CENTRE OF EXCELLENCE
DEFENCE AGAINST TERRORISM
ANKARA, TÜRKİYE, 2025

SOF ROLES IN CT CRISIS RESPONSE SEMINAR

(14-16 May 2025)

A Multi Domain Response to Maritime Counter Terrorism

SOF ROLES IN CRISIS/CT SEMINAR: A MULTI DOMAIN RESPONSE TO MARITIME COUNTER TERRORISM

NATO Centre of Excellence
Defence Against Terrorism
Ankara, Türkiye

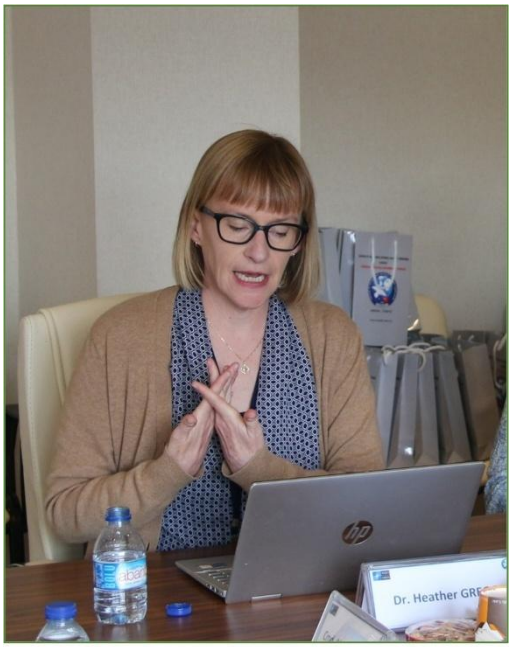
14-16 May 2025

Table of Contents

Executive Summary

The idea for the SOF Roles in Crisis/CT Management seminar began in 2022 as a collaborative effort between NATO SOFCOM in Mons, Belgium, and the NATO Centre of Excellence Defence Against Terrorism (NATO COE-DAT) in Ankara, Türkiye. These stakeholders developed this workshop with three broad goals in mind:

1. To engage NATO Special Operations Forces (SOF) partner nations and emerging partner nations
2. To provide an opportunity for NATO SOF allies, partner nations, and emerging partner nations to network and build relationships
3. To share best practices in crisis responses to terrorist incidents and explore how SOF can help inform these responses, including the roles that SOF may play in the actual response or before the crisis.



Dr.Heather GREGG

The first iteration of the three-day workshop was held in Ankara at NATO COE-DAT's headquarters from 6-8 July 2022. Twenty-five individuals from eleven countries—Algeria, Australia, Egypt, France, Hungary, India, Slovakia, Tunisia, Türkiye, United Kingdom, and the United States—attended the workshop, representing a range of military ranks and civilians focused on counter-terrorism (CT) at the tactical, operational, and strategic levels.

The second iteration of the three-day workshop was held in Ankara at NATO COE-DAT's headquarters from 3-5 May 2023. Thirty-one participants from 14 countries attended the workshop—Austria, Azerbaijan, Belgium, Egypt, France, Georgia, Italy, Jordan, Malta, Niger, Sweden, Türkiye, United Kingdom, and the United States—representing a mixture of SOF units and conventional forces of different ranks and positions.

This current workshop focused on the need for a Multi-Domain Operational (MDO) Approach to Counterterrorism in the Maritime Environment and was held again in Ankara at NATO COE-DAT's headquarters from 14-16 May 2025. Thirty-three participants from 12 countries attended (Türkiye, Albania, Cameroon, Denmark, Germany, United Kingdom, Hungary, Latvia, Poland, Romania, Ukraine, and USA). This iteration of the workshop included the NATO Maritime Security Centre of Excellence (NATO MARSEC) from Istanbul, Türkiye, in addition to NATO SOFCOM, and NATO COE-DAT as key stakeholders.

The workshop began with an overview of MDO, stressing NATO's definition and priorities. An MDO mindset was then applied to a range of threats and opportunities in the maritime environment, including CT and counter-piracy operations; the employment of unmanned systems and other emerging technologies in the modern battlespace; the protection of critical

infrastructure at sea; and the evolving and adapting role of SOF across all domains, with special emphasis on the maritime environment.

Some of the key takeaways from this workshop include:

- MDO provides a holistic and flexible framework that synchronizes land, air, sea, cyber, and space domains to address increasing hybrid and complex security threats and will enhance the effectiveness of various missions when properly integrated.

- SOF serves as a key enabler in MDO-CT operations, offering early presence, unique access and placement, and the ability to operate across all domains simultaneously. SOF can be a role model for an MDO mindset.

- Maritime security involves more than piracy or naval warfare; it includes environmental, legal, and technological dimensions. Critical infrastructure in the maritime environment is under-protected and highly interdependent, especially energy, and data critical infrastructure, presenting key vulnerabilities for countries and regions around the world.

- The convergence of terrorism, organized crime and other irregular threats require integrated, cross-domain responses that includes actionable intelligence, law enforcement, and military actors.

- SOF can be a force multiplier in the maritime domain and can help penetrate coastlines, work in underwater environments, and foster interoperability and collaboration among allied forces. SOF offers a more flexible and cost-effective approach than conventional forces. Naval SOF is a critical asset in CT, particularly given its multidomain proficiency.

- Creating a team with the right mix of capabilities is crucial for anti-piracy success, including naval SOF, medical professionals, intelligence, and individuals with arrest authority. STRATCOM and diplomacy are also important in counter-piracy operations. It is possible to be militarily successful but create political complications if counter-piracy operations are not holistically thought out.

- Emerging technologies are rapidly reshaping the battlespace, though maritime adaptation lags behind land and air base systems. The deployment of USVs and UAVs in the Black Sea demonstrates the significant operational impact these weapons systems can have on the modern battlespace. The effects of electronic warfare remain a persistent challenge in the modern-day battle space.

- Doctrine, training, and lessons learned in operations should be a virtuous cycle that improves operational performance and capabilities.

A little about NATO COE-DAT

HQ Supreme Allied Commander Transformation
Directorate of Multi-Domain Force Development

Quality Assurance Accreditation Certificate

The core processes and procedures of the Centre of Excellence – Defence Against Terrorism (COE DAT) were reviewed and identified as being aligned with NATO Quality Standards. Therefore, the Institution qualifies for:

UNCONDITIONAL ACCREDITATION

Certificate ACT/MDFD/ETPP/TT-0022/SER:NU:

Effective: **01 January 2025** Expires: **31 December 2030**

The Centre of Excellence – Defence Against Terrorism was found to have:

a. Sound internal procedures for the assurance of quality;
b. Procedures that are applied effectively at each level to ensure the quality of education and training;
c. Effective and regular processes of reviewing the curriculum and implementing required changes and enhancements;
d. Accurate, complete and reliable information about its curriculum.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

Placido TORRESI
Rear Admiral ITA NAVY
Deputy Chief of Staff, Multi-Domain Force Development

NATO accredited education & training facility

NATO's three declared core tasks of Collective Defence, Crisis Management, and Cooperative Security.

As a strategic level think tank for the development of NATO DAT activities sitting outside the NATO Command Structure, COE-DAT supports NATO's Long-Term Military Transformation by anticipating and preparing for the ambiguous, complex, and rapidly changing future security environment. COE-DAT is able to interact with universities, think tanks, researchers, international organizations, and global partners with academic freedom to provide critical thought on the inherently sensitive topic of CT. COE-DAT strives to increase information sharing within NATO and with NATO's partners to ensure the retention and application of acquired experience and knowledge.

A little about NATO SOFCOM

NATO Special Forces Command (NATO SOFCOM) is the primary point of development and synchronization of all NATO Special Operations activities, providing strategic SOF advice to Commanders. Since its inception more than a decade ago, NATO SOFCOM has consistently supported NATO and Partner CT efforts. Its NATO Special Operations University (NSOU) continues to deliver over thirty different courses that include aspects of CT (serving both allies and partners), directly support execution of CT missions, or provide essential pre-deployment training for SOF missions. NSHQ capabilities include Mobile Training Teams (MTTs), through which it delivers training directly to whole-of-government teams, interagency groups or regional stakeholders. NSHQ has developed Multinational SOF Advisory Teams (MSATs), which allow nations to reduce redundancy by harmonizing bilateral SOF initiatives with NATO Partnership mechanisms, to include efforts focused on the Middle East, North Africa, the Sahel and beyond. Further, NSHQ's revisions to doctrine strengthen interoperability and guidance to national and NATO defence planning efforts.

Additionally, NATOSOFOCM continues to Develop Comprehensive Defence handbooks, courses, exercises and experiments (NATO SOFOCM is piloting products and courses tailored for SOF now; potential to expand and/or connect to ongoing larger NATO Counter Hybrid Threat, Comprehensive Defence and Resilience efforts). NSHQ has been working in collaboration with COE-DAT for over a year to enhance its CT efforts with the provision of a CT seminar.

A little about NATO MARSEC COE

NATO Maritime Security Centre of Excellence in Istanbul, Türkiye, is both a center for academic research as well as a hub for practical training in the field of maritime security, along with relevant domains. MARSEC COE strives to achieve the necessary collaboration amongst stakeholders from government, industry, academia and private sector.

The mission of the MARSEC COE is to expand the capabilities of NATO and Partner Nations by providing comprehensive innovative and timely expertise in the field of Maritime Security Operations.

MARSEC COE's vision is to become an internationally recognized focal point as well as comprehensive expertise and knowledge provider in the area of maritime security, thus expanding capabilities of NATO and Partner Nations.

Maritime Security has different dimensions, including but not limited to Maritime Situational Awareness (MSA), Law enforcement, maritime safety, maritime environment, maritime science and technology, maritime trade and economy, maritime law, and public health. Therefore, in national terms, Maritime Security can only be achieved by a "whole of government" approach. If we succeed in applying this approach together with like-minded countries in a multi-national environment, we can attain our common Maritime Security objectives.

In sum, MARSEC COE approach to Maritime Security is based on multi-national cross-functional inter-agency co-operation.

