Welcome to the 10th NMIOTC Annual Conference! The annual conference was held on Jun 4-6, 2019 at the NMIOTC in Crete, Greece. This year at the conference there were speakers the delivered a wealth of knowledge regarding hybrid threats and solution. Discussed in the article are highlights of the speakers, but complete in-depth notes of the 3-day conference can be requested from Lieutenant Colonel Wendi Brown at 1wendibrown@gmail.com.

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 statement that stimulated conversation 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 good by providing the use of advanced modern technical ships, effective and efficient operational processes and procedures, and staff trained for daily and defensive maritime operations.

The second keynote speaker was Mr. Michael Soul who is the NATO HQ Head of Operations. He stated 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 being a quick responder.
- How to handle internationals cooperation and promote partners to create synergies.

Commodore Marcell Halle CAN (N) from MARCOM Deputy Chief of Staff Plans gave the introduction speaking how hybrid threats and warfare is 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 Being technologically outdated creates emerging security challenges against critical infrastructures (which include attacks against submarine cables and oil pipelines), energy,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 solutions to hybrid threats and warfare is a combination of U.S. Strategic Command (USSTRATCOM), intelligence, surveillance, reconnaissance (ISR) equipment, and Special Forces.

The conference sessions started with **Chris Kremidas Courtney, 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 means a threat to 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 for deterring Maritime Hybrid Threats include:

- Being Resilience
- Port Control and Security Compliance
- Political Level: Attribution and Crisis Decisions

- Credible and measured response
- Escalation and building off-ramps into response
- Deterring 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 citizen 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: create 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 Resolution, 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/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 are 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 cybersecurity 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 are 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 4 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, whose 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

- 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 Franceso 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 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 their vulnerabilities were military, economic, and information. The case study on Libya were about terrorist attacks and the vulnerabilities were military and economic. The case study on GPS were 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 The strategic solution includes:
- 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 works 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 human 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 maritime
- 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 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.

Threats presented by Modern Hybrid Warfare:

- Speed of decision-making in liberal 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:

- 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 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. D**r. 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

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

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.)

The keynote speaker for the third day was **Pawel Hercynski, the Director of Security and Defense Policy European External Action Service.** He stated the progress of the EU and NATO relationship has grown closer and closer. USA has pressured 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 it 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 were 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 has 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 requirement 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.

Dimitrios Maniatis, the Chief Commercial Officer of the Diaplous Group. DIAPLOUS Maritime Services Maritime Services is a leading maritime security provider, delivering first class services to an ever-expanding portfolio of shipping companies from all over the globe, including some of the largest oil majors. The Company's mission is to provide the shipping industry with a wide range of efficient solutions. In particular, they provide unarmed and armed services within the High Risk Area in the Indian Ocean, and they are also prepared to offer similar services in West Africa and other piracy areas, whenever the existing situation allows. The company continually improves the suitability, adequacy and effectiveness of its IMS (Integrated Management System), while evaluating its objectives and continuing suitability, adequacy and effectiveness through the Management Review procedure, so it can achieve its goals, taking into account a number of parameters which include the Company's performance, incidents reports, training needs and customers' evaluation.

Nikitas Nikitakos, a Professor at University of the Aegan 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, and 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, and banking and finance, emergency services, natural gas and oi, and government services. Resilience is a major tool for protection against hybrid warfare. Becoming resilience includes security, risk management, crisis and emergency management, and business continuity.

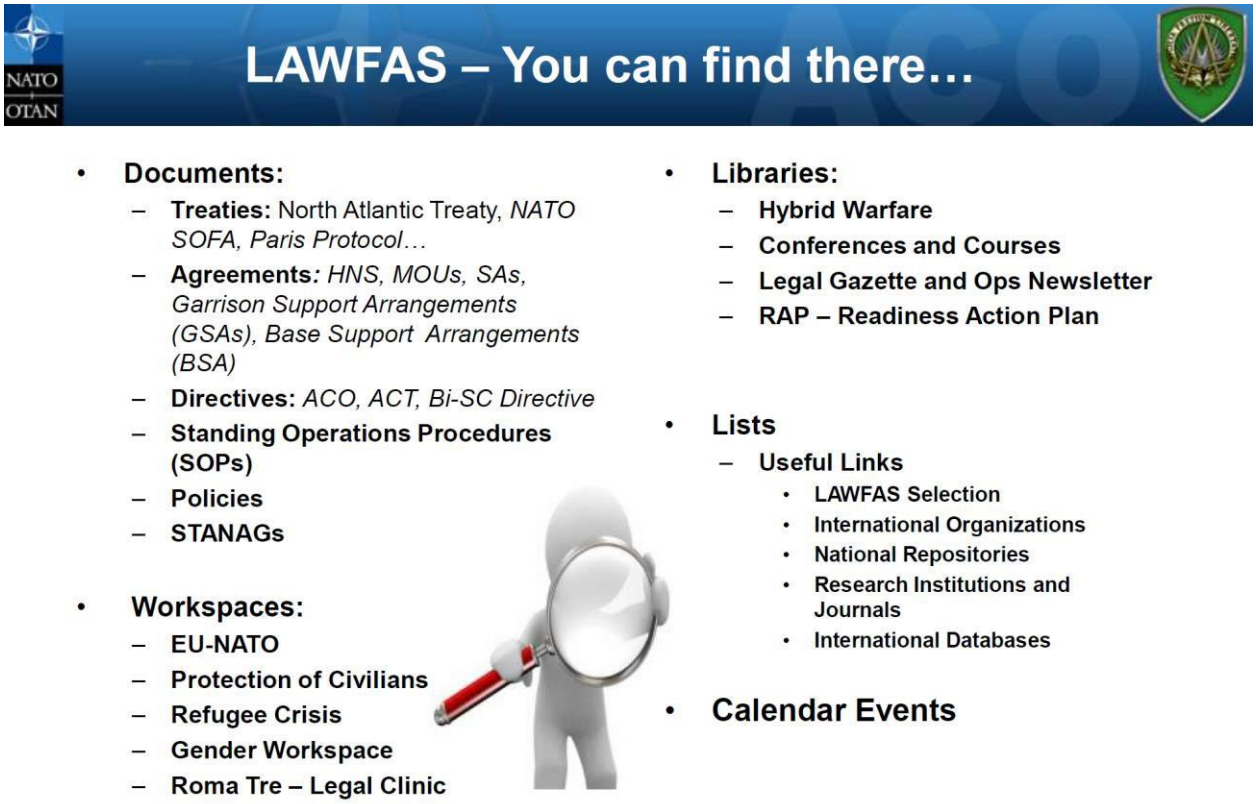
Borja Montes Toscano from NATO ACO Office of Legal Affairs discussed the Legal Advisor Workshop – Functional Area System (LAWFAS). LAWFAS is a web portal, based on SharePoint, that creates a connected and interactive community of NATO and national legal offices to support, facilitate and improve legal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

LAWFAS – The Three Pillars

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	
LAWFAS is an interactive tool, which provides legal support to NATO and Member States and Universities, acts as a **Paralegal On-Line Service**	
Legal Clinic with the universities (Roma Tre and Paris Pantheon Sorbonne) and research institutions on topics of interest • **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)	

NATO Unclassified



Mr. Borja Montes Toscano from NATO ACO Office of Legal Affairs 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 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 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.