MARITIME INTERDICTION OPERATIONS

Journal

Issue 27 • 2025 • ISSN: 2241-438X

NMIOTC

NATO OTAN

MARITIME INTERDICTION OPERATIONS JOURNAL

DIRECTOR

CPT G. CATAPANO ITA (N)

DIRECTOR OF TRAINING SUPPORT

EDITOR

CPT G. CHAIDEMENAKIS GRC (N)

CHIEF OF STAFF

LAYOUT PRODUCTION

LT CDR I. GIANNELIS GRC (N)

COVER PHOTO: www.cnn.gr

You may send your comments to: chaidemenakisg@nmiotc.nato.int

CONTENTS

NMIOTC
Commandant's Editorial

Welcome to the twenty-seventh edition of the NMIOTC Journal.

This year's edition takes a closer look at an issue that extends far beyond NATO and the military community—one that affects every corner of the globe: climate change, with a particular emphasis on the maritime domain. The pace of change and its far-reaching consequences are evident to us all. There is little need to catalogue statistics or disasters to grasp its global scale and impact. The maritime environment, in particular, stands among the most vulnerable and therefore demands urgent and sustained attention.

This raises a number of critical questions: What role can—and should—NATO play in addressing these challenges? How might climate change influence illegal activities at sea? What lies ahead for regions such as the Arctic?

Drawing on their expertise and experience, our contributors offer thoughtful analysis and informed perspectives on these issues. A clear and consistent

theme emerges throughout their work: the importance of dialogue and the active engagement of all relevant stakeholders. While addressing the root causes of climate change remains an urgent priority, the effective sharing of knowledge, data, and resources—alongside strengthened cooperation—will be essential to ensuring that NATO remains adaptable and fit for purpose.

As in previous editions, the second part of the Journal turns to developments in the cyber domain. It explores NATO's efforts in cyber defence, particularly in responding to—and harnessing—disruptive technologies. Our experts also examine how the European Union is adapting its cybersecurity approach to keep pace with rapid technological change.

As you read this year's NMIOTC Journal, you will notice recurring themes. These are not coincidental; they reflect the interconnected nature of today's challenges—issues that demand a comprehensive, coordinated, and forward-looking response.

Enjoy reading!

Pavlos Angelopoulos
Commodore GRC (N)
Commandant NMIOTC

Climate change in the Arctic

Consequences for naval forces

By Pedersen Knutsen

Introduction

The Norwegian government launched the slogan "High North, low tension" in 2005, summarising its policy aim of maintaining low tension and cooperative frameworks, even though Arctic states might have diverging interests. The approach relates to the concept of *Arctic exceptionalism*, the notion that the Arctic has been "a place apart", shielded from the worst tensions of international politics. It has been tied to the 1987 Murmansk Speech by Mikhail Gorbachev, where he labelled the Arctic a 'zone of peace'.[1]

Since the Russian full-scale invasion of Ukraine in February 2022, Arctic exceptionalism has deteriorated, and Norway's Arctic ambition has become to simply preserve Arctic *stability* in the face of emerging security dilemmas.[2] Meanwhile, 2024 was the third warmest year on record for the Arctic and the first year to exceed the 1.5-degree target of the Paris Agreement. It was also the third consecutive warmest summer on Svalbard.[3]

These climate changes constitute an important intervening variable between great power competition and armed conflict in the Arctic. Scholars and analysts debate whether climate change may have an impact on the possibility of conflict in the Arctic.[4] We contribute to these debates by connecting two research questions about climate security. First, *"how does climate change impact security dilemmas and the potential for armed conflict in the Arctic?"* Second, *"how will climate change impact naval operations and capabilities in the Arctic?"* To answer this question, we use the Norwegian Navy as a case study.

---

[1] M. Gorbachev, *The Speech in Murmansk: At the ceremonial meeting on the occasion of the presentation of the Order of Lenin and the Gold Star Medal to the city of Murmansk* (Novosti Press Agency Publishing House, 1987).