SOF Roles in CT / Crisis Response Seminar 2025
Director's Opening Remarks
14 May 2025

Good morning, ladies and gentlemen, our distinguished participants. I am Colonel Halil Sıddık AYHAN, Turkish Army, and Director of NATO Center of Excellence – Defence Against Terrorism.

I would like to welcome you to our capital city Ankara and to the third iteration of "SOF Roles in Counter Terrorism – Crisis Response Seminar."

As you might have learned already, this seminar is a joint effort that we organize regularly together with NATO SOFCOM, represented by Lt. Col. Karl Hearne whom I would like to offer a special welcome.

Also, I would like to welcome representatives from MARSEC COE Navy Captain Levent BAHADIR and Navy Captain Mehmet Deniz ÇETİKLİ, who will be essential in facilitating this year's seminar and our focus on maritime security.

I would like to offer a warm welcome to our Academic Advisor Dr. Heather Gregg. We are grateful for her expertise and advice, which was instrumental in the planning of this event.

Also, let me give our special thanks to the distinguished speakers, whose academic and operational experience will ensure high quality discussions and takeaways of this seminar.

Today, I would like to give you just a hint about the wide range of COE-DAT's activities that support and influence NATO's fight against terrorism. We provide three core functions to the Alliance CT efforts:

- We are an **Education and Training Facility** providing courses and mobile education targeting partner nations.
- We are also the **Department Head** for NATO's counter-terrorism, including the synchronization of the ever-growing demand for counter-terrorism education and training.
- We also serve as a **think-tank** to transform NATO's understanding of terrorism and counter-terrorism through research projects, book development, lessons-learned workshops, and conferences.

As NATO's hub for counter-terrorism, our wide network of military, government, and industry experts is vital to our success to stay up to date within the community of interest.

The high professionalism and expertise of participating allied and partner Special Operations Forces proved crucial to making this seminar successful in the past, while helping

us gain a better understanding of the interoperability, intelligence sharing, and whole of society approaches required for effective crisis management and counter-terrorism. I hope that with your effective participation, this year will be equally beneficial for our SOF stakeholders.

All of you attending our Seminar this week will help COE-DAT and NATO SOFCOM continue expanding our network and develop new relationships that will undoubtedly help us in the fight against terrorism. I look forward to meeting with you all this evening at our Icebreaker social event in the Grand Mercure Hotel.

Thank you again for your attendance and support.

Halil Sıddık AYHAN
Colonel (TUR A)
Director, COE-DAT

DAY I

May 14, 2025

Overview of Multi Domain Operations and CT in the Maritime Environment

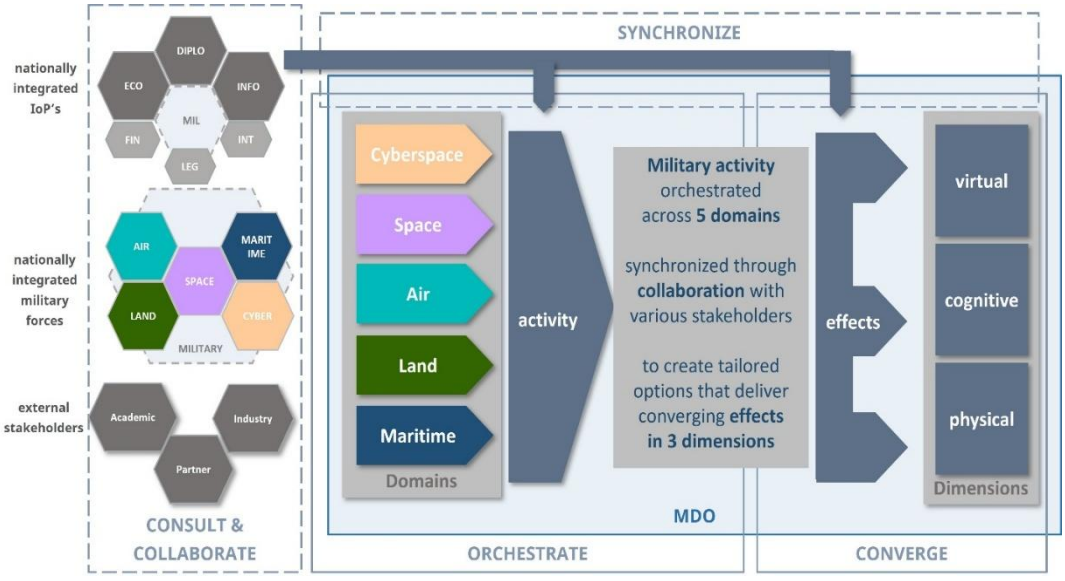
"What is MDO and Why is it Important for a SOF CT/Crisis Response?"

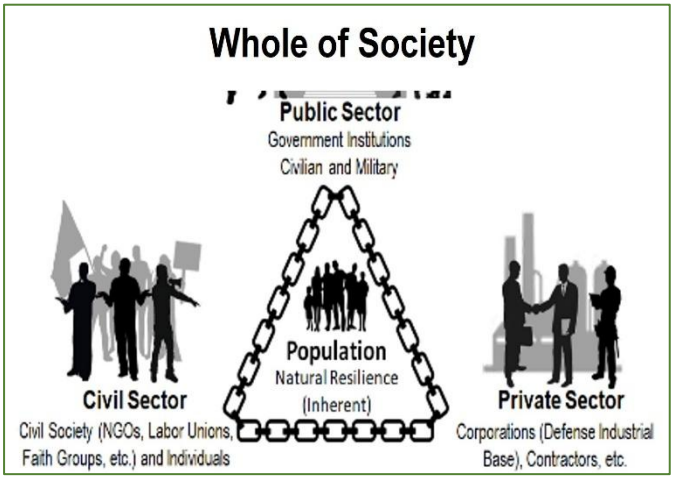
Colonel Jose Cabrera,
U.S. Air Force

The workshop began with an overview of Multi-Domain Operations (MDO) from U.S. Air Force Colonel Jose Cabrera, Deputy Director of COE-DAT and Senior U.S. representative to the Centre.

Col. Cabrera stressed the importance of MDO as NATO's approach for planning and addressing a range of actors, including state actors such as Russia and China, but also nonstate actors that perpetrate acts of terrorism. As an evolving concept, MDO emphasizes that modern-day wars require a holistic, synchronized response across all the domains warfighting (land, sea, air, space, cyber) but those actions must also be coordinated with nonmilitary activities and include both warfighting but also other instruments of national power, like diplomacy, economic power, and governance. MDO aims to bring all these effects together.

Elements of MDO





Applying MDO to counter-terrorism (CT) is a relatively new concept and one that needs further study. Col. Cabrera stressed the growing complexity of threats posed by non-state actors, particularly the convergence between terrorist organizations and diverse criminal networks, which blur the boundaries between military, intelligence, and law enforcement responsibilities, creating significant challenges for security forces. As with conventional war, an MDO approach to CT requires a whole-of-government, all-security-forces, and a whole-of-society approach to address underlying issues that cause terrorism. Furthermore, countries need to create a shared threat awareness and develop ways of sharing information, in addition to improving security cooperation. An MDO approach to CT also requires improving governance and Rule of Law, as well as building resilient societies.

SOF has skills that will help enable MDO, including the ability for unique access and placement; the training to work closely and over time with allies and partners; tactics, techniques and procedures to project power; methods for shaping the environment and enabling fires; and the ability to rapidly test emerging technologies. SOF is also "joint" by design and is accustomed to working with a broad range of security forces. The future battlefield will likely be shaped by the convergence of space and cyberspace, alongside a growing anticipation of irregular warfare. Within this evolving landscape, the flexibility and cross-domain capabilities of SOF stand out as a model for how the right mindset and integrated operations might function under an MDO structure.

Key Takeaways:

- MDO provides a holistic and flexible framework that synchronizes land, air, sea, cyber, and space domains to address increasing hybrid and complex security threats.
- MDO is not a rigid structure but a flexible, holistic approach that can enhance the effectiveness of various missions when properly integrated.
- The convergence of terrorism, organized crime and other irregular threats requires integrated, cross-domain responses involving intelligence, law enforcement, and military actors.
- SOF serves as a key enabler in MDO-CT operations, offering early presence, unique access and placement, and the ability to operate across all domains simultaneously.
- SOF can serve as a role model for a MDO mindset and for integrating domains in CT operations.

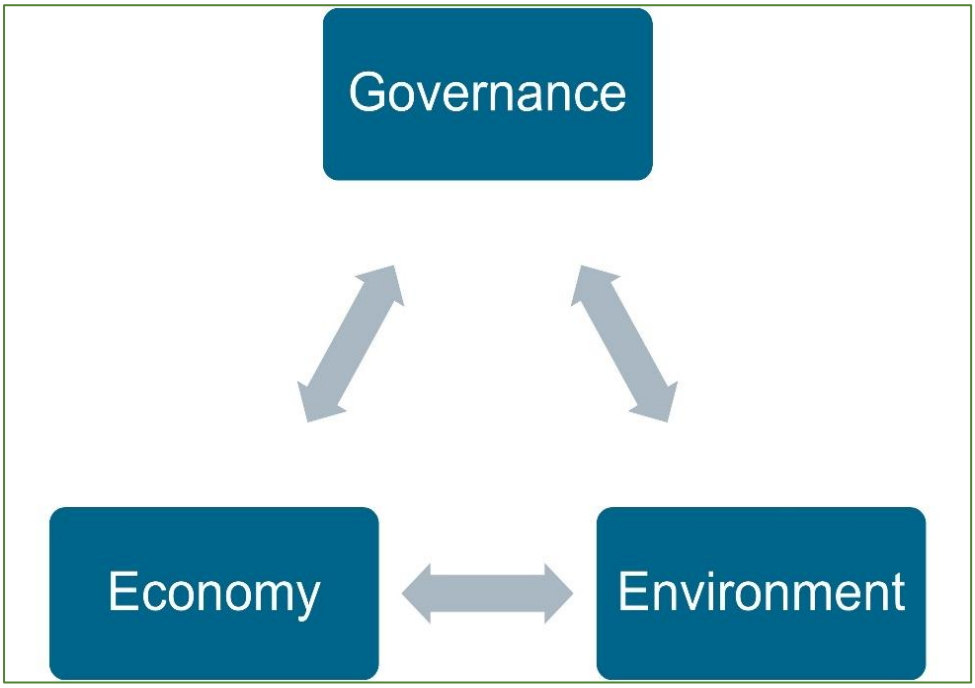
"Overview of Maritime Environment"

Mr. Carl Wrede,
DLR e.V, Germany

The morning then turned to an overview of the maritime environment provided by Mr. Carl Wrede, Deputy Director of the Institute for the Protection of Maritime Infrastructures at the German Aerospace Centre (DLR e.V.) in Bremerhaven, Germany.

