



Issue 19
2nd Issue 2019
ISSN: 2242-441X

nmiotc

*Maritime Interdiction Operations
Journal*

NATO MARITIME INTERDICTION OPERATIONAL
TRAINING CENTRE

Towards Grey Waters

Building a Comprehensive Approach to
Countering Hybrid Threats in the Black
Sea and Mediterranean Regions

NNSA partners with NATO on first-ever
maritime pilot course

HN Littoral Warfare Med



NMIOTC



NATO

Maritime Interdiction Operational Training Centre

SAVE THE DATE

11th NMIOTC Annual Conference 2020

“Interagency and whole of society solutions to maritime security challenges”

3rd –4th June 2020

SAVE THE DATE

4th NMIOTC Conference on Cyber Security in Maritime Domain

30th September –1st October 2020

**For more information visit:
<http://nmiotc.nato.int>**

CONTENTS



COMMANDANT'S EDITORIAL

4

Editorial by Stelios Kostalas
Commodore GRC (N)
Commandant NMIOTC

MARITIME SECURITY

6

Towards Grey Waters
by Major Patrick 'Hoesy' VAN HOESERLANDE BEL (AF)

9

Building a Comprehensive Approach to Countering Hybrid
Threats in the Black Sea and Mediterranean Regions
by Chris Kremidas-Courtney

14

NNSA partners with NATO on first-ever maritime pilot course

28

HN Littoral Warfare Med
by Captain Spyridon Lagaras

10TH NMIOTC ANNUAL CONFERENCE

16

10th NMIOTC Annual Conference
Speech by Capt. P.N. Tsakos

19

10th NMIOTC Annual Conference Wrap Up
by Wendi brown

NMIOTC COURSES & ACTIVITIES

31

NMIOTC TRAINING

41

HIGH VISIBILITY EVENTS

47

MARITIME INTERDICTION OPERATIONS JOURNAL

Director

Commodore S. Kostalas GRC (N)
Commandant NMIOTC

Executive Director

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

Editor

Commander 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

Last September, we had the great pleasure to welcome to NMIOTC in Souda Bay, Crete the "Hybrid Threat Event Experts Panel". This forum focused on the enhancement of collaboration and coordination between security organizations from across the Mediterranean and Black Sea region in countering hybrid threats and provided the platform for the exchange of ideas and best practices.

The concept of the 'hybrid threat' and its potential impact on modern democratic societies requires no further explanation here, suffice to

say that NATO has a well-defined strategy, which identifies its roles in addressing such threats and in countering hybrid warfare activities. This strategy encourages all Alliance member states to be both more aware of the hybrid threats present and to build their resilience to them. For the maritime domain it should be noted that all activities and operations are particularly susceptible to hybrid and cyber threats, especially with recent technological advancements and the use of increasingly sophisticated platforms. NMIOTC's response to these challenges is training and ca-

capacity building. As our name suggests, MIO provides the means by which we can Delay, Disrupt and Destroy any hybrid or asymmetric threat emerging from the maritime domain before it has chance to impact us or our friendly forces.

I want to assure you that NMIOTC remains totally committed to improving our resilience to hybrid threats through its courses and events and **"Countering Hybrid Threats Year 2019"** provides an excellent illustration of such activities. As some of our readers may know, this year's

10th NMIOTC Annual Conference was focused on countering hybrid threats in the maritime domain. Our conference gave the opportunity for the full breadth of stakeholders, both public and private sector and from many different countries (navies, government bodies, maritime associations and shipping industries, international organizations and bodies and academia and researchers) to discuss issues pertaining to maritime security and the ways in which challenges such as evolving hybrid threats at sea can be addressed. Further details of the this conference can be found within this issue of our journal.

The 3rd NMIOTC Cyber Security Conference similarly provided excellent opportunities for the same stakeholder community to discuss issues related to the emerging cyber threats to the maritime environment, highlighting how they are highly interconnected with hybrid threats.

Following such key conferences, NMIOTC was, along with the US Institute of Governance, extremely well placed to co-organize the aforementioned Experts Panel. This forum provided yet another opportunity for our NATO center to engage with the international com-

munity to improve the understanding of potential hybrid threats and provide ways to respond to such maritime security issues. I am convinced that this issue's article **“Building a Comprehensive Approach to Countering Hybrid Threats in the Black Sea and Mediterranean Regions”** will inform future planning and transformation relating to these issues, with the ultimate aim to reduce potential hybrid threats to the international maritime community for many years to come.

Stelios Kostalas
Commodore GRC (N)
Commadant NMIOTC



Towards Grey Waters

by Air Force Major Patrick ‘Hoesy’ VAN HOESERLANDE

The Growing Grey Zone

When we gaze under the water surface, we can detect different types of military systems, but three are of interest here: submarines, torpedoes and mines. According to the editors of Encyclopaedia Britannica these are defined as (only the naval part of the definitions are withheld):

- Submarine: any naval vessel that is capable of propelling itself beneath the water as well as on the water’s surface.
- Mine: in naval operations, a usually stationary explosive device that is designed to destroy personnel, or ships, when the latter come in contact with it.

- Torpedo¹ : a cigar-shaped, self-propelled underwater missile launched from a submarine, surface vessel or airplane and designed for exploding upon contact with the hulls of surface vessels and submarines.

These are currently three distinct different kind of systems. We can categorize the standard representatives of these systems according to a three-axis system of acoustic signature, size and mobility. With ‘Acoustic Signature’ defined as the noise the system produces, ‘Size’ the external dimensions of it and ‘Mobility’ a combination of speed and maneuverability. Mobility is something different from autonomy, a term nowadays heavily discussed in

other articles. We can easily put our three types of underwater systems into this analytical space:

- Submarine: the silent hunters of the deep are compared to the other two other systems quite large. To execute their mission they must be very mobile and running silent, although they may be noisy at higher speeds.
- Mine: this small device is silently waiting for its victim. Mobility is sacrificed in favor of a extremely low acoustic signature.
- Torpedo: a torpedo penetrates defense systems by speed, even if that means being noisy. Although there exist some big ones, a torpedo is compared to a sub small.

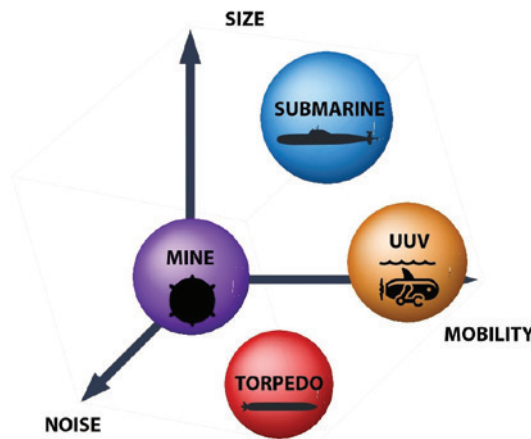
	Acoustic Signature	Size	Mobility
Submarine	Low	Big	High
Torpedo	High	Small	Very High
Mine	None	Small	None

¹ Strangely enough, torpedo is the old name for a naval mine (Tamara M. Melia, ‘Damn the Torpedoes, A Short History of Naval Mine Countermeasures 1777-1991’).

In the last decade, a fourth group has entered the underwater realm: the Unmanned Underwater Vehicles (UUV). These systems are relatively small, quite silent and mobile. In the begin-

ning, they were tethered and in small numbers, but recently with increasing autonomy levels they deserve a group of their own.

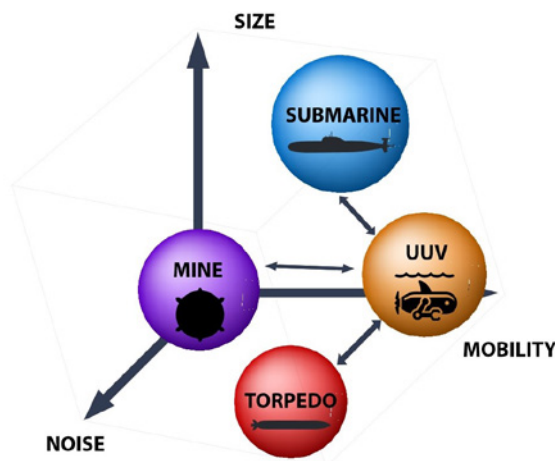
Putting these 4 groups as bubbles, this is just a visual representation of the existing variations within the types to support the reasoning, on our three axes gives the illustration below².



The first three have their own type of warfare and certainly their 'anti': Anti-Submarine Warfare, Mine Counter-Measures and Anti-Torpedo Measures. Nowadays, there is no such domain for UUVs, although they (will) pose a very specific challenge that cannot be solved by the application of the other anti-warfare areas. It is time to think about filling this gap. However, before starting to do this, there are reasons to study the issue more comprehensively. For one, submarines are getting smaller. This is done by adding more intelligent modules to a sub, requiring less people to run the boat and thus a possible reduction of the size for the same type of missions. With a limited set of missions or the application of modu-

larity, it is possible to reduce the size even further and operate in shallower waters. However, because big subs have their own set of advantages, this introduction towards smaller subs will not result in a shift of our submarine bubble along the length axe but in an extension of the bubble touching the UUV bubble. This bubble inturn will inflate along the 'size' axe with the introduction of large UUVs and XLUUVs. Soon, if not already, there will be an overlap between submarines and UUVs blurring the distinction. Is an XLUUV that different from a small unmanned submarine? And what is the different in hunting them? As similar inflation and future overlap will occur between UUVs and mines. The last will become more mobile³

able to swim, when detected or triggered by something else, to another position, and this multiple times. UUVs could be used to move static mines around creating a dynamic minefield or, being equipped with an explosive module, swim somewhere to wait for the right opportunity to hit a target. A torpedo may be fired and go into silent, slow mode while approach a ship. It may even sink to the bottom and wait silently before striking. A UUV can easily be equipped with an explosive head to attack a ship blurring the distinction between a torpedo and a UUV. Considering the paragraphs above, our bubble graphs turns into the following representation.



² Is there a military interest in filling the vacant corners?

³ We do not talk here about mobile mines as they are currently defined as a mine that is able to swim to its position where it will act as a 'normal' mine.

Impact on Under Water Warfare

The blurring of the distinctions between the different systems necessitates the creation of a more integrated approach⁴. Systems and TTPs specialized in combatting the corner threats will be too easily outmaneuvered in the near future. For example: although taken into account the low costs of dumb mines, this type of naval mines will stay the preferred weapon for the creation of high-risk areas, but

mixed with a few mobile types or UUVs, the area suddenly turns into a dead trap for a MCM vessel or even a MCM UUV. A submarine detecting a ASW screen can create havoc by launching a large, armed UUV infiltrating the barrier.

It will be hard to marry the three types of warfare, not only from a technical point of view but also from a doctrinal, and indeed from every DOTMLPFI line. History is against us. The lines are cut deep into the fabric of the Navy,

but we do not really have a choice. It is a weakness in our defenses that the other side will certainly seek to exploit if we are not able to plug it.

The overlapping zones will slowly, but surely do away with the distinction between blue and brown water navies to turn our seas and oceans in to gray waters. How to operate in those dangerous waters is question that sounds much like a need to develop a concept.



Air Force Major Patrick 'Hoesy' VAN HOESERLANDE works as concept developer in HQ SACT. He graduated from the Belgian Royal Military School with a Master in Engineering Science followed by a Master in Business Administration. Currently he is leading the development of a Naval Mine Warfare concept, facilitates the Mountain Warfare concepts and instructs in NATO School Oberammergau.



Disclaimer:

Opinions, statements and projections stated in this article are solely those of the individual author. They do not reflect the opinions or policy of NATO, HQ SACT or any of its affiliates nor is the content endorsed by those entities.

⁴ The blurring of the types of systems was also observed during the Naval Mine Warfare Disruptive Technology Assessment Game (DTAG) organized by HQ SACT in November 19.

Building a Comprehensive Approach to Countering Hybrid Threats in the Black Sea and Mediterranean Regions



by Chris Kremidas-Courtney

Introduction

The future security of the Black and Mediterranean Sea region depends upon a cooperative and collective ability to understand and shape conditions to counter traditional and emerging threats. Resurgent ‘great power competition’ and insidious non-state threats introduce disquieting alternatives to democratic governance, market economies, and social egalitarianism.

