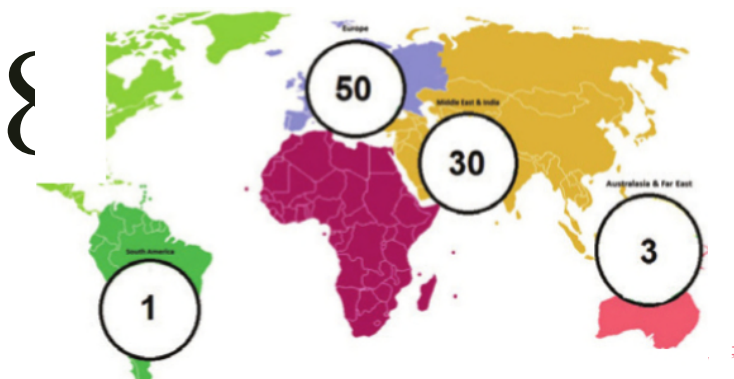


Fig 1. Distribution of Stakeholders Views

were followed by Russian Federation laser-based A-60 aircraft ASAT operation, dazzling and blinding sensors to result in physical damage. In each case correct threat hazard evaluation from multiple intelligence sources and integration will determine various courses of action, likely objectives, desired outcomes, and how to prioritise them.

4. Research Findings

4.1 Stakeholder Asset Questionnaire Consultation

From 4 years of ongoing discussion with various global space and maritime professionals we engaged various stakeholders to establish their thoughts around current and future space-based requirements and activities. Consultation took place via a combination of face-to-face interview, telephone consultation, email conversation and questionnaire. During this research, we received responses from 90 stakeholders. We summarise engagement with stakeholders and some of these responses.

4.2 Record of contact with shareholders

Fig. 1 provides the geographical distribution of questionnaire respondents, with breakdown by global region. Ninety stakeholders gave answers to some or all of the questionnaire questions.

4.3 Findings from Stakeholder Consultations

Responses in this paper came from questionnaire responses and informal discussions with upstream satellite data providers and launchers, and maritime professionals (downstream sector). Analysis of results, together with information received through conversations revealed the types of services(s) of interest to organisations participating, and their weighted importance, differing by nation as well as between upstream and downstream.

Surveillance technical capabilities- Responders were asked technical requirements on issues related to space-based systems. The questionnaire asked respondents to indicate how important specific capabilities of a surveillance system were to them. Respondents rated the importance of 'night and day', 24/7 capabilities; 'all-weather' surveillance which operate in all-weather conditions including cloud cover; and 'persistence' space-based capabilities, on a scale of 1 (not at all important) to 5 (very important). Respondents were asked about AIS, temporal frequency requirements for data-acquisition, and importance of target detection. Maritime professionals were asked to state the most important space-based capability, and their geographical interest. We also canvassed response on navigation-related sensors, and

the importance of earth observation capabilities development, primarily for Middle-East and UK maritime professionals.

Persistence- the ability to provide continuous maritime and littoral surveillance of any chosen area for required period, is a high requirement for the downstream satellite user community. From questionnaire data from 10 Middle East responses (3 nationalities). Persistence has a very high regard downstream with

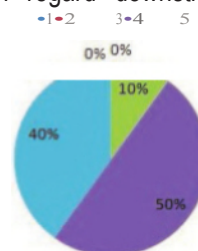


Fig 2. Middle East Persistence Responses

90% responding 4-5 (Fig. 2). Typical comments include "The persistent system would be required in the event of a piracy incident, enabling surveillance of movement of hostages", although a common criticism was "We do not have the capacity to process data any faster than weekly, except in crisis conditions following a piracy incident." Upstream returns (Fig. 3) were provided from (11) different companies in the launch sector, providing good correlation again with categories (4) and (5) with downstream Middle East end-users. It may be inferred upstream companies are judging the end-user market correctly.

Night-Day capability End-user 'Night-Day' importance data from Qatari Coastguard responses

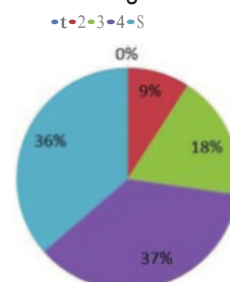


Fig 3. Upstream Persistence Responses

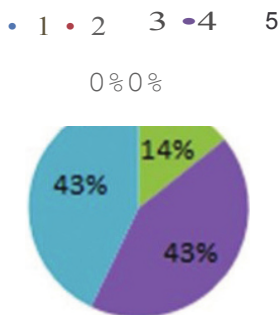


Fig 4. Downstream Qatar Night-day Responses

is shown (Fig. 4). Typical responses here: “Because you want a safe coast you have to work night and day and in all weather conditions,” and “Our mission has to be done 24/7 partial coverage would not offer the operational capability requirement.”

Temporal Surveillance The perception of temporal range requirements from 13 Saudi Arabian end-users, are spaced a cross the range (Fig. 5), but

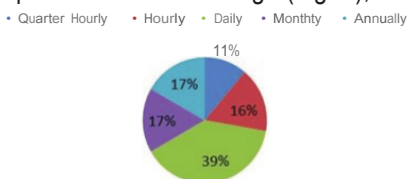


Fig 5. Saudi Arabia Temporal Frequency requirements

favour at least daily measurements. Frequency requirements vary. Some respondents gave more than one answer. One South American response on this temporal issue stated “An hourly frequency is enough to hail all ships inside the area of maritime operation.”

- High Resolution SAR
- Domain
- Low (sub km- few km)
- 1-30m
- High Resolution below 1m



Fig 6 Current Resolution Requirements

Another UK response “Guaranteed daily, and then hourly when needed would be very useful for flooding applications.” There is no universal

specific frequency requirement but frequency requirements are universal.

Resolution and Target Selection Current resolution requirements responses are varied, Fig. 6. For general updates of the maritime picture daily updates are sufficient (i.e. domain). Taken alongside Fig. 7, skiffs up to 10m

- Sm resolution
- Any Shiptr-king
- Boat recognition
- Fast boats and skiffs
- Target ships

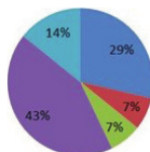


Fig 7 Current Important Target Selection

and small fast boats (c. 20ft) provide the dominant category (43%). 1-3m resolution allows vessel recognition, whilst 300m+ is sufficient for tankers or large ships. 10% state they need sub-few km resolution, nearly ¼ want 1-30m medium resolution for identification. 16% want optical resolution below 1m, whilst 25% of respondents state they require high resolution SAR. Nearly ¼ of end-users only require domain awareness. Responses are provided from 14 upstream and downstream stakeholders. Fast boats and skiffs are the biggest specific category, which if combined with the 5m category accounts for 72% of responses. One response from Qatar “4-5m rib, look for clear view of any vessel entering Qatar Coast illegally to be able to complete successful mission without putting any Coastguard personnel in danger.”

Most important space-based capability we tried to gauge perception of the importance of space-based sensing and communications capabilities from various maritime professionals. The importance from 33 UK respondents provided evidence of the overwhelming importance associated with GPS, being the single-most important space-based capability. Whether end-users are right to give this emphasis on space-based GPS capability is not the focus of this

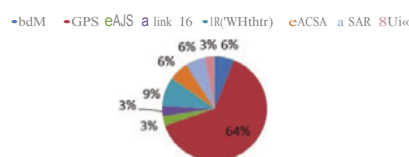


Fig 8 Most Important Space-Based Capability

paper.

All-Weather capability

9 respondents generated the data indicated here, with all-weather capability regarded as dominant, i.e. very important, and 8 out of 9 responses within categories 4-5 (Fig. 9). The following typical response of all-weather capability is clear, “It will manage the coastal area and offshore area in bad weather when small boats (CoastGuard) cannot go offshore.”

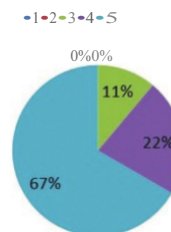


Fig 9 Qatar Coastguard All Weather

5. Summary

Maritime security and surveillance markets have grown in recent years and will continue to grow over future decades. Some market-players stress the trend towards Smart Data Analytics, with mixed optical/SAR tailored information, improving SAR utility and earth observation data. SAR is a strong market-area within maritime persistent stare, supporting commercialisation of space-based high resolution SAR with other capabilities, likely in consortia composed of multiple partners. One UAE respondent wanted “A satellite which can provide earth imaging, detecting piracy, reckoning and illegal ships”. This paper provided discussion of current space-based assets, applications, importance and vulnerabilities, with quantified findings covering: persistence, Night-Day, S-AIS, surveillance frequency, resolution and target selection, with all-weather capabilities. Expectations, in some cases are well-matched, and

less so in other categories. Mismatch between user groups is important, and shows there is work to be done gauging and bridging demand for specific customer services, matching

upstream with downstream users. The range of responses is considered representative of the space-based sensors market. With increased use of advanced on-board processing, all

digital components, software-defined radios, packet-based protocols, and high performance cloud-computing, the attack potential for cyber and physical attack is greatly expanded.