[2] R. Jervis, "Cooperation Under the Security Dilemma," *World Politics* 30, no. 2 (1978), https://doi.org/https://doi.org/10.2307/2009958; B. O. Knutsen and M. N. Pedersen, "How to Understand Climate Change as a Threat Multiplier in the Arctic," *Arctic Review on Law and Politics* 15 (2024), https://doi.org/https://doi.org/10.23865/arctic.v15.6500;
"Does Anyone Still Understand the 'Security Dilemma'?," Foreign Policy 2022, Accessed 10 September, 2023, https://foreignpolicy.com/2022/07/26/misperception-security-dilemma-ir-theory-russia-ukraine/.

[3] Copernicus, *Global Climate Change Highlights* 2024, Copernicus Programme of the European Commission (Brussels, 2025), https://climate.copernicus.eu/sites/default/files/custom-uploads/GCH-2024/GCH2024-PDF-1.pdf.

[4] E.g. B. O. Knutsen and M. N. Pedersen, "How to Understand Climate Change as a Threat Multiplier in the Arctic.";
T. Koivurova and A. Shibata, "After Russia's invasion of Ukraine in 2022: Can we still cooperate with Russia in the Arctic?," *Polar Record* 59, no. e12 (2023), https://doi.org/ https://doi.org/10.1017/S0032247423000049.

This short paper is organised as follows. First, we discuss the possible connections between climate change and security in the Arctic, relying on Robert Jervis' approach to security dilemmas in international relations.[5] Lastly, we analyse the impact of climate change on naval forces in the Arctic.

Climate change and security

The connection between climate change and security can be elusive. Climate change is not a direct cause of conflict. Therefore, we rely on the *threat multiplier* concept, launched by the US Center for Naval Analyses (CNA).[6] The threat multiplier concept was spearheaded by the CNA's Sherri Goodman, and labelled climate change as such because it could "seriously exacerbate already marginal living standards [...] causing widespread political instability and the likelihood of failed states".[7] In more general terms, "The threat multiplier concept refers to the tendency of climate change to multiply existing threats to security".[8]

Climate change may exert an indirect influence on established scarcities, tensions, and other drivers of insecurity.[9] New risks may emanate not from climate change directly, but due to its interaction with an aggravation of "other environmental, economic, social and political stressors that can threaten national stability".[10] This indirect relationship can be observed in the Arctic context, where melting sea and land ice and warming oceans lay bare new resources such as oil, minerals, and fish, driving increased interest.

The threat multiplier concept has drawn criticism from some scholars. For instance, Jan Selby has commented that "evidence from this research is generally weak and contradictory, and, in some cases, non-existent".[11] Selby has previously argued against the concept's application to the eruption of the Syrian Civil War.[12] However, as we have previously argued, the threat multiplier concept enjoys widespread support amongst scholars and analysts,[13] and we thus argue it provides the best lens through which we can understand the connection between climate change and security.[14]

The Arctic is the fastest warming region in the world, warming 4-7 times faster than the average global warming.[15] While only some four million people inhabit the region, the Arctic makes up approximately four percent of the Earth's surface. This underlines the entirely unique nature of climate change in the Arctic, as well as its importance. Climate change manifests particularly strongly in the maritime domain.

Projections show that the Arctic could be ice-free in the summer as soon as 2030,[16] while others show 2050.[17] A receding ice sheet eases access to coveted resources and trade routes like the Northern Sea Route (NSR). Ocean warming in the Arctic is 2.3 times faster than