Mr. Wrede stressed that the maritime environment should not be viewed merely as a geographic space but as a multidimensional environment that directly affects global trade, offshore energy production, food supply chains, data transmission through subsea cables, and maritime power projection. Given this, he focused on three broad aspects of the maritime environment: governance, economy, and the environment, stressing that each of these categories have key challenges and opportunities for security.

Relevance of Maritime Domain

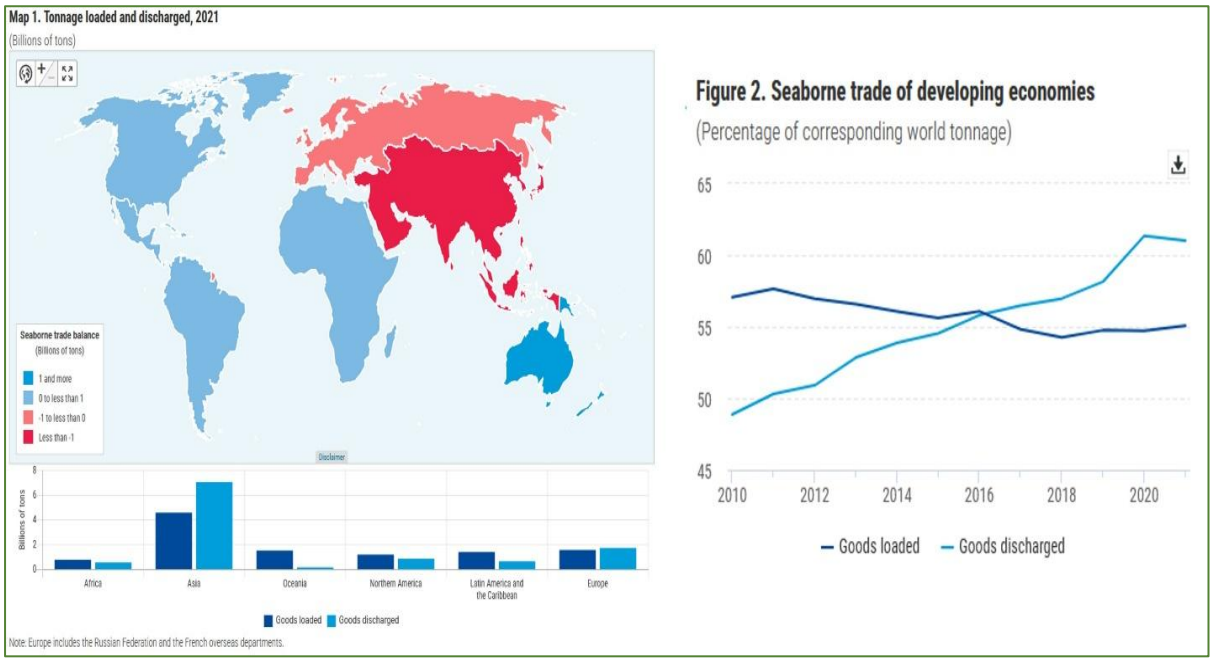


Governance of the maritime environment was created with the goal of facilitating and maximizing freedom for trade and economic wealth. Apart from piracy, security was not a governing priority. These norms were later codified in the UN Convention on the Law of the Sea (UNCLOS), and stipulate territorial waters, contiguous zones, exclusive economical zones, and the high seas. But, with regard to security, gaps remain in both the laws and norms that

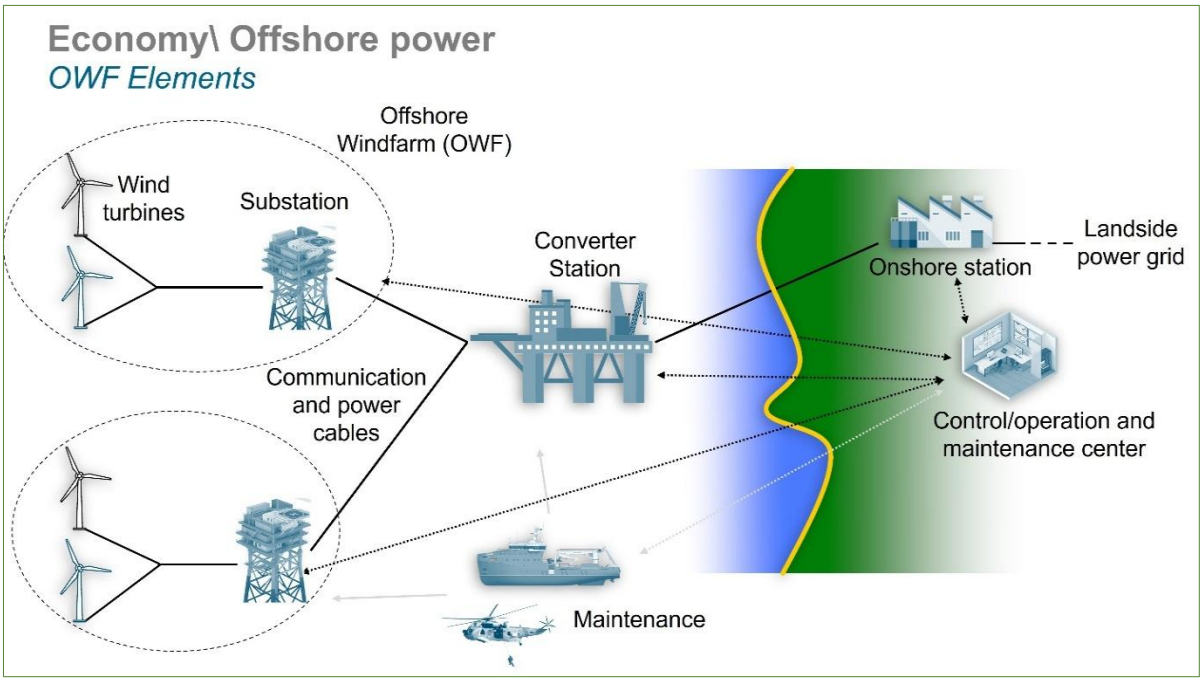
govern the maritime environment. Many criminal and terrorist acts at sea, including smuggling and piracy, fall into legal gray zones where jurisdiction is unclear and state responses are limited or contested.

Wrede further explained that crimes at sea often exploit the structural weaknesses of the maritime environment. Factors such as wide spatial extension, open accessibility, delayed intervention times, multidimensional exposure, and unclear legal status significantly increase vulnerabilities at sea. These same features also mean that security risks in the maritime domain do not always stem from traditional security threats or direct attacks.

The maritime environment is crucial for the global economy. Ninety percent of trade and shipping travel via the sea. Moreover, trade is not unidirectional, all countries both import and export goods via the sea. The dependence of the global economy on the maritime environment makes it vulnerable to piracy, terrorism and other security threats. Even a single attack at sea has the potential to disrupt international trade for extended periods.



In addition to trade, countries are increasingly dependent on fuel and energy transport via the sea, including offshore power, wind and their cables in particular, fuel pipelines, and the transport of fuel via ships. Data traffic via underseas cables are the backbone of digitization and the world's dependency on these cables for communication and information is another massive dependency. Currently, there is no alternative to deep sea cables. Satellites cannot solely handle the amount of traffic that sea cables transmit. Critical infrastructure, like subsea cables, is especially vulnerable because of their connection to land. In coastal areas, accessing these cables can be done with minimal effort and does not require the use of SOF or other highly trained forces. The collapse of sea-based structures, such as bridges, canals and ports, can also cause disruptions to trade and other maritime activities. Maritime tourism is also important for the global economy, especially littoral based tourism. All these economic issues present huge security challenges and vulnerabilities for countries and regions around the globe.



Finally, the environment, including weather and conditions at sea, presents unique challenges in the maritime domain. Seas have harsh and unpredictable environments that make their navigating and managing security challenging. Climate change will continue to make seas more unpredictable and present new challenges for navigation and for ports. Changes in the salinity of oceans and seas will affect sonar, which requires attention. Environmental spills are another major concern for the maritime environment, with the potential to affect maritime based economic activities such as fisheries, tourism, as well as the ecological balance. And increasing accessibility to the High North will present challenges and opportunities to navigation and governance.

Wrede concluded his presentation by emphasizing that there are many ways to cause harm in the maritime environment, drawing particular attention to the rise of state-sponsored maritime militias, such as those developed by China, operating as a second navy to support military and paramilitary objectives.

Key Takeaways:

- Maritime security involves more than piracy or naval warfare; it includes environmental, legal, and technological dimensions.
- Critical infrastructure in the maritime environment is under-protected and highly interdependent, especially energy, and data critical infrastructure, presenting security challenges for countries and regions around the globe.
- Certain areas of maritime security remain unaddressed by existing legal frameworks such as UNCLOS, particularly in the context of Critical Infrastructure at sea.