References

1. UK Royal Academy of Engineering Report: Global Navigation Space Systems <https://www.raeng.org.uk/publications/reports/global-navigation-space-systems>
2. ESA 2008, [esa.int/Our_Activities/Observing_the_Earth/Copernicus/Why_is_space_relevant_for_maritime_issues/\(print\)](http://esa.int/Our_Activities/Observing_the_Earth/Copernicus/Why_is_space_relevant_for_maritime_issues/(print))
3. Guerriero, M., Willett, P., Coraluppi, S., & Carthel, C. (2008). Radar/AIS data fusion and SAR tasking for maritime surveillance. In Proceedings of 11th international conference on information fusion.
4. geocento.com/satellite-imagery-case-studies/satellite-imagery-can-help-on-maritime-surveillance
5. esa.int/Our_Activities/Telecommunications_Integrated_Applications/Satellite_-_Automatic_Identification_System_SAT-AIS
6. monitor-systems-engineering.com/anti_piracy_terrorism_maritime_security_specialist_partner_products.html
7. copernicus.eu/sites/default/files/documents/Copernicus_Briefs/Copernicus_Brief_Issue3_Pirate_Sep2013.pdf
8. sentinel.esa.int/web/sentinel/user-guides/sentinel-1-sar/applications/maritime-monitoring
9. emsa.europa.eu/csn-menu/csn-service.html
10. [esa.int/Our_Activities/Observing_the_Earth/Copernicus/Why_is_space_relevant_for_maritime_issues/\(print\)](http://esa.int/Our_Activities/Observing_the_Earth/Copernicus/Why_is_space_relevant_for_maritime_issues/(print))
11. tos.org/oceanography/assets/docs/26-2_dierking.pdf
12. ceos.org/document_management/Publications/Data_Applications_Report/DAR_Summary-Brochure_Digital-Version_Dec2015.pdf
13. ukspace.org/wp-content/uploads/2015/07/LE-Case-for-Space-2015-Case-Studies.pdf
14. uaces.org/documents/papers/1301/carpenter.pdf
15. emsa.europa.eu/emsa-documents/download/3349/2361/23.html
16. controp.com/port-security/
17. RP Rajagopalan "India's Changing Policy on Space Militarization: The Impact of China's ASAT Test", India Review Vol. 10, No.2, 2011, pp. 354-378.
18. RP Rajagopalan "Having Tested its ASAT Capability, India Should Help Shape Global Space Norms", ORF Commentaries, 29, March 2019.



Fotios Moustakis is an Associate Professor of Strategic Studies and Director of Dartmouth Centre for Sea Power and Strategy, University of Plymouth at Britannia Royal Naval College. He is also the Programme Manager for the MA Degree in Applied Strategy and International Security at the Hellenic National Defence College, Athens. His research interests are in the areas of International & European security, with special emphasis on strategy, western interventions in the post- Cold War Era, and international terrorism.

He has published widely in a number of refereed and policy practitioner journals such as Defence Studies, Defence and Security Analysis, European Security, Mediterranean Quarterly, Central Asian Survey, Contemporary Security Policy, Mediterranean Politics, Jane's Intelligence Review, Conflict Security Research Series-Sandhurst, and Contemporary Review.



Dr Chris Lavers is an Engineering lecturer, and has taught Maritime Earth Observation and Remote Sensing topics at Britannia Royal Naval College (BRNC) since 1993, with special interest in space-based platforms, and man-made disasters, and applications of high resolution satellite imagery. He has been on national committees for Environmental Sensing, and Earth Observation, and has provided expert commentator evidence to a UK House of Commons Parliamentary Satellites and space inquiry report.

He is also Subject Matter Expert (Radar and Telecommunications) at BRNC, Dartmouth, UK, and Principal Scientist at the Dartmouth Centre for SeaPower and Strategy. He has published 15 books, 6 in the REEDS Engineering Maritime Series', besides 200 papers and articles. He is currently a Visiting Fellow at The Changing Character of War Centre, Pembroke College, Oxford.

A Decade of Disruption: Cyber in the Maritime Environment

by Chris Parker
& Dinos A. Kerigan-Kyrou

The Monaco Yacht Show: the global superyacht event of the year. A flotilla of hundred million-dollar yachts with no expense spared opulence for the super-rich. Over 200 superyachts, the most expensive, bespoke built assets on earth; home to the wealthy - and surely cyber secure? Instead, an expert cyber investigator¹ within minutes was able to digitally identify 10 ships as 'exploitable'²; by end of day one over 80 vessels were effectively 'unlocked'. This included many superyachts exposing their owners and crews. Beyond the lone cyber security stand at the 'MYS', there were 150 others including five stands for electric gang-planks and several for bespoke linen,

motorised surf boards, and sumptuous leather seats. In a world of budgets for all possible luxuries it seems odd that securing the cyberspace around the vessel has fallen off the plan.

The maritime sector is well known in professional IT circles to be well behind land-based sectors in understanding the risks to OT (Operating Technology), as well as the more easily seen Information Technology (IT). How can assets so vastly expensive and containing such high worth cargo be so exposed – is it just because they are afloat? Why is maritime cyber security so far behind when the maritime industry's fire and safety drills are first

class? How can the insurance industry begin to cope with this level of emerging cyber risk? Experts are discussing these aspects now with key stakeholders and there is considerable unease. There have been increasing malware attacks and data penetration against maritime platforms and IT; the level of cyber security systems, processes and knowledge is globally assessed as poor. The high risks rising in maritime cyber security should give IT & OT stakeholders cause for alarm and a call to action. Cyberplus has designed a system-of-systems turning Super Yachts into certified CyberYachts®³. But how can the situation experienced in Monaco's gathering of elite ships

1 Attending show as a technical partner with Cyberplus Ltd UK.

2 Legal and ethical reasons mean professional experts effectively can go to the equivalent point of 'trying the door lock' but not beyond into exploitative action. Exploitable means that in a short degree of time and effort significant data or control could be compromised. Source: Cyberplus Ltd UK.

3 <https://cyberplus.co.uk/cyberyacht/>

have come about?

There are maritime cyber security challenges for these superyachts - but also for ferries, cargo vessels and of course for the military. The new Zumwalt-class destroyer first deployed in 2013 with a crew of only 158, compared with 329 on the Arleigh Burke-class of 22 years earlier has a tenfold increase in defence capabilities. The Zumwalt-class is reliant on electronic, integrated systems and platforms for its military abilities and operational systems⁴. CDR (ret'd) Zachary Staples and Maura Sullivan (US Navy) state: "All ships operate three main networks:

- + the voyage network supporting the vessel's safe navigation.
- + the engineering network controlling propulsion, material handling, and auxiliary systems.
- + the administrative network supporting business operations and crew welfare."

U.S. Navy vessels also have a combat systems network, state Sullivan and Staples. This is the 'interconnectedness' of operational and information technology networks. "The interconnectedness of operational and information technology networks means that traditional information technology tools and perimeter-based security solutions are inadequate for cyberphysical systems."

Modern vessels - both military and

civilian - increasingly comprise what is known as 'the Internet of Things' (IoT). IoT consists of internet devices (or 'things'), receiving and transmitting data. These devices contain sensors and actuators performing critical functions. While they may not resemble computers, this is exactly what they are - computers running software and 'firmware' (a computer program stored within the hardware). The number of IoT in vessels is growing exponentially. For example, power management, loading and stability, container monitoring, alarms, bridge control consoles, Electronic Chart Display and Information System (ECDIS), the Automatic Identification System, Navigation Decision Support (NAVDEC), Voyage Data recorders, Computerized Automatic Steering, and the Global Maritime Distress and Safety System (GMDSS); all of these increasingly comprise IoT. All of these are connected to the internet - the same internet we use for Facebook, Amazon and Skype. (Contrary to popular belief, there is no separate 'secure' internet for shipping and critical infrastructure - it is all the same internet).

And the increase in IoT is not only within vessels. Ports increasingly feature multiple examples of IoT including port security, access control, CCTV, gates, ID cards, automated cargo handling equipment, Terminal Operating Centres, cranes, and integrated supply chain logistical systems. Port IoT devices are directly interacting with

vessels' IoT including communications, GPS (Global Positioning System), lock operations, maintenance and management, pollution and environmental control systems⁶.

NMIOTC has previously examined the cyber security concerns of maritime IoT both within the Journal⁷ and at the NMIOTC Annual Cyber Security Conferences. Moreover, research conducted by CERN in Geneva indicates that around a third of IoT devices are 'open door' (i.e. no security whatsoever), and at least two thirds have very poor security⁸.

In 2013 a key test of maritime cyber vulnerability was made by University of Texas Austin. A 60m superyacht was coerced off course with a GPS spoofing device. A modern yacht's position is entirely reliant on GPS. Using the device a researcher was able to act as an attacker replacing the legitimate GPS, emitting fake signals toward the vessel's antennas. The 'attacker' was able to easily cause a 3-degree change in course. Furthermore, the real course of the ship was faked to the crew leaving them misled as to the true tack of the ship, and believing false situational and directional information. Unlike GPS signal blocking or 'jamming', the method of 'spoofing' will not trigger any alarms on a ship's navigational equipment. The false signals were indistinguishable from authentic signals, allowing the spoofing attack to happen covertly.^{9 10}

4 See: Dr. Elena Mandalenakis, "Cyber Threat Scenarios for Maritime Power," NMIOTC - Journal of the NATO Maritime Interdiction Operational Training Centre 15, no. 2 (2017): 6-16; Dinos A. Kerigan-Kyrou, "The NATO Cybersecurity Generic Reference Curriculum: Application to the Maritime Environment," NMIOTC - Journal of the NATO Maritime Interdiction Operational Training Centre 15, no. 2 (2017): 28-31. Also see: Dr. Elena Mandalenakis, "Political Implications of Cyber Space on State Power," NMIOTC - Journal of the Maritime Interdiction Operations Centre 13, no.2 (2016): 15-24; and: Adrian Venables, "Maritime Cyberpower Projection," NMIOTC - Journal of the NATO Maritime Interdiction Operations Centre 14, no.1 (2017): 15-28.