Today, state and non-state actors are challenging nations, institutions, and private companies through a wide range of overt and covert activities targeted at their vulnerabilities. Both NATO and the European Union refer to these aggressive acts as “hybrid threats.” As we’ve seen recently in both Crimea and the South China Sea, a hybrid approach lowers the political price for aggression, making regime

change and territorial annexation possible “on the cheap.”

Hybrid threats use subtle, far-reaching, and opportunistic methods – and seldom with a return address. In certain cases, they can be more brazen, but operate in a legal and normative ‘gray zone’ in which the impacted state has few good response options without escalating the situation into armed conflict.

NATO and EU Response to Hybrid Threats

In the wake of Russian aggression in Ukraine in 2014, NATO developed and adopted a Hybrid Warfare Strategy in December 2015. In early 2016, the European Union adopted its Joint Framework for Addressing Hybrid Threats. Both documents call for working to improve resilience, security and continuity of governance. Both documents also call for greater NATO-EU coop-

eration in addressing hybrid threats.

Since June 2016, both organizations have agreed on dozens of areas in which to focus their efforts. Neither organization has fixated on an exact definition of hybrid threats, but instead concentrated on identifying their characteristics and working approaches so that they can coordinate efforts to effectively counter these threats.

Within NATO it can be difficult to reach a consensus on Article 5 (collective defense) in the face of a hybrid campaign; however, a stricken ally can always bring its security concerns to the alliance via Article 4, under which allies can exchange views and information and discuss issues prior to taking any action. Thus, Article 4 consultations are the most likely venue for the North Atlantic Council to first discuss options when facing hybrid aggression against an ally.

Within the European Union, Article 42 (7) of the Treaty of the European Union and Article 222 of the Treaty on the Functioning of the European Union are the most applicable to hybrid threats. Though similar to NATO's Article 5 in that it is triggered by an armed attack on a member-state, Article 42(7) can also be applied to some situations below the threshold of armed attack. Article 222 (the Solidarity Clause) applies more broadly to natural or man-made disasters, terrorist attacks and situations that align more closely with a hybrid campaign. It is also tied to the EU's Solidarity Fund, which can provide immediate funding to recovery and response efforts.

Both NATO and the EU recognize hybrid threats as a distinct category of adversary that possesses distinctive attributes and capabilities. Hybrid threats are distinguished from traditional adversaries by their novel exploitation of information networks, engagement in 'lawfare', and oblique employment of high-end military capabilities via proxies, which provides them with strategic tools that were once exclusively controlled and monitored by state actors under established rules and precedents.

Currently NATO and the EU are working together on enhanced cooperation in four areas: civil-military planning, cyber defense, information-sharing and analysis, and coordinated strategic communications. Since 2016, they have agreed on 74 areas of deeper cooperation, 20 of which relate to countering hybrid threats. The European Centre of Excellence for Countering Hybrid Threats, established in 2017 in Helsinki, effectively contributes to strengthening NATO-EU cooperation in this area. Both organizations' personnel have participated in a number of the center's activities.

In September 2018, NATO's North Atlantic Council and the EU's Political and Security Committee held the first-ever scenario-based discussion on hy-

brid threats, and subsequent parallel exercises have validated the improved cooperative working mechanisms being put into place at staff and senior levels. Also since 2018, NATO adopted the concept of establishing Counter Hybrid Support Teams (CHST) to give ad hoc assistance to allies in the event of a hybrid crisis.

The first CHST was deployed to Montenegro in November 2019, and it remains to be seen how Allies requesting their assistance may integrate them into their own national processes.

In any case, determining attribution of potential hybrid attacks and decisions on responses to them (including any public announcements) remains a sovereign responsibility of the stricken nation. Internally, providing credible deterrence to hybrid threats is straightforward: building and maintaining resilient, credible and capable governance that raises the price of hybrid aggression and reduces its chance for success. To do so requires cooperation and collaboration from all entities.

Hybrid Threats in the Black Sea and Mediterranean Region

The Black Sea and eastern Mediterranean region is home to several NATO Allies and partner countries. The region is of particular security concern for Europe, since it serves as a strategic maritime corridor at southern Europe's four-way intersection with Eurasia, North Africa, and the Middle East. Threats emanating from these peripheral regions range from hostile state actors to terrorists and insurgents who deliberately aim to disrupt governance, reduce stability, and challenge the Western liberal world order.

At a gathering of regional hybrid experts from throughout the region held at the NATO Maritime Interdiction Operations Training Center (NMIOTC) in September 2019, the panel identified the following five major categories of hybrid threats in the region:

- Economic and Energy Coercion
- Disruption of Governance
- Disinformation Campaigns
- Lawfare
- Paramilitary Threats

Economic and Energy Coercion.

Moscow uses both direct and indirect economic pressure to influence politics, security, and trade in Europe. Throughout Europe, Moscow exploits its dominant role in energy provision. State-owned gas giant Gazprom and its subsidiaries leverage European dependence on natural gas to shape political agreements and trade arrangements in their favor. For example, Romanian imports of natural gas from Russia soared by 26.8 percent in 2018, despite extensive offshore gas deposits in Romania's Black Sea exclusive economic zone. In an ironic and frustrating twist, last year Romanian lawmakers increased taxes on domestic production of natural gas, further incentivizing increased dependency on Russian imports and stymying opportunities to develop energy independence.

Disruption of Governance.

Russia also exerts its historical political influence in the Black Sea region to disrupt or discredit Western-oriented democracies. In Moldova, Moscow leverages identity politics, a large pro-Russian bloc of Moldovan emigrants, and weak government institutions in Chisinau to maintain influence and counter NATO-EU alignment. Moreover, Russia supports the breakaway regions of Transnistria and Gagauzia with Kremlin subsidies and on-the-ground 'peacekeeping' forces to actively challenge Chisinau's control. Russia employs similar tactics in Georgia's breakaway provinces of Abkhazia and South Ossetia; Ukraine's Donbass region; and the disputed region of Nagorno-Karabakh between Azerbaijan and Armenia.

Disinformation Campaigns. Disinformation might be considered the 'go-to' play for hybrid aggression, from so-

phisticated disinformation campaigns down to tactical level deception. In one tactical example, last summer a Russian Navy frigate audaciously shadowed and harassed the USS Gravelly missile destroyer navigating as part of a carrier battle group in the eastern Mediterranean. The intent became clear when the Russian frigate displayed maneuver 'distress' symbols as it adjusted course towards the Gravelly. Immediately thereafter, the Russian ministry of defence issued an official statement and 'decksides' video that captured the USS Gravelly's "dangerous maneuvers."

This calculated tactical example is one small element of a broader strategic disinformation campaign that includes misrepresentation of international law, election meddling, and culturally and ethnically divisive social media campaigns aimed at disrupting governance, eroding public trust, and proliferating pro-Russian sentiment in former Soviet states.

Lawfare. Lawfare is a term used to describe the manipulation, misapplication, or exploitation of laws to avoid attribution for hostile actions, engage in disruptive operations and shape political and socio-economic conditions, and justify questionable military interventions. While Russia's "peaceful" annexation of the Crimean peninsula to "defend the rights of Russian-speakers living abroad," is by no means the only example of Russian engagement of so-called 'lawfare' in eastern Europe. Indeed, one hybrid panel lawfare expert noted that Rus-

sia regularly deploys invading military forces as thinly-veiled "peacekeepers" to impose Russian control in disputed territories in Georgia, Moldova, and Ukraine. In the maritime domain, Russia willfully abuses maritime law to assert dubious territorial claims, disrupt or deny freedom of navigation, and encroach on the sovereign waters of allies and partners.

Paramilitary threats. Russia avoids attribution and legal accountability for full-spectrum attacks by exploiting paramilitary and criminal groups as proxies. The most notorious incident of Russian proxies is of course the downing of Malaysian Airlines flight 17. After five years of investigation, international courts have finally brought the case to trial, asserting that the civilian airliner was shot down by a Buk missile system that was covertly deployed from the Russian city of Kursk into eastern Ukraine. Moscow likewise leverages highly organized Russian-aligned criminal groups throughout the region as proxy agents. The European Council on Foreign Relations published a detailed policy brief that exposes Russian-affiliated criminal groups engaging in 'black cash' fund sourcing, launching cyber attacks, influencing corrupt politicians, and even carrying out targeted assassinations in direct or oblique support to Kremlin authorities.

NATO, the EU, and affected nations must take concerted and unified actions to counter these and other hybrid threat activities. A more predictive and pro-active collective posture could prevent or mitigate many 'below

the threshold' actions, while a credible and capable military option should be openly maintained as option of last resort to deter and defend against these threats. Given the complexity of the threat, it is necessary to employ a comprehensive approach that combines political, socio-economic, information, and military tools to identify, mitigate, counter, and failing all else, recover from the effects of hybrid warfare.

The Comprehensive Approach

The Comprehensive Approach (CA) is a way to achieve a common understanding and approach among all actors of the International Community through the coordination and deconfliction of political, development and security efforts in solving an international crisis. CA focuses on building a shared understanding of the problem, developing a shared overarching vision of the solution and facilitating coordination of effort while respecting the roles and individual mandates of multiple entities.

At the Lisbon Summit in November 2010 and in its new Strategic Concept, the Alliance "...decided to enhance NATO's contribution to a comprehensive approach to crisis management as part of the international community's effort and to improve NATO's ability to deliver stabilization and reconstruction effects."

The effective implementation of a comprehensive approach requires all actors to work together with a shared sense of responsibility and openness, taking into account and respecting each other's strengths, mandates and roles, not to mention their decision-making autonomy. In other words, the Comprehensive Approach is not hierarchical but rather it is a collaborative effort among equals.

NATO's experience from operations, including Afghanistan and in addressing piracy, has demonstrated that managing complex conflicts and cri-



ses requires a wide range of internal and external actors, including governments, civil society, the private sector and international agencies, to work together in a coherent and coordinated effort.

Hybrid Warfare: The Comprehensive Approach in the Offense

Looking through the military and security lens, Hybrid Warfare appears to target critical vulnerabilities and seeks to create ambiguity in order to hinder swift and effective decision-making. Taking a broader perspective, Hybrid Warfare is actually the comprehensive approach (CA) in the offense. Where CA seeks to create space for friendly actors to strengthen governance, hybrid warfare seeks to shrink it.

Where CA strengthens and enables governance, hybrid warfare weakens it. Where CA seeks to build trust and societal cohesion, Hybrid Warfare seeks to sow mistrust and confusion between segments of the population as well as between the people and their government.

Where CA seeks to heal a society's divisions and seek reconciliation, Hybrid warfare targets a society's deepest historical wounds to make them bleed again.

As recent history tells us, hybrid warfare lowers the political price for aggression. Thus, building resilience against it is an effective deterrent because it raises the price for such aggression while reducing its chance for success.

Building Resilience through a Comprehensive Approach

When we refer to resilience, we mean resiliency of institutions and people to deal with natural and manmade disasters, social cohesion, and the ability of civilian infrastructure and capabilities to support military operations – and vice versa. Resilience is therefore an

important aspect of deterrence by denying the hybrid actor an easy target: dissuading an adversary by convincing them an attack will not be successful.

While civil preparedness is a national responsibility, NATO Allies have a collective interest, as spelled out in Article 3 of the Washington Treaty (self-help and mutual aid), to build resilience together since a gap or vulnerability in one of our countries can impact other Allies' security.

Resilient societies are more able to bounce back after a crisis and they to restore functions much faster than less resilient societies. In resilient societies, continuity of government and essential services are more reliable and able to be sustained during natural and manmade crises.

Both NATO and the EU, as well as their member states stress the need for a posture of resilience in the face of uncertain security conditions and the ambiguity associated with hybrid threats. The term resilience carries similar connotations between NATO, EU, and member states, but there are a few important distinctions:

At the national level, resilience is a matter of sustaining national sovereignty and integrity in the face of national crises, including direct and oblique attacks from hostile actors. National resilience strategies focus on mobilizing a whole-of-society response to disruptive attacks or catastrophic events.