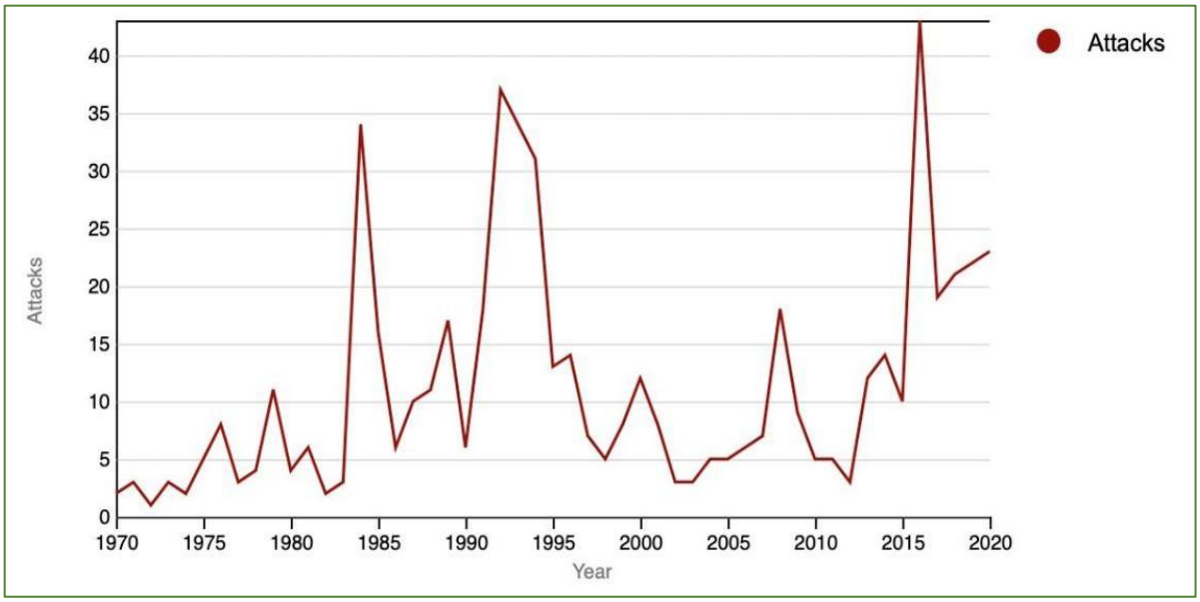
"Overview of Threat Actors,"

Mr. William Liffick
Former U.S. Coast Guard
Special Operations Officer

Former U.S. Coast Guard officer William Liffick provided a sweeping overview of various threat actors in the Maritime environment.

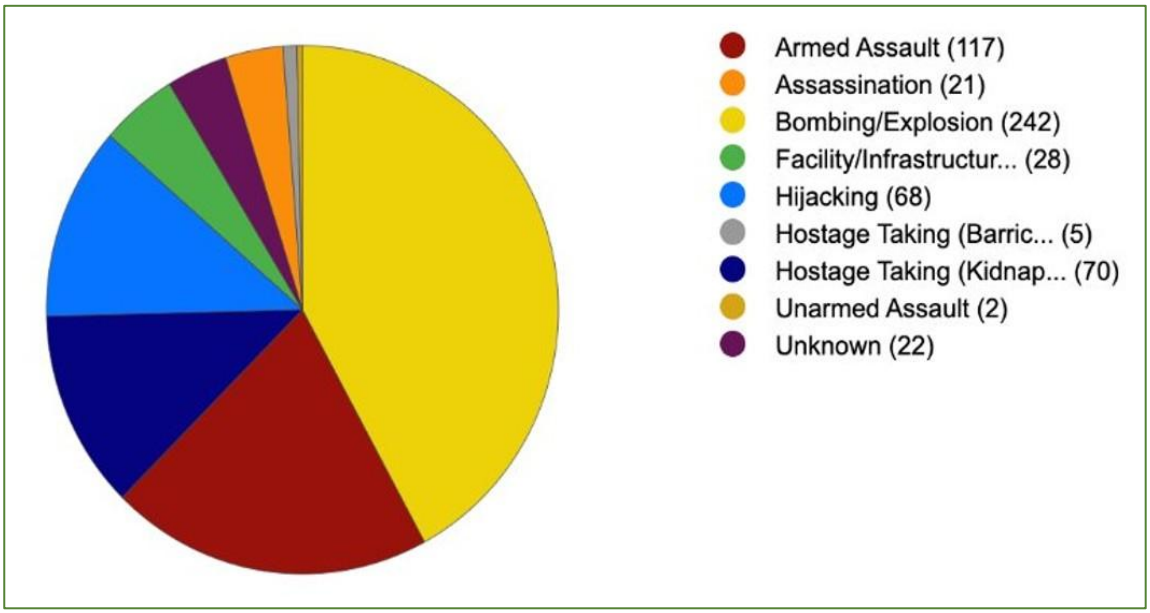
Using data from 1970-2020, Mr. Liffick demonstrated that terrorist activities at sea have been relatively few, especially when compared to land-based terrorist incidents. However, addressing maritime terrorism is important because certain terrorist activities at sea could have major consequences for trade and present considerable challenges for CT, given the uniqueness of the maritime environment. Furthermore, terrorist activities at sea could have cascading effects and impact activities in all other domains. Finally, terrorists could use the maritime environment to facilitate other forms of terrorism, including transporting chemical and biological materials, weapons, and counterfeit goods.

Number of Attacks since

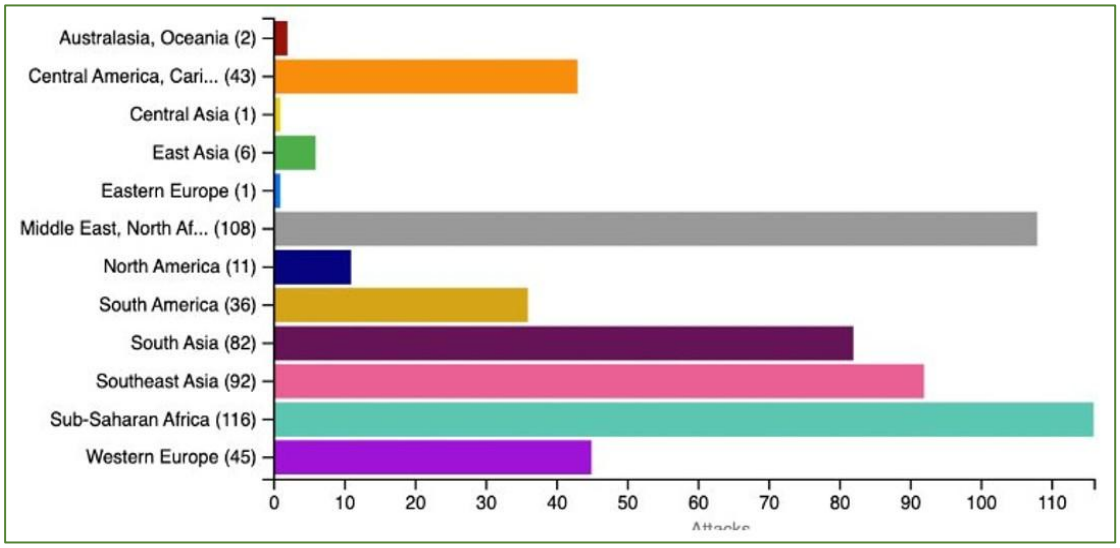


Given these points, maritime terrorism should still be treated as a serious concern due to key vulnerabilities at sea, including undefined or poorly monitored maritime boundaries, limited detection capabilities, and the critical importance of ports and canals for global trade.

Type of Attacks since 1970



Region of Attacks since



Where maritime boundaries are unclear or loosely controlled, terrorists can exploit the lack of oversight. Although similar weapons and tactics are used in comparison to attacks on land, maritime targets remain appealing because of their strategic importance and the difficulty of detection. Ports and canals are critical for global trade, yet they are highly exposed and hard to monitor effectively.

Logistics of distribution and illegal smuggling represent a major vulnerability in ports and at sea. Currently, there is no clear international strategy or plan in place to contain or prevent such activities. Lack of access to containers means authorities are often unable to inspect for

or detect chemical, biological, or nuclear weapon materials at sea, which increases the risk of undetected transport and use of such threats. Mr. Liffick described this challenge as looking for a "needle in a needlestack."

Furthermore, the threat is evolving with drones and cyber tools, as seen in South America where drones are increasingly used in narcotic operations, and in North Africa where non-state actors and violent extremists exploit these technologies.

As an example of the complexity of protecting and addressing potential terrorist activities at sea, Mr. Liffick provided the scenario of a cross-country ferry being hijacked. Which country is responsible for CT operations? Who responds and how? Who takes the lead and deconflicts a military response if needed? Who conducts search and rescue? If chemical, biological, radiological or nuclear weapons are used, do we have the ability to work in a contaminated space? These questions all reflect the complexity of a terrorist incident in the maritime environment and the need for coordinated preparation and response.

Key Takeaways:

- Maritime terrorism consists of low probability and high consequence attacks; however, when such incidents occur, they have a significant impact on trade, regional security, and naval capabilities.
- Significant vulnerabilities in the maritime environment could make terrorist activities appealing, including vulnerabilities to sea vessels, critical infrastructure at sea, and ports.
- The unique multinational nature of the maritime environment makes a response to a terrorist incident difficult, including who has jurisdiction, and who should respond to the attack and how.

"Overview of Innovations in Technology"

Colonel Vadym Slyusar,
Ukraine Army

Ukrainian Army Colonel Vadym Slyusar, an expert on military technology, provided a detailed overview of recent innovations in unmanned and autonomous systems in Ukraine's fight against Russia's illegal invasion and full-scale war since 2022. He focused specifically on unmanned systems at sea, highlighting the growing relevance of Unmanned Surface Vehicles (USVs) and First-Person View (FPV) drones, with a specific emphasis on their combat use and battlefield applications.

USV Magura

Regarding unmanned sea-based systems, he discussed USV strike teams in Ukraine and noted the effectiveness of these systems and their ability to conduct long-range strikes up to 800 kilometres. These systems have been used as part of sea denial strategies and in asymmetric targeting of bridges and tankers. Furthermore, these USVs are often combined with UAVs and loitering munitions for complex multi-domain operations. The successful employment of these systems has forced Russia to deployed pontoons around the Crimean Bridge to block or absorb incoming USVs and prevent them from reaching critical infrastructure points.