5 Zachary Staples, Maura Sullivan, "Cyber Lessons from the USS McCain and USS Fitzgerald Collisions", in: 'The Maritime Executive', available at: <https://www.maritime-executive.com/editorials/cyber-lessons-from-the-uss-mccain-and-uss-fitzgerald-collisions>

6 Kerigan-Kyrou, NMIOTC Journal (2017), op.cit.

7 Kerigan-Kyrou / Mandalenakis, NMIOTC Journal (2017), op.cit.

8 Dr. Stefan Lüders, CERN. 2012 Presentation at the ITU; available at: [www.itu.int/en/ITU-T/studygroups/com17/Documents/tutorials/2012/11-CERNComputerandGridSecurityITU\(2012\).pdf](http://www.itu.int/en/ITU-T/studygroups/com17/Documents/tutorials/2012/11-CERNComputerandGridSecurityITU(2012).pdf)

9 The University of Austin, Texas, UT News, July 29, 2013. Available at: <https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/>

In 2017 two very high-profile US Naval collisions occurred. On June 17 the USS Fitzgerald, Arleigh Burke-class destroyer collided with the Philippine flagged container ship MV ACX Crystal, 80 nautical miles SW of Tokyo. Seven sailors aboard the Fitzgerald tragically lost their lives and three were seriously injured.¹¹ Just two months later on August 21, the USS John S. McCain, also an Arleigh Burke-class destroyer, collided with the Liberian-flagged tanker Alnic MC off the coast of Singapore, east of the Strait of Malacca. There were 10 tragic fatalities. The report into both incidents states multiple contributory factors.¹² It is important to note that ADM John Richardson, Chief of Naval Operations stated "...to date, the inspections we've done show that there's no evidence of any kind of cyberintrusion."¹³ While CDR (ret'd) Zachary Staples (former Director, Center for Cyber Warfare US Naval Postgraduate School), asserts that we simply do not have the "basic tools" to definitely answer the question: "were we hacked or did we break it?"¹⁴

At a cyber security briefing in Man-

chester in July 2019 attended by one of the authors, an ethical hacker stated that if a cyber breach leads to a collision between a military vessel and a non-military vessel, it is much more likely that it will have been the non-military vessel that is breached because the military vessels have far superior levels of cyber security.¹⁵ In other words, if a terrorist or other hostile wants to cause a maritime attack or 'accident' by breaching cyber security he does not actually need to target the military vessel at all. He only needs to target the civilian vessel (that will be in the vicinity of the military vessel), with its far inferior levels of cyber protection. To change the words of CDR (ret'd) Staples: We - the military - do not need to be hacked in order for the 'break' to occur.

What to do?

Dr. Stefan Lüders, head of cybersecurity at CERN states that the security of the Internet of Things must be built into the manufacture of the devices.¹⁶ Moreover upgrading of the security through the lifetime of the device needs to be incorporated in all mari-

time IoT easily and without any additional cost.¹⁷ However CERN state that this situation, far from getting better "is getting worse."¹⁸

Second, cyber security needs to become the responsibility of everyone involved in the maritime environment. Because, if it is not, the number of 'ways in' for a nefarious actor will grow so exponentially there will be no chance to prevent them from successfully attacking the maritime cyberspace.¹⁹

Third, maritime cybersecurity regulations need to greatly improve. In aviation the two powerful regional regulators, EASA in the EU and FAA in the US are, de facto, the global regulators of aviation. Both have established IoT and cybersecurity standards for aircraft and for Air Traffic Management which supersede those of ICAO, the global - and much weaker - aviation regulator.²⁰ In the maritime environment the European Maritime Safety Agency and the United States Maritime Administration do not yet have the global impact for the maritime that

10 As April Danos of Port Fourchon Louisiana (US National Maritime Security Advisory Committee, and a leading authority on maritime cybersecurity), states: "We are blind, useless and potentially locked out of our own house if we [the maritime community] are hacked. And let's face it, it isn't 'if' it's 'when'." April Danos, Security Industry Association, March 16, 2016 'Keeping Cargo Moving: Maritime Cybersecurity' with Brett Rouzer, US Coast Guard Cyber Command. For further information on port security see: Danos 'Innovative Approaches using Information Technology' (2013), at: aapa.files.cms-plus.com/SeminarPresentations/2013AnnualConvention/Danos%2C%20April.pdf

11 For full report see: Dept of the Navy, Office of the Chief of Naval Operations, Memorandum for Distribution. 'Enclosure (1) Report on the Collision between USS FITZGERALD (DDG 62) and Motor Vessel ACX CRYSTAL'; 'Enclosure (2) Report on the Collision between USS JOHN S MCCAIN (DDG 56) and Motor Vessel ALNIC MC', October 2017.

12 Dept of the Navy, Office of the Chief of Naval Operations, Memorandum for Distribution, op.cit.

13 Stars and Stripes 'Admiral: "No evidence of hacking in McCain, Fitzgerald collisions"'. August 30, 2017. See: <https://www.stripes.com/news/admiral-no-evidence-of-hacking-in-mccain-fitzgerald-collisions-1.485229>

14 Zachary Staples, Maura Sullivan, op.cit

15 Cybersecurity Seminar at IT infrastructure company 'UKFast', Manchester, UK, July 18, 2019. Name of speaker, an 'ethical white-hat' hacker, was not revealed.

16 D.A. Kerigan-Kyrou "Applying the NATO / PfPC Cybersecurity Generic Reference Curriculum in an Increasingly Interconnected Landscape," Vox Collegii, Journal of the NATO Defence College Vol. XVII (July 2018), 4-9.

17 See: D.A. Kerigan-Kyrou, "The Internet of Things: Transforming Our Approach to Defence", An Cosantóir - Defence Forces Ireland (April 2019), 25.

18 Email to Kerigan-Kyrou from Dr. Stefan Lüders, CERN, August 31, 2017.

19 See: D.A. Kerigan-Kyrou, "Protecting Cyberspace - A Hybrid Threat Requires a Hybrid Response", An Cosantóir - Defence Forces Ireland (May 2019), 18-20.

20 In the current debate concerning re-introduction of the Boeing 737 MAX after fatal accidents it is the FAA, EASA and to a lesser extent the Australian Civil Aviation Safety Authority which are in the lead. ICAO is largely irrelevant.

EASA / FAA have for aviation. Thus, the regulation concerning maritime cybersecurity has largely been left to the global UN regulator, the IMO.

The problem with the IMO is that, like ICAO, as a global state-based organisation most rules and procedures must be decided by unanimity. This process of rule-making leads to a weakening and a delay in making regulations. It is likely to be because of this that the new IMO cybersecurity recommendations: IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3), are non-binding.²¹ The IMO states the Guidelines “encourage administrations to ensure that cyber risks are appropriately addressed in existing safety management systems... no later than the first annual verification of the company’s Document of Compliance after 1 January 2021.”²² However, January 1, 2021 is not a deadline in any meaningful sense, unless regional administrations make its recommendations mandatory.

That said, the Guidelines are a good starting point and the authors believe this to be a sound and effective document because it emphasises culture, leadership and an organisational ap-

proach to cybersecurity. For example, Section 3,3 states:

“3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.”²³

This is an excellent approach by the IMO and the authors hope that regional authorities are not only ‘encouraged’ to implement the Guidelines but insist and enforce these cyber security requirements.

Summary

From super yachts in Monaco to cargo vessels in the Pacific, the targeting of civilian vessels directly affects NATO and Allied militaries and indeed global security. Such a situation of targeting the ‘weakest link’ could result in future incidents involving NATO and NATO partner nations’ vessels.

The threat to all vessels, both military and civilian, will grow exponentially

over the coming years. The number of interconnected devices aboard and within the whole maritime environment, whether at sea or ashore, will expand to unimagined levels.

The IMO’s approach to cyber security has been very late indeed. However, its guidelines are welcome as they emphasise a managerial and organisational approach to maritime cybersecurity. While there are huge challenges enforcing such rules in a global organisation such as the IMO, it is crucially important that the new Guidelines become obligatory for the global maritime community.

The IMO Guidelines on maritime cyber risk management are a good start - but they are only the very beginning of this necessary cyber-enhancement process. As former US Secretary of State Madeleine Albright stated in her report ‘NATO 2020’, there is a blurring of the ‘military’ and ‘non-military’ challenges. This is particularly clear in the maritime cyber security environment. And because of this a NATO Maritime cyber risk mitigation effort needs to emerge and energise soon.²⁴ The threat is already here.



Chris Parker MBE is co-founder (2015) of www.Cyberplus.co.uk and an expert on cyber risk mitigation, enhancement processes and management systems. A former British military officer, he was a NATO Brigade Joint Operations Chief of Staff in Kosovo 2001 and since 2007 been a US\$ 1B construction mega-project director, oil and gas exploration COO and cyber security business leader. A regular speaker and conference chairman, Chris has a master’s degree in Technology and is a Chartered Manager.



Dinos A. Kerigan-Kyrou is an instructor on the NATO DEEP (Defence Education Enhancement Programme), based at the Partnership for Peace Consortium. He is responsible for the cyber security training on the Joint Command & Staff Course of the Defence Forces Ireland. Dinos is a co-author of the NATO / PfPC Cybersecurity curriculum.

21 IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3). July 5, 2017. Available at: <http://www.imo.org/en/OurWork/Facilitation/docs/FAL%20related%20nonmandatory%20instruments/MS-C-FAL.1-Circ.3.pdf>

22 IMO: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx

23 Section 3.3, page 3, IMO Guidelines on Maritime Cyber Risk Management, op.cit.

24 STANAG 2525: ‘Allied Joint Doctrine for Communications and Information Systems’ provides a NATO standard but the authors argue this needs to be built upon to emphasise the ‘military’ and ‘non-military’ environment. This blurring, or merging, was identified by Secretary of State Albright in ‘NATO 2020: Assured Security; Dynamic Engagement’, 24. See <https://www.nato.int/strategic-concept/strategic-concept-report.html>



MAKING MARITIME STRATEGY WORK: A NEW TAXONOMY

by Dr. Ian Ralby¹

Around the world, navies, coast guards and marine police forces have, in recent years, developed and adopted “maritime security strategies,” but many of those strategies fail to progress beyond words on a page. Finding the will and the resources required to implement them is often elusive, and so even well-drafted strategies accomplish little more than collecting dust on a shelf. While many institutions and entities reference “maritime strategy,” they are actually using one term to describe many different things. So identifying what it is, how it was produced and how it will be used is vital to being able to gauge the degree to which it might succeed. Based on growing practice, a strategy drafted by an inclusive process that integrates

maritime security, governance and economic activity, and whose implementation begins with communicating the vision and rationale of the strategy, is most likely to be backed by the will and resources to effect meaningful change in the maritime domain. When a strategy makes the case for investment into maritime security by showing likely return on investment through a safe, secure, stable and prosperous blue economy, the state is more likely to pursue its thorough implementation. Consideration, therefore, must be given not just to producing a maritime strategy, but to what is needed for the vision expressed by it to be realized. Around the world, navies, coast guards and marine police forces have, in recent years, developed and adopt-

ed “maritime security strategies,” but many of those strategies fail to progress beyond words on a page. Finding the will and the resources required to implement them is often elusive, and so even well-drafted strategies accomplish little more than collecting dust on a shelf. While many institutions and entities reference “maritime strategy,” they are actually using one term to describe many different things. So identifying what it is, how it was produced and how it will be used is vital to being able to gauge the degree to which it might succeed. Based on growing practice, a strategy drafted by an inclusive process that integrates maritime security, governance and economic activity, and whose implementation begins with communicating

¹ Dr. Ian Ralby is CEO of I.R. Consilium, LLC and a Maritime Crime Expert for the UN Office on Drugs and Crime. He has worked with states and regional bodies around the world – directly, through the US Government, or through international organizations – particularly in Africa and the Caribbean, on developing maritime strategy. This analysis is based on his experience in working with different states and studying the general trends in maritime strategy development around the world

the vision and rationale of the strategy, is most likely to be backed by the will and resources to effect meaningful change in the maritime domain. When a strategy makes the case for investment into maritime security by showing likely return on investment through a safe, secure, stable and prosperous blue economy, the state is more likely to pursue its thorough implementation. Consideration, therefore, must be given not just to producing a maritime strategy, but to what is needed for the vision expressed by it to be realized.