NATO's resilience concept prioritizes the preservation of essential government functions in the face of a crisis or conflict; nations must be prepared to "endure" long enough to allow the Alliance to organize a collective response. In addition to the direct application of national level civil emergency preparedness to deter against and mitigate the effects of hostile actors,

NATO also secures additional deterrence value by reassuring Allies and Partners in other ways. These include its sustained cooperation and presence in key nations, the development of dual-use shared awareness capabilities, and the enhancement of whole-of-society readiness without broadcasting overtly aggressive overtones that may escalate regional tensions on the Alliance's periphery.

The European Union also recognizes that market pressures, mass population shifts, political discord, and belligerent actions by neighbors threaten regional unity and common security. EU's global strategy emphasizes that "[f]ragility beyond our borders threatens all our vital interests. By contrast, resilience – the ability of states and societies to reform, thus withstanding and recovering from internal and external crises – benefits us and countries in our surrounding regions, sowing the seeds for sustainable growth and vibrant societies."

Together with its partners, the EU therefore promotes resilience in its surrounding regions. A resilient state is a secure state, and security is key for prosperity and democracy." In addition, the EU pledges to implement both multi-dimensional and multi-phased approaches as part of an expanded 'comprehensive approach'.

Both NATO and the EU do make efforts to share their best practices on resilience with partners in the Black Sea and Mediterranean region but there is much room for improvement. A few examples include; the need to bring a comprehensive approach to these regions to counter hybrid threats, conducting hybrid tabletop exercises among EU, NATO, and partner nations, and conducting joint studies and analyses of regional issues which identify vulnerabilities in legal regimes, trade norms, disinformation, and societal cohesion.

Building a Resilience Bridge between NATO, EU, and Regional Partners

NATO and the EU must recognize that their partners in the Black Sea and Mediterranean regions are on the front lines of hybrid aggression. These countries stand as a bulwark against deeper penetration by hybrid threats, but are also the unfortunate proving ground that tests the limits of Western resolve. It is essential to enable our partners on the periphery with unwavering political rhetoric and support for democratic institutions, economic assistance, and security cooperation including defense capability development and targeted direct military support that sends a clear message to hostile actors.

To do so means thinking of collective security in a regional sense beyond just the members of NATO and the EU. Thus, a key task before us is to bring together NATO, EU, and their partners together into a regional community of interest to build resilience, share best practices, and enable re-

gional collective security against hybrid threats. In turn, this community of interest will enable a regional comprehensive approach which will not only build more effective resilience against hybrid threats but also against transnational threats such as illicit trafficking and terrorism since the response mechanisms are largely the same.

There has been much important conceptual work on countering hybrid threats over the last decade, but the time is ripe to further operationalize and institutionalize a comprehensive approach for whole-of-government assessment and action. Improving civilian participation, not to mention civilian leadership, in security planning will require significant introspection, expansion of civilian planning capabilities, and a shared commitment amongst military, security sector, and civilian actors.

At the national level, governments must be more resilient in the face of continuous aggression. This includes sober assessments of national risk and investments in national capacity

to prevent, mitigate, and recover from deliberate attacks on governance, persistent disinformation campaigns, probing of critical infrastructure, and exploitation of economic and energy dependencies.

Regionally, we will only deter hybrid aggressors if we are unified in political will, present an honest and compelling narrative in defense of Western ideals, and rapidly commit to decisive actions when necessary. This is will not be an easy task. Even if there is sufficient political will and adequate resources, it will take time to build inter-organizational trust and competence since it is not possible to “surge” trust - it must be built over time.

In light of Russian aggression in Ukraine and eastern Europe, and the challenging security conditions in the Mediterranean and Europe’s southern borders, political leaders must continue to build an informed and agile deterrent and preventative posture, lest they allow security conditions to deteriorate at the hands of more agile external actors.

Chris Kremidas-Courtney currently serves as the Multilateral Engagement Coordinator for U.S. European Command. He is recognized as one of the US Department of Defense’s leading experts on countering hybrid threats and NATO’s comprehensive approach; he organizes and facilitates seminars and exercises on these topics among high level NATO, EU, and member state officials. His previous positions include serving as the Acting Director of Training and Exercises for the Hybrid COE, Political Advisor to the Commander, NATO Training Mission – Iraq and Assistant Political Advisor to Commander, Joint Forces Command Naples. He has also served as Chief Strategist for US Joint Task Force North, NATO Policy Planner at the US Delegation to NATO, and as Deputy Defense Policy Advisor for the US Mission to the European Union (EU). Previously he served as Regional Cooperation Manager for the Mediterranean region at the EUCOM Joint Interagency Counter-Trafficking Center (JICTC) and served a 22-year career as a US Army strategist and intelligence officer.

Mr Kremidas regularly publishes in European journals and makes media appearances on countering hybrid and transnational threats. He is also the course designer and chief facilitator for NATO Comprehensive Approach seminars throughout Europe and the United States.

He earned a master’s degree with honors in Strategic Studies from the Swiss Federal Institute of Technology (ETH Zurich) and a Bachelor of Arts in Political Science from Ball State University. Mr Kremidas serves on the Stratcom Hybrid program faculty at Rey Juan Carlos University in Madrid, the only graduate-level program on hybrid threats in the world. He is also a distinguished honor graduate of the NATO Defense College and a veteran of Operation Iraqi Freedom.





NNSA partners with NATO on first-ever maritime pilot course

National Nuclear Security Administration partnered with NATO to complete its first-ever Maritime Pilot course, “Radiological Threats in a Maritime Environment,” at Souda Bay Naval Base in Crete, Greece, Sept. 9-13. US Department of Energy and NNSA subject matter experts delivered the course content, which focused on searching for and identifying illicit radiological sources in commercial maritime settings.

NATO’s Maritime Interdiction and Operational Training Facility hosted the training program for 29 participants from nine different nations: Australia, the Czech Republic, Egypt, Greece, the Netherlands, Turkey, Spain, the United Arab Emirates, and the United States. The global prevalence of commercially available radiological sources and maritime transportation of goods makes this type of training

crucial to prevent the malicious use of radioactive materials.

“NNSA’s Office of Nuclear Incident Policy and Cooperation is looking to form a partnership with this facility because it’s one of the best maritime training centers in the world,” said NNSA Foreign Affairs Specialist Andrae Brooks. “The facility provides a unique and world-class maritime training environment, and NATO shares



Andrae Brooks explaining NNSA’s role in supporting NATO with emergency preparedness and response training.

NNSA's global outlook on supporting realistic, adaptive training for international partners."

The Pilot Course included lectures, table-top exercises, hands-on equipment demonstrations, and practical training on Rubberized Hardened Inflatable Boats, or RHIBs. The Greek naval training vessels Aeres and Akylon were used to conduct radiological search exercises using NNSA's specialized tools. Participants enhanced their knowledge of radiation detectors and radiation protection concepts, radiation search techniques, and detection strategies. The course also provided opportunities to prepare, plan, and provide command and control activities for radiation emergency response operations.



The Spectral Advanced Radiological Computing System used during maritime search operations on a Rubberized Hardened Inflatable Boat.

The Department of Defense's Defense Threat Reduction Agency provided radiological sources and radiological safety subject matter expertise to round out the multinational presence. NNSA is expanding and aligning its NATO portfolio of radiological courses

to support nations in the Partnership for Peace, Partners Around the Globe, Mediterranean Dialogue, and Istanbul Cooperative Initiative.



Small work groups tackle maritime planning operations during a tabletop exercise.



10th NMIOTC Annual Conference CAPT. P.N. Tsakos Speech

Your Excellencies,
Chiefs of the Hellenic and Romanian Navies,

Admirals, Generals,
Distinguished Guests,
Ladies and Gentlemen,

It is a privilege to speak today in front of such a distinguished group of experts. Personally, I am not an IT or cyber security or hybrid threats expert. I am simply a Captain of the Merchant Marine.

We all know that seventy percent of the surface of the Earth is covered by water, 90% of global trade are transported by sea which leads me to suggest that our planet should, more appropriately be called Planet Ocean.

Some 350 million passengers and about 3.5 billion tons of cargo per year pass through European seaports and waterways including several choke-points such as the English Channel, the world's busiest shipping lane, the Danish Straits, the Bosphorus Straits, and the Strait of Gibraltar.

In addition, there are many more choke points all over the world which pose security concerns such as the Hormuz Straits and the Malacca Straits which are located at the crossings of major marine trade routes. For example,

20% of oil shipped around the world passes through the Strait of Hormuz.

Therefore, it should come as no surprise that the protection of the world's shipping routes has come to be an essential component of security.

I come from the small Greek island of Chios which may be considered the cradle of Greek shipping. My island represents approximately 50% of Greek shipping, which is by the way 50% of European shipping, and European shipping is 40% of the world's shipping. So overall my small island controls approximately 10% of the world's shipping.

This is a great accomplishment that we owe to our forefathers and to the generations before us who inspired us since childhood, to love and devote ourselves to the sea and who taught us that success comes from hard work, dedication and commitment to seamanship. They taught us that our future lies in the sea and for us this was a one-way street: a matter of destiny.

But my island should not be regarded solely as the island of ship owners. To the contrary, it is mainly the island of Greek seafarers. Generations after generations we served on the ships in

all capacities, from deck boys all the way to becoming Captains or Ship Engineers. As such the concern for safety and security was flowing in our bloods and in our mentality. We were fully aware of the risks at sea.

From childhood we were informed that maritime transport was always an adventure and full of risks. At school we learned of the adventures of Jason and the Argonauts, of the existence of Scylla and Charybdis, but of the Sirenes as well. We learned about Theseus and how he killed Minotaur (not far from here) but also that he forgot to change the sails which resulted in the death of his father king Aegeus and hence the name Aegean Sea.

In Odyssey written by Homer, our great poet from Chios we learned about the cunning Odysseas and how he had to overcome a myriad of obstacles, storms and shipwrecks before finally after 10 long years of wandering in the Mediterranean Sea, reached his loved island of Ithaca.

In the Peloponnesian war between Athens and Sparta we learned that Pericles the great Athenian statesman and general said «Μέγα το της

Θαλάσσης Κράτος” which means “Great is the country that controls the sea”. We also learned of the famous naval battle of Arginousae, near my hometown of Kardamyla, in which Athens won over Sparta. However, in the aftermath of the battle, a storm prevented the Athenians assigned to rescue the survivors of the 25 disabled or sunken Athenian ships from performing their duties, and a great number of sailors drowned. When the public learned this in Athens, the admirals who had commanded the fleet were tried as a group and six of them were executed.

These were the stories, the adventures but also the morals we grew up with. So, in my age and in my time, we had a pretty good knowledge of the known perils of the sea. We understood well the dangers of storms, hurricane, waves, wind, collisions, fire, smoke, sinking, flooding and capsizing, loss of propulsion or steering, and all other hazards resulting from the unique environment of the sea.

During the past decades we also got accustomed to the old and resurfacing problem of piracy. The dramatic upsurge over the last two decades in

incidents of piracy and armed robbery against ships off the coast of Somalia, the Malacca Straits and lately the Gulf of Guinea has shown that this “old” threat is far from extinct.

Especially where one finds inherent state weakness and attacks take place along vital maritime trade routes, piracy can pose a threat not only in terms of local or regional security, but also of international security.

These ruthless pirates put the lives of our seafarers at risk. The assistance of governments and NATO helped to deter and disrupt these pirate attacks, while protecting vessels and helping to increase the general level of security in these regions.

So, while piracy off the coast of Somalia has dropped dramatically, the threat of piracy has not been fully contained, however, as it has increased in other areas, including the waters around West Africa, Malaysia and Indonesia. This new piracy, however, is different in that it is focused on armed robbery and kidnapping of seafarers rather than hijacking of vessels.

While each maritime threat poses dis-

tinct challenges, threats are often interconnected. In Somalia for instance, the combination of weak maritime governance, a legacy of illegal, unregulated and unreported fishing, a surge in piracy, and possible links with terrorism, creates a complex and particularly dangerous environment.

More attention should also be drawn on terrorism at sea. We all recall with horror the notorious “Achille Lauro” incident in the Mediterranean. – which prompted the creation of the IMO Rome International Convention on Prevention and Suppression of Unlawful Acts at Sea. In addition, as a result of the 9/11 attacks in New York and Washington, IMO adopted the “International Ship and Port Facility Security (ISPS) Code” and a legal document to prevent carriage by sea of nuclear, chemical and biological substances while introducing the Long-Range Identification and Tracking of ships system.