FPV Kamikaze with Termobaric Munitions

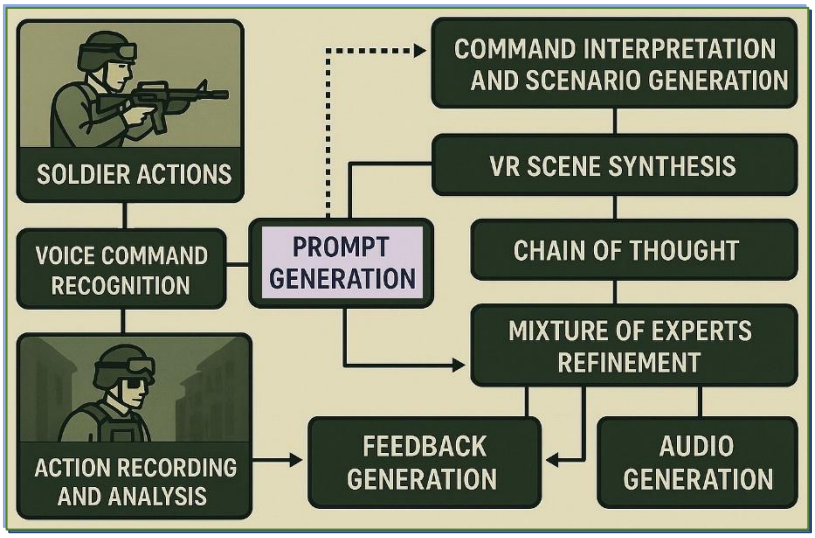
Improvised FPV Loitering Munitions

Other critical innovations include the continuing evolution of FPV drones, which have proven highly effective in land-based Intelligence, Surveillance and Reconnaissance (ISR) and strike roles, especially as loitering or kamikaze platforms equipped with 3D-printed or

thermobaric munitions. The use of fiber-optic guidance systems has enabled more secure and precise missions that evade electromagnetic warfare measures. Drones have been equipped with onboard object recognition to detect ships, boats, mines, personnel, and underwater threats. And the use of multi-agent drone systems allows for swarm coordination and autonomous behavior.

Perhaps the most important innovation on the battlefield right now is the emerging use of AI in weapons systems. AI-assisted decision support is being developed for soldiers through personal assistant systems capable of text processing, translation, mission planning, and tactical prediction. AI-guided FPV drones can maintain a lock-on-target, even if communications are lost.

LLM for Training



Some near-future technological innovations may include combining fiber-optic control with AI guidance to increase precision; the integration of drone systems into soldier-level battlefield roles; Large Language Models (LLMs) being integrated into VR-based combat training for generating scenarios and enabling more adaptive soldier-environment interaction; and AI playing a role in real-time battlefield decision-making, mission planning, and logistical support.

Key Takeaways:

- Emerging technologies are reshaping the battlefield, though maritime adaptation lag behind land and air base systems.
- USVs and FPV drones show strong promise, especially when combined with AI and real-time data processing.
- Legal, environmental, and operational constraints still pose limits to full maritime integration.

Takeaways from Day One Breakout Sessions

In the afternoon, participants broke out into four small groups to discuss the morning's briefings. These groups identified the following takeaways:

Regarding MDO

- There is still confusion over what MDO is, and what about it is new.
- While MDO as a concept is not entirely new, it continues to evolve as a concept, and the depth and speed of integration across domains makes it challenging, particularly in the cyber and space domains.
- The limited availability of trained personnel, especially in high-demand sectors like cyber, will be a challenge for implementing MDO, as will information sharing in cyberspace between states.
- Digital infrastructure and effective Command and Control (C2) structures are needed for MDO to work effectively, but it is unclear how they should look at this time.

Regarding threats and opportunities in the maritime domain

- Maritime threat actors could be defined as any actor—state or non-state—capable of disrupting maritime operations or controlling strategic maritime chokepoints.
- Ecoterrorism, which includes deliberate attacks or disruptions aimed at damaging infrastructures that affect the environment and national stability, is also a concern in the maritime environment.
- Critical Infrastructure is not limited to undersea elements like cables or pipelines, but also includes interconnected systems on land, such as ports and energy facilities, making securing these vital resources challenging.
- The complexity of the threat landscape makes it difficult to implement comprehensive strategies.

Regarding technological innovations

- Cheap and widely available technologies, like drones, may make it easier for non-state actors to carry out disruptive actions in the maritime domain and elsewhere.
- Artificial Intelligence (AI), Cyber capabilities, Autonomous Unmanned Systems, and chemical weapons are just some of the existing and future threats in the maritime environment.

DAY II

May 15, 2025

SOF Activities in the Maritime Domain

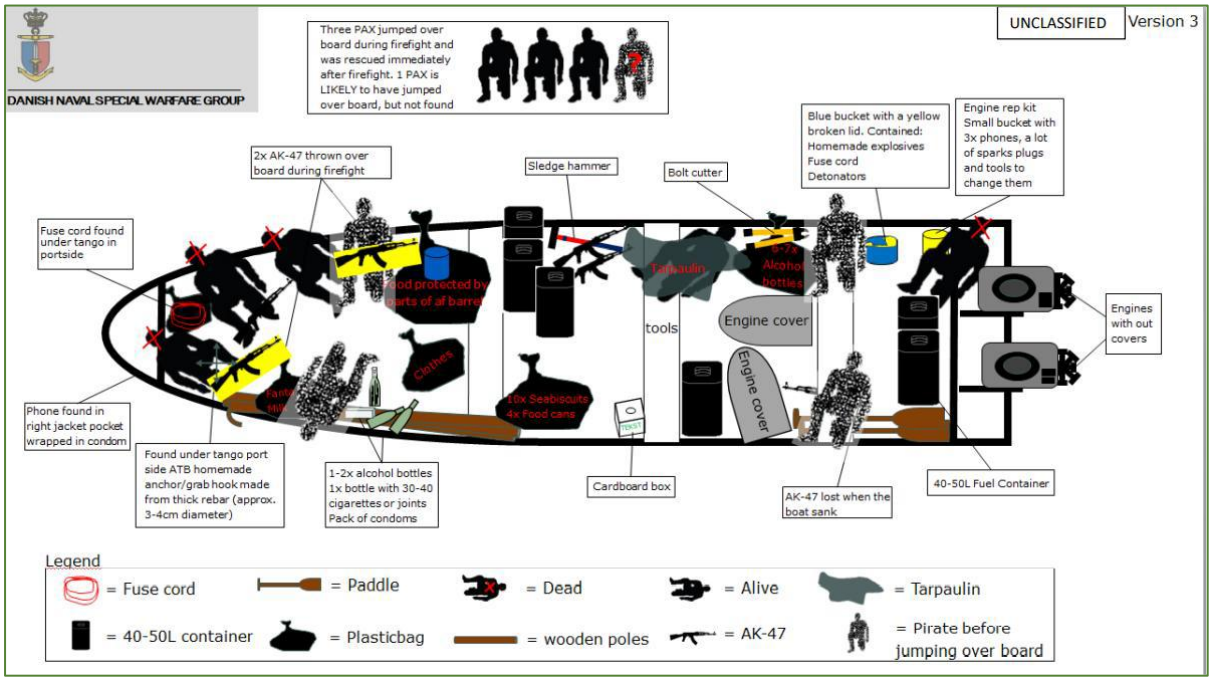
Day two began with a panel that focused on specific countries' experiences with SOF activities in the maritime environment.

"SOF CT/Counter-Piracy Operations: The Danish Experience"

CDR Alexander With,
Royal Danish Defense College

In 2021, Denmark deployed the frigate Esbern *Snare* to the Gulf of Guinea with the mission of reducing piracy and ensuring freedom of navigation for commercial vessels transiting these waters. Pirates in the Gulf of Guinea were targeting commercial ships because they were relatively slow, unarmed, easy to board, and because most countries were willing to pay the ransom for the crew. As the home to the largest shipping company in the world, Maersk, ensuring freedom of commercial navigation was in Denmark's national interest.

CDR Alexander With, Royal Danish Navy, delivered an in-depth presentation on the tactics used by pirate groups in the Gulf of Guinea, including their preparation, targeting methods, and boarding equipment. He then described the operational sequence of the Danish response and the role of military assets, including actionable intelligence, how helicopters were used to find pirates, and the composition of the Danish frigate that interdicted the pirates. He noted that, in addition to SOF and other forces, the team utilized an anthropologist to explain symbols and the behavior of pirates.



CDR With highlighted one of Denmark's counterpiracy operations that resulted in the death of several pirates, the wounding of another, and the capture of several more, presenting challenges for how to repatriate the living pirates and what to do with the wounded pirate in keeping with humanitarian concerns. His analysis emphasized the practical challenges of a real-time naval response, and the tactical decisions made under pressure in a hostile environment.

Critically, CDR With noted that Denmark's counterpiracy operations were a success from a military standpoint and helped reduce piracy activity by 82 percent in the Gulf of Guinea. However, the operations were challenging from a political standpoint and received criticism from some actors in the region and back at home, particularly regarding the injured pirate that had to be brought back to Denmark for treatment.

Key takeaways:

- Creating a team with the right mix of capabilities is crucial for anti-piracy success, including naval SOF, medical professionals, intelligence, and individuals with arrest authority.

- Intelligence is crucial, and good intelligence requires working with allies and partners. Denmark relied on the Maritime Domain Awareness Trade - Gulf of Guinea (MDATGOG) to get actionable intelligence, a British and French-led centre. The Danish navy also used helicopters in combination with intelligence to track down the pirates.