The Strategic Case for Maritime Security

Fundamentally, a strategy provides the answer to the question: why? Why is a certain action being taken? Why is a certain asset being procured? Why is a certain organizational structure being pursued? In implementing a strategy, the words “in order to” should govern every decision being made. In other words, the answer to “why” should be “in order to” effectuate the strategy as adopted. In the maritime context, however, a fundamental question is often overlooked: why secure the maritime domain?

As Professor Bueger’s analysis reflects, there is little consensus as to the precise meaning of the term “maritime security.” Regardless of its specific definition, however, politicians and policy makers can easily deem “maritime security” to be a waste of time, energy and money. Though it is widely recognized that 70% of the earth is covered in water and 90% of world trade happens by sea, voters, constituents and citizens – that is to say, people – do not live on the water, and so the maritime domain is rarely of central political interest. Furthermore, it is also increasingly evident that there is likely to be an endless array of threats that hinder security in the maritime space, meaning that trying to stop them could be an unending drain on the economy. Why, then, invest national treasure and precious

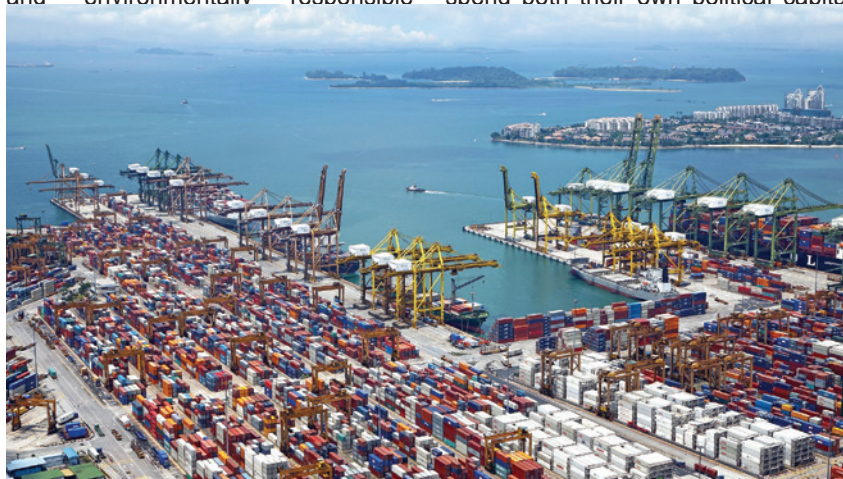


political will into an uninhabited area plagued by never-ending challenges? The demise of most maritime security strategies is a failure to convincingly answer this question.

Thanks to the resurgence of piracy over the last fifteen years, it is now recognized that at least some effort is needed to ensure that maritime commerce continues to flow. As the adage goes, “no shipping, no shopping,” and even landlocked states recognize that without maritime commerce, most goods would not be readily available in stores, and the modern way of life would be noticeably altered. Beyond that minimal recognition, however, most states suffer from some degree of maritime wealth blindness, partially or even completely unaware of the economic benefit to the state that a secure, well-governed and well-regulated maritime space could provide. The fact that wealth blindness is starting to be addressed as the “blue economy” – the inclusive, sustainable and environmentally responsible

exploitation of the maritime domain – captures the imagination of politicians and policymakers. But the link with maritime security remains woefully lacking.

Given the rise in popularity of the blue economy, but the lack of a corresponding rise in investment into maritime security, a redefinition of maritime security is a necessary starting point for developing an effective maritime strategy. “Maritime security” cannot just be about protecting the state against the unending array of maritime threats. That is an expensive proposition that will drain the state’s economy and focus attention on a part of the state where no one lives. Instead, maritime security must be seen as protecting the maritime space for the enrichment of the state and the betterment of life on land. It must be understood as the process of creating a safe and secure maritime domain to allow the blue economy to flourish. Only then will politicians be willing to spend both their own political capital





and the state’s economic resources on maritime security. Understanding this reality is a prerequisite for identifying a strategic approach that will succeed.

Maritime Strategy Taxonomy

Recognizing the political and economic context of maritime security helps shine a light on the key difference among three distinct types of maritime strategy, all of which include maritime security as a central focus. In general terms, a maritime security strategy sets forth a vision for how to secure the maritime domain. What that means to states, however, varies greatly, and as a result there has been widespread imprecision regarding the term “maritime security strategy.” Excluding “naval” or “sea power” strategies that focus on maritime defense and require a blue water navy, the three types of maritime security strategies are as follows:

1. National Maritime Security Strategy (NMSS)
2. State Action at Sea Strategy (SASS)
3. Integrated Maritime Strategy (IMS)

In an NMSS, there is one pillar: security. As a result, the only agency or agencies that need to be involved are those whose express focus is maritime security. This usually translates into the navy, coast guard, and/or marine police force being the entities that draft

and expect to implement it. While some such strategies help to guide the approach of the maritime law enforcement agencies, they often fall short when it comes to resourcing the actions needed to properly implement the strategy. The world’s coastline is littered with unimplemented NMSSs.

A SASS is different than an NMSS as it is inherently focused on two distinct pillars: security and governance. While security may be the principal goal of a SASS, the strategic approach to achieving that goal is, by definition, multi-agency, requiring the collaboration, cooperation and coordination of all the maritime-related ministries, agencies and departments. Tying security to governance tends to make more sense to political leaders who recognize the need to govern the full extent of the state’s territory, but it still does not translate into the mobilization of economic resources to support maritime security.

An IMS, by contrast, contains three pillars: security, governance and the maritime economy. Not just whole-of-government, but whole-of-society, this type of strategy bridges the public-private divide to pursue the full economic potential of the country’s coastline and maritime territory. It is here that the case can be made to the political classes that they must invest in maritime security. By providing that security, the state can ensure good and effective governance in the maritime

domain. That, in turn, creates the space for the maritime economy (and within it the blue economy) to flourish, yielding numerous benefits to the state including substantial employment, trade and economic activity, coastal tourism, and both food security and food sovereignty. This type of strategy embodies the definition of maritime security that casts it as a net gain to the state, rather than a drain on its coffers.

Somewhat complicating matters, however, is the increasing need to “nest” strategies. In other words, the strategies must align in such a way that all the different strategies of the state fit together. A single pillar NMSS, therefore, could become nested into a SASS or an IMS with some modifications to tie the security, governance and, in the case of the IMS, economic pillars together. At the same time, the security pillar of any of the three types of strategy could be nested into a National Security Strategy, where the maritime aspects are integrated with land, air, cyber and any other pillars that the state chooses to address in that purely security focused strategy. And, as the trend of developing blue economy strategies continues to grow, such strategies must be nested into the wider maritime economic portions of an IMS.

At the end of the day, the interconnectedness of maritime security, maritime governance and the maritime economy cannot be ignored. No pillar exists in practice without the others, so developing a vision for the maritime domain that integrates the three pillars is the most efficient and effective way to approach maritime strategy development.

The Strategy Development Process

While the type of strategy that is developed matters, so too does the process by which it is conceived, drafted and adopted. While the



previous section talked about single agency and multi-agency or multi-stakeholder strategies, a major problem around the world is the “no-agency strategy.” Recognizing the potential benefit of a strategy and identifying the lack of one in a given state, a variety of international organizations, donor states, foundations, and other well-meaning organizations have “helped” such states by developing strategies for them. The problem here is that, no matter how “good” the resulting document is, it is not owned by anyone in that state, and thus has no custodian with a vested interest in seeing it implemented. And that nullifies any potential. Failure to develop the buy-in of the key stakeholders in the drafting process often leads to failure of the strategy. Even in a single agency strategy, there are multiple stakeholders, and at least some engagement is usually necessary to pave a path to successful implementation. In the case of an IMS, there can be dozens of stakeholders, including both an array of private sector actors and the general public, and widespread consultation is often correlated to successful implementation.

An initial step in developing a strategy, therefore, is to identify who should be

involved in the process and what degree of involvement they should have. There is no uniform list of the “correct” stakeholders or the “right” process, but all too often, maritime strategies leave out key maritime stakeholders. If done well, however, the process of developing the strategy will either create or strengthen relationships between those stakeholders in order that they can work together. In that respect, there are at least four types of collective action:

1. Collaboration – working with unity of effort and unity of purpose
2. Cooperation – working with unity of purpose
3. Coordination – working to align efforts, actions and purposes
4. Deconfliction – working to ensure efforts, actions and purposes do not interfere

Recognizing the differences among these types of collective action can help identify who needs to be in the strategy development process and translate the relationships that are formed or strengthened through it into permanent mechanisms able to be used to implement the strategy.

In general, there are six layers of collective action needed to secure,

govern and develop the maritime space:

1. Intra-agency (within ministries, agencies and departments)
2. Inter-agency/Whole-of-Government (between ministries, agencies and departments)
3. Bilateral/Regional (between two or more states within a region)
4. Inter-Regional (between two or more regional entities)
5. International (between two or more states of different regions)
6. Public-Private/Whole-of-Society (between the government, private sector, civil society and the general public)

If these six cooperative layers are not all addressed in a) the process to develop the strategy, b) the strategy itself, and c) the implementation plan, the strategy’s likelihood of complete implementation is limited.