The situation in Somalia also demonstrates how a maritime threat which has partially developed in territorial waters can have implications for global security. Adequate maritime governance and law enforcement capacity at sea is therefore essential in





Tsakos Group fleet, during the 10th NMIOTC Annual Conference

preventing and addressing maritime security threats. Management of the high seas poses a different challenge, as the imperative of security must be balanced against the principle of freedom of navigation.

Currently though, these problems are getting worse whilst new ones and more critical are emerging.

These are the cyber-attacks !

They have arisen because of the rapid development of technology and digitalization. While computer systems aboard ships and ashore are self-con-

tained, they are prone to inside threats and hacking from the outside are also possible as evident from the crippling cyber-attack against the Danish shipping giant Maersk in June. This attack seized the industry’s attention after it cost the company in excess of \$200 million and led to a temporary shut-down of the largest cargo terminal in the Port of Los Angeles.

Many of the current threats in the maritime domain such as terrorism, proliferation of weapons of mass destruction (WMD), illegal trafficking in drugs, people / arms and piracy are of a transnational or global nature,

and therefore require a concerted approach.

Today’s maritime challenges go beyond the narrow conception of defense in a scenario of interstate conflict. They are more diverse, complex, unpredictable, and intertwined.

This current challenging environment demands new thinking and a shift in strategic approach. Securing the maritime domain today, definitely requires for a broad approach that would bring together the whole spectrum of respective stakeholders, to include national and International agencies –navies, coast guards, custom agencies and police, along with the maritime industry and shipping companies.

Such an approach should therefore be co-operative, through bilateral, regional or multinational initiatives, and comprehensive, taking into account the sources of merging maritime threats emerging at or to the world’s seas. NMIOTC, which hosts us today, is the only NATO Education and Training Center fully dedicated to Maritime Operations. The Hellenic Shipping Industry, effectively controlling an important part of the global shipping, entrusts such NATO and global efforts to enhance Maritime Capacity Building and to guarantee Freedom of Navigation, and looks forward in even closer cooperation and exchange of expertise, to the common benefit of global peace and security through open and secured Oceans.

Thank you for your attention,

Capt. Panagiotis N. Tsakos
 Founder
 Tsakos Group of Companies



Captain P.N. Tsakos is a Captain, a shipowner and philanthropist. He comes from a family with a long maritime tradition and he established Tsakos Shipping and Trading S.A. in the 1970’s and subsequently built up a series of companies in the shipping sector which comprise the “Tsakos Group of Companies”.

He has received numerous awards, he is the founder of “Maria Tsakos’ Foundation” in Montevideo Uruguay and “Maria Tsakos” Foundation- International Centre for Maritime Research and Tradition” in Chios, Greece and is widely and internationally recognized as an iconic shipping magnate.



10th NMIOTC Annual Conference 2019 “Countering Hybrid Threats: An Emerging Maritime Security Challenge”

by Lieutenant Colonel Wendi O. Brown, USAR

The 10th NMIOTC Annual Conference was held on Jun 4-6, 2019 at the NMIOTC in Crete, Greece. This year at the conference there were speakers who delivered a wealth of knowledge regarding hybrid threats and solutions.

The NMIOTC was honored to have **Captain Panagiotis N. Tsakos, the Founder and President of Tsakos Group** as the primary keynote speaker. Captain Tsakos made thought provoking a statement that stimulated conversations throughout the 10th NMIOTC Annual Conference: “Over 90% of global trade is conducted by sea.” This statement was the foundation of the 10th Annual NMIOTC conference.

Captain Tsakos Key Points:

- It is important for the Tsakos Group to understand maritime operations and more importantly maritime security. With 90% of global trade depending on the shipping industry, maritime security is ABSOLUTELY NECESSARY.
- The Tsakos Group exhibits high standards to secure transportation of goods by providing the use of advanced modern technical ships, ef-

fective and efficient operational processes and procedures, and trained staff for daily and defensive maritime operations.

The second keynote speaker was **Mr. Michael Soul, the NATO HQ Head of Operations**. He stated that NATO must conduct strategic planning to address current and future maritime threats. NATO Maritime has 3 main concentrations to address:

- How to handle piracy attacks in Africa.
- How to handle terrorism and be a quick responder.
- How to handle international cooperation and promote partners to create synergies.

Commodore Marcell Halle CAN (N) from MARCOM Deputy Chief of Staff Plans gave the introduction, and spoke on how hybrid threats and warfare are nothing new and will remain a continuous struggle and global challenge. Hybrid threats use sophisticated technology, which is outpacing the ability to solve maritime security problems. Being technologically outdated creates

emerging security challenges against critical infrastructures (which include attacks against submarine cables and oil pipelines), energy, transportation, communication. The current solution to hybrid threats and warfare are a combination of U.S. Strategic Command (USSTRATCOM) intelligence, surveillance, reconnaissance (ISR) equipment, and U.S. Special Forces.

The conference sessions started with **Chris Kremidas Courtney, the Multilateral Interagency Engagement Coordinator at U.S. European Command**. He stated how hybrid threats pose a challenge to countries, institutions, and the private sector through overt and covert activities. Hybrid threats threaten governance, which includes sovereign territory, trust of the people, rule of law, information systems, financial systems, and energy services. Topics vulnerable to Maritime Hybrid Threats include commercial, cyber (takeover control of machine or ransom of equipment of data), energy, undersea cables, communications, territorial vulnerabilities, and threats to maritime security forces.

Methods to deter Maritime Hybrid Threats :

- Being resilience
- Port control and security compliance
- Political level: attribution and crisis decisions
- Credible and measured response
- Escalation and building off-ramps into response
- Detering state vs proxy actors
- National vs multilateral organizations

Emerging Requirements to Counter Maritime Hybrid Threats:

- Review legal framework and rules of engagement
- A national and EU wide foreign investment screening process for critical infrastructure and sensitive technologies
- Ability to operate and regain control of contested commercial spaces
- Ability to differentiate clandestine hybrid threat vessels from commercial and privately-owned vessels
- Ability to operated and regain control of contested cyber space
- Ability to detect and attribute hybrid threats on shore and at sea
- Ability to operate quickly and decisively in a contested public information environment
- Collaboration of government, private sector, and academia conduct table topic and scenario-based exercises

Tia Lohela, Special Adviser in the European Centre of Excellence for Countering Hybrid Threats, spoke on how the Hybrid Center of Excellence (CoE) supports the institutions and improve response, through the use of:

- Networks
- Conduct trainings
- Participate in exercises and scenario-based discussions
- Develop and analyze trend mapping and intellectual matchmaking
- Recognize and address high level threat

Major (Retired) Athanasios Kosmopoulos, Data Protection Officer, Hellenic Ministry of Digital Policy Telecommunication and Media spoke on domains that are vulnerable to hybrid threats. They include technology, diplomacy, information, infrastructure, economy, legal, military, society, politics, bureaucracy, intelligence, and religion. Tools used to conduct hybrid threats are bots, leaks, hacking, fake news, terror, lack of legislation, blackmail, pressure, and social unrest. To fight hybrid threats, it helps to have a Democracy Sphere, which consists of citizens and institutions. Trust is the critical element needed to create a Democracy Sphere. Trust is the vulnerable area and where the hybrid threat may attack. The main objective of hybrid threat is FUD: It creates Fear, Uncertainty, and Doubt.

Prof Dalaklis Dimitrios, Associate Professor at the World Maritime University spoke on how hybrid warfare is a blend of conventional, irregular, and cyber warfare. Everyone is connected with each other based on personal electronic devices being connected to the Internet. Shipping in the Era of Digitalization is the Fourth Industrial Revolution, which includes cloud computing, mobile devices, IoT platforms, location detection technologies, advance human-machine interfaces, authentication and fraud detection, 3D printing, smart sensors, big data analytics, multilevel customer interaction or customer profiling, and augmented reality. Humans tend to be the weakest link. Advanced technology, education, and trainings are needed to combat the Era of Digitalization.

Peter Cook, Director of PCA Maritime Ltd – Maritime Security Consultant and Lecturer spoke on how the commercial shipping industry is driven by three factors:

- Shipping companies, operators, managers, and charters

- Marine Insurance
 - Hull and Machinery
 - Cargo
 - Professional and Indemnity (P&I)
 - Additional War Risk Premium (AWARP)
 - Kidnap & Ransom
 - Flag State (commercial entities)
 - Top Three Flags by Tonnage: More than 70% of the commercial fleet is registered under a flag which is different from the country of ownership.
 - Panama
 - Liberia
 - Marshal Islands
- Maritime Cyber Risk Management for ships is written based on International Safety Management (ISM) Code from the International Maritime Organization. The forward plan includes quantum computing, 5G, blockchain, AI, robotics and drones.

Dr. Eleni-Maria Kalogeraki from the University of Piraeus, Dept of Informatics spoke on how the CyberSEC4 Europe is establishing and operating a pilot program for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation. CyberSec4Europe

- Aligns and interconnects a vast pool of research excellence in existing centers and research facilities, bringing together cyber security expertise in an interdisciplinary manner while developing a governance model for this activity and the future European Cybersecurity Competence Network.
- It consolidates and reinforces the cooperation and synergies between the research and industrial communities.
- It addresses key EU Directives and Regulations, such as the GDPR, PSD2, eIDAS, and ePrivacy.

CyberSec4Europe's long-term goal and vision is an EU that has all the capabilities required to secure and maintain a healthy democratic society, living according to European constitutional values (e.g. privacy and sharing) and being a world-leading digital

economy.

Maritime Security Standards include:

- International Ships and Port Facilities Security Code (ISPS)
- International Safety Management Code
- EC Regulation No 725/2004 on enhancing ship and port facility security
- EC Directive 2005/65 on enhancing port security
- MSC 96-4-1 - The Guidelines on cybersecurity on board ships
- IMO-PKI guidance 2015
- MSC 96-4-2 - Guidelines for Cyber risk Management
- MSC 96-4-5 - Measures aimed at improving cybersecurity on ships
- IEC: 2016 MARITIME NAVIGATION AND RADIOCOMMUNICATION EQUIPMENT AND SYSTEMS - Cyber Risk Management Guideline

Another keynote speaker was Vice Admiral Alexandru Mirsu ROU (N), Chief of the Romanian Navy. First, he spoke on the evolution of hybrid warfare, which entails four phases – potential military threat, direct military threat, immediate military threat, and military conflict. Second, he discussed the types of hybrid threats to include Special Forces, irregular forces, organized crime, info warfare propaganda, diplomacy, cyber warfare, economic warfare, regular military forces. Third, he provided a map of the Black Sea Region, which is bordered by several countries to include three NATO nations, Bulgaria, Romania, and Turkey, and then discussed the Black Sea challenges and proposed solutions.

Black Sea Challenges:

- Energy resources - both supplier and transport corridor
- Rapid militarization of Crimea and the Black Sea
- Several hotspots at various temperatures (Transnistria, Donbass, Crimea, Azov Sea, Abkhazia and South Ossetia, Nagorno-Karabakh)
- New route for migration, and trans-national crime
- Highway for “Syrian Express” to include being a new route for migration and transnational crime

Proposed solution includes:

- A 360-degree understanding of maritime operational environment
- A holistic approach to include joint, interagency, and multinational elements
- Development of key capabilities
- Effective cooperation

CDR Loreiro Francesco ITA (N) of the Italian Navy General Staff

spoke on maritime vulnerabilities, characteristics of maritime hybrid war, and three case studies. The maritime vulnerabilities are shipping, cyber, energy supply, territorial areas, maritime security forces, information activity such as fake news. The characteristics of maritime hybrid warfare are surprise and camouflage, no certain attribution, ambiguity, inexpensive platforms. The case study on Yemen displayed how Yemen’s coast has been attacked by Houthi militants. The Yemen case study proved that their vulnerabilities were military, economic, and information. The case study on Libya was about terrorist attacks and the vulnerabilities were military and economic. The case study on GPS was air and naval attacks. This case study demonstrated the GPS vulnerabilities are military, economic and safety, manipulation, interference, and loss of signal.

The operational solution includes:

- The use of the military solution
- Multi-entities cooperation to create a resilience, credible, and capable governance
- A joint military approach in which all services and national agencies cooperate and share information to reduce any gaps and vulnerabilities which can be exploited by hybrid and transnational threats.
- A national approach, where ministers, military forces, agencies academics and civil society stakeholders cooperate.
- A comprehensive approach in which all the nations work together with

international organizations and entities such as NATO, EU, UN and civil society, collaborating and coordinating to face these challenges together.