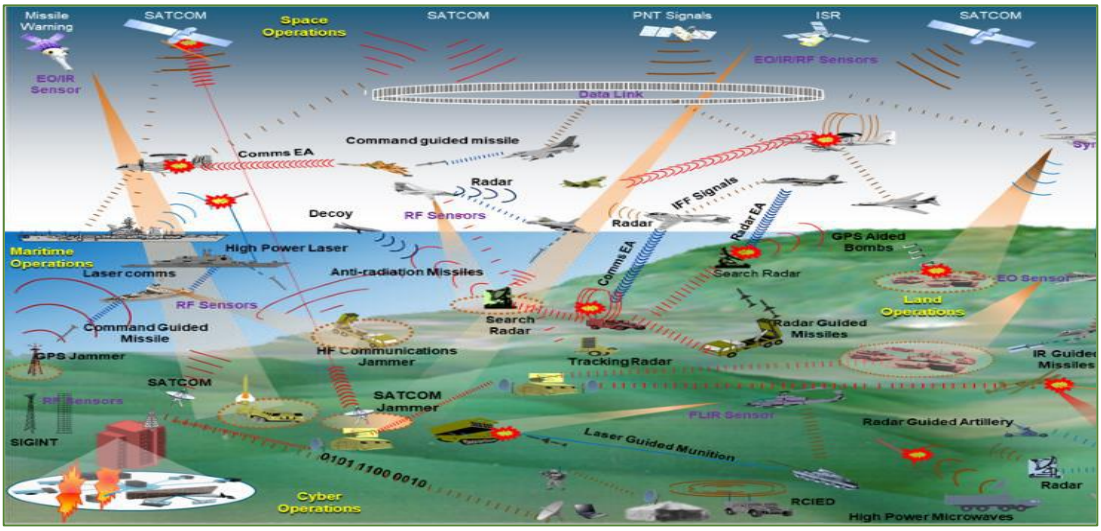
- Counter piracy from a military standpoint is easy relatively easy if you have the right toolbox, but managing the political piece also requires explaining operations back home, diplomacy with countries in the region, and devising a plan for what to do with pirates that live.

"SOF and Maritime Operations in the Black Sea"

CDR Dave STARKEY,
Royal Navy (UK)

Focusing on the operational complexity of contested maritime environments, CDR Dave Starkey addressed the growing need for MDO in the maritime context, using Ukrainian Naval Forces operations in the Black Sea as his case study.

CDR Starkey defined contested environments as operational spaces where access is actively denied, both physically and electronically. He described how contested environments materialize in practice, including advanced radar systems, mines, and anti-access strategies. In the maritime domain, challenges arise from naval mines, anti-ship missile systems, and persistent surveillance. These activities are further intensified by technology and irregular tactics, including cyber intrusions, electronic warfare, surprise attacks, deception, and the manipulation of civilian populations.



CDR Starkey emphasized that traditional models of warfare are no longer sufficient in today's contested environments, which demand an integrated approach across all domains: land, sea, air, cyber, and space. He underscored the growing necessity of involving SOF in maritime contexts, including for penetrating coastlines and operating in underwater environments, but also for fostering interoperability and collaboration among allied forces.

As a case study, CDR Starkey discussed activities in the Black Sea between March 2022 and March 2024. These operations demonstrate the successful implementation of unmanned systems and MDO. He noted that Ukraine's use of Unmanned Surface Vehicles (USVs) and Unmanned Underwater Vehicles (UUVs) led to the degradation of approximately 40 percent of the Russian fleet in the Black Sea with an estimated financial loss to Russia of over $1.5 billion. All of this occurred without Ukraine having its own navy.

Key takeaways:

- The deployment of USVs and UAVs in the Black Sea demonstrates the significant operational impact these weapons systems can have on the modern battlespace.
- Speed, maneuverability, and communication resilience are critical factors for operational success in the maritime environment.
- SOF can be a force multiplier in the maritime domain and can help penetrate coastlines, work in underwater environments, and foster interoperability and collaboration among allied forces.
- Electronic warfare remains one of the biggest obstacles to mission success, especially with regard to maintaining communications.

"The Concept of Navy SOF in Countering Terrorism"

Capt. Mehmet Deniz ÇETİKLİ,
Turkish Naval Forces

Turkish Navy SOF are small, highly trained elite units capable of conducting high-risk, covert missions across land, air, and sea. Capt. Mehmet Deniz ÇETİKLİ, provided an overview of Turkish Navy SOF, and their abilities to counter terrorist activities across all domains of warfighting, beginning with their initial use in World War II and progression through Cold War deployments to their post-Cold War transformation.

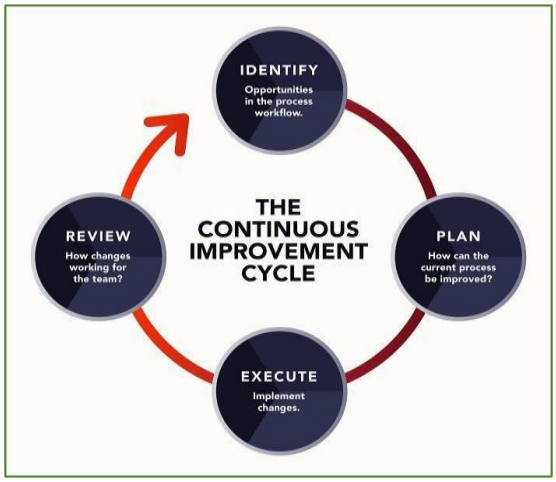
Grounding his analysis in Edward Scott's framework, Capt. Çetikli defined maritime terrorism through five key elements: unlawful activity, acts of violence and disruption, psychological intimidation and fear, political motivation, and specific demands.

Capt. Çetikli then provided succinct summaries of key Turkish SOF operations, including:

- Operation Lucky S (1993), a joint effort involving Turkish SAT commandos, the U.S. DEA, and local police units the Suez Canal.
- Operation Kartepe (2011), in which Turkish SOF successfully freed a sea bus and 24 passengers hijacked by a PKK terrorist organization affiliated suicide bomber.
- Operation Euphrates Shield (2016–2017), conducted under the right of self-defense articulated in Article 51 of the UN Charter.
- Operation Commander Tide (2017), in which Turkish SOF, in coordination with the coast guard, police, and gendarmerie seized more than 1,070 kilograms of illegal narcotics.

- Operation Olive Branch (2018), which involved Turkish SOF working alongside the Free Syrian Army in northern Syria and included training and capacity building for local forces.

- Operation Active Endeavour (2001), initiated in response to the 9/11 attacks and marking NATO's first invocation of Article 5. This operation later transitioned into Operation Sea Guardian in 2016, which adopted a broader, more flexible mission that supports capacity-building and covers the full range of maritime security tasks.



Capt. Çetikli concluded his presentation by emphasizing the need for SOF to continually adapt to the changing threat environment. To illustrate the strategic role of SOF within NATO's structure, Capt. Çetikli used a clear metaphor: NATO is a fortress, and SOF is the hidden sword inside—silent, precise, and activated only when the outer defenses are breached. He highlighted the increasing use of technologies by terrorists, including artificial intelligence, machine learning, and use of drones, has made the operational landscape more complex and unpredictable. While these units are already highly capable, Capt. Çetikli argued that the evolving nature of threats requires SOF to regularly update their training, revise operational doctrines, and enhance interagency coordination.

Takeaways:

- SOF must continuously adapt to dynamic and evolving threats, including the increased use of advanced technologies by terrorist groups.

- Naval SOF is a critical asset in counterterrorism, particularly given their multidomain proficiency.

- Highly trained SOF units can be adapted to a variety of missions. SOF offers a more flexible and cost-effective approach.

- Efficiency of SOF units can be increased with regularly updating training programs, revising strategic policies, and enhancing interagency coordination.

“Counter Terrorism within Maritime Security”

Capt. Levent BAHADIR,
MARSEC-COE

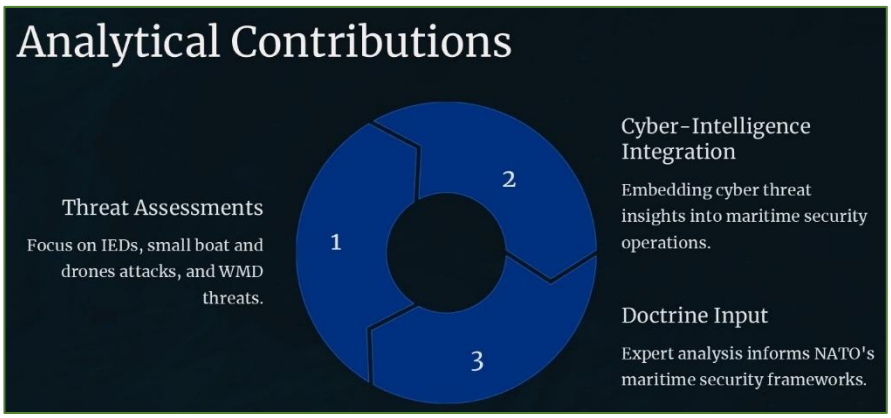
In his presentation titled *"Counter Terrorism within Maritime Security,"* Captain (N) Levent BAHADIR provided a comprehensive exposition of the NATO Maritime Security Centre of Excellence (MARSEC COE), headquartered in Istanbul, Türkiye. The Centre, established under the leadership of the Republic of Türkiye and officially sponsored by Greece, Romania, and Portugal, stands as a pivotal NATO-accredited institution dedicated to enhancing the Alliance’s capacity in addressing maritime security threats, including those associated with terrorism.

Captain Bahadır underscored MARSEC COE’s multidimensional mandate, which revolves around three primary pillars: the provision of education and training to partner and Allied nations; the development, refinement, and dissemination of NATO maritime doctrines; and the systematic evaluation and feedback of operational activities and exercises to ensure continuous institutional learning and adaptation.

The central theme of the presentation was the dynamic and evolving character of threats in the maritime domain. Captain Bahadır emphasized that the Centre's contributions follow a cyclical model of adaptation, responsive to the fluid nature of emerging risks. Among the core contributions highlighted was MARSEC COE’s engagement in threat analysis, particularly concerning non-traditional and asymmetric threats. These include the employment of improvised explosive devices, the use of small boats in swarm or suicide-style attacks, the

proliferation and potential deployment of Unmanned Aerial Vehicles (drones), and the risk of maritime conveyance of weapons of mass destruction.