The Strategy Implementation Process

Even if a maritime strategy makes a strong case for investment into maritime security, and even if all the stakeholders are integrated into the process in a highly inclusive and consultative manner, the strategy

may still fail to be successfully implemented. Taking a strategy from paper to practice requires five key elements:

1. Capacity
2. Capability
3. Authority & Jurisdiction
4. A Legal Framework
5. Will

In blunt terms, capacity is having a boat, capability is knowing how to use it, authority and jurisdiction provide the legal basis – both enabling and constraining – for interdiction operations, the legal framework provides both the laws to enforce and the process by which to achieve legal finish, and will is required to fund, operate and maintain all aspects within the law enforcement ecosystem. When it comes to maritime strategy implementation, the state must have the tools – vessels, radar, marine patrol aircraft, etc. – to achieve the stated strategic ends; must be able to actually take on the tasks required

to realize them (seamanship, legal expertise, procurement ability etc.); must have the legal authority and jurisdiction in place to secure, govern and develop the maritime space; and must back all these aspects with adequate political will.

Given, therefore, the overarching importance of political will, it really must be considered as the starting and ending point for how to successfully develop, adopt and implement a maritime strategy. Political will is why the three-pillar IMS is so important for making the convincing case to invest political and economic capital into maritime security. Political will is why an inclusive process is so important for making sure that no constituency can convince the political class not to endorse the strategy on account of their exclusion. And political will is the make-or-break for ensuring that the state exercise its capacity, capability, authority and jurisdiction in the implementation process.

Conclusion

Maritime strategies are in vogue these days as a preliminary, low-cost and tangible step for states to signal their intent to improve maritime security. They are, however, a dead end unless they produce the political will not only to adopt but to resource them to complete implementation. This requires tying maritime security to maritime governance and, most importantly, to the maritime economy. Political will is already growing behind pursuing the blue economy, so it is imperative that security operators use maritime strategies as a way to make the case that maritime security is inextricably linked. Only with a safe, secure, and stable maritime domain can a prosperous blue economy thrive. And only with a compelling case for investing in maritime security will the numerous maritime strategies around the world make the transition from adoption to implementation.



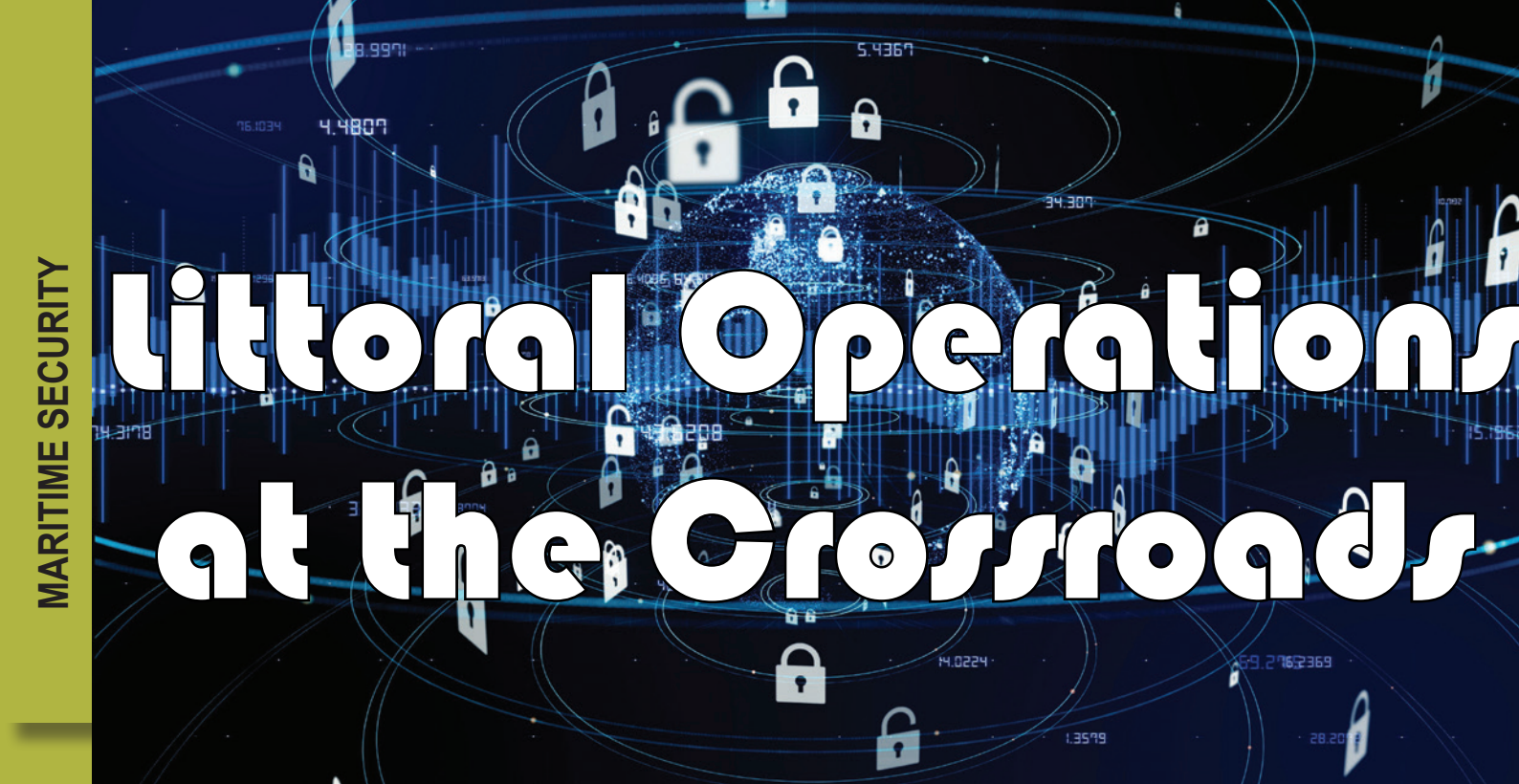
Dr. Ian Ralby is a recognized authority on issues at the intersection between law and security with particular expertise in maritime law and security, energy security and the regulation and oversight of private security companies. Dr. Ralby is a Maritime Crime Expert at the United Nations Office on Drugs and Crime's Global Maritime Crime Programme, an expert advisor to the United Nations and NATO on security matters, a Nonresident Senior Fellow at the Atlantic Council, and CEO of his own consultancy, I.R. Consilium. From 2015-2019, he was also Adjunct Professor of Maritime Law and Security at the U.S. Department of Defense's Africa Center for Strategic Studies

Dr. Ralby's work primarily concentrates on maritime law, security and strategy with an emphasis on the interdiction of transnational crime, and the development and governance of the maritime domain, including the blue economy. In addition, he is lead author on the most extensive study ever published on downstream oil theft and illicit hydrocarbons activity

and was heavily involved in the development of various international instruments and mechanisms aimed at regulating the private security industry.

His practice centers on advising and assisting governments, international organizations and multinational companies with security and legal matters. He has worked with clients around the globe on complex problem-solving including: extensive work on maritime domain issues in Africa, the Caribbean, Europe, the Indian Ocean, the Pacific Islands and South East Asia; addressing energy crimes around the globe; forming cooperative security regimes at the regional and sub-regional levels; horizon scanning for future security concerns; devising approaches to confronting specific crimes including illegal fishing, piracy, armed robbery at sea, environmental dumping, and the smuggling or trafficking of drugs, weapons, humans, resources, contraband, counterfeit goods, antiquities and cultural property. Dr. Ralby has also spent time embedded both as an international law advisor to a government in the Balkans and as a maritime security advisor in the Caribbean, and provided support to the Iraqi Judges on the trials of Saddam Hussein and his top lieutenants. He remains an active advisor to several allied Western Governments on matters relating to both private security and maritime affairs, and has assisted a number states with developing national maritime strategies.

He earned a B.A. in Modern Languages and Linguistics and an M.A. in Intercultural Communication at the University of Maryland, Baltimore County; a J.D. at the College of William and Mary; and both an M.Phil. in International Relations and a Ph.D. in Politics and International Studies at St. John's College of the University of Cambridge.



Littoral Operations at the Crossroads

by Edward Lundquist

The OpTech – EASTMED workshop brought together 52 defense leaders, operators, scientists, analysts, and think tank experts from 12 different NATO and partner nations to explore the unique operational and technological challenges to security and defense in the complex littorals of Eastern Mediterranean region, with an eye to great power competitions.

The OpTech workshops foster close collaboration with allies and partners across governments, academia and industry, and expand operational perspectives and the awareness of advanced technology solutions. The most recent, OpTech - EASTMED benefits from the intellectual leadership of the LOC and the Center for Network Innovation and Experimentation at the U.S. Naval Postgraduate School and is supported by the U.S. Navy Office of Naval Research, Senior National Representative and Saab and hosted by the NATO Maritime Interdiction Operational Training Center, Souda Bay Crete.

The Littoral Operations Center at the U.S. Naval Postgraduate School has provided the Intellectual leadership and has been a convening authority for related events in Monterey and for the Littoral OpTech global series of workshops of which there have been five to date -- Stockholm, Tokyo, Cartagena, Halifax and Crete. Each one of the workshops has focused on the operational and technology challenges facing regional littoral states. The global series of workshops has gathered over two dozen allies and partners, over 400 leaders and experts across all military domains.

Few areas on earth host more transnational activity than the Eastern Mediterranean littorals. The dynamic flow of diplomatic, military, information and economic power expands along a congested and contested crossroads with impact across the Eurasian continent. "The complex interconnectivity that surges within this area is made secure only through cooperation," said retired Swedish Navy Captain Bo Wallander,

senior naval advisor for the Swedish defense company, Saab; a principal investigator for the LOC, and the moderator for the workshop. "Together, we gained geostrategic perspective and explore solutions to those operational and technological challenges."

Saab USA has the supported collaborative research efforts at the LOC that include the very unique perspective of Sweden a country with a long and complex littoral - some would say an extreme littoral geography.

The workshop, as with the previous OPTECH events, examined the growing importance of viewing the littoral zone seaward and landward of the shoreline in a comprehensive manor, and as an all-domain battle space that should be recognized for the unique and inseparable combat challenges it poses. Recent high-level documents and concepts speak directly to this, including the Navy's Design for Maintaining Maritime Superiority 2.0, issued in December 2018; the Distributed Maritime Operations concept;

the joint Navy-Marine Corps Littoral Operations in a Contested Environment, released in 2017; Expeditionary Advanced Base Operations concept; and the 2019 Commandant's Planning Guidance are focusing minds and actions.