Erivn Prenci, the Senior Project Manager Maritime Security Sub-Directorate from INTERPOL stated over 194 countries connected to Interpol. His highlights were crimes in the phases of chain of custody, global database on maritime security, maritime domain, challenges, and collaborations. The chain of custody, which the proper case hand over process to increase chance of successful prosecution has four main phases. They are: assessing the situation, acquiring the data, analyzing the evidence, and reporting findings. The Interpol global database on maritime security has four goals. The first goal is to collect and store maritime crime information. The second goal is to analyze maritime crime information. The third goal is to produce intelligence products. The fourth goal is to expand their relationships.

Maritime crimes include:

- Maritime Piracy (Hijacking)
- Armed Robbery Against Ships
- Kidnapping for Ransom
- Trafficking (Drugs, Weapons, People, Goods)
- Illegal, Unreported and Unregulated Fishing (IUU)
- Forced Labor/Slavery
- Smuggling Exotic Plants Ocean Waters
- Pollution/Discharging in Ocean Waters
- Document Fraud
- Unauthorized Entry
- Financial Crime
- Cyber Crimes
- Maritime Terrorism (CBRN)

Maritime challenges include:

- Safety from possible situational threats
- Adverse weather and conditions
- Multi-agency and multi-national coordination
- Returning terrorist fighters to hu-

- man trafficking
- Smuggling of drugs, weapons, and contraband
 - Maritime terrorism
 - Interrogating and interviewing suspect
 - Debriefing /interviewing hostages
 - Challenging legal framework

Collaboration with Naval Forces:

- First responders' important partner to combat crime effectively in the maritime domain
- Information exchange mechanism in place with naval forces under national flag (via NCB)
- Information exchange with EU NAVFOR
- HOA: Positive identification of suspects lead to handover for regional prosecution

Alexandra M. Friede from the Helmut Schmidt University/University of the Federal Armed Forces Hamburg – Interdisciplinary Research Network Maritime Security

stressed that threat perceptions matter! Threat perceptions have an impact on nation-state policy-making/priority-setting in security and defense. Shared threat perceptions are an essential factor in enabling and facilitating cooperation in security and defense. Threat perceptions are especially relevant for countering hybrid threats at sea because it requires enhanced cooperation.

Dr. Fotios Moustakis the Associate Professor of Strategic Studies stated that The NATO Parliamentary Assembly Committee (2015) defines hybrid warfare as the use of asymmetrical tactics to probe for and exploit weaknesses via non-military means (such as political, informational, and economic intimidation and manipulation) and are backed by the threat of conventional and unconventional military means.

Modern hybrid warfare threats include:

- Speed of decision-making in lib-

eral democracies is too slow

- Careful formulation of foreign policy
- The hesitancy of some civilian agencies and NGO to cooperate with Defense, hinders attempts to get inside an adversary's decision-making cycle

Skills and priorities entail:

- Reprioritize lost skills of intelligence, such as strategic deception planning
- Practice the effective exchange of information with NGOs and agencies
- Invest sufficiently in human capital, appropriate through-career training and education policy
- Solid professional military foundation, emphasis on cognitive skills to recognize or quickly adapt the unknown
- Small unit leaders with decision-making skills and tactical cunning to respond to the unknown, and the equipment to react or adapt faster than the adversary

There needs to be a culture of innovation, adaptability, and agility of decision-making. Hybrid warfare requires hybrid response.

There were several speakers from Stellenbosch University. Francois Very, a Professor at SIGLA of Stellenbosch University, spoke about hybrid warfare at sea. The professor stated that hybrid warfare is a combination of regular and irregular warfare. At

times the two types of warfare operate independently of each other and other times in conjunction with each other. Dr. Michelle Nel, from SIGLA of Stellenbosch University stated the law is at war with maritime security. There is no law that applies to hybrid war and specifically spoke about the situation in Africa. She stated that Africa has weak governance, poor border and port security, which makes Africa susceptible to hybrid threats and transnational crimes. Captain Mark Blaine, from SIGLA of Stellenbosch University stated the South Africa Development County (SADC) maritime security challenges include piracy and armed robbery, maritime terrorism, trafficking and smuggling, illegal fishing and poaching, and inefficient and insecure commercial ports. However, the one of the major strategic initiatives is the Africa's Integrated Maritime Strategy (AIMS) 2050. The SADC maritime security strategy includes three priorities and three lines of military action in the military concept.

Three SADC priorities are:

- Eradication of Somali piracy in Southern Africa
- Securing West coast of Southern Africa
- Securing Southern Africa's vast rivers and lakes

Three lines of military action in the military concept are:

- Prevention of piracy by reducing maritime vulnerability
- Interruption/termination of piracy

SADC: The Case for a Coast Guard (function)



• Navies vs Coast Guards: African Realities

	Coast Guard	Navy	African Maritime Forces
Missions	Maritime safety, law enforcement, environmental protection, and border security within Exclusive Economic Zone	War, international sea lanes, and foreign policy on high seas/outside of national boundaries	Primarily maritime safety, law enforcement, environmental protection, and border security within Exclusive Economic Zone, some foreign policy and peacekeeping abroad
Assets	Tugs, patrol cutters, aids to navigation, harbor patrol and other small boats, fixed and rotary wing aircraft for search and rescue, interdiction	Amphibious landing ships, surface combatants, vessels for aerial warfare, submarines, support vessels	Hodgepodge of donations, corvettes, small patrol boats, some amphibious landing craft, and submarines
Bureaucratic affiliation	Various: homeland security, department of fisheries and oceans, ministry of infrastructure and transport	Ministry/department of defense	Ministry/department of defense
Training	Operations of assets, coast guard missions	Operation of assets, war	Operations of assets, war
Partnerships	National (judicial, fisheries, ports, etc.)	Military (army, air force, etc.)	National (judicial, fisheries, ports, etc.)

consistent with international law

- Highlighting rights and responsibilities of flag and coastal states

SADC shared the results of their case study as to why South Africa needs a Coast Guard: (Figure, page 36)

The keynote speaker for the third day was **Pawel Hercynski, the Director of Security and Defense Policy European External Action Service**. He stated that the progress of the EU and NATO relationship has grown closer and closer. USA has pressured the EU to do more in security. As a result, a Global Strategy for the European Union's Foreign and Security Policy was developed and is great reference book. Hybrid warfare is countered through intergraded approach. The solution for countering hybrid warfare is to produce an effective and efficient EU Fusion Cell, staff level coordination, and collaborating with USSTATCOM; USSTRATCOM has a critical role countering the adversary that uses hybrid warfare. The goal is to have joint exercises which will include hybrid warfare.

The second keynote speaker for the third day was **Rear Admiral Olivier Bodhuin FRA (N), the Deputy Commander EUNAVFOR MED SOFIA** (European Union Naval Force Mediterranean). He focused on why Europe decided to reconsider its position towards crises near its borders and commits to a common effort to avoid further loss of life in the Mediterranean Sea. As a result, the business operation of smugglers and traffickers was disrupted, and number of irregular migrants was reduced to a manageable level. The core mission of EUNAVFOR MED OPERATIONS SOPHIA is to fight smuggling and to save lives at sea. They represent structured and effective response to tackle migration and to contribute to the stabilization of Libya as a key component of the EU integrated approach. They are a key EU Maritime Security

Provider in the Central Mediterranean successfully countering illicit activities in the high sea and supporting the LCG through training. They are a model of synergy between internal and external security domains of EU required to effectively fight organized crime.

Ezio Lama the Maritime Security Policy Officer from EU External Action Service provided a blueprint of the EU Maritime Security Strategy. The action plan has three main features. The first feature is to have both a civilian/military approach. The second feature of the action plan is to reaffirm the role of the EU as a substantial global maritime security provider. The third feature is to provide a new structure with substantial impact developing regional approaches to global issues (Gulf of Guinea, Horn of Africa, South East Asia, Black Sea, etc.). The action plan is in cooperation with international partners to include the European Commission, United Nations Office on Drugs and Crime, NATO, African Union, and Asean Regional Forum.

John H. Bernhard, the former Ambassador of Denmark to OSCE, OPCW, and IAEA spoke about how hybrid threats not only apply to civilian and military communities, but overall threats apply to nuclear warfare. There are two major nuclear issues. The first issue is nuclear security, which consists of protection against nuclear terrorist (most immediate threat to global security). The second issue is nuclear safety, which are the measures to take to protect people and property from the effect of nuclear activity. The problem is there are no mandatory international requirements on how to transport nuclear material. The International Atomic Energy Agency only provides recommendation, which causes a nuclear security issue. Chemical and biological have better regulations. In 1975, stock piling biological weapons were a total ban. In 1992, chemical weapons banned. There has been some progress with

handling hybrid threats, but government still needs to conduct international cooperation to respond and resolve nuclear security issue.

Nikitas Nikitakos, a Professor at University of the Aegean discussed the four stages of hybrid warfare. The four stages are in this order:

- Demoralization of the target society,
- Destabilization of the target society,
- Precipitation of a crisis in the target society,
- Seizing control of the target society by internal forces acting in concert with the attacker.

Industries that make-up the critical infrastructure are major targets for hybrid warfare. These industries include transportation, communications, electric power, water supply, banking and finance, emergency services, natural gas and oil, and government services. Resilience is a major tool for protection against hybrid warfare. Becoming resilient includes security, risk management, crisis and emergency management, and business continuity.

Borja Montes Toscano from NATO ACO Office of Legal Affairs discussed the Legal Advisor Workshop – Functional Area System (LAWFAS). LAWFAS is a web portal, based on SharePoint, that creates a connected and interactive community of NATO and national legal offices to support, facilitate and improve legal support for the Alliance in its operations and activities.

LAWFAS:

- Has become the only legal tool at the international, operational, and managerial branches
- Provides the only organized searchable repository of legally significant NATO documents (5,000+ and growing);
- Transforms the provision and support of NATO legal advice
- Supported and maintained by a

team of two people – an international lawyer and a SharePoint Administrator

- Number of users:
- Unclassified Network: 765
- NATO Secret Network: 160

Mr. Borja Montes Toscano also spoke on unmanned maritime vehicles. There are challenges at sea to be noticed when using unmanned maritime vehicles such as maritime zones, South China Sea, Crimean delimitation of maritime ships, and seizure of USNS by Chinese authorities. Legal resilience at sea can be reached through the Legal Operations Response Cycle, which includes identification, assessment, strategy, definition, and response.

The unmanned maritime vehicles have several tasks:

- Intelligence, surveillance, and reconnaissance for threatening activities on the surface
- Mine counter measures operations
- Anti-submarine warfare
- Communication/Navigation Network Nodes (CN3)
- Conduct persistent monitoring of known routes employed by terrorists, pirates, or drug smuggler
- Conduct harbor surveys after natural disasters
- Provision of humanitarian relief
- Conduct beach reconnaissance prior to an amphibious assault
- Payload delivery
- Information operations
- Time critical strikes

CLOSING REMARKS

The honorable keynote speaker, Captain Tsakos, Founder and President of The Tsakos Group, stated that it is important for the company to understand maritime operations and more importantly maritime security. With 90% of global trade depending on the shipping industry, maritime security is ABSOLUTELY NECESSARY. The in-depth high standards of his company demonstrate secure transportation

LAWFAS – The Three Pillars

<p>The goal of LAWFAS is to capture relevant documents, facilitate document researches and ensure an easy access to all relevant information NATO-wide, as a Repository</p>	
<p>LAWFAS is an interactive tool, which provides legal support to NATO and Member States and Universities, acts as a Paralegal On-Line Service</p>	
<p>Legal Clinic with the universities (Roma Tre and Paris Pantheon Sorbonne) and research institutions on topics of interest</p> <ul style="list-style-type: none"> • Autonomous Weapons and Humanitarian Access in Non-International Armed Conflicts (2018 Roma Tre) • Detention in NIAC and Updated Commentaries to the 1949 Conventions (I) and (II) (2019 Roma Tre) • Theory of Implied Powers in International Organizations and Subsidiary Organs in NATO Operations and Missions (2019 Paris) <p style="text-align: center; font-size: small;">NATO Unclassified</p>	

LAWFAS – You can find there...