[5] See R. Jervis, "Cooperation Under the Security Dilemma."
[6] Military Advisory Board, *National Security and the Threat of Climate Change*, Center for Naval Analyses (2007), https://www.cna.org/archive/CNA_Files/pdf/national%20security%20and%20the%20threat%20of%20climate%20change.pdf.
[7] Ibid., 6.
[8] S. Goodman and P. Baudu, *Climate Change as a "Threat Multiplier": History, Uses and Future of the Concept,* Center of Climate & Security (Washington, D.C., 2023), 5
[9] C. E. Werrell and F. Femia, "Climate Change as Threat Multiplier: Understanding the Broader Nature of the Risk," (The Center for Climate and Security, 12 February 2015), 2.
[10] S. Goodman and P. Baudu, *Climate Change as a "Threat Multiplier": History, Uses and Future of the Concept*, 5-6.
[11] C. S. Hendrix et al., "Climate change and conflict," *Nature Reviews & Environment* 4 (2023): 144, https://doi.org/https://doi.org/10.1038/s43017-022-00382-w.
[12] J. Selby et al., "Climate change and the Syrian civil war revisited," *Political Geography* 60 (2017), https://doi.org/https://doi.org/10.1016/j.polgeo.2017.05.007.
[13] E.g. A. Below, "Climate change: The existential threat multiplier," i *Understanding new security threats*, red. M. Gueldry, G. Gokcek, and L. Hebron (Abingdon: Routledge, 2019); T. Ide, "Rise or Recede? How Climate Disasters Affect Armed Conflict Intensity," *International Security* 47, no. 4 (2023), https://doi.org/https://doi.org/10.1162/isec_a_00459; Werrell and Femia, "Climate Change as Threat Multiplier: Understanding the Broader Nature of the Risk."
[14] B. O. Knutsen and M. N. Pedersen, "How to Understand Climate Change as a Threat Multiplier in the Arctic."
[15] K. Isaksen et al., "Exceptional warming over the Barents area," *Scientific Reports* 12, no. 1 (2022), https://doi.org/https://doi.org/10.1038/s41598-022-13568-5; M. Rantanen et al., "The Arctic has warmed nearly four times faster than the globe since 1979," Communications Earth & Environment 3 (2022), 168, https://doi.org/https://doi.org/10.1038/s43247-022-00498-3.
[16] C. Heuzé and A. Jahn, "The first ice-free day in the Arctic Ocean could occur before 2030," *Nature Communications* 15 (2024), https://doi.org/https://doi.org/10.1038/s41467-024-54508-3.
[17] D. Notz and SIMIP Community, "Arctic Sea Ice in CMIP6," *Geophysical Research Letters* 47 (2020), e2019GL086749, https://doi.org/https://doi.org/10.1029/2019GL086749.

the global average, contributing to ocean acidification.[18] Boreal fish species are migrating northwards,[19] precipitating increased interest in Arctic fishing. Maritime extreme weather will become more frequent and more powerful. This will lead to larger waves, more wind, temperature variability, precipitation, and fog.[20]

Climate change and security in the Arctic

Climate change acts as a threat multiplier in the Arctic by affecting the risk of *security dilemmas.* These dilemmas occur when states seek to enhance *their* defensive capabilities, inadvertently causing neighbouring states to feel threatened. They then implement their own security-enhancing measures, prompting the first state to require further enhancement of their defences. Thus, an armament spiral commences, leaving both states less secure.[21]

Robert Jervis proposed a matrix to understand how security dilemmas emerge.[22] The matrix, shown in Figure 1, assesses the extent to which states are able to distinguish one another's posture, and whether a region or situation favours offensive or defensive strategies. The Arctic has previously found itself safely in the doubly safe quadrant.

We have argued that climate change primarily affects the risk of security dilemmas in the Arctic by making the region more offensive-oriented. The Arctic climate has previously inhibited mobility, which, alongside Arctic Exceptionalism, has rendered the region clearly defensively oriented. However, as interest and accessibility in the Arctic increase, the region will approach a more balanced situation between offensive and defensive favour, moving towards the third quadrant.[23] This does not mean that armed conflict is necessarily more likely, but that the situation will become less predictable.

	Offensive advantage	**Defensive advantage**
Indistinguishability of posture	**(1)** Doubly dangerous	**(2)** Security dilemma, but security requirements may be compatible
Distinguishability of posture	**(3)** No security dilemma, but aggression possible. Status quo states may follow different strategies than aggressors. Warning given.	**(4)** Doubly safe

Figure 1: The security dilemma matrix proposed by Robert Jervis.