"In this littoral context, and with my research at NPS and through the Op-Tech Workshop series, I have come to realize the growing importance of cyber and space and within these domains the function of networks," said Steve Benson, Saab's program manager in Monterey and cofounder of the LOC. "Networks must be adaptive, resilient, self-healing, and hidden/deceptive if needed. They must protect and enable naval platforms subject to higher risk in the littorals. They are the future armor."

Participants looked at the geo-political region through the lens of the different warfighting domains and the technologies that enable warfighting success. According to Al Elkins, warfighting and technology strategy lead for the F-35 office of the chief strategy officer, a key finding of the workshop was that allies and partners must begin planning now. "NATO and the EU must begin planning today for the uncertain, volatile future and for the level of effort that will be required should there be near peer competition, conflict or significant proxy war. As with most other regions, we are dealing with both super-powers and a world of "small, many, smart, lethal" adversaries. We have to think strategy first."

The Mediterranean has become a key human smuggling conduit, which has had a destabilizing effect on the NATO and EU nations in Europe. There has been an astonishing number of illegal drugs or trade coming from China. And participants have noted that Russia has realized that creating a crisis that sparks the movement of refugees can preoccupy and distract the European nations from countering its other activities in the region.

Elkins said the event was worthwhile, characterizing his fellow participants as "motivated, smart, thoughtful,

principled and experienced," and the networking value of the workshop as "topnotch."

"The excellent briefings on the recent activities and capabilities of Russia and China set the stage for a lively discussion" said Guy Thomas, chief executive officer of Baltimore, Md.-based C-SIGMA LLC. "The ensuing discussion over the following two and a half days was most enlightening and vision expanding. The panels took on such subjects as disruptive technologies, policies and operational concepts in all domains--subsurface, surface, air, land, cyber and space; as well as the growing role of both China and Russia in the area, as well as possible counters."

According to Thomas, "Each of the participants, all experts in their various fields, shared the view that enhanced maritime security and situational awareness was a highly desired goal, and all brought unique expertise, experiences and views to the discussion."

Strategy analyst Lt. Cmdr. Peter Thomsson of Swedish Defence University said the workshop was an opportunity to meet and work with professionals from academia, government and business to discuss regional issues with global impact and global issues with regional impact. He said the event gave him a better appreciation of the Eastern Mediterranean truly as a "global crossroads, where economic, political and security interests overlap and interact."

Thomsson described his fellow participants as "a very knowledgeable group with high expertise on a range of subjects and great willingness to share."

The NMIOTC hosts were welcoming, and the delegates enjoyed Chania, which Thomsson described as "a pearl on the Mediterranean dating back to antiquity."

Ret. Rear Adm. Vic See, former US Navy PEO Space Systems, found the discussions on Cyber and protection of advanced systems and networks extremely important. "In thinking of the China Silk Road from Northern Europe

to the Red Sea discussions, and then the known operations of the shipyards, the weak cyber protections strike me as a high-risk area should a bad actor want to shut things down and make a economic problem for many. We had some very good discussions about some of this and what is being done, and not being done."

Swedish Navy Cmdr. Rolf Hultman is the military advisor for the Permanent Representation of Sweden to the EU in Brussels found the workshop to be a productive and "refreshing experience."

"There were interesting panels and stimulating conversations in what I found to be a very openminded and honest discussion climate, especially the panel and follow-up discussions regarding China and its strategic courses and strategic goals in the region," said Hultman. "For me, both personally as well as professionally, it was very valuable to meet and interact with so many distinguished delegates." Jerry Hendrix, a retired captain and now vice president of the Telemus Group, said the world is seeing a confluence of commercial investments and broader strategic interests. "China is making massive investments in ports and infrastructure, but nations who enter these partnerships fail to see how one-sided they are and how they are being militarized."

Russia understands they hit a population center in Syria, for example, and raise pressure on Europe and fragmenting the alliance.

The region is becoming a confluence of potential superpower competition. Russia is allied with the Syrian government of Bashar al Assad, while China has essentially taken control of Greece's major port of Piraeus.

Russia is not a major economic power, but has super-power ambitions, and is "playing a bad hand better than anyone else." It has replaced the United States as the power-broker in part of the region.

China has a much stronger economy and unmatched industrial capacity. In the event of a major war, China would

rapidly build tanks, airplanes and ships in much the way the U.S. did in World War II against Germany and Japan.

And, it was noted, the U.S. and western Europe no longer has that same level of industrial capacity. "In the event of a world war today, the large western countries won't be able to re-arm," Hendrix said.

As Chairman of the European Working Group on Non-Lethal Weapons, an inter-governmental organization, Italian Navy Ret. Rear Adm. Massimo Annati is constantly trying to achieve more knowledge about the scenarios where non-lethal weapons, or "intermediate force capabilities," can play a role, in order to better understand challenges and opportunities.

"I decided to attend the Littoral OpTech East Med because I believed it would focus on the grey area characterizing current hybrid warfare scenarios, and I was right," Annati said. "In addition to the different presentations and talks, I believe the seminar wargame was very useful: in these instances, people tend to become more involved, and that brings more ingenuity and fresh ideas to the table. The networking is priceless, you mix-up with people of different experience and nationality, confronting ideas and added-value free-flow talks."

Greg Melcher, chief operating officer for the Centre for the Study of New Generation Warfare in Washington, D.C., characterized the group as "An excellent mix of current and former

operators, technologist, acquisition specialist and policy leaders. The break-out group participation was extremely good and everyone provided excellent inputs and creative ideas. The questions throughout showed a very deep understanding of the issues and challenges in the region. There were many opportunities to develop new partnerships."

Melcher led the group through a simulated scenario, which engaged the participants in sharing their own areas of expertise. The wargaming simulation was conducted in parallel as part of the OpTech. The working group sessions to capture workshop conclusions and recommendations through the lens of the wargaming scenario/vignettes.

"The objective was for each of the working groups; policy, technology, and operations to use the knowledge gained over the last 2 days to "de-escalate" the potential conflict that would be the likely next step of the scenarios briefed over the two days of the workshop," Melcher said. "Each group was asked to provide their observations, identification of gaps, challenges, findings, recommendations and action items."

The out-briefs addressed all of these areas and would serve as a good starting point for the development of a document that would identify requirements and gaps for the Eastern Med. "The simulation provided a mechanism by which practical stra-

tegic political-military requirements were imposed upon operational and technical discussions," Melcher said. "As much as some of the participants insisted on interpreting the threat in traditional terms, the full-spectrum nature of Russian New Generational Warfare represented in the simulation provoked an overwhelming majority to contemplate defensive requirements throughout the depth of Allied Defenses. The idea of political subversion through the mechanism of so-called 'reflexive control' was understood by many to be playing a prominent role in the weakening of the European Union and NATO. Further the non-kinetic elements were brought forth as primary driver in each vignette, challenging the workshop participants to understand, at a certain level, that conflict was already underway, even if no shooting had begun."

"Having everyone active and fully involved to reach your outcomes was really interesting and productive," said Commodore Stelios Kostalas of the Hellenic Navy, the commandant at NMIOTC in his closing remarks. "This Workshop was another major stepping stone for our NATO centre to engage with the international community to create opportunities for a better understanding and to support security at sea."



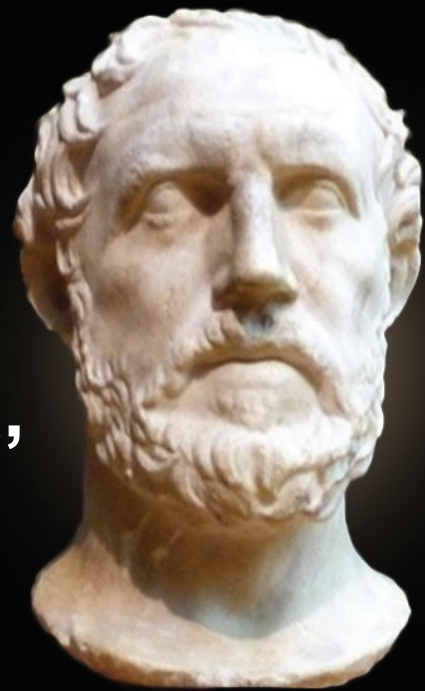
Capt. Edward H. Lundquist, U.S. Navy (Ret.) is a senior-level communications professional with more than 28 years of public affairs, public relations, and corporate communications experience in military, private association, and corporate service. During his 24-year naval career, Lundquist qualified as a Surface Warfare Officer and later served as a Public Affairs Officer. He retired from active duty in 2000.

He is a principal science writer for MCR Federal, LLC. Lundquist is a member of the executive committee for the Surface Navy Association and serves as vice president of the Greater Washington Chapter. He writes frequently for publications including *Armed Forces Journal*, *Surface Warfare*, *Unmanned Systems*, *Naval Forces*, *Warships International*, *Maritime Reporter*, and others.

Sea Control

“He who controls the sea, controls everything”

— *Thucydides*



by Todd Bonnar

Near peer competitors such as China and Russia, as well as regional influencers such as Iran, are increasingly deploying all elements of their national power to achieve their global ambitions. In many cases, they are gaining a competitive advantage and exploiting our vulnerabilities in order to redefine the norms of the entire international system on terms more favorable to themselves. While rarely rising to the level of conflict, Iranian, Chinese and Russian actions are frequently confrontational as witnessed numerous times in the Straits of Hormuz, as well as in the Black and South China Seas.

It is indisputable that the world's economy floats on seawater. It is equally indisputable that international maritime transportation is the tool that keeps the global economy moving. The world economy has surged over the last half century, and that growth has been largely driven by globalization and the consequent reduction in barriers to trade. Any operational disruptions in maritime transportation have wider consequences for society, making the development and implementation of

an updated maritime strategy and the management of the trans-Atlantic sea lines of communication a strategic, combined and joint priority for our Alliance.