<ul style="list-style-type: none"> • Documents: <ul style="list-style-type: none"> – Treaties: North Atlantic Treaty, NATO SOFA, Paris Protocol... – Agreements: HNS, MOUs, SAs, Garrison Support Arrangements (GSAs), Base Support Arrangements (BSA) – Directives: ACO, ACT, Bi-SC Directive – Standing Operations Procedures (SOPs) – Policies – STANAGs • Workspaces: <ul style="list-style-type: none"> – EU-NATO – Protection of Civilians – Refugee Crisis – Gender Workspace – Roma Tre – Legal Clinic 		<ul style="list-style-type: none"> • Libraries: <ul style="list-style-type: none"> – Hybrid Warfare – Conferences and Courses – Legal Gazette and Ops Newsletter – RAP – Readiness Action Plan • Lists <ul style="list-style-type: none"> – Useful Links <ul style="list-style-type: none"> • LAWFAS Selection • International Organizations • National Repositories • Research Institutions and Journals • International Databases • Calendar Events
---	--	---

of goods by providing use of modern technical advanced ships and staff and personnel that has been trained for daily and defensive maritime operations. The mission of The Tsakos group is strongly supported by the speeches given at this conference, which is a collaboration of the government, military, legal, technology, intelligence, and academia sectors to create a dynamic interactive synergy to ensure maritime safety at the tactical, operation, and strategic level. Every speech for all 3 days responded to Tsakos' statement. Every speech in one form or another responded to how global trade can remain effective and efficient and not become disruptive or at least mitigate risk of maritime attacks.

10th NMIOTC ANNUAL CONFERENCE 4-6 June 2019
Countering Hybrid Threats: An Emerging Maritime Security Challenge

AGENDA

TIME	TOPIC	SPEAKER
4 June 19		
0830-0915	Registration – in processing	
0915-0920	Admin / Security Brief	Lt Cdr Konstantinos Papanastasis GRC (N)
0920-0950	NMIOTC Welcome Address Host Nation Welcome address	Commodore Stelios Kostalas GRC (N) (NMIOTC Commandant) Vice Admiral Nikolaos Tsounis HN Chief of the Hellenic Navy General Staff
0950-1045	Keynote Speakers	Captain Panagiotis N.Tsakos Founder & President of TSAKOS GROUP Mr Michel Soula NATO HQ Head of Operations Section A
1045-1115	Group Photo - German Flag raising Ceremony	
1115-1145	Coffee Break - Networking	
1145-1200	Keynote Speaker	Commodore Marcel Halle CAN(N) MARCOM Deputy Chief of Staff Plans
1200-1330	SESSION 1 Moderator: Dr Alexandros X.M. Ntovas (Director International Shipping Law Queen Mary, University of London) a. Countering Hybrid Threats in the Maritime Environment. b. Hybrid CoE; hybrid threats and maritime domain c. Preventing and responding to hybrid threats: Consolidated Resilience and Holistic Immunity	a. Mr. Chris Kremidas Courtney (US EUCOM) b. Ms Tiia Lohela M. Soc. Sc (Special Adviser in the European Centre of Excellence for Countering Hybrid Threats) c. Major (ret) Athansios Kosmopoulos (Data Protection Officer, Hellenic Ministry of Digital Policy, Telecommunications and Media)
1330-1430	Lunch Break – Networking	
1430-1600	SESSION 2 Moderator: Prof. Nikitas Nikitakos (University of the Aegean) a. The Cyber-Security Element of Hybrid Warfare: Is there a Need to “Formalise” Training Requirements? b. Hybrid threats and the commercial maritime industry c. CyberSec4Europe: “Maritime Transport” Demonstration Case	a. Prof. Dalaklis Dimitrios (Associate Professor (Safety & Security) in the World Maritime University) b. Mr. Cook Peter (Director PCA Maritime Ltd - Maritime Security Consultant and Lecturer) c. Dr. Eleni-Maria Kalogeraki (University of Piraeus, Dpt. of Informatics)
1600-1605	Wrap up of the day	LTC US ARMY Wendi Brown
5 June 19		
0900-0905	Opening Remarks	LTC US ARMY Wendi Brown
0905-1000	Keynote Speakers	Vice Admiral Alexandru Mirsu ROU (N) Chief of the Romanian Navy Mr Samuel Kame – Domguia African Union
1000-1030	Coffee Break - Networking	
1030-1230	SESSION 3 Moderator: Dr. Dinos A. Kerigan-Kyrou (Instructor NATO DEEP) a. Hybrid Threats into Maritime environment – Italian Navy perspective b. Countering hybrid threats – INTERPOL perspective	a. CDR Loreiro Francesco ITA (N) (Italian Navy General Staff) b. Mr Ervin Prenci (INTERPOL- Senior Project Manager Maritime Security Sub-directorate)

	<p>c. Maritime cooperation and hybrid threat perceptions in the Baltic Sea region.</p> <p>d. The Threat of Non-linear War against the West: How do we prepare Hybrid warriors for Hybrid warfare?</p>	<p>c. Mrs Alexandra M. Friede M.A. (Helmut Schmidt University /University of the Federal Armed Forces Hamburg - Interdisciplinary Research Network Maritime Security)</p> <p>d. <u>Dr Fotios Moustakis</u>, MA Hons, MSc, PhD, PGCAP, FHEA (Associate Professor of Strategic Studies, Director of Dartmouth Centre for Sea Power and Strategy, University of Plymouth at Britannia Royal Naval College, School of Law, Criminology & Government)</p>
1230-1330	Lunch Break - Networking	
1330-1500	<p>SESSION 4 Moderator: Dr. Dinos A. Kerigan-Kyrou (Instructor NATO DEEP)</p> <p>a. Hybrid Warfare at Sea: Perspectives</p>	<p>a. Prof. Francois Vrey (SIGLA,</p>

6 June 19

0900-0905	Opening Remarks	LTC US ARMY Wendi Brown
0905-1000	Keynote Speakers	<p>Mr. Pawel HERCZYNSKI Director Security and Defence Policy European External Action Service</p> <p>Rear Admiral Olivier Bodhuin FRA(N) Deputy Commander EUNAVFORMED SOFIA</p>
1000-1030	Coffee Break - Networking	
1030-1215	<p>SESSION 5 Moderator: Mr. Charles Sellers, (Deputy Political Counselor of US Embassy Athens)</p> <p>a. European Union Maritime Security Strategy: the promotion of cooperation with NATO and the efforts to better tackle hybrid maritime threats.</p> <p>b. The International Political and Legal Framework for Addressing Hybrid Threats</p> <p>c. Hybrid threat in Maritime Domain, Case study</p>	<p>a. Mr Ezio Lama (Maritime Security Policy Officer EU External Action Service)</p> <p>b. Mr John H. Bernhard (Former Ambassador of Denmark to the OSCE, OPCW and IAEA)</p> <p>c. <u>Mr Dimitrios Maniatis</u> (Chief Commercial Officer, <u>Diaplous Group</u>)</p>
1215-1315	Lunch Break - Networking	
1315-1500	<p>SESSION 6 Moderator: Mr. Chris Kremidas Courtney (US EUCOM)</p> <p>a. Hybrid warfare and Critical Infrastructure resilience'</p> <p>b. Unmanned Maritime Vehicles: How to build Legal Resilience</p>	<p>a. Prof. Nikitas Nikitakos (University of the Aegean)</p> <p>b. <u>Mr Borja Montes Toscano</u> (NATO ACO Office of Legal Affairs)</p>
1500-1510	Final Wrap up	LTC US ARMY Wendi Brown
1510-1515	Way Ahead	Captain Rosario La Pira ITA(N)
1515-1530	NMIOTC Farewell Address	Commodore Stelios Kostalas GRC (N) (NMIOTC Commandant)

END OF CONFERENCE

Lieutenant Colonel Wendi O. Brown, USAR

LTC Brown was commissioned through the Reserve Officer Training Corp (ROTC) at Howard University in Washington, D.C. Following graduation, she completed Adjutant General (AG) Officer Basic Course (OBC) at Fort Benjamin Harrison, IN. Upon completion of OBC, she immediately went into IRR due to overstrength of the U.S. Army Reserves. LTC Brown's first assignment was a Troop Program Unit (TPU) at the 200th Military Police Brigade in Gaithersburg, MD. Her next assignment was Public Affairs Officer for the Army Morale Welfare and Recreation (MWR) at Fort Belvoir, VA. LTC Brown was brought on active duty and held a number of positions with the Office of Chief Army Reserve at the Pentagon. She was then selected to serve at the Headquarters, Department of Army G-1 Staff. While at the Pentagon, she completed her AG Career Captain Course. Her next assignment was a TPU soldier in the S1 for Headquarters, Defense Logistics Agency at Fort Belvoir, VA.

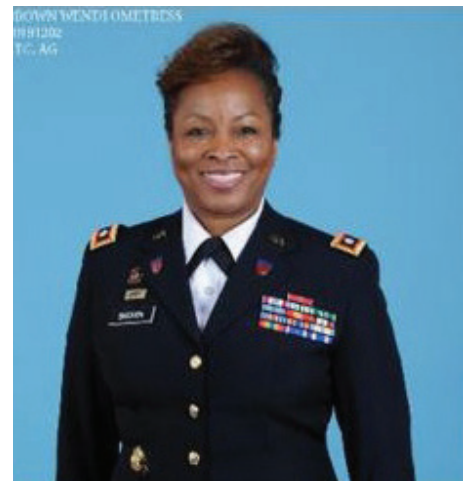
LTC Brown deployed to Afghanistan for one year in support of Operation Enduring Freedom (OEF) under Army Materiel Command as a Retrograde Planner for the first six months and as a Logistics Task Force Commander for the last six months. She

was asked to extend for a second tour in support of OEF for Headquarters, United States Forces – Afghanistan, South Detachment where she was the J7. Upon her return from 18 consecutive months in combat, LTC Brown earned a Project Management Project (PMP) certification and joined the 200th Military Police Command at Fort Meade, MD as the TPU Senior Personnel Officer.

Within a year, she was selected to be an Executive Officer in the J3/Joint Operations Center at the Headquarters, United States European Command in Stuttgart, Germany. In this position, she completed the Intermediate Level Education (ILE), Command General Staff College (CGCS) Distance Learning. While completing ILE, she was also completing her Master of Science in Cybersecurity from the University of Maryland University College. After two years in the J3/Joint Operations Center, LTC Brown was selected as a Coalition Exercise Planner in the J6 C4ISR/Cyber Directorate at Headquarters, United States European Command in Stuttgart, Germany. In this position, she completed Master of Science in Cybersecurity where she graduated in December 2016 summa cum laude, earned her Information Technology Infrastructure Library (ITILv3) certification, and earned her Comp TIA Security Plus (Sec +) certification.

LTC Brown's last assignment was a Joint Operations Center Team Chief for the Headquarters, United States Africa Command in Stuttgart, Germany. Currently, she is assigned to the U.S. European Command in Stuttgart, Germany.

Email: 1wendibrown@gmail



HN Littoral Warfare Med



by Captain Spyridon Lagaras GRC (N)

This article intends to provide an approach in dealing with challenges that are present in the Eastern Mediterranean and is an extract of a presentation in the LITTORAL OPTECH Workshop that took place on the 5th -7th of November 2019 in NMIOTC.

The environment that the Hellenic Navy usually operates in, which includes the Aegean Archipelago and the Eastern Mediterranean, is the littorals and is a place at sea where things that directly affect almost all nations happen. The reason being that half of the world's population lives within 200km from the shore, while at the same time 75% of all sea trade passes, at some point, from the littorals. And, needless to say, sea trade represents 90% of all world trade. So economically wise controlling

the littorals is the essence of sea power. The entire Mediterranean is covered under heavy marine traffic, and the Hellenic Navy has learned to live and operate with ease in its eastern part.

