# 12th NMIOTC Annual Conference Speakers' Inputs

The 12th Annual NMIOTC Conference «Opportunities and threats from Innovative and Disruptive technologies: Shaping the future of Security in the Maritime Domain» was held on June 1-2, 2021 at the NMIOTC in Souda Bay, Crete, Greece. In the beginning Commodore Charalampos THYMIS, the NMIOTC Commandant, welcomed the attendees. This year was another unique experience because COVID kept many of the speakers and participants from attending physically the conference. However, the conference that was conducted in blended mode, with in-person and virtual participation, still presented speakers that delivered valuable knowledge and information about emerging disruptive technology that is necessary for maritime security challenges. Wendi O. Brown, Lieutenant Colonel U.S. Army Reserve, provided this report. (email: 1wendibrown@gmail.com).

**June 1, 2021 –Keynote Speeches**

**Keynote Speaker: Rear Admiral Rene TAS**
**ACOS Capabilities in Headquarters SACT Norfolk**

We are leaving in a very transformational time and the speed of the change has been increasing in the last decades with big impact in our profession as war fighters. This is especially true in the maritime domain, where innovative technology, such as Artificial Intelligence and unmanned systems, are pushing us to re-evaluate and rethink doctrines and strategies that have been in place since the advent of the modern naval warfare. It is very important for NATO to be at the forefront of this path. NATO has many future programs in place that will enable the Alliance to stay one step ahead in the coming years. One example is the Dynamic Messenger exercise that is an unmanned system exercise planned for 2022 that will be a large-scale test to demonstrate unmanned systems capabilities in the maritime domain and in operational environment. NATO must be prepared for the involvement of new technologies in warfare, including in congested water environment. Our adversaries are planning to challenge us in all domains and we must be prepared to fight in such multidomain scenario. As we deepen the discussion of this topic, everyone will be mindful on how much new and disruptive technology will impact our work in the maritime domain now and in the years to come and also on how we, as the Leadership of the NATO maritime enterprise, are entrusted by all nations to ensure the Alliance remains the global leader in innovation. By doing so we will continue to provide free and safe use of the seas to all our nations, so that prosperity can be maintained and achieved as it has been since the founding of the Alliance over 70 years ago.

**Keynote Speaker: Vice Admiral Manuel Martinez, Director for Engineer and Naval Shipbuilding at Division de Planes del Estado Mayor de la Armada**
**Title: New Challenges and Technologies for current and future Spain Navy Warships**

Effective military capabilities can take decades to research, develop, procure, field and integrate. But new threats can emerge with little warning. To address this imbalance, European militaries, and the European Defense Agency (EDA) must plan ahead to anticipate future capabilities needs and adapt to the fast pace of change in the technology and threat environments.

U.S. Government Accountability Office states four broad categories for emerging threats:
• Adversaries Political and Military Advancements
- Chinese Global Expansion, Russian Global Expansion, Iranian Political and Military Developments, North Korean Military Developments
- Foreign Government Capacity and Stability
- Terrorism
- New Alliances and Adversaries
• Dual-Use Technologies
- Artificial Technologies
- Quantum Information Science
- Internet of Things
- Autonomous and Unmanned Systems
- Biotechnology
- Other Emerging Technologies
• Weapons
- Weapons of Mass Destruction
- Electronic Warfare, Hypersonic Weapons, Counterspace Weapons, Undersea Weapons, Cyber Weapons
- Missiles
- Intelligence, Surveillance, and Reconnaissance Platforms
- Aircraft
• Event and Demographic Changes
- Infectious Diseases
- Climate Change
- Internal and International Migration

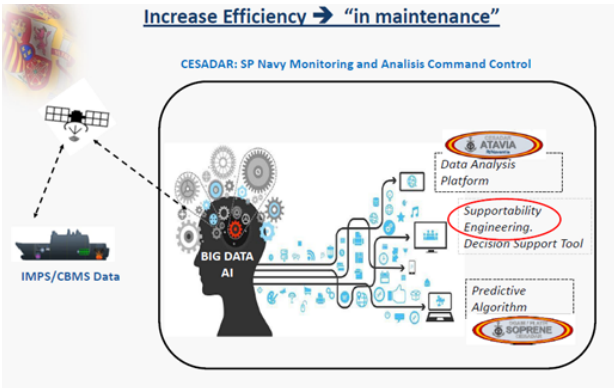
From Spain's Navy
• Several Enabling Technologies:
- Artificial Intelligence, Quantum Computing, Nano Technology
- Cloud Computing

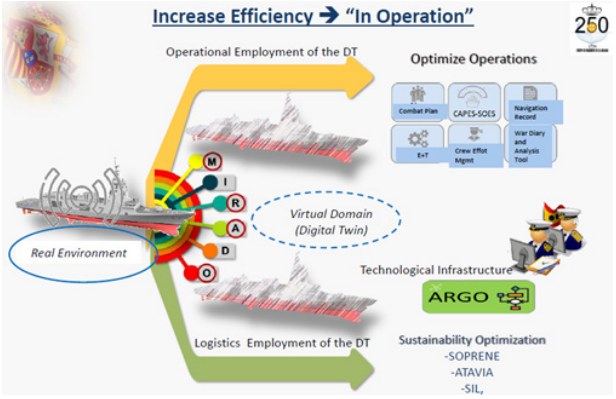
- Unmanned Vehicles, Robotics

• New Battlefield
- Cyber Space
- Cognitive Space (IW)
- Legitimate Battlefield
- Public Opinion Battle Space

• New Weapons
- Hypersonic Weapons
- New Generation of Submarines
- UXVs
- Cyber Attacks

• New Framework – New Scenarios
- No declared enemies
- No governance
- Open to
    - A variety of missions
    - Very Different Stakeholders
    - Disruptive Tech
    - Open information
- Technology is available to everyone
- Reduction of development cycle


Spain Navy Project 4E
4E is envisioned as block of "technological projects" to develop capabilities to be included in a number of different future European combat escorts which will be built by European Industry.