As Rear Admiral JC Wylie, USN explains in his original exposition of cumulative and sequential strategies of the early 1950s, maritime strategy is “one in which the world's maritime communications systems are exploited as the main avenues by way of which strength may be applied to establish control over one's enemies”. What the Admiral was referring to is the basic tenet of establishing sea control as the foundation of a maritime strategy. Sea control does not mean command of all the seas, all the time, certainly not in times of peace. Rather, it is the capability and capacity to impose localized control of the sea when and where it is required to enable other military objectives and to hold it as long as necessary to accomplish those objectives.

On a daily basis, surface naval forces of the Alliance's nations and partners

are conducting peaceful operations across the globe. Joint forces at sea protect freedom of maneuver, secure the sea-lanes for global trade and economic growth, defend and promote key national interests and prevent competitors and adversaries from leveraging the world's oceans against us. Naval forces fulfill these crucial roles, which are the necessary preconditions to ensure the free movement of trade and commerce and to safeguard the interests of NATO and partner nations all the while maintaining a strictly defensive posture. The persistent forward presence of the Alliance's naval forces backed by credible combat capability deters potential aggression and seeks to limit regional frictions from escalating to conflict.

Should this defensive deterrence fail the potential adversaries NATO forces may be expected to deter or defeat in the future will possess weapons and targeting capabilities designed to effectively delay and reduce the ability of NATO's maritime forces to launch operations. In this “fight tomorrow”, it is possible that future amphibious op-

erations become more likely to be conducted to support sea control in littoral areas by degrading or destroying Anti Air Area Denial (A2D2) weapons and sensors. Modern A2AD systems are optimized to engage ships and aircraft, at faster speeds and longer ranges than ever seen in the past. Due to the threat to amphibious ships from anti-ship cruise missiles, torpedoes, and mines, shaping and launching operations will need to be conducted from farther away than those today thus requiring a greater degree and span of sea control in both blue water and the littorals.

A2D2 strategy with its technological advances, improved long range targeting and standoff weaponry are driving changes on how we are approaching the conduct of amphibious operations. The long-standing notion that that amphibious forces could launch and fight their way ashore from amphibious ships parked dozens of miles offshore has now been challenged and in many parts of the world, a review of the old way of thinking is well overdue. Groups like the Russia, China and even Iranian-backed Houthis in Yemen have varying levels of stand-off capabilities that could inflict “mission kill” damage to an amphibious striking group. In fact, almost immediately upon assuming command, the new US Marine Corps Commandant, Gen. David H. Berger, issued a new set of orders to his commanders, calling for a complete re-work of the core amphibious mission of the USMC.

“The ability to project and maneuver from strategic distances will likely be detected and contested from the point of embarkation during a major contingency,” “It would be illogical to continue to concentrate our forces on a few large ships. The adversary will quickly recognize that striking while concentrated (aboard ship) is the preferred option. We need to change this calculus with a new fleet design of smaller, more lethal, and more risk-worthy platforms.” Naval strategists thus are

seeing an ever-increasing level of confluence between the “brown and blue water” thus increasing the complexity and span of control for tactical and operational level commanders. This, in part, is driving iterative changes within the Alliance’s Maritime Strategy.

In the maritime domain the success to this maritime strategy requires an understanding of persistent relationships, time, space, risk, oceanography, the global supply chain, critical infrastructure and the environment, as well as the nature of the risk, and the capabilities, readiness and location of one’s competitors. Designed to secure the linkage between North America and Western Europe, the establishment of JFC Norfolk coupled with the reinstatement of the US Navy’s Second Fleet provides NATO and the USN with a significant foundational piece in this maritime strategy and a critical manoeuvre arm capable of exercising sea control in times of potential conflict.

Naval forces outfitted with robust defensive systems and armed with credible standoff weaponry, survivable in both contested and communications degraded environments, help to secure sea territory and in the event of conflict, would enable forces to flow for follow-on power projection operations. NATO’s ability to launch, conduct and sustain combined and joint operations within NATO’s area of interests, far from the shores of the Alliance’s individual nations provides a distinct deterrence message to potential adversaries.

Joint Force Command Norfolk will contribute to NATO’s leadership in support of a sea control based maritime strategy. JFC Norfolk will capitalize on its dual hatted US Second Fleet Commander and staff to maintain situational awareness in the Atlantic, participate in ongoing planning efforts, coordinate with Allied and coalition forces and establish persistent relationships across multiple lines of effort.

In times of crisis or conflict, JFC Norfolk will be directing assigned forces to enable power projection, defence of the SLOCs and ensuring the trans-Atlantic reinforcement necessary to the defence of Europe including amphibious operations.

It has been decades since international relations in the world order dictated competition for sea control, sea lines of communication, access to world markets, and diplomatic partnerships. Nations such as China, Iran and Russia seek to accumulate/consolidate power and re-define international norms, potentially at the peril of diplomatic, economic, and military bonds that link NATO allies and partners. We are seeing other nations such as Japan developing newly formed amphibious brigades and validating TTPs with U.S. and Australian forces during a recent large-scale exercise in Australia as they seek to address China’s sea control strategy in the South and East China seas. The future success of NATO and its member nations depends in part on the Alliances’ maritime forces and their ability to similarly rise to this challenge and ensure that our force composition and C2 are aligned properly in order to positively influence the pressures that continue to shape our modern security environment.

Potential adversaries will continue to improve their ability to contest the sea and air around their territory, increasing the range at which sea control and follow on amphibious operations must occur and making NATO’s ships and amphibious forces more vulnerable. The increasing use of the maritime domain—the oceans, seas, waterways, and seafloor; the rise of global information systems, especially the role of data in decision making; and the increasing rate of technological creation and adoption of automation are fundamental areas of study required in support of the Alliance’s refinements to its maritime strategy



Biography

Combined Joint Operations from the Sea Centre of Excellence

Captain Todd Bonnar, Royal Canadian Navy Warfare Analysis Branch Head

Captain Todd Bonnar, MSC, CD joined the Canadian Armed Forces as a Direct Entry Officer in 1997. After completing Maritime Surface Officer classification training in HMCS VANCOUVER in 1998, he was selected to represent Canada in an exchange with the Royal Australian Navy in HMAS HOBART and HMAS ANZAC during which time he participated in the UN Peace Keeping Mission to East Timor.

He returned to Canada's West Coast fleet in 2000 and subsequently served as the CANFLTPAC Flagship's Above Water Warfare Officer in HMCS ALGONQUIN. During this time he deployed to the Persian Gulf in support of OP APOLLO, Canada's response to the September 11th attacks earning a Task Force Commander's commendation for his Intelligence work. Captain Bonnar completed his Operations Room Officer course in 2004, returning to HMCS ALGONQUIN where he served as both the Flagship's Weapons Officer and Combat Officer. During this tour he also completed his Area Air Warfare Commanders qualification.

He was promoted to the rank of Commander on 6th of June 2010 at Juno Beach on the shores of Normandy, France and assumed the position of Executive Officer, HMCS PROTECTEUR in July 2010. In January 2012, he "Fleet'ed Up" and assumed the position of Commanding Officer. During his tenure in PROTECTEUR, he participated in numerous deployments in support to counter narcotics efforts in Central America with Joint Inter-Agency Task Force (South), earned the Operational Support Medal (Expeditionary) as well as a Commander Canadian Joint Operations Command commendation.

In 2017 he represented Canada as Chief of Staff and Deputy Commander of NATO's high readiness maritime Task Group, Standing NATO Maritime Group One, participating in Operation REASSURANCE in the Baltic Sea and Operation SEA GUARDIAN, NATO's enduring counter-terrorism and security operation in the Mediterranean, earning the Meritorious Service Cross for his leadership of the Task Group.

Shore duties saw him briefly at Canadian Forces Fleet School Esquimalt as the Acting Division Commander for Warfare Training Division in 2003 before being posted to Halifax for the Operations Room Officer course. In 2007, he was the J3 Operations at Canadian Expeditionary Forces Command in Ottawa, integrally involved with full spectrum joint operations in Afghanistan. In 2014 he assumed command of the Naval Officer's Training Centre charged with developing and mentoring the future cadre the Royal Canadian Navy's commanding officers. In 2015 as part of RCN Transformation, he assumed the inaugural command of Naval Fleet School (Pacific), the largest school in the Canadian Forces. Upon his return from duties at sea in Europe, he was promoted and assigned the position of Warfare Analysis Branch Head at CJOS COE in Norfolk, VA.

He holds a Bachelor of Social Sciences Degree from the University of Ottawa and a Masters of Defence Studies with a focus on Chinese Domestic Policy, from the Royal Military College of Canada. He is a graduate of CF Joint Command and Staff Programme 36.

He enjoys the truly outstanding support of his family and credits any success to his beautiful wife, Erin and his two amazing daughters, Kamryn and Lauryn. He spends what spare time he has in the gym training and trying to master his poor guitar skills. An avid fan of the Ottawa Senators hockey club, he tries to keep the dream alive and laces up the skates whenever possible.



Visit of the Hellenic Diplomatic Academy

On Wednesday 22nd of January 2020, ten (10) Candidate Diplomats from the Hellenic Diplomatic Academy of Ministry of Foreign Affairs, escorted by the Director of the Academy Plenipotentiary Minister, Mr Nikolaos Piperigos, visited NMIOTC and were informed about the mission, roles and activities of the Centre.



Memorandum of Understanding between NMIOTC and Diaplous Group

On January 24, 2020, in Souda Bay Crete, the NATO Maritime Interdiction Operational Training Centre and Diaplous Group, a globally leading Maritime Security Company, operating in more than 27 countries, signed a Memorandum of Understanding for the development of partnership, with regards to enhancing through synergetic efforts between NATO's but also private sectors capabilities, in areas of Maritime Security. Specifically, Maritime Risk Management, Piracy, Lessons Learned and Best Practices concerning armed and unarmed protection of merchant vessels, hostage release ops along with negotiation techniques and exchange of know-how in areas of common interest.

NMIOTC was represented by the Commandant, Commodore Stelios Kostalas GRC (N), and Diaplous Group by the CEO, Mr. Manolis Lazaridis.



NMIOTC Annual Information Meeting & Advisory Board 2020

The NMIOTC Annual Information Meeting (AIM) and Advisory Board (NAB), chaired by NMIOTC Commandant, were held at the Center's premises on Tuesday 4th February 2020.

During the meetings, representatives from Sponsoring Nations were informed about NMIOTC activities and achievements of 2019 and also provided advice to the Commandant for the effective execution of his mission.

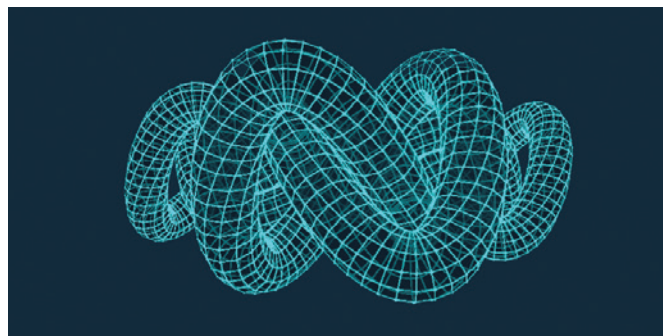


Cyber Gordian Knot 2020

NATO Maritime Interdiction Operational Training Centre (NMIOTC) in collaboration with Plymouth University organized the 2nd Cyber Defense Exercise for Navy (2nd CDX-N) called "Cyber Gordian Knot 2020" on 6th of February 2020.

The purpose of the exercise was to offer recommendations that could help each participant to detect, respond, prevent, and contain threats to their systems.

Trainees acting as rapid reaction teams had to defend pre-built networks against hostile attacks conducted by Red Team (RT) members. Each trainee team had a similar network consisting of approximately 4 virtual machines which were initially unknown to them and contained vulnerabilities.



Pilot Course 26000 “Tactical Emergency Care for First Responders in Maritime Operations”

Pilot Course 26000 “Tactical Emergency Care for First Responders in Maritime Operations” was conducted at NMIOTC’s premises from 17th to 21st February 2020.

The aim of this course was to provide to all combatants and first responders (SOF and conventional personnel) involved in Maritime Operations basic knowledge and skills in delivering necessary pre hospital care with limited equipment and in confined spaces. Furthermore, critical and essential skills were taught so as the first responders would be able to assist medical personnel to provide more complicated medical assistance and deal effectively with a mass casualty situation. Ten (10) participants from three (3) countries attended the course (Bahrain, Greece, and USA). Training was delivered by National Association of Emergency Medical Technicians (NAEMT) certified instructors and other affiliate augmenters specialized in Stress Management, drowning prevention and HAZMAT. In addition, an assigned Medical Director was closely monitoring all medical interventions performed throughout the course in absolute coherence with NAEMT’s policies, and NATO TTPs.



NMIOTC Presentation at NATO Military Committee / Permanent Session NATO HQs, Brussels

On Monday March 9th 2020, the NMIOTC Commandant, Commodore Stelios Kostalas GRC (N), was invited to the NATO HQs in Brussels and presented to the NATO Military Committee/Permanent Session (MC/PS) the activities of the Center, under the title “Shaping the Maritime Human Capital through Innovative Education and Training”.

The NMIOTC Commandant briefed the members of the MC/PS on the mission, training capabilities and undertaken tasks of NMIOTC in coping with current and future challenges for the Alliance emerging in the Maritime Domain.

It is worth mentioning that this has been the first time that a NATO Training Center had the opportunity to present its activities at such a high NATO administration level.



RESIDENT COURSE “1000” COMMAND TEAM MIO ISSUES

Course 1000 “Command Team MIO Issues” was delivered between 9-13 March 2020 by NMIOTC’s instructors. The objective of the course is to assist Staff Officers and Naval Units’ Command Teams in the efficient application of NATO common standards in the planning and execution of Maritime Interdiction Operations (MIO). The course was attended and successfully completed by a total of seven (7) trainees, coming from five (5) countries (Azerbaijan, Georgia, Jordan, Morocco and Tunisia)



RESIDENT COURSE “2000-3000” BOARDING TEAM MIO ISSUES

Courses 2000/3000 “Boarding Team Theoretical and Practical Issues” were delivered between 16-20 March 2020 by NMIOTC’s instructors. The courses were attended by a total of twenty one (21) trainees, coming from ten (10) countries (Azerbaijan, Bahrain, Egypt, Germany, Georgia, Mauritania, Poland, Romania, Tunisia and Ukraine).



US NAVSCIATTS-NMIOTC INSTRUCTORS DEVELOPMENT PILOT COURSE

In the period of 3-13 March 2020 the Instructor Development Pilot Course was delivered by a NAVSCIATTS Mobile Training Team (MTT) at NMIOTC premises.

This course is part of the ongoing formal training cooperation between NMIOTC and NAVSCIATTS and the main objective of the course was to train NMIOTC Sea Trainers in the Standards, Procedures, and Instructive Methodology utilized by NAVSCIATTS (US SOCOM).

The course was attended and successfully completed by a total of seventeen (17) trainees.



NMIOTC'S CHANGE OF COMMAND

On Monday 6th April 2020, a Change of Command was held in NMIOTC. Commodore Stelios Kostalas GRC (N) handed over the Command to Commodore Panagiotis Papanikolaou GRC (N).





*Training of FGS HAMBURG Boarding Team,
January 27, 2020*



*Training of HS ADRIAS Boarding Team,
February 12-13, 2020*



*Training of HS ZEYS, HS KALLIROI and HS TRIHONIS,
February 24-25, 2020*



*Training of HS MARIDAKIS Boarding Team,
March 11-12, 2020*



*Training of HS HYDRA Boarding Team,
May 13-15, 2020*



*Training of Underwater Demolition Team, preparing for Operation IRINI ,
May 13-15, 2020*



*Training of HS SPETSAI Boarding Team,
May 14-15, 2020*



*Training of GRC SOF Team,
May 18-22, 2020*



*Training of NASKRI Security Team,
May 19-21, 2020*



*Training of GRC SOF Team,
June 1-5, 2020*



*Training of HS NAVARINO Boarding Team,
June 4-9, 2020*



*Training of Souda Naval Base Guards,
June 10-12, 2020*



*Visit of the Diplomatic Academy,
January 22 2020*



*Visit of Commodore, Destroyer Squadron 60 and
Commander Task Force 65, Captain Joseph Gagliano US N
January 28, 2020*



*Visit of Defence Attache of United Kingdom in Athens,
Captain Timothy Ferns RN
January 30, 2020*



*Visit of the Hellenic Naval Academy,
February 22 2020*



*Visit of Chief of the HNGS, Vice Admiral Stylianos Petrakis GRC (N),
February 25, 2020*



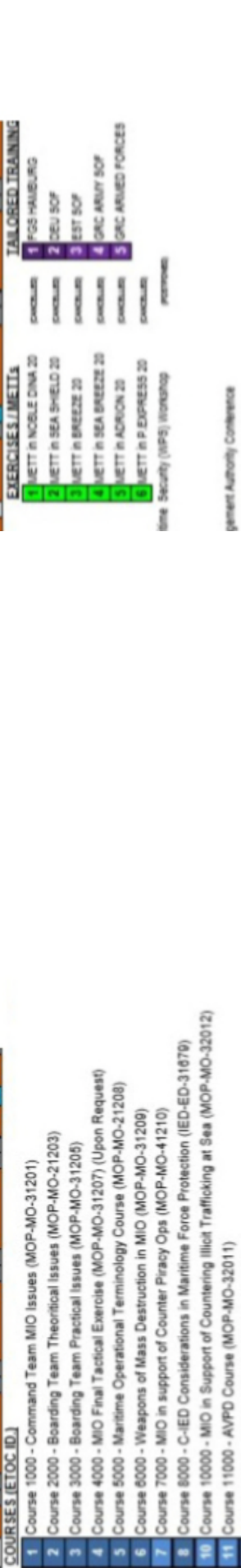
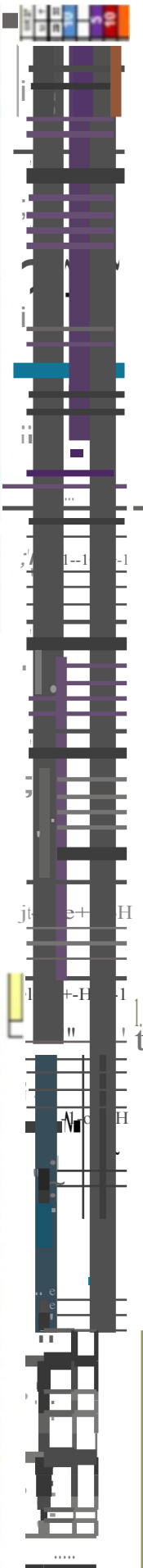
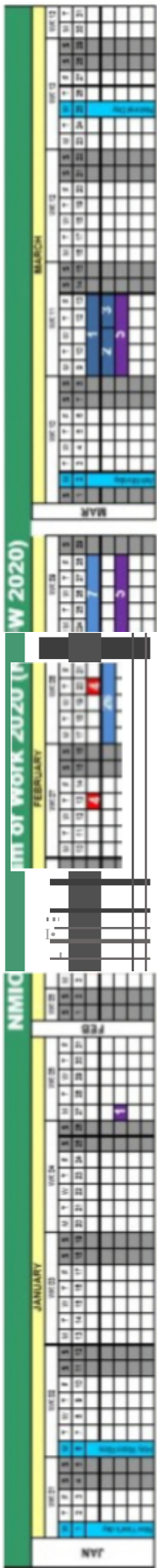
*Visit of Defence Attache of France in Athens,
Colonel Charles Aballea FRA (A)
June 4, 2020*



*Visit of the Greek Minister of National Defence
H.E. Mr Nikolaos Panayiotopoulos,
the U.S. Ambassador to the Hellenic Republic H.E. Mr Geoffrey R. Pyatt
and the Chief of the Hellenic National Defence
General Staff General Konstantinos Floros,
June 12, 2020*



*Visit of Defence Attache of Italy in Athens
Colonel Enrico Frasson ITA (AF),
June 30, 2020*



D



NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

Phone: +30 28210 85710
Email: studentadmin@nmiotc.nato.int
nmiotc_studentadmin@navy.mil.gr

Webpage: www.nmiotc.nato.int