Greeks do not perceive the Mediterranean as just another theatre of operations, they perceive it as their home for which they have intimate knowledge of, since they have been sailing in these waters for more than 4000 years ago. The Hellenic Navy does not need any time to adjust its operations and its personnel's mentality in order to operate in these waters. The challenge that the Mediterranean provides to the navy, could be roughly broken down to five elements which are:

- a. Interstate competition
- b. Terrorism at sea
- c. Organized Crime
- d. Illegal Migration
- e. Environment and energy

Interstate competition is currently on the rise mostly due to the Syrian conflict as well as other destabilizing factors, such as the Libyan civil war or aggressive policies followed by some countries in the area. The East Med is being witness to an unprecedented naval built up from different countries but especially from Russia, whose naval presence in the area is the greatest since the end of the Cold War. The high density of naval units in the area in conjunction with high tension, due to the ongoing conflicts and confrontations, creates a volatile environment that can quickly develop into a crisis. This situation increases both tensions as well as the possibilities for an actual armed

conflict, which due to the confined environment could easily escalate and have collateral damage. A simple but important example of the side effects of interstate competition in the area is the fact that there have been numerous reports from the area east of the Republic of Cyprus on GPS signal jamming and spoofing, affecting not only military but merchant vessels as well.

While terrorism has not yet made an entrance on the shipping lanes of the Mediterranean, the fact that the Middle East as well as a large parts of North Africa are on terrorist turmoil, terrorist attacks like those we witnessed recently in the Persian Gulf cannot be ruled out. In fact they should be expected very soon. Organized crime walks hand-in-hand with terrorism and indeed we are currently actively pursuing crime on the seas, a situation that seems to have an increasing tendency. A new addition to this already tensed environment, is the migration crisis that is on the rise. The migrant fluxes are always present and the fact that the Turkish shores are very close to Greek islands makes the whole situation difficult to regulate, if we want to keep our humane principles.

Also a new addition, are the new carbohydrate deposits that have been discovered in the area, a condition that has created new challenges both for securing the safety of extraction as well as the safety of their transportation.

The Hellenic Navy, as an ever present pillar of security in the area, is actively involved to address all off those issues. First of all, lot of resources are being put into work, in order to achieve and constantly maintain a full situational awareness on the entire region. Of course, the Aegean environment particularly, provides a unique network of islands that are utilized by the Hellenic Armed Forces and the Hellenic Coast Guard in order to install Radars and a plethora of other sensors and systems, constantly feeding the Navy with a real time recognized maritime picture.

The Hellenic Navy in close collaboration with the Hellenic Coast Guard that provides additional sensors and facilities enhancing the RMP process and providing indispensable help in monitoring and regulating the migrant flows in the Aegean. Such an example is the view on maritime traffic in the Aegean which is provided by the Greek AIS stations.

Of course, RMP by itself is of nouse, if fighting units cannot exchange information effectively. What we have found is that the scarcest resource at the moment is bandwidth. For the enormous needs of modern military communications the electromagnetic spectrum is too limited, while satellite communications though reliable, are rather expensive. Taking advantage of the Aegean islands the Hellenic Navy has created a very high bit rate line of sight communications network, skyrocketing the units' ability to safely exchange tactical information, increasing redundancies in an already heavily cluttered environment.

Taking a leaf from the handbooks of littoral warfare, the Hellenic Navy has also invested on shore based missile systems since the 90's and in collaboration with the Hellenic Army artillery on the islands of the Aegean can impose Sea Denial and Sea Control on wide areas. Apart from continuously monitoring every vessel in the Aegean, the Hellenic Navy possesses the capability to strike any hostile ship in the Aegean and in big parts of eastern Mediterranean from at least two different sea or land based systems, in addition to the air-strike capability provided by the Hellenic Air Force, as well as Hellenic Army's attack helicopters. It is essential for all three arms to be working together with a common spirit of jointness and ever-developing common doctrine, items that have received special focus and dedicated training by the Hellenic Armed Forces.

Despite the recent recession that Greece has been through, the Hellenic Navy while not being able to acquire

new units on great numbers, is actively investing in new technologies and is currently in the stage of sea trials for new Greek made unmanned naval systems as well as UAVs. The Hellenic's Navy class 214 (AIP) submarines are amongst the most capable conventional submarines in the world and in conjunction with the rigorous training their crews receive, they are a strong deterrent in the Aegean and the eastern Mediterranean. The ROUSSEN class fast patrol boats, operating under a doctrine that promotes integration and interoperability, thus creating a strong and capable defensive/offensive capability, can project power in the area of operations of the Hellenic Armed forces. At the same time the Navy is actively enhancing its SOF capabilities through new specialized ships and material. The high priority given to the Hellenic Armed forces can be illustrated from the fact that even through fiscal difficulties, Greece is scoring high on the Defense Expenses even among traditionally wealthier countries and despite the economic recession has managed to maintain a strong and reliable Naval force.

Finally, all the above mentioned measures cannot provide actual benefits if you work alone, so the Hellenic Armed forces are building partnerships with other nations, that share the same mentality, in the Eastern Mediterranean. But for partnerships to work effectively, interoperability (the essential ingredient for operational success) depends on improving and sustaining engagement between the partner and allied navies in the Mediterranean. This can only be achieved through sustained commitment to direct and frequent engagement among operational forces. Thus, the Hellenic Navy is currently acting as a "hub", bringing many nations together in the common effort for peace and security, while at the same time has an almost constant participation in UN, NATO and EU operations, within the wider

area of the Mediterranean as well as neighboring seas.

In addition to that, as an example of the close cooperation with various nations in the Eastern Mediterranean, it is worth mentioning the trilateral MEDUSA exercises that are taking place biannually since 2015. The specific type of exercise is actually a follow up of the bilateral exercises Alexandria and Alexandroupolis between Egypt and Greece. The latest MEDUSA 9 exercise took place in November 2019 in the wider area of Crete and South Peloponnese with the participation of a joint force comprised of 14 ships and submarines from Egypt, Cyprus and Greece along

with a strong contingent of Army, Air Force and Marine units from the three nations. Furthermore, the Hellenic Navy regularly exercises with the Israeli Navy as well as Adriatic Sea Navies in ADRION type exercises.

For the future in the area of East Med littorals, it seems that stealth is living on borrowed time. The enormous amount of both sensors as well as non-military open sources, creates an environment where concealment will be difficult or nearly impossible to achieve. It is therefore imperative to use our assets having that in mind. Especially for the Aegean we believe that the future belongs to low cost and partially expendable unmanned

combat systems that in conjunction with a dense network of shore based sensors can provide surveillance in sea, air and subsurface and engage in combat en masse. In the wider Mediterranean area the Hellenic Navy invests in new high seas surface units with enhanced staying power and with long range precision weapon systems that are augmented by unmanned combat systems of all sorts. Modern submarines will remain a crucial factor on the operations, while we will never give up on our well established alliances in the area.

Captain S. Lagaras (GRC-N), Commandant HNTTS

Captain SPYRIDON LAGARAS, Hellenic Navy (HN), was born in Athens at the 9th December 1967. He entered the Hellenic Naval Academy in 1985 from which he graduated in June 1989, as an Ensign.

He has served as Division Officer onboard HS LIMNOS (F451), HS KOSTAKOS (P25), HS ADRIAS (F459) and as Executive Officer on HS SPETSAI (F453). From 2002-2004 he assumed the Command of the Fast Patrol Boat HS VLAHAVAS (P74), a Type 148 FPB. Also he has served as a Staff Officer in C3 Division (Weapon Systems) at the Hellenic Navy General Staff from 2005-2009. From 24 June 2009–12 May 2011 he assumed Command of HS NIKIFOROS FOKAS (F466), an S-TYPE frigate. He has served at the Supreme Headquarters Allied Powers Europe (SHAPE NATO), Mons (Belgium), from June 2011 to June 2014. From 2014 to June 2017 he served as the Chief of Staff of the NATO Maritime Interdiction Operational Training Centre (NMIOTC). From 30 June 2017 to 2 March 2018 he was the Chief of Staff of Frigates Command. From the 9 January 2018 up to the 13 May 2019 he assumed the duties of the Commandant of the Second Frigates Squadron. Since the 14 May 2019 he is the Commandant of the Hellenic Navy Tactical Training School (HNTTS).

He has successfully attended a number of military and civilian schools among which are the following:

- General and Specialized training at the Hellenic Navy Training Center - Speciality in Weapons Systems (1993)
- Naval Postgraduate School (NPS) in Monterey, California USA 1996-1999, where he earned a MSc in Electrical Engineering and a MSc in Applied Physics (Weapons Systems Engineering)
- Hellenic Naval Staff and Command College
- Supreme Joint Staff War College (2005)
- National Technical University of Athens (NTUA), where he earned his PhD in Electrical and Computer Engineering (2008)
- Hellenic National Defence College (2018)

He has participated in multinational operations Desert Shield, Desert Storm, Enduring Freedom, Active Endeavour, Atalanta (CO HS NIKIFOROS FOKAS – F466) and as a Commandant of Operation Sea Guardian (OSG) FOCOPS 19-1 in (Feb 2019).

He is married and has two children.



Libyan Navy and Coast Guard “VBSS Operations” Informative Course

From 26th June to 19th July 2019 NMIOTC provided the VBSS Operation Informative Course in favour of EUNAVFOR MED Operation SOPHIA. The duration was fifteen (15) working days with the participation of forty one (41) trainees from Libyan Navy and Coastguard.

Upon completion, trainees were able to, participate in planning of missions and maritime interdiction basic operations, execute proper tasks as a member of a VBSS Team or as a member of a Security Operation.



Libyan Navy and Coast Guard Maritime Communications Course

From 10th June to 26th July 2019 NMIOTC, in cooperation with “PALASKAS” Hellenic Training Centre, hosted the “Naval and Maritime Communication Course” for Libyan Navy and Coastguard, in favour of EUNAVFOR MED Operation SOPHIA, with the participation of eighteen (18) trainees and one tutor from Libyan Navy and Coast Guard Forces.

The aim of this course was to enhance Libyan Navy and Coast Guard personnel’s skills in Maritime Communications Tactics, Techniques and Procedures (TTPs) within the framework of EUNAVFORMED - Op. SOPHIA.



Course 7000 “MIO in Support of Counterpiracy Ops”

From 1st to 5th of July 2019, the Resident Course 7000 “MIO in Support of Counterpiracy Operations” was conducted at NMIOTC.

In total, 8 trainees coming from 3 countries (Brazil, Greece and Norway) attended the course.



Pilot Course “Radiological Threat in Maritime Operations”

From 9th to 13th September 2019, NMIOTC co organized with US National Nuclear Security Administration (NNSA) the Pilot Course “RADIOLOGICAL THREAT IN MARITIME OPERATIONS” for 29 trainees coming from nine different countries: Australia, Czech Republic, Egypt, The Netherlands, Turkey, Spain, United Arab Emirates, United States of America and Greece.

The objective was to provide specialized training for radiological emergency preparedness and response operations in maritime environment.

The content of the course was delivered by Subject Matter Experts (SMEs) from U.S. Department of Energy and NNSA. The trainees participated in theoretical lectures followed by demonstrations and practical training on board RHIBs and TP ARIS. They revised their knowledge about radiation detectors and radiation protection concepts, radiation search techniques and detection strategies. The course prepared them to plan, command, and control radiation emergency response operation.

The successful outcome of this Pilot Course and positive participants’ feedback are a solid foundation for future iterations to be scheduled for the year 2020.



Course 18000 “Maritime Biometrics Collection and Tactical Forensic Site Exploitation”

From 9th to 20th of September 2019, the Resident Course 8000 “C-IED Considerations in Maritime Force Protection (MFP)” was conducted at NMIOTC premises. The objective of the course is to address the existing and emerging C-IED threats, focusing on those faced by vessels when operating in confined and shallow waters as well as in non friendly ports. In total, 15 trainees coming from 9 countries (Bahrain, Egypt, Greece, Italy, Morocco, Slovenia, Spain, Tunisia, United Arab Emirates) attended the course. Lectures and practical drills were delivered by NMIOTC Sea Trainers and Instructors in cooperation with augmenters from the UK, Greek Army and Hellenic Police.



Course 8000 “C-IED Considerations in Maritime Force Protection (MFP)”

From 9th to 20th of September 2019, the Resident Course 8000 “C-IED Considerations in Maritime Force Protection (MFP)” was conducted at NMIOTC premises. The objective of the course is to address the existing and emerging C-IED threats, focusing on those faced by vessels when operating in confined and shallow waters as well as in non friendly ports. In total, 15 trainees coming from 9 countries (Bahrain, Egypt, Greece, Italy, Morocco, Slovenia, Spain, Tunisia, United Arab Emirates) attended the course. Lectures and practical drills were delivered by NMIOTC Sea Trainers and Instructors in cooperation with augmenters from the UK, Greek Army and Hellenic Police.