[18] A. H. Hoel, *The Geopolitics of Fish in the Arctic*, NUPI (Oslo, 2020), https://www.jstor.org/stable/pdf/resrep25736.pdf; Q. Shu et al., "Arctic Ocean Amplification in a warming climate in CMIP6 models," *Science Advances* 8, no. 30 (2022), eabn9755, https://doi.org/https://doi.org/10.1126/sciadv.abn9755.
[19] A. H. Hoel, *The Geopolitics of Fish in the Arctic*.
[20] M. N. Pedersen et al., *Kinas ambisjoner i Arktis som "nær-arktisk" stat, Forsvarets forskningsinstitutt* (Kjeller, 2025), https://www.ffi.no/publikasjoner/arkiv/kinas-ambisjoner-i-arktis-som-naer-arktisk-stat.
[21] R. Jervis, "Cooperation Under the Security Dilemma."; G. H. Snyder, "The Security Dilemma in Alliance Politics," ibid.36, no. 4 (1984), https://doi.org/10.2307/2010183.
[22] R. Jervis, "Cooperation Under the Security Dilemma."
[23] B. O. Knutsen and M. N. Pedersen, "How to Understand Climate Change as a Threat Multiplier in the Arctic."

Our research on the impact of climate change on Russian Arctic capabilities suggest that climate change will also impact the distinguishability of posture.[24] Russia considers climate change an economic opportunity more than a security threat, leaving climate mitigation and adaptation woefully inadequate.[25] Russian Arctic capabilities will be adversely affected by climate change, but Russia seems unable to sufficiently adapt them. Meanwhile, Russia seems certain that NATO and all its activities in the Arctic are inherently hostile to Russia.[26] This shows a lack of *willingness* to distinguish posture. As climate change further weakens Russian Arctic forces, this attitude is likely to worsen. As such, climate change may also make Russia less willing to distinguish the posture of NATO members in the Arctic, pushing the future of the Arctic towards the highly uncertain centre of Jervis' matrix.

The impact of climate change on the Norwegian Navy

This section analyses the direct impact of climate change on the platforms, infrastructure, and personnel of the Royal Norwegian Navy (RNN). We focus on the maritime domain for two key reasons. First, the Arctic region is approximately 70 percent ocean.[27] Second the maritime domain is the most important domain for Norway.[28]

Platforms

The main RNN platforms are frigates, corvettes, submarines, minesweepers, assault craft, logistics ships, and patrol vessels.[29] Climate change primarily affects them through activity in the Arctic. As the ice sheet retreats, areas and resources become more accessible. New actors enter the region, and extant actors increase their presence.[30] This increases the need for patrolling, Search and Rescue (SAR), fisheries inspections, and assertion of sovereignty.[31] Unless *capacity* is increased, this means that climate change can result in an increased workload for existing capabilities.

Furthermore, climate change precipitates new requirements for the construction of vessels. Parts and components such as rudders, hulls, and sonar may suffer damage caused by icing and extreme weather.[32] Icing on deck may damage stability and antennae, and limit crew accessibility.[33] Ocean acidification poses new risks to hulls. The ice sheet is also thinning and may fracture more easily, leading to large chunks of ice that may cause blunt force trauma to hulls.[34]

Extreme weather presents naval platforms with new challenges. Ice melting provides wind with more surface area to develop, contributing to larger waves.[35] Extreme weather also complicates the planning and execution of naval operations. The maritime domain will experience more frequent and more powerful storms, more fog, and more drift ice.[36] This will make navigation more difficult, reduce visibility, and expose vessels and personnel to increased physical risk.[37]

As the temperature of the upper layer of the

[24] M. N. Pedersen and B. O. Knutsen, *Vi er her for å fiske - klimaendringenes konsekvenser for russisk strategisk tenkning i Arktis*, Forsvarets forskningsinstitutt (Kjeller, 2025), https://www.ffi.no/publikasjoner/arkiv/vi-er-her-for-a-fiske-klimaendringenes-konsekvenser-for-russisk-strategisk-tenkning-i-arktis.
[25] D. Javeline et al., "Russia in a changing climate," *WIREs Climate Change* (2023), https://doi.org/https://doi.org/10.1002/wcc.872.
[26] J. Wilhelmsen and A. R. Hjerman, "Russian Certainty of NATO Hostility: Repercussions in the Arctic," *Arctic Review on Law and Politics* 13 (2022), https://doi.org/https://doi.org/10.23865/arctic.v13.3378.
[27] "Arktis," Store norske leksikon, Last updated 10.03.2025 2005-2007, Accessed 15.04., 2025, https://snl.no/Arktis#-Geologi.
[28] Defence Commission of 2021, "Forsvar for fred og frihet," (Oslo, 2023).
[29] "Sjømateriell," The Norwegian Armed Forces, Last updated 07.06.2023 2023, Accessed 15.04., 2025, https://www.forsvaret.no/om-forsvaret/utstyr-og-materiell/sjo.
[30] B. O. Knutsen and M. N. Pedersen, "How to Understand Climate Change as a Threat Multiplier in the Arctic."
[31] M. N. Pedersen et al., *Klimaendringenes påvirkning på Forsvarets plattformer, infrastruktur og personell*, Forsvarets forskningsinstitutt (Kjeller, 2025), https://www.ffi.no/publikasjoner/arkiv/klimaendringenes-konsekvenser-for-forsvarets-plattformer-infrastruktur-og-personell.
[32] Ibid.
[33] M. D. Bowes, *Impact of Climate Change on Naval Operations in the Arctic*, Center for Naval Analysis (Alexandria, VA, 2009),
[34] M. Mayer and I. H. L. Monsen, *The future Arctic operating environment*, Forsvarets forskningsinstitutt (Kjeller, 2024),
[35] M. J. R. Simpson et al., *Sea-Level Rise and Extremes in Norway: Observations and Projections Based on IPCC AR6*, Norsk klimaservicesenter (Oslo, 2024),
[36] "Climate Change as a Factor Impacting Current and Future Commercial Fisheries in the Arctic Region," The Arctic Institute, Last updated 24 October, 2023 2023, Accessed 5 December, 2023, https://www.thearcticinstitute.org/climate-change-factor-impacting-current-future-commercial-fisheries-arctic-region/.
[37] M. N. Pedersen et al., *Klimaendringenes påvirkning på Forsvarets plattformer, infrastruktur og personell.*

Arctic ocean increases, sonar will become less effective, making submarines more difficult to detect, and the range at which they can be detected will decrease.[38] This will reduce our ability to detect Russian submarines in the Arctic. This is a particularly alarming trend, given that the Russian Northern Fleet hosts seven strategic submarines in the Arctic. However, Allied submarines will also become more difficult to detect, offering the same advantage.[39]

Infrastructure

The main mode of access to littoral naval bases is by sea. Land-based infrastructure, primarily roads, remains important to the supply, maintenance, and running of these bases. As such, these bases are affected by both land-based and maritime climate changes.

The Scandinavian landmass is still rising after the last ice age, mitigating the negative impacts of sea-level rise. Nevertheless, sea-level rise contributes to storm surges reaching further inland, posing significant risk to coastal infrastructure and installations. This risk is further exacerbated by sea ice melting. Bigger and more frequent waves reaching the shore poses a risk and exacerbates the frequency and reach of storm surges.

Flooding will become more frequent towards 2050 in all areas with naval bases. Madla and Ramsund are located near rivers, putting them at particular risk of flood damage. While they are in municipalities with increasing flooding risks, Haakonsvern, Sortland, and Trondenes are not near rivers. The direct risk to Naval infrastructure is limited, flooding may cause extensive damage to civilian infrastructure in the vicinity of Naval bases, resulting in greater indirect risk.

Geographical Positioning Systems (GPS) are weaker in the Arctic due to satellite geometry, ionospheric effects, and multipath errors.[40] It appears unlikely that climate change will have a significant *direct* adverse impact on communication systems, but Arctic systems will be negatively affected by a climate change-induced increase in the *operating tempo* in the Arctic. The systems, on the other hand, are adapted to contemporary Arctic operations.

Personnel

Naval personnel will be adversely affected by climate change. Temperature increases, more extreme weather, more zero-degree crossings, and more precipitation will alter when soldiers can operate, how much they can do, what they can and should wear, and where they can deploy to.

A zero-degree crossing (ZDC) is defined as a day during which the temperature crosses 0°C. Most of Norway is projected to experience more ZDCs. The West Coast is a key exception, where fewer ZDCs are projected. This trend is observed because these regions are already mild, not because they are less affected by climate change. Further temperature increases thus mean that these areas will not have any ZDCs because the temperature is likely to remain above 0°C throughout the year.

An increase in the frequency of ZDCs may increase the occurrence of cold weather-related injuries. Most cold-weather injuries occur between 0°C and 15°C, when it is wet, windy, cold, and humid. Fingers and feet are particularly exposed.[41] It is precisely these temperatures that become more common because of more ZDCs. This means that soldiers will likely need to readjust from cold and dry winters to milder and more humid winters, which makes dressing appropriately more difficult.

Similarly, more frequent and powerful extreme weather at sea poses a risk to naval personnel. Working on deck may become dangerous and visibility may be dramatically reduced, complicating navigation.

---

[38] A. Gilli et al., "Climate Change and Military Power: Hunting for Submarines in the Warming Ocean," *Texas National Security Review* 7, no. 2 (2024), https://doi.org/https://doi.org/10.26153/tsw/52240.
[39] M. N. Pedersen et al., *Klimaendringenes påvirkning på Forsvarets plattformer, infrastruktur og personell.*
[40] National Research Council, *National Security Implications of Climate Change for U.S. Naval Forces* (Washington, D.C.: The National Academies Press, 2011).
[41] "Kaldværsskader – og forebygging av dem," The Norwegian Armed Forces, Last updated 11. februar, 2022 2022, Accessed 14. november, 2024, https://www.forsvaret.no/soldater-og-ansatte/soldat/kaldvaersskader-forebygging

Lessons for NATO

Perhaps the most important lesson for NATO in the context discussed in this paper, is the relative operational advantage Allied capabilities can gain from climate adaptation. Climate change is global. Even though the impacts are regional, climate risk can be avoided by none. Russian military adaptation remains largely absent in the face of these risks. This fact provides NATO with an opportunity to gain an operational advantage by adapting its capabilities to climate change *better* than its most prominent Arctic adversary, Russia.

However, the above opportunity must be tempered with caution. As we have shown, climate change renders the Arctic more prone to security dilemmas. Thus, action taken by NATO and its members must ensure that a security dilemma is not triggered, which would result in less security and a nullification of any operational advantage.

Second, climate change has myriad repercussions for naval forces. This is pertinent in the Arctic, as it is primarily a maritime region. Platforms, infrastructure, and personnel will face an operational environment in constant change. Climate adaptation is thus not merely an issue of preserving an operational advantage vis-à-vis a potential adversary, but a matter of ensuring that we have operational abilities at all.

Shaping the Alliance's Approach in the Maritime Domain from a Holistic Security and Governance Perspective

*By **Maj Gen (Ret) Philippe Boutinaud** & **Viola Csordas**,*
Geneva Center for Security Sector Governance

1. Introduction: Why Climate Change Matters for Maritime Security

The consequences of climate change are no longer distant or abstract, they are manifesting with growing frequency and severity across the globe. Coastal flooding, sea level rise, extreme weather events, and ecological degradation are already destabilizing communities, economies, and ecosystems. While the impacts vary regionally, they share one characteristic: they do not respect borders. Climate change is a global challenge that undermines stability at every level, local, regional, and international.

For NATO, this new reality demands urgent attention beyond the operational adaptation. As the ultimate line of response in many crises, defense and security forces must anticipate and prepare for the accelerating impacts of climate change, particularly in the maritime domain. Encompassing open seas, coasts, estuaries, and riverine zones, it is the most exposed and strategically consequential domain[1]. It is where environmental disruption collides with geopolitical competition, human insecurity, and fragile governance.

In addition, maritime security can no longer be defined solely by kinetic threats or traditional military postures. It must also be understood from a people-centered governance perspective.

[1] "NATO Climate Change and Security Impact Assessment," accessed June 30, 2025, https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/240709-Climate-Security-Impact.pdf.

Climate change is a risk multiplier to coastal communities, disrupting livelihoods, and creating new pathways for destabilization, including organized crime, displacement, trafficking and various forms of instability. At the same time, militaries are being called upon not only to deter threats, fight against aggressors but also to respond to natural disasters, monitor ecological degradation, and support civil protection and humanitarian institutions in complex emergencies.

Therefore, how can NATO shape its maritime approach to meet these challenges through a holistic lens? One that integrates environmental sustainability, economic resilience, and good governance? Drawing on lessons from various global contexts, the security sector must be recognized not merely as a responder, but