Crucially, Captain Bahadır drew attention to the rising prominence of cyber intelligence within the maritime security architecture. He stressed that cyber threats constitute a persistent and cross-cutting vulnerability across all dimensions of maritime activity. In this regard, cyber intelligence capabilities are not merely supplementary but foundational to effective maritime counterterrorism responses.



In a second major area of focus, Captain Bahadır addressed the role of MARSEC COE in shaping NATO's doctrinal landscape. Through sustained collaboration with other NATO Centres of Excellence—most notably other COEs in the Maritime domain—MARSEC COE contributes to integrating advanced technologies, such as autonomous maritime platforms and aerial surveillance drones, into strategic effects. These engagements allow the Centre to anticipate future threat vectors and identify opportunities for capability development.

Captain Bahadır concluded his remarks by reaffirming the Centre's strategic mission: to assist NATO in recalibrating its counterterrorism posture for the maritime environment. This includes the delivery of tailored education programs to partner nations, as well as the provision of informed strategic guidance to NATO leadership. In doing so, MARSEC COE offers its support to strengthen the Alliance's readiness and adaptability in the face of a rapidly transforming threat landscape at sea.

Takeaways:

- MARSEC COE provides a unique space that focuses on maritime operations, including CT, and helps NATO understand the emerging threats in this domain from an MDO perspective.
- Hostile activities in the maritime environment require dedicated cyber intelligence to counter. This is one of MARSEC COE's priorities.
- Doctrine, training, and lessons learned in operations should be a virtuous cycle that improves operational performance and capabilities. This is MARSEC's goal.

Discussion

The case studies raised several questions from participants. The Director of COE-DAT, Colonel Halil Sıddık AYHAN, raised a particularly salient question regarding the Danish experience in the Gulf of Guinea:

"Although terrorist organizations (TO) threaten the stability and security of the country and the well-being of its citizens, it is undeniable that fighting them provides some benefits to the security forces. The security forces that fight against the TO gain combat experience, operational readiness, technological advancement and adaptation, improve intelligence network and achieve faster decision-making mechanism as in the example of NATO that gained this experience in Afghanistan and Turkish Armed Forces that had this capability fighting against PKK. So how did this counter-piracy mission in the Gulf of Guinea affect Denmark's naval forces, for example in operational doctrine, tactical capabilities or revising the standards or operational procedures etc."

CDR With responded:

"The greatest new knowledge was that pirates who are spiritual/religious might greatly overestimate their chances of winning a gunfight against a superior force and thereby decide to engage in what we would consider suicidal encounters. Our SOF and helicopter contingent did reevaluate their TTP's, but I don't think they changed too much due to 1) What we did already worked and was the refinement of previous counter piracy tactics developed after our operations off the Horn of Africa, and 2) Russia invaded Ukraine and that changed the focus of the Danish navy away from counter piracy. I agree that experience from fighting can give valuable lessons, but it can also take focus away from one's primary competencies. As of current, the primary goal of the Danish military is deterrence and the ability to fight a peer adversary. Focusing on pirates is probably a distraction in that regard."

Exercise: A maritime CT Scenario and the Need for MDO Solutions

In the afternoon, participants turned to a discussion-based exercise designed to bring together core concepts explored throughout the workshop, especially the application of MDO in complex terrorist activities at sea.

Participants were given the following “synthetic” scenario based on fictitious geography, countries, and terrorist groups:

On 16 May 2025, Crelix’s commercial carrier ship “Hope” declares ***force majeure*** due to a problem with the engine in the straits of Almandrada. It is carrying a dangerous amount of ***ammonium nitrate*** and is requesting permission to dock on the international shared port belonging to the nation of Averis and Baldora. Upon hearing this the northern country of Dunessa sends a comprehensive intelligence report that the ship has a remotely controlled explosive device onboard and was destined to carry out a terrorist attack on Dunessa’s soil. This report details the terrorist group “Green Resolve” was planning to detonate this device to disrupt commercial shipping further up the strait to bring awareness to the environmental impacts of the shipping sector and the dependence on commercial goods. They believe in sustainable small economics and despise the globalized commercial industry. While the specification of the device is unknown, it could be triggered remotely by a satellite signal. The utmost care must be taken to ensure that the device does not detonate since the secondary explosion of the ammonium nitrate could cripple shipping traffic for weeks, costing the global economy billions, cause catastrophic damage to facilities, and kill hundreds of civilians. The ship is requesting to dock on a shared island in the middle of the strait where both Averis and Baldora have a shared military and civilian presence due to a bilateral security agreement.

You and your team must devise a whole of government plan to apprehend the terrorists and crew, disable or eliminate the threat, and consider a response plan if the device were to detonate.

Participants were divided into four groups and each given a course of action (COA) from which to create an operational plan. Responses were limited by country-specific and UNCLOS laws and required an international, MDO, and whole-of-government approach to counter.

COA 1: A discreet SOF assault to render the vessel safe in port. The *Hope* will be allowed to come to port, where SOF forces will board the ship, posing as port authorities and engineer staff, to secure the device and the ship.

COA 2: Vessel boarding while ship underway in territorial waters. SOF intercepts and boards the ship while in shared territorial waters between Averis and Baldora. The crew will disembark, and SOF will deactivate the device.

COA 3: Cyber and electromagnetic attack (CEMA) on ship in international waters. The ship will be stopped via a CEMA attack, and electronic jamming will prevent the device from detonating, allowing SOF to board and secure the ship.

COA 4: The ship is stopped, immobilized, and sunk in international waters. Naval assets will order the ship to stop, disembark the crew, and then sink the ship.

Discussion

Each of these COAs required participants to think beyond the maritime environment and include an MDO, whole-of-government approach to their answer as well as assessing risk and likeliness of success.

Group One focused on a SWOT analysis (Strengths, Weaknesses, Opportunities and Threats) for bringing the ship to port.

- **Strengths** included the covert nature ensured an element of surprise with the assumption that they could exploit intelligence assets and leverage joint operations, which were already well-practiced among involved actors.
- **Weaknesses** included high operational complexity due to the number of actors involved and potential interagency friction.
- **Opportunities** included practicing interoperability and coordination and testing real-time command flexibility and discreet coordination.
- And **threats** included political fallout in the case of failure, environmental damage in the case of uncontrolled detonation, and the erosion of public trust if STRATCOM fails to manage the narrative.

Group Two focused on **Operational Planning** for boarding the ship in territorial waters, specifically:

- The operation was designed to proceed in a non-escalatory manner, involving four nations and the flagship owner as stakeholders.

- The planning was structured around a coalition task force supported by all relevant departments, including the ministry of foreign affairs, to ensure broad coordination.
- Tasks were allocated based on national systems and agency structures, and efforts were made to establish which agency would hold responsibility for specific aspects of the operation.
- Real-time intelligence sharing was essential for maintaining operational coherence.
- STRATCOM planning was integral to preventing panic. Only critical institutions such as hospitals and local police would be informed in real time, and only if a worst-case scenario occurs.

Group Three focused on **Operational Planning** to execute a CEMA attack on the ship**:**

- A combined headquarters between Averis and Baldera would synchronize efforts.
- Stakeholders were clearly defined. The Department of Defense was assigned as the lead agency, supported by Cyber Command, Department of Justice (DOJ) and STRATCOM.
- Response actions included regaining cyber control of the vessel, using SOF to board the vessel, and using EOD to secure the explosive device.
- After securing the vessel, the ship would be escorted through a safe maritime corridor to a designated harbor.
- A coordinated STRATCOM plan would be vital to delivering a consistent external message and preventing mis- and disinformation from spreading.
- Legal justification for the operation was based on UNCLOS; the vessel posed a threat to the environment, civilian maritime traffic, and critical infrastructure.

Group Four focused on **Operational Planning** for shipping the sink in international waters:

- Averis Special Operations Forces (SOF) were assigned to board the vessel, due to their advanced maritime training.
- Baldera contributed SWAT and EOD units to support the tactical phases of the operation.
- Coordination with the vessel's flag state was considered essential due to the legal, political, and financial consequences of a total loss.
- The group discussed advance arrangements with environmental agencies to address seabed contamination and the long-term ecological impact of sinking the ship.
- The issue of crew compliance was raised as a key variable that could affect successful execution of the plan.

DAY III

May 16, 2025

Summary of Workshop

The workshop concluded with a summary discussion based on the presentations and exercise. Key takeaways included:

- MDO provides a holistic and flexible framework that synchronizes land, air, sea, cyber, and space domains to address increasing hybrid and complex security threats and will enhance the effectiveness of various missions when properly integrated.
- SOF serves as a key enabler in MDO-CT operations, offering early presence, unique access and placement, and the ability to operate across all domains simultaneously. SOF can be a role model for an MDO mindset.
- Maritime security involves more than piracy or naval warfare; it includes environmental, legal, and technological dimensions. Critical infrastructure in the maritime environment is under-protected and highly interdependent, especially energy, and data critical infrastructure, presenting key vulnerabilities for countries and regions around the world.
- The convergence of terrorism, organized crime and other irregular threats require integrated, cross-domain responses that includes actionable intelligence, law enforcement, and military actors.
- SOF can be a force multiplier in the maritime domain and can help penetrate coastlines, work in underwater environments, and foster interoperability and collaboration among allied forces. SOF offers a more flexible and cost-effective approach than conventional forces. Naval SOF is a critical asset in CT, particularly given its multidomain proficiency.
- Creating a team with the right mix of capabilities is crucial for anti-piracy success, including naval SOF, medical professionals, intelligence, and individuals with arrest authority. STRATCOM and diplomacy are also important in counter-piracy operations. It is possible to be militarily successful but create political complications if counter-piracy operations are not holistically thought out.
- Emerging technologies are rapidly reshaping the battlespace, though maritime adaptation lags behind land and air base systems. The deployment of USVs and UAVs in the Black Sea demonstrates the significant operational impact these weapons systems can have on the modern battlespace. The effects of electronic warfare remain a persistent challenge in the modern-day battle space.

- Doctrine, training, and lessons learned in operations should be a virtuous cycle that improves operational performance and capabilities.

Biographies

Navy Captain Levent BAHADIR:

Graduated from the Turkish Naval Academy in 2003. He served as a Communications Officer onboard a ship from 2003-2005 before successfully completing Maritime SOF Selection Course in 2006 and joining the Turkish Maritime SOF Command.

Between 2006-2021, CAPT Bahadir assumed numerous posts in Turkish Maritime SOF Command, including SOMTU (Special Operation Maritime Task Unit) Commander, SOFEVAL (SOF Evaluation) Staff Officer, Operation Branch (J3) Staff Officer, SOMTG (Special Operation Maritime Task Group) Commander, Head of Logistic Branch (J4), and Head of Personnel Branch (J1).

CAPT Bahadir NATO, EU and UN deployments include: Operation ACTIVE ENDEAVOR (As SOMTU Commander in 2009 and 2011), UNIFIL (As SOMTU Commander in 2009), Operation OCEAN SHIELD (As SOMTU Commander in 2010), Operation UNIFIED PROTECTOR (As SOCC LNO to MCC onboard ITS GARIBALDI in 2011), Operation ALTHEA (As J2 Staff Officer in 2016-2017), Operation Sea Guardian (As SOCCE Commander in 2019-2021), and SHAPE Office of Special Operations (OSO) in Mons, Belgium (As SO in 2021-2024).

CAPT Bahadir's academic background includes a bachelor's degree in Industry Engineering from the Turkish Naval Academy (2003); a master's degree in Maritime Safety, Security and Environment Management from Dokuz Eylül University (2015); and a PhD in Security Research from the Turkish National Defence University (2024).

Since August 2024, CAPT Bahadir has been assigned as MARSEC COE WMD SO and is also acting Concept and Doctrine Branch Head.

Colonel Jose CABRERA:

Currently serves as the Deputy Director at NATO COE-DAT. He is a Combat Rescue Officer in the United States Air Force. He also serves as the United States Senior National Representative at NATO COE-DAT.

Colonel Cabrera previously commanded Pararescue units at the Team, Squadron, and Group level and served as a joint planner in multiple headquarters staffs. He has led combat missions in Operations Iraqi Freedom, Enduring Freedom, Unified Protector, New Dawn, and the Horn of Africa.

Colonel Cabrera is a graduate of the National Defense University Eisenhower School and holds master's degrees in International Relations, Operational Art and Science, and National Resource Strategy.

Navy Captain Mehmet Deniz CETIKLI:

He was born in 1981. He graduated from the Turkish Naval High School in 1999 and from the Turkish Naval War College in 2003.

Captain CETIKLI was deployed at the Amphibious Brigade from 2003-2005. In 2006, he qualified as a Navy Special Force Operator and, from 2006-2019, he served in various positions within the Navy SOF Community.

In 2019, Captain CETIKLI was assigned as Head Exercises Planning post of NATO Maritime Interdiction Operational Training Center at Crete-Greece, a position he held until 2022. From 2022-2024, he was assigned to the NATO Maritime Security Centre of Excellence (NATO MARSEC) as the WMD Staff Officer.

Currently he is the Commanding Officer of Turkish Navy SOF South.

Captain CETIKLI is married to Mrs. İnci CETIKLI and has one son and daughter. He speaks English and Greek.

Dr. Heather S. GREGG:

She is a research fellow for the Future Security Initiative at Arizona State University and senior nonresident fellow at the Foreign Policy Research Institute.

Dr. Gregg's academic focus is on irregular warfare, hybrid threats, terrorism and counterterrorism, causes of extremism, and leveraging culture in population centric conflicts, including resiliency and repairing communities and national unity in the wake of war and political instability. She has held several academic positions in the U.S. Department of Defense, including professor of Irregular Warfare/Hybrid Threats at the George C. Marshall European Center for Security Studies (2023-2024), professor of military strategy at the U.S. Army War College (2019-2022), and associate professor at the Naval Postgraduate School in Monterey, California, where she worked primarily with Special Operations Forces (2006-2019).

Dr. Gregg holds a PhD in Political Science from the Massachusetts Institute of Technology, and a master's degree from Harvard Divinity School. She has published extensively on irregular warfare/hybrid threats, religiously motivated conflict, and terrorism

Lt Col Karl HEARNE:

He is a British Special Operations Forces Officer. He is currently Head of Global SOF Partners Team and Couter Terrorism Lead at NATO SOCOM Headquarters in Mons, Belguim, a position he has held since October 2022.

Lt Col Hearne has 37 years of military service, with 31 years in Special Operations Forces. He has deployed operationally across Africa, the Levant, Afghanistan, the Arabian Peninsula and the Balkans. Previous postings have included training positions, but the majority of his career has been operationally focused in UKSF roles.

Lt Col Hearne's civilian educational achievements include earning an MSc in Security and Risk Management in 2008 from Loughborough University in the UK. Lt Col Hearne is a British late entry officer, so he has promoted through the ranks before commissioning. This is his first NATO tour and his last before he retires in 2026.

Mr. William LIFFICK:

He is a former U.S. Coast Guard Special Operations Officer renowned for expertise in maritime counter terrorism, intelligence, and transnational crime.

Mr. Liffick spent most of his career in Special Operations combating Maritime Counter Terrorism and securing critical infrastructure before transitioning to military intelligence. Working closely with the Intelligence Community, he leveraged joint capabilities and a multi-billion-dollar asset registry to enhance operational effectiveness in high-risk environments. Specializing in special operations integration in Central and South America, he led efforts to disrupt transnational crime and enhance regional stability with 30+ nations. He earned accolades and underscored the military's vital role in safeguarding national interests and protecting critical infrastructure.

Mr. Liffick holds a master's degrees in international relations and global security and other certificates from the U.S. Naval War College, NATO, and Texas A&M Bush School of International Affairs. He remains passionate about advancing security initiatives and shaping international strategic policies as an instructor at the NATO School Oberammergau teaching Maritime Counter Terrorism and as a contributing author to NATO's Counter Terrorism Reference Curriculum.

Colonel Vadym SLYUSAR:

He is the Chief of R&D Group, Central Research Institute of Armaments and Military Equipment, Armed Forces of Ukraine.

Colonel SLYUSAR earned his Ph.D. in 1992, became a Doctor of Sciences in 2000, a professor in 2005, and an Honored Scientist and Technician of Ukraine in 2008. Since 2009, he has been a Member of the Editorial Board of the SCHOPUS-indexed journal *Radioelectronics and Communications Systems*.

Colonel Slyusar has almost 40 years of research experience in the areas of radar systems, wireless communications and, more recently, AI. His scientific portfolio includes 72 patents and almost 1020 publications. Additionally, he has been the scientific advisor of 16 PhDs and two Doctors of Science.

Currently, Colonel Slyusar is the Head of the National Delegation in NATO Army Armaments Group (NAAG) and NATO Technical Exploitation Group (NTEG).

Commander Dave STARKEY:

He joined the Royal Navy in 2005 as a Warfare Officer, specialising as a Mine Clearance Diving Officer and EOD/IEDD Operator, a Principle Warfare Officer and is also Commando trained.

CDR Starkey has deployed on numerous operations in the maritime and land domain and is an experienced Staff Officer, having planned and delivered both Royal Navy and Joint Operations. Dave also spent three years creating and then delivering bespoke training to generate Battlestaffs in the UK and internationally. Dave has held command appointments as Commanding Officer of several Diving and EOD Units including Delta Squadron, Echo Sqn, The Autonomy Team and Gibraltar CDE. He has also been Chief of Staff to three Battlestaffs.

Dave is currently responsible for delivering Maritime Operations for UKSF.

Commander Alexander WITH:

Royal Danish Navy, is currently a military analyst at the Royal Danish Defence College, in Copenhagen, Denmark.

Commander WITH is a former army captain. He holds a master's degree in international security and law at the Center for War Studies, University of Southern Denmark. He has been deployed with both the Danish Army and Navy, including as a pirate hunter in the Gulf of Guinea from 2021-2022.

Commander WITH teaches joint operations, in addition to researching the war in Ukraine. He has written extensively about military history and the war in Ukraine, including the chapter "Sea control or maritime hide and seek: Russia meets Ukrainian A2/AD in the Black Sea" in the book *Russia at War*, to be published in English this summer.

Mr. Carl WREDE:

He is Deputy Director of the Institute for the Protection of Maritime Infrastructures at the German Aerospace Centre (DLR e.V.) in Bremerhaven, Germany.

Mr. Wrede's responsibilities include the strategic planning of interactions of the institute with decision makers in policy, security and defense as well as stakeholders from the private sector. He joined the organization in 2018 and held various positions within the institute and the German Aerospace Center itself where he coordinated the development of a naval defence research roadmap.

Until 2018, Mr. Wrede was Head of Corporate Security at a Hamburg based shipping company with responsibility for the protection of several thousand seafarers and close to 200 ships on worldwide voyages. He took on this role after retiring from active seafaring as a nautical officer in merchant shipping in 2013.

Mr. Wrede is a permanent member of various working groups on maritime security, cyber security of maritime systems and ethically sound technology development in the security and defence sector. He holds a B.Sc. in Nautical Science and Logistics from Flensburg University of Applied Sciences and an M.Sc. in Risk, Crisis and Disaster Management from the University of Leicester, UK.

CENTRE OF EXCELLENCE DEFENCE AGAINST TERRORISM ANKARA, TÜRKİYE, 2025

Colonel Halil Sıddık Ayhan (TUR A)
Director, COE-DAT

Acknowledgments

Project Director
Col. Tamas Kender

Project Co-Director
Col. Serkan Karagöz

Academic Advisor
Dr.Heather Gregg

Contributors

Col. Jose A. Cabrera
Col. Vadym Slyusar
Cpt.Levent Bahadır
Cpt.M.Deniz Çetikli
CDR Alexander With
CDR Dave Starkey
Lt.Col. Karl Hearne
Mr. Carl Wrede
Mr. William Liffick

www.coedat.nato.int