The three technological projects are:
• AAW Destroyer 7000T
• ASW Frigate 6000T
• Multipurpose Frigate 4000T

**Keynote Speaker: Brigadier General Davide Re Italian Air Force, NATO Strategic Direction – South (NSD-S) HUB Director**
**Title: Opportunities and threats from innovative and disruptive technologies: Shaping the future of security in the Maritime domain**
NSD-S Hub Mission
Be a Virtual Docking Station that shares comprehensive information sharing, anticipates threats and challenges (Horizon Scanning), and identifies opportunities in the assigned area of interest with a wide variety of International/ Regional actors.
NSD-S Hub Vision
A focal point for NATO to interact and cooperate with relevant Actors, integrate the regional perspective into NATO mindset, and assist Partners to contribute to projecting security and stability.
Innovative technologies are necessary, because of the complexity of modern society fast evolving dynamics among which the growing dependence on technology and "internet of things".
Just as a mere reference and example, 97% of internet traffic and $10 trillion in daily financial transactions pass through 1.2 million km under-sea cables: this means that everyone of us may be affected and victim of potential cyber-crimes, also in remote locations.
How innovative disruptive technologies impact Africa and the Middle East
• Technological change has been even more transformative and disruptive for the global South than for Europe and North America.
• Waterways in the Middle East could easily become chokepoints and secure maritime domain maximizes the gains for Africa.
• Understanding technological innovation is necessary to secure the maritime environment.

Dynamics of the Horn of Africa (HoA)
• HoA hosts 1/3 of African population and attracts many Global Powers striving to control its natural resources and trade routes (10% of world global trades).
• International disputes, instability areas, unemployment and marginalization as promoters of VEOs and foreign ter-

rorist networks.
• Maritime security and thorough understanding of main drivers of instability is key to protect the routes crossing the Gulf of Aden and the Red Sea.
• International cooperation and dialogue to ensure Freedom of Navigation from Bab al Mandab to the Suez Canal.

Energy Security
Recent history has shown how fundamental is the protection of Critical National Infrastructures in a wide array of evolving challenges and threats (e.g., weaponized drones, cyber-attacks, malwares, etc.)
• Attacks on Infrastructures & Routes:
- Chokepoints (supply disruption)
- Kinetic Attack (vulnerable targets)
- Cyber Attack (increasing digitalization)
• Deniability Strategy:
- Use of non-State Actors/Proxies
- Cyber Domain Anonymity

NSD-S Conclusion:
Foster HUB network to better understand potential risks and possible opportunities with selected International/Regional Actors through mutual respect and with an African and Middle-Eastern point of view.
Focal point for NATO on different Areas of cooperation to enable support to Partners and to Non-NATO Partners in projecting security and stability.
Only a joint coordinated effort is key to enhance understanding of EDTs capabilities, while exploring viable solutions, possible applications and trustful cooperation to tackle together today and tomorrow's threats and challenges.

**Keynote Speaker: Rear Admiral Jean-Michel Martinet, Deputy Operation Commander of EUNAVFOR MED Operation "IRINI"**
**Title: European Naval Forces in the Mediterranean - Operation IRINI**

Core Task: Countering Illicit Arms Trafficking (CIAT)
UN Security Council Resolutions:
• UNSCR 1970 (2011) – Establishing the Arms embargo
• UNSCR 2292 (2016) – Authorizing boardings and diversions
• UNSCR 2578 (2021) – Extending UNSCR 2292 mandate up to 3 June 2022
Secondary Tasks:
• Gathering Information Oil Smuggling: UNSCR 2146 (2014), UNSCR 2362 (2017), UNSCR 2509 (2020), UNSCR 2571 (2021),
• Contribution to the Human Smugglers Business Model disruption
• Training and Monitoring LCG & N

Summary of CIAT & GIOS Results


**Lecture: EU Coordinated Maritime Presences: Where do we stand and what's next**
**Captain (Navy) Stathis KYRIAKIDIS (EL N), Head of Division OPS Coordination, European Union Military Staff, Deputy Director of the EU Maritime Area of Interest Coordination Cell (MAICC)**

EU Coordinated Maritime Presences Concept:
• It is complementary to the EU Maritime Security Operations
• It creates new opportunities to enhance EU presence beyond the ongoing CSDP operations
• It maximum benefits from the EU M-S' naval presences around the globe
• It does not affect the EU's ability to launch a CSDP Operation
• The military assets remain under national OPCON

The role of the EU CMP Maritime Area of Interest Coordination Cell (MAICC):
• It collects situational awareness information based – mainly - on the parent OHQs' reports and open sources
• It analyses and disseminates strategic assessments, within the EU M-S
• It establishes relations with maritime partners
• It is not a Maritime Operations Centre (no shift rotation)

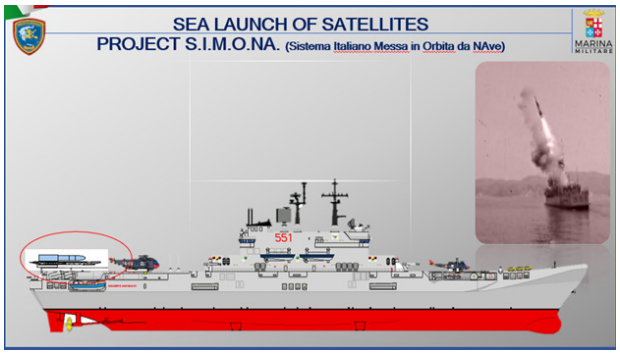
**Lecture: Dilemmas of Deterrence in an Era of Emerging Destructive Technologies**
**Professor James Henry Bergeron, Political Advisor to the Commander Allied Maritime Command**

Does Emerging Destructive Technologies undermine or stabilize our ability of deterrence? Some scholars see Emerging Destructive Technologies as stabilizing while others view it as destabilizing.

Three things to consider when using deterrence:
• Mutual sphere of activity
• Requires knowledge of adversary capabilities
• Requires specific parameters of time

**Lecture: Innovation technologies in the Italian Navy – the future combat naval system in the 2035 multi-domain operation**
**Captain Marco Casapieri, Chief of Space Section of the Italian Navy General Staff**

Starting from 2020, ITN created the Technological Innovation Network, led by the General Staff, which connects all the Technical Centers of the Navy and oversees the ITN main technological areas of interest in which it is strategical to achieve/maintain a competitive advantage (underwater, AI, Quantum, Robotics, Autonomy, sensors and weapons against the hyper-sonic threat, air-independent energy sources and technologies related to space domain).
The Future Combat Naval System 2035 project is based on macro capabilities drawn from these technological areas of interest, encompassed in a specific operational framework.
The FCNS35 macro capabilities are declined by the operational environments (Surface, Underwater, Air, Littoral, Space) or identified by their transversal effects (Unmanned Systems, Multi Domain C2, Enhanced Maritime Situational Awareness, Harbour and critical infrastructure protection, Key Enablers).




**Lecture: Modern technological threats from a ship-owner's perspective**
**Dr. George Pateras, Hellenic Shipping Chamber**

Technological challenges in the maritime industry
• Communication/"Big Data Transfer". Developing the effective means to pass info to the end user.
• Detection of GPS navigation system jamming attempts.
• Creating backups for cyber attack cases.
• Variations on how necessary autonomous ships are and whether they are worth the risks.
• Insurance exclusions for computer viruses.

Despite the negative applications that may disrupt seaward trade, innovative technologies are a must for the, environmentally friendly, development of the supply chain.

**Lecture: Commercial and military use of unmanned/ autonomous vehicles in the light of hybrid threat**
**Commander Georgios Giannoulis, Hybrid Center of Excellence**

There are 4 degrees of autonomy
• Ships with automated processes and decision support.
• Manned but remotely controlled ships.
• Unmanned and remotely controlled ships.
• Fully autonomous ships.

Advantages of Unmanned/ Autonomous Marine Vehicles
• Operating for prolonged period of time without burdening and endangering crew personnel.
• Can support various missions, ranging from recreational and commercial uses to those of militaries
• Minimize operational costs for shipping companies (increased cargo capacity due to absence of accommodation spaces, decrease of fuel consumption by incorporating green power, savings from crew salaries)
• Military applications
- minimize the casualties in case of war conflict
- Force multiplier in the battlefield,
- Perform different types of operations (ISR, AAW, ASW, ASuW),
- Operate without any limitations in NBC environment.
- Offer high level of stealth characteristics and difficulties in attribution, key ingredient for hybrid campaign
- Are ideal for a hybrid actor in controlling the escalation level in low-intense conflicts

Challenges of Unmanned/ Autonomous Marine Vehicles
• Outdated or missing regulatory framework
• Possible absence of human decision-making process
• Vulnerable to cyber attacks
• Congested information to be processed from multiple sensors can lead to serious failure

**Lecture: Windward's Predictive Intelligence Platform. A maritime AI platform to manage all maritime domain awareness and intelligence needs.**
**Mr. Dror Salzman, Windward Intelligence Research Manager**

Deceptive Shipping Practices:
• AIS Handshake
• Global Navigation System Manipulation

Windward supports operational missions and intelligence analysis with Maritime AI to critical organizations.

• Maritime Intelligence
• Law Enforcement
• Defense

**Lecture: EU-NATO Cooperation in Maritime Situational Awareness: Advancements and Limitations**
**Mr. Joao Almeida Silveira, Independent Policy Analyst, Research at Portuguese Institute of International Relations (IPRI)**

Maritime Situational Awareness (MSA) is an essential maritime security task. The task has become more challenging in the last decades because of the global proliferation and intensification of activities, actors, and interests at sea.
Aware of the challenge, the EU and NATO have been developing efforts in streamlining institutional responses, as well as in improving doctrines and instruments to enhance MSA. The efforts included autonomous actions, as well as activities within the framework of their strategic partnership, particularly after the Warsaw Summit of 2016. At Warsaw, within a broader movement to deepen their strategic partnership, the EU and NATO committed to the improvement of interinstitutional cooperation in several areas linked with MSA, including in coordination, information sharing, and lessons learned6.
MSA is a process that blends civilian and military as well as public and private inputs to achieve an accurate picture of the maritime domain.
As a process MSA involves four main interconnected and indissociable elements:

Surveillance and Data Collection
• Maritime Surveillance
• Data Collection
• Regulatory Initiatives

Data Fusion and Knowledge Development
• Data Fusion & Data Sharing
• Analysis & Knowledge development

Coordination and Knowledge Dissemination
• Information sharing & Communication Systems
• Command & Control

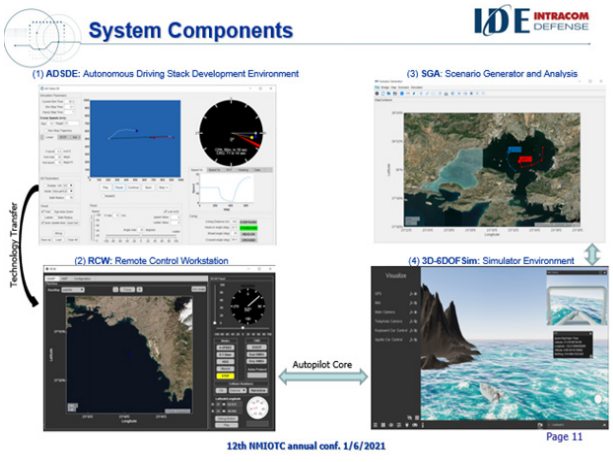
Management and Improvement of MSA Structures
• Technology Development
• Education & Training
• Lessons Learned
• Capacity Building

The empirical evidence contained in the MSA literature indicate that after the Warsaw Summit, the cooperation between the EU and NATO advanced mostly through ad hoc and sectoral activities. Informal, but sanctioned, staff-to-staff exchanges were the main mechanism in the advancement of EU-NATO relations, albeit relevant structural initiatives such as the establishment of the CoE Hybrid. Informal, ad hoc, and sectoral initiatives are positive, yet they should be regarded as steps towards a structured and comprehensive relation, where informality and ad hoc solution plays a role, but not a central one. Thereby, the full potential of EU-NATO cooperation remains to be unleashed.

**Lecture: A Simulation of Training Platform for Unmanned Surface Vehicles**
**Dr. Chrissavgi Dre, Deputy Director New Technologies, Intracom Defence**
**Dr. Ioannis Dagres, Senior Engineer, Intracom Defence**

Intracom Defence Situational Awareness
• Unmanned Surface Vehicles (USVs) will be a key component of naval operations in the future, especially for countries like Greece.
• Modern USVs demonstrate high performance, autonomy, robustness, reliability, data/communications, interoperability, mission versatility. Furthermore, they are designed for safety, easy deployment, operation and maintenance.
• Simulation and training platforms can play a key role in the design of robust sea vehicles as they reduce time and cost for design testing and sea-trials.
• A novel simulation and training platform for the design of Unmanned Surface Vehicles is presented.