Course 5000

“Maritime Operational Terminology Course” (MOTC)

From 16th to 27th September 2019, the NMIOTC Maritime Operational Terminology Course (MOTC) was conducted at NMIOTC premises with the support of NATO Allied Command Transformation (ACT).

The aim of the course was to instruct NATO and partners maritime and military officials in Maritime Operations Terminology and explain operational procedures in order to prepare them to take part in NATO-led Maritime Operations and Exercises. The course was attended by 15 trainees, from 10 countries (Azerbaijan, Bahrain, Bulgaria, Colombia, Egypt, Greece, Tunisia, Turkey, UAE and Ukraine). They had the opportunity to work closely and share their experience with NMIOTC and US Navy Instructors.

Upon completion of the training, trainees improved their knowledge in the terminology and procedures used in NATO publications and doctrines and became more interoperable with NATO forces during NATO/PfP/MD/ICI/PatG maritime exercises or NATO-led maritime operations. MOTC also enhanced the participant’s understanding of how to plan and execute such exercises in accordance with NATO publications in a simulated environment. Graduates acquired the skill set necessary to integrate easily into staffs or Tactical Groups participating in NATO-led maritime operations and exercises. Upon completion, trainees were able to, participate in planning of missions and maritime interdiction basic operations, execute proper tasks as a member of a VBSS Team or as a member of a Security Operation.



Hybrid Threat Event Experts Panel

The Hybrid Threat Event Experts Panel co-organized by the US Institute for Security Governance (ISG) and NMIOTC was held in the Center’s premises from 17th to 19th Sep 2019.

During these three days, nineteen (19) experts coming from twelve (12) different NATO and Partner nations and representing the military, academia, public and private sector National and international Agencies and Organizations, provided invaluable inputs in order to identify, understand and address the issue of “Countering Hybrid Threats in the Mediterranean and Black Sea Region”. An extensive Comprehensive Approach led to identifying and analyzing the threats, current conditions, factors, vulnerabilities, Stakeholders and ways to counter current and future Hybrid Threats.

A “food for thought “ report will be issued by NMIOTC and US ISG which will summarize the forum’s outcomes in order to enhance awareness, knowledge, expertise and benefit the built-up of Hybrid Threat resilience in general.



Course 25000
“Drafting, Production and Maintenance
of NATO Standards Course”

From 30th September to 4th of September 2019, Course 25000 “Drafting, Production and Maintenance of NATO Standards” was delivered at NMIOTC premises, with the cooperation of Warsaw Military University of Technology (MUT), HNDGS and NATO Standardization Office (NSO). The course provided comprehensive knowledge to facilitate understanding of the procedures for development, production and maintenance of NATO standardization documents. In total, nine (9) lecturers and twenty six (26) trainees coming from twelve (12) countries attended the course.



Course 21000
“Medical Combat Care in Maritime Operations”

Resident Course 21000 “Medical Combat Care in Maritime Operations” was conducted at NMIOTC’s premises from 30th Sep to 11th of October 2019.

The goal of this course was to transfer knowledge and enhance trainees’ skills so as to provide combat medical care from the point of injury in the mission/theatre to the final transfer to the closest Medical Treatment Facility.

Eleven (11) participants from three (3) countries attended the course (Greece, Lithuania and USA). Training was delivered by US National Association of Emergency Medical Technicians (NAEMT) instructors and other augmenters specialized in Stress Management, telemedicine 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 regulations.



Course 2000 “Boarding Team Classroom Issues” & 3000 “Boarding Team Practical Issues”

The resident courses “2000” and “3000” were conducted at NMIOTC’s premises from 7th to 18th October 2019. The course “2000” provided the theoretical training to Boarding Teams’ personnel to better plan and conduct boarding operations. The course “3000” which followed focused on the associated practical training for safe and effective Maritime Interdiction Operations. In total, 19 trainees from 6 countries (Colombia, Egypt, Greece, Jordan, Montenegro, and Ukraine) attended both courses.



Course 12000 “C-IED in Maritime Interdiction Operations”

The Resident Course “12000” was conducted at NMIOTC premises from 14th to 18th of October 2019. This “NATO Approved” Course fills an operational gap in capability and contributes to counter-threat operations conducted by Boarding Teams when searching for securing and exploiting evidence, which are fundamental to the counter-threat process. The aim was to educate and train international Boarding Team personnel in NATO TTPs (Tactics, Technics and Procedures) to undertake expedient weapons intelligence tasks on board vessels and other maritime infrastructure in support of C-IED operations. In total, 8 (eight) trainees coming from 4 (four) countries (Greece, Italy, Switzerland and U.A.E) attended the course.



Course 14000 “Maritime IED Disposal” (M-IEDD)

Resident Course 14000 “Maritime IED Disposal” was conducted at NMIOTC’s premises from 21st to 25th of October 2019. The aim of this course was to educate and train EOD personnel to competently undertake IEDD Operations on-board vessels and other maritime infrastructure in support of C-IED and relevant operations. The training covers the subject concepts, philosophy and principles, equipment, ship insertion and maritime focused on IEDD methodologies, and best practices in the maritime environment.

In total, 15 trainees from 7 countries (Belgium, Canada, Germany, Greece, Italy, Latvia and U.A.E) attended the course. Training was delivered with the participation of Subject Matter Experts (SMEs), in cooperation with NMIOTC Sea Trainers.



Multilateral Exercise “MEDUSA 9”

In the context of the multinational exercise “MEDUSA 9” and under the auspices of HNDGS, NMIOTC provided a tailored practical training package to 53 members of SOF Teams and Boarding Teams from the participating Nations and 101 Cadets of the Egyptian Naval academy, focusing at improving their skills and performance in support of Maritime Interdiction and security in maritime domain.

On Saturday 2nd of November, the Deputy Chief of the HELFLEET Rear Admiral I. Drymouisis GRC (N) accompanied by Rear Admiral Hesham Safwat Mahamed EGY (N) Alexandria Naval Base Commander, Captain Th. Chatzopoulos GRC(N) Tactical Commander of exercise and the Commanding Officers of the Naval Units that are participating to the exercise, visited to NMIOTC premises. During their visit they were briefed on the mission, roles and activities of NMIOTC.

On Tuesday 5th of November, an Egyptian delegation consisting of Major General Osama Mohamed Helmey Farag Elsaïd EGY (AF), Major General Tarek Abdalla Ahmed Abdalla EGY (M) and Commodore Mahmoud Ibrahim Abdelfatah EGY(A), visited to NMIOTC premises. During their visit they were briefed on the mission, roles and activities of NMIOTC the delivered training during the subject exercise and additionally they had the opportunity to discuss the potential for future training of Egyptian armed forces in NMIOTC premises.



Littoral Op Tech – East MED Workshop in NMIOTC

The fifth in a series of regionally focused Littoral Operations and Technology Workshops was hosted by NMIOTC from 5th to 7th November 2019.

The purpose of the workshop was to acquire/ expand the geostrategic understanding of coastal areas of the Eastern Mediterranean and exploring operational and technological challenges to their security and defense.

The workshop was attended by 52 highly ranked officials, scientists, researchers, analysts and specialists from 12 countries (Canada, Egypt, Germany, Greece, Israel, Italy, Netherlands, Norway, Poland, Sweden, UK and U.S.A.).



Memorandum of Understanding (MOU) between NMIOTC and Deloitte Greece

The NATO Maritime Interdiction Operational Training Center and Deloitte Greece have signed a Memorandum of Understanding for the development of partnership, with regards to the exchange of know-how in areas of common interest. Such areas of cooperation include inter alia Cyber Security, Management and Administration, implementation of Quality Assurance and Best Practices procedures.

The conclusion of the cooperation agreement took place on September 30, 2019 at the NMIOTC premises in Souda Bay, Crete. NMIOTC was represented by the Commandant, Commodore Stelios Kostalas GRC (N), and Deloitte Greece by the Head of the Legal Department, Mr. Emmanouil Asikis.



Inauguration Ceremony of NMIOTC Coastal Urban Training Area (CUTA)

The official Inauguration Ceremony of the newly developed NMIOTC Coastal Urban Training Area was held on Wed 13 Nov 19.

The ceremony was attended by the Commandants of local Greek and US military authorities the Commanding Officer and a delegation of staff officers of NAVSCIATTS and US SOCOM along with Military Attaché from the US Embassy in Athens. The Multi-Purpose Coastal Special Ops Area ("Kill-Vill"), a configuration of a Coastal urban landscape not only will diversify NMIOTC's training capabilities but also it will be another powerful tool in NMIOTC's training toolbox by incorporating new training concepts in areas like:

Hostage Release Ops, Coastal Counter Terrorism & Anti-Piracy Ops, Urban Warfare Techniques, Tactical Sweep & Breaching TTPs, Critical Coastal Installations Security Ops and Non combatant Coastal Evacuation Operations.



Visit of Com NAVSCIATTS and US SOCOM Delegation

The Commanding Officer and a delegation of staff officers of NAVSCIATTS and US SOCOM along with a Military Attaché from the US Embassy in Athens visited NMIOTC on 13th Nov 19.

The scope of the visit was to endorse and exchange Letters of Intent and discuss future cooperation between NMIOTC and NAVSCIATTS (US SOCOM).

In addition they had the opportunity to participate to the official inauguration ceremony of NMIOTC newly developed Coastal Urban Training Area as well as to be informed about NMIOTC's mission, facilities, training and transformational capabilities.



Pilot “Enhanced Maritime Capacity Seminar”

NMIOTC delivered the Pilot “Enhanced Maritime Capacity Seminar” (11-13 Nov 19 and 18-20 Nov 19), under the auspices of HNGS, attended by nineteen (19) staff and vessel officers from “MARIA TSAKOS Foundation”.

The objective of the seminar was to increase Maritime Awareness and familiarize senior merchant shipping personnel, with various aspects of Maritime Security spectrum, under the NATO CIV-MIL Cooperation Policy.



Maritime Sniper Course

NMIOTC delivered the “Maritime Sniper Course” (15th - 20th Dec 19), conducted by ISTC Sniper Section’s Instructors and it provided participating trainees with the opportunity to conduct sniper shooting from moving land, maritime and airborne platforms against immobilized and moving floating targets. attended by sixteen (16) trainees from six (6) countries.





*LIBYAN CG & Navy VBSS Ops Informative Course,
May 1-19, 2019*



*HMCS HALIFAX Boarding Team training,
September 2-5, 2019*



*Training of Hellenic Navy Command Team in Simulator,
September 02-06, 2019*



*Training of Kazakhstan Coast Guard,
September 09-17, 2019*



*Training of ITS FASAN Boarding Team,
September 09-13, 2019*



*Training of GRC EMAK (Special Disaster Unit),
September 19-20, 2019*



*Training of DEU Forces for Boarding Deployment,
October 14-25, 2019*



*Training of ITS MARTINENGO,
October 29 - November 01, 2019*



*Exercise NIRIIS 19,
November 23-24, 2019*



*Swedish SOF Team Training,
November 25 - December 4, 2019*



*Trilateral Special Boat Team Training,
December 2-13, 2019*



*Training of Polish SOF Team,
December 09-20, 2019*



*Visit of NATO Assistant General for Defence Investment Division,
Mr. Gordon "Skip" Davis Jr.
July 1, 2019*



*Southeast Europe Brigade (SEEBRIG) visit,
July 9, 2019*



Visit of Delegation from the Nikola Vaptsarov Navy Academy of Bulgaria, July 24-25, 2019



Visit of SNMG2 Commander Task Unit, Captain Joachim Brune DEU (N), September 16, 2019



*Visit of the D.A. of Egypt, Colonel Mohamed Marei EGY (AF)
September 20, 2019*



*Visit of DACOS J4 PJHQ Colonel John McCrann,
October 2, 2019*



*Visit of NRDC-GR DCOS PLANS,
Brigadier General Manlio Scopigno ITA (A)
November 19, 2019*



*Visit of NSOS Dean of Academics,
Lieutenant Colonel Joseph Harding CAN (A),
December 4, 2019*



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