Products
• Communication Systems
• Missile Applications
• Security Solutions
• Unmanned Systems
• Hybrid Power Systems
System Components
• Autonomous Driving Stack Development Environment
• Remote Control Workstation
• Scenario Generator and Analysis
• 3D-6DOF Sim: Simulator Environment



Future Plans
• Explore various open-source stacks (e.g. MOOS IvP, Apollo, Autodrive) and build a complete USV AD stack
• Extend the Scenario Generator with C2 functionalities
• Extend the LGSVL to support high fidelity (near real-time) communication links and jammers
• Explore the adoption of HLA to be able to join Federate Distributed Simulations

**Lecture: Arming Autonomous Vessels**
**Mr. Matthew Searle, CTO Maritime Arresting Technologies**

Choice of Weapons:
• Kinetic
- Surface: Direct fire, small missiles, kamikaze UXVs
- Sub-surface: Energetic, Super cav. , armed UUVs / torpedoes.
• Non-Kinetic (Non-Lethal) weapons
- Dazzling lasers
- 95Ghz microwaves
- Pulsed energy
- Plasma balls
- Drogue lines
- Nets
- MVSOT occlusion technologies

Politics and Ethics: Any use of kinetic weapons in foreign or domestics port will have political consequences. If used against misidentified innocent victims will cause significant moral and ethical issues.

Arming AXVs with non-kinetic effectors allows instant response
• Electric power allows instant launch
• No need for crew to scramble
• Small size and low cost allow multiple units to be fielded
• Use of non-lethal / non-kinetic effectors allows low level launch authorization

Non-lethal weapons add capability to the kill chain
• Non-kinetic effectors act like a spider's web
• Buys time for manned units to arrive
• Captured target allows more time for kinetic response if needed

Stingray Interceptor C-UUV Net
• The fully automated Stingray interceptor net is a non-kinetic system that can be deployed against any potential threat without risk to persons or property.
• The Stingray net is deployed across the path of the incoming underwater threat at up to 20 knots, taking less than 10 seconds to set.
• Forms an invisible barrier from sea surface to seabed.
• The underwater threat collides with the net and becomes entangled.
• The captured threat is towed out of harm's way.

**Lecture: Unmanned Aerial System for Maritime Domain Awareness (MDA) – A Ship Captain's Perspective**
**Mr. Mark A. Russell, Director, International Business Development of Martin UAV**

Maritime Domain Awareness is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment. The maritime domain is defined as all areas and things related to the sea, ocean, or other waterways, including all maritime-related activities, infrastructure, people, cargo, ships, and other vehicles.

What information can UAS give the captain, today?
• Cameras
- EO "Super Zoom", EO/IR, Laser Marker/Pointer
- Laser Target Designator, AI, Processing, HD Imagery
• AIS (Automatic Identification System)
- UAS extend AIS 200-300km+
• Wide Area Surveillance "ViDAR"
- Helicopter – using EO/IR, needed 30 mins to locate man in water (sea state 2), in 4km x 4 km area.
- Kestrel – only 90 secs
• Synthetic Aperture Radar (SAR)
- All Weather Radar, Day/Night, Maritime & Land
• Communications & Video Relay
- Extended Range, MANET, VOIP/ROIP, Video, C2

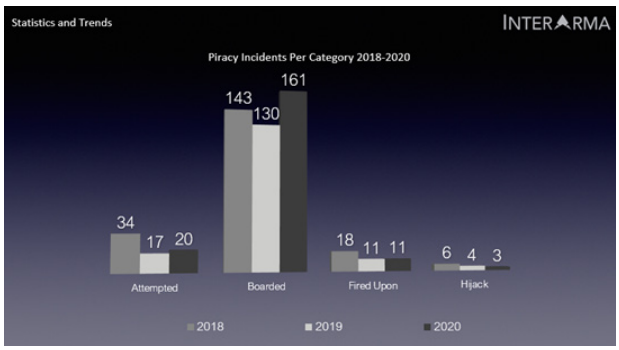
The VBAT is a VTOL system designed specifically for maritime (small ships) and does not have a launcher or recovery unit. No equipment on the deck. It can deliver the MDA capabilities and take off/land in a 3m x 3m space on the ship, operating out to 150km from the ship, day and night. This capability was not possible 2 years ago. The VBAT is operational now with US and Allied forces.

**Lecture: A review on current Maritime Threats Scenery and operational challenges outlining needs and cost-effective solutions of technology**
**Mr. Alexandros Lyginos, CEO of Interarma Ltd**

For the past 3 years, we observe a slight fluctuation in the total number of piracy incidents occurred worldwide, whilst almost half of them are reported in West Africa waters. This fact shows the instability in Political, Social and Economic Environment remains within the subject regions.

Piracy Per Year
• 2018: 201
• 2019: 162

• 2020: 195




New Technologies Preventing Piracy
• Artificial Intelligence (AI) has made headway to enhance maritime safety, optimize business operations and processes, and aid in voyage planning and vessel maintenance.
• The use of AI-based systems to create fully automated piracy alerts can allow seafarers a few moments to react, potentially saving lives.
• In cracking down on maritime piracy, one must first understand how pirates operate and make their advances. Behavioral analytics, a new holistic interpretation of raw empirical data, can dramatically enhance the crew's situational awareness by monitoring data and motion within the vicinity of a vessel in detail.
• This information includes identifying the number of boats and other neighboring ships within the same waters, the routes and speeds it crosses paths to determine distinct patterns, unknown correlation and provide clarity to ambiguities.

**June 2, 2021 – NMIOTC Keynote Speeches**

**Keynote Speaker: Rear Admiral Kiril Mihaylov**
**Commander of the Bulgarian Navy**
**Title: Implications of Disruptive Technologies for Smaller Navies**

Identifying disruptive technologies and their use in the military domain early is vital to achieving superiority on the battlefield. Countries with small navies are not usually expected to lead the way to technological breakthroughs and innovations, since this endeavor involves a lot of resources and financial commitments. But making sure to observe closely the trends in the naval community and implementing such innovations would yield surprising results. Synergizing the military and civil industries can lead to a fundamental change in operational technologies and strategies and only through working together can we exploit the opportunities that disruptive technologies provide. Furthermore cooperation and collaboration between entities, such as NATO and EU for example, would pave the way to better understanding how those existing technological achievements may be utilized in a principal way of advancement in different military domains.

**Keynote Speaker: Rear Admiral Mihai Panait**
**Chief of the Romanian Naval Forces**
**Title: Emergent, Innovative and Disruptive Technologies – Opportunity or Threat?**

Future Emergent and Disruptive Technologies
• Big Data and Advanced Analytics
• Artificial Intelligence
• Autonomy Materials
• Space
• Hypersonic

Maritime Implementation of Emergent and Disruptive Technologies I
• Artificial Intelligence – drones communicate with each other to work as a group using AI operators can control the entire swarm at once
• Opportunity – cheap or less expensive drones
• Threats – swarms of drones for anti-ship warfare launched by commercial vessels, give the adversary the benefit of plausible deniability used for ISR missions or as loitering munitions

Maritime Implementation of Emergent and Disruptive Technologies II
• Big Data Advanced Analytics (BDAA)
- OSINT enthusiasts routinely post pictures on social media covering naval vessels positions and activities
- Source of pictures is free or inexpensive imagery from commercial satellites
- Huge amount of data available and info on maritime assets
• Opportunity – can augment own maritime domain awareness
• Threat – can have an impact on operations states with underdeveloped ISR assets or non-state actors could potentially pay for such pictures in an effort to plan an attack

Maritime Implementation of Emergent and Disruptive Technologies III
• Novel materials and manufacturing
• Opportunity – Increased performance (speed, distance, effects etc.)
• Threat – Arms race and losing technological advantage

**Keynote Speaker: Major General Alaa Abdulla Seyadee**
**Commandeer of Bahrain Coast Guard**
**Title: Maritime Domain – An Approach to Information Sharing and Management**

Strategic Approach
Bahrain costal surveillance system was designed and installed of multiple integrated coastal surveillance sensors to provide the Coast Guard with a comprehensive maritime situational awareness and Command and Control capability. Includes establishing maritime surveillance sensor sites and a state-of-the-art Regional Command Center. Fused sensors include X and S-Band surface search radar, Infrared Electro-Optical long-range cameras and AIS base stations.

Strategic Approach Phases
• Phase 1 = Technology & Partner Evaluation
• Phase 2 = System planning and product selection
• Phase 3 = Base Line AIS system
• Phase 4 = System Enhancements
Vessel Identification Transceivers
Customized transceivers issued and securely installed on every vessel. Full vessel and operator details captured electronically at point of installation.

Command and Control
National maritime data center. Ergonomic command and control center with state-of-the-art visualization technologies and automatic data analysis and incident management.

Data Utilization and Information Sharing
Real time coverage across entire gulf. A total of 50 million position reports every week processed and correlated in real time.

The Future
• Integrate new sensor systems
• Enhance data analytics
• Refine command and control

**Keynote Speaker: Brigadier General Bart Laurent**
**Director of the Operations of the European Union Military Staff**
**Title: Future of Security in the Maritime Security**

The key elements to develop the EU future strategies, especially in the global maritime environment are resilience and capabilities development along with emerging disruptive technologies.

Resilience to adapt our structures, processes, our hard- and software is needed, as 'events' may dictate and foresight should indicate. The use of, and protection against, remotely operated vehicles of different sorts is just one of the 'events' that show how relatively small technological developments may bring about big changes in military actions.

Emerging Disruptive technologies, ranging from Artificial Intelligence (AI) and quantum technologies to hypersonic weapons and new space technologies have a serious potential to revolutionize our military capabilities, strategies and operations. The EU has a strong potential in EDTs, indicated by a vibrant industry and start-up landscape in fields such as AI and robotics, but for sure, more effort is needed to match the level of development in this field of our partners and competitors.

In November 2020, as a kick-off for the work on the Strategic Compass (SC), the EU has originated its first intelligence based comprehensive, 360-degree analysis of the full range of threats and challenges the EU currently faces or might face in the near future. In the analysis, the risk for the EU not being prepared to react to the new threats and challenges was mentioned. Building on the threat analysis and other possible thematic input, the EU will define policy orientations and specific goals and objectives in four baskets:
• Crisis Management
• Resilience
• Capability development
• Partnerships

**Lecture: Maritime security and smart technologies: Turning the attention to Africa**
**Professor Francois Vrey, PhD Research Coordinator Security Institute for Governance and Leadership in Africa- SIGLA**
**Captain Mark Blaine, Stellenbosch University, South Africa**

Maritime security and smart technologies: Turning the attention to Africa
The information below is directly from
https://howafrica.com/the-top-10-most-powerful-navy-in-africa/ :

"A 'Blue Water Navy' is a navy that has the ability to perform all aspect of naval operations. They can travel, navigate, and support naval operations deep in the ocean. A navy with Blue Water capabilities has the support systems and infrastructure to travel unhindered to a part of the world's waters.
• Examples of Blue Water Navy in Africa:
- Egyptian Navy
- Algerian National Navy
- South African Navy

A Navy can be called 'Green Water Navy', if it has the ability to project its naval operations far beyond it shores but is still limited in its deep ocean operations. A Green Water Navy can travel and navigate long distance but can only do so in a limited time due to its lack of deep water opera-

tions support infrastructures and platform
• Examples of Green Water Navy in Africa:
- Nigerian Navy
- Moroccan Navy
- Tunisian Navy
- Equatorial Guinea Navy

The Brown Water Navy is a navy primarily focused on littoral warfare. They usually excel in 'swarm attacks' using numerous small boats to overwhelm an opponent. The major type of ships Brown Water Navies possesses are mainly small gunboats and patrol ships.
The primary role includes maritime patrol, combating sea criminals, coasts guard duties, harassing enemy forces, and mine sweeping and clearing.
• Examples of Brown Water Navy in Africa:
- Angolan Navy
- Tanzania Navy
- Sudanese Navy
- Ghanaian Navy
- Kenyan Navy
- Namibia Navy
- Cameroonian Navy

A Constabulary Corp possess no credible deterrence platforms neither do they have any warfighting capabilities or skills. Its main role is to safeguard the seaports and harbors from criminals and other vices.
• Examples of Constabulary Corp
- Libyan Navy
- Togolese Navy
- Senegal Navy
- Mauritius Navy
- Eritrea Navy
- Gabon Navy

There are many African countries that are landlocked that do not own or operate a navy."

The Way Forward for Maritime Security Capacity Building
• Material
- Equipment and Infrastructure
• Human Capacity Building
- Training Courses & Education
- Mentoring
- Workshops & Tabletop Exercises
• Institutional
- Strengthening organizational structures
- Law Making

**Lecture: Maritime security, smart technologies and the law: An African perspective**
**Dr, Michelle NEL, Facility of Military Science, Stellenbosch University, South Africa**

There is a concern with regard to the use of technology in Africa from a HUMAN RIGHTS perspective. Science and its offspring technology have been used in this century as brutal instruments of oppression.
African Maritime Legal Framework
• Domestic Law
• United Nations Convention on the Law of the Sea (UNCLOS)
• Co-operation agreements
• 2050 Africa's Integrated Maritime Strategy
• International humanitarian law
• International human rights law

**Lecture: Beyond the Responsibility Gaps in the Use of Autonomous Weapons**
**Mr. George Kiourktsoglou, Greenwich University**
The use of autonomous weapons can be dangerous and hinder government relations globally. This statement leads to ethics being major factor when discussing the use of autonomous weapons.

A New Ethical Framework within a Democratic Political Context
The following issues must be addressed when discussing the ETHICs of the use of autonomous weapons
• No Human Agency
• No Vectoral (causal) Attribution
• No Universal Legal Uniformity
• Split between high- and low-tech militaries

**Lecture: 3D Printing Security Issues**
**Dr. Nikitas Nikitakos, Professor, Dept. of Shipping Trade and Transport, University of the Aegean**

Additive Manufacturing is the process of joining materials to make objects from 3D model data, usually layer upon layer, as opposed to subtractive manufacturing methodologies. On an Additive Manufacturing printer, costs are roughly the same for producing complex objects and simple ones. Fabricating an ornate and complicated shape does not require more time, skill, or cost than printing a simple block, once the digital design is completed. The industry will undoubtedly continue to develop worldwide over the next few decades, and the abilities of the printers will be vastly different than they are today in ways that are not completely predictable.

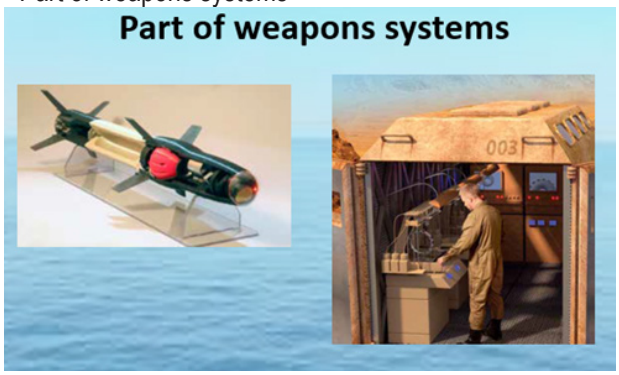
The Additive Manufacturing Framework
Capital versus scale: Considerations of minimum efficient scale can shape supply chains. AM has the potential to reduce the capital required to reach minimum efficient scale for production thus lowering the manufacturing barriers to entry for a given location.

Capital versus scope: Economies of scope influence how

and what products can be made. The flexibility of AM facilitates an increase in the variety of products a unit of capital can produce, which can reduce the costs associated with production changeovers and customization and, thus, the overall amount of required capital.

Additive Manufacturing and Future Security Threats
• Weapons Proliferation
- VEOs (Violent Extremist Organizations) represent some of today's greatest security threats, and they are only going to be even more dangerous with the proliferation of AM.
- Homemade weapons
- Advanced technology weapons
- Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE)
• Drugs
• Miniature explosive drones


• Part of weapons systems




Additive Manufacturing is occurring but we need to consider government policy, law, and ethics.

**Lecture: The Role of Emerging and Disruptive Space Technologies in Maritime Information Warfare**
**Ms. Lucy Lim, NATO Office of the Chief Scientist, NATO Science & Technology Organization**

Emerging and Disruptive Technologies
The EDTs will be increasingly intelligent, interconnected, distributed, and digital.
These technology trends will drive four key military capability trends:
• Ubiquitous Sensors and Autonomous Systems
• Increased importance of Battle Networks
• Expanding Operational Domains
• Increased reliance on Precision Warfare

Maritime Domain Awareness
• Space technologies are vital to Maritime Domain Awareness because of:
- The expeditionary requirements of naval operations
- Global maritime security architectures
- Ability to track and identify vessels of interest
• Sensors
- Quantum sensors
- Unprecedented detection
- Smaller vessels
• Nano Satellites
- Expand area coverage
- Cost effective
- Reduce revisit times and data downlink latency

• Synergies
- Combination of space technologies and new analytical methods
- Increase speed and efficiency of analysis

Position, Navigation and Timing
• Global Navigation Satellite Systems (GNSS) support:
- Electronic Chart Display and Information System
- Automatic Identification System
- Automatic Track Control
• Quantum
- Precise gravity gradient measures
- Mobile platforms
• Artificial Intelligence
- Detection of spoofed signals
- Integration of multiple sensor modalities

Networks are the physical foundation of the information battlespace.
In MIW, SATCOM plays an integral part in delivering networked capabilities.
• SATCOM is limited:
- Cost of launching satellites
- Stabilizers needed for on-board antennas
- Relatively low bandwidth incapable of supporting applications requiring high data rates
• High-throughput Satellites
- Take advantage of frequency reuse
- Support high bandwidth applications
• Artificial Intelligence
- Space-Air-Ground integration
- Interference management

- Beam Hopping
• Quantum Comms
- Info transmission across 'turbulent' water
- Secure comms

Conclusion
Space technologies will play a central role in warfare defined by achieving narrative dominance. The latest innovations in space-based capabilities will be essential aspect of future Maritime Information Warfare systems. Scenario-based testing will further enhance NATO's understanding of the value of space technologies and intersections with Emerging Disruptive Technology's in operations.

**Lecture: Emerging and Disruptive Technologies: EDA efforts in the field**
**Dr. Georgi Georgiev, Project Officer Maritime Capabilities Support, CAP, EDA**

EU Global Strategy is vital for European security. Active work on EDT essential for European strategy autonomy

European Defense Agency (EDA) efforts are based on three different perspectives
• Technological
• Operational
• Industrial

EDA efforts for research, technology, and innovation
• Post-quantum cryptographic algorithms
• AI C2 Systems for cyber
• Disruptive fuel: Hydrogen technologies for military operations
• Energy storage for high energy demand applications
• AI based technologies combined with big data
• Quantum information networks
• Internet of things for defence
• Muscular, brain and cognitive UI (MUSCIUS)
• Hybrid multifunctional metamaterials
• EMRG and hypervelocity projectile
• AI based multi-sensor seeker head
• Swarms, swarming and multi-robot cooperative systems

**Lecture: AI opportunities, requirements, and barriers for adoption of AI in maritime use cases**
**Mr. Darek Saunders, Head of Border Security Research Observatory AI Research and Innovation Unit Capacity Building Division**


Representative use cases for the application of Artificial Intelligence solutions in Border Management.
• Automated Border Control
• Surveillance Towers
• UAS
• Maritime Domain Awareness
• Object Recognition
• Robotic Systems
• Machine Learning Optimalization
• Predictive Asset Maintenance
• Geospatial data Analytics

Expected future Artificial Intelligence Maritime Domain Awareness Capabilities
• Main operational response trigger
• Identify and assess abnormal behavior
• Identify new threats
• Integration of ad-hoc data sources

**Lecture: ARSx2: A marine area surveillance system using UAS, assisting anti-privacy measures and contributing to hostages and/or vessels recovery**
**Mr. Evan Christodoulou, CEO of A. S. Prote Maritime**

A. S. Prote Maritime Ltd was founded in 2013 in Cyprus with the sole purpose of providing armed and unarmed security services to merchant ships, against piracy.
From 2017 our activities have expanded to the use of new digital technologies in merchant shipping, the maritime environment and relevant market.

Reasoning of using UAVs against piracy
i) The need to improve existing measures to encounter piracy and provide other non-military options.
ii) Almost all previous attempts to assist in the fight against piracy by using UAVs:
• remained only at a theoretical level and never developed
• were of a purely military nature
• were completely failed private efforts, poorly organized and staffed with inappropriate personnel, based on the naïve idea that "anyone can fly a UAV

The Project ARSx2

The innovative project ARSx2 deals with the development of a maritime surveillance system, consisting of two UAVs, for the prevention of piracy or other illegal activities, as well as the monitoring of pirate incidents in progress, and search and rescue cases at sea.

• Phorcys

- The first UAV, called "Phorcys", is a small and flexible VTOL hexacopter on a Y6 configuration. Its compact and stocky structure enables it to operate in tropical weather environments. Equipped with a powerful hybrid EO/IR stabilized camera with object tracking capabilities, humans, and items such as guns, canisters, etc. can be identified from a safe distance. Phorcys will act as the "long arm" of the private guards and/or the crew aboard merchant ships.

• Ceto

- The second, easy to use by non-specialists fixed-wing UAV, called "Ceto", is used in emergency cases as a "rescue beacon". It is deployed when a vessel is already or will be occupied by pirates, while real-time position, images or video are transmitted to the patrolling authorities and rescue organizations. Its purpose is, either to follow the vessel captured by the pirates or the ship of the pirates with hostages, during ongoing piracy action by transmitting at appropriate frequencies emergency signals as well as critical information, such as images etc.

ARSx2 System Advantages

• Increased maritime surveillance ability
• Early warning of potential pirate threats
• Capture, process and analysis of data
• Real-time high precision intelligence to control stations and rescue authorities
• Remote operation with mission management and autonomous commands
• Reliable network protocols for fast, safe and robust data transmission
• Assistance to search and rescue operations
• Monitoring of a pirate attack or hostage situation
• Recognition and monitoring of marine hazards
• Alleviation of risk of injury or death of humans during or after a pirate attack
• Reduced insurance costs for crews, ships, and freights
• Reduced economic loss of countries adjacent to high-risk areas
• Optimization of ship routes
• Fuel saving
• Ship rental time saving
• Security of the movement of humans and goods

**Lecture: Security Challenges in 2030: The Challenge of Reality vs Unreality**

**Mr. Christopher Kremidas-Courtney, Senior Fellow, Friends of Europe; Lecturer Institute for Security Governance (ISG); Lecturer, Geneva Center for Security Policy**

The World by 2030

• Democracy versus Authoritarianism
• Women will own 55% of the world's wealth
• Over 7.5 billion internet users by 2030
• Cybercrime will be $10.5 Trillion by 2025
• Next Industrial revolution: Sub-Saharan Africa
• Most populous country: India, Largest economy: China
• India's economy larger than Germany or Japan
• Increasing impact of climate change
• Major economic shifts as a result of all above
• Reality versus Unreality: by choice (recreation) and due to disinformation

- Augmented Reality (AR) is a live direct or indirect view of a physical, real-world environment whose elements are augmented by computer-generated sensory. i.e. Augmented Reality Glasses

- Emergence of improved affordable wearable devices such as

AR glasses in 2023 - will begin to replace mobile phones

- Virtual Reality (VR) is a simulated experience that be similar to the real world.

- Numerous positive applications for military training, mental health, recreation, enabling handicapped and elderly, travel business, education, medical, communications

- VR enables an immersive experience – future developments include the ability to plug directly into human nervous system

- AR and VR Implications for Security

• Espionage: recruiting of sources & subsequent activities in VR metaverse
• Hacking of AR systems to spoof navigational use by public and private actors
• Disinformation: More precise and potent delivery means via AR and VR and AI-enabled bots
• Deeper societal divisions due to an emerging split based on competing forms of reality

- Disinformation-Driven Violence 2020-21

• Attacks on 5G towers – over 200 in Europe alone
• Various Qanon attacks to include train derailments, attack on Canadian PM residence, etc
• Attacks on vaccine centers
• August 2020 attempted storming of Bundestag (German Federal Parliament)
• January 6, 2021 attack on U.S. Capitol

- How to be prepared for AR/VR?

• Regulate and build safeguard into security of AR and VR

**Lecture: SYNORIS – The "Chariot" of Modern Maritime Warfare**
**Mr. Evangelos Mantas, DevSecOps Engineer at Infili Technologies**

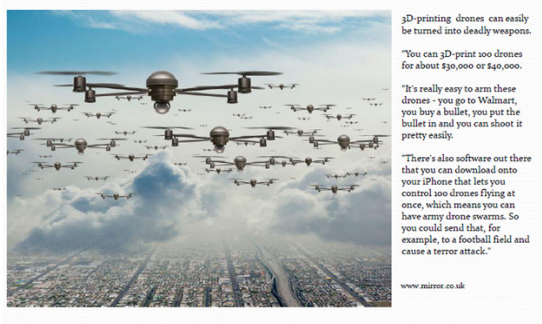
Why Use Unmanned Underwater Vehicles (UUV)
• UUVs are far less expensive to operate and maintain than manned platforms.
• Enhanced payload is able to maintain constant awareness and long-range coverage of the field. Extended surveillance periods and data collection, enables a better understanding of long-term behavior patterns and trends.
• Improved range coverage, as they allow manned platforms to pursue tasks elsewhere.
• UUVs keep human personnel and expensive equipment away from danger.

Unmanned Underwater Vehicles are used for:
• Marine Exploration
• Wreckage Discovery
• Research
• Search and Rescue
• Technology advancement enable them to conduct autonomous and more complex mission scenarios

The latest UUV capabilities include the detection of submarines, such the Synoris UUV platform, providing an easily deployable solution to assist and enhance the situational awareness of the underwater battlefield in littoral and open seas environments, using hydrophones as passive sonars to discover hostile vessels otherwise undetected by traditional detection equipment. The envisioned network of autonomous UUV can cover a greater area, providing real and near-real time feed of the "underwater traffic".

**Lecture: Threats and Operational Advantages of UAS in maritime and coastal environments**
**Dr. Christos Skliros, Head of Engineering, Hellenic Drones**

Threats to the maritime and coastal environment
• Interference
• Intelligence, Surveillance, and Reconnaissance (ISR)
• Weaponization




Commercial Small Unmanned Aircraft System (sUAS) can significantly help fight against malicious drone attacks.

Drone Detection Technologies
Radar technology can provide the effective detection of drones within an area, even able to
detect long range It can be successfully paired with other technologies, such as RF or optic to
provide thorough coverage if desired
• Pros
- Longer range and constant coverage. Provides multiple drone detection and tracking
• Cons
- It can be severely affected by nearby RF pollution Blind Sectors Requires authorizations from local authorities and experiences difficulties in detecting small drones. No pilot localization

Radio frequency analyses the RF spectrum within the protected area, searching for any form of communication between the drone and its remote control RF can even identify the drone make and model
• Pros
- Features like drone and pilot localization as well as drone characterization It provides passive technology and multiple drone detection

• Cons
- It does not detect autonomous drones Likewise, local RF pollution may also reduce effectiveness

Optic cameras allow visual direction and identification of approaching drones and their
payloads Acting like a radar, optics may also be successfully combined with RF technology in
providing thorough coverage
• Pros
- The visuals can be retained and used for forensic evidence of drone intrusions It has passive technology
• Cons
- Without the RF or radar back up, false alarm rates are often high Blind Sectors The performance is often impacted by light or weather conditions which usually results in difficulties detecting smaller drones nearby No pilot localization

Acoustic sensors are best in recognizing drone sounds from a database of drone acoustic
Signatures
• Pros
- It can detect autonomous drones while providing azimuthal information on incoming drone direction
• Cons
- The sound database must be updated in persistent to be effective Drones today are also becoming more and more

soundless as technology advances. Encounters difficulties tracking modified drones. No pilot localization.

Technologies for Drone Neutralization
Jamming, allow safe return to home drone while safeguarding the point of interest
• Pros
- No collateral damages from intercepting drone (fall in urban areas, crowded ports, refineries etc.
• Cons
- It does not defeat autonomous drones with the exemption of systems with GPS jamming capacity. It can interfere the ambient communications Requires authorizations from local authorities.

Mitigation (wi fi spectrum restriction), allow safe return to home drone while
safeguarding the point of interest
• Pros
- No collateral damages from intercepting drone (fall in urban areas, crowded ports, refineries etc. No authorizations from local authorities.
• Cons
- It does not defeat autonomous drones It can interfere the ambient communications

Selecting The Best C-UAS Solution

How to choose the best anti drone solution that provides the best optimal airspace
security at the best cost and efficiency ratio while serving you in the longest time
possible?

Checklist: About the Technology
• The 'Modular' –Is the technology scalable up and down to better fit profiles on your site?
• Upgrades –Is it a good long-term investment? Could it be easily updated to stay one step ahead of other drones' evolution without the risk of replacing everything?
• Durability–Is the technology durable enough to outstand different weather situations?
• Easy Installation and Integration –Is the technology easy to use and requires minimal training? Does it include an easy-to-use interface?
• Costs of Operation –How much is the cost to run the technology? Will it consume a big amount of electricity? Does it require dedicated staff to operate the system?
• Reactive/Accuracy –What is the technology's way of detecting false alarm rates? How quickly can it detect drones within its area of coverage?
• Pilot/Localization –Is the technology able to locate the pilot and the drone which in turn will give you the options to apprehend the person behind the intrusion?
• Effectiveness (Even against multiple drones) –There are bigger security threats against drone swarms.
• Interference/Obstruction –Authorities may be extremely sensitive about the 'frequency pollution'. Does the provider's technology provide low interference or even passive?
• Reasonable Price and High Quality –Protecting your airspace is considered as an investment but it doesn't mean breaking your bank. Does your provider offer a fair cost to quality ratio?

**CLOSING REMARKS**

With eight keynote speakers and 24 powerful lectures from established maritime security experts and academic professionals, this conference successfully addressed and discussed emerging disruptive technologies to significantly improve maritime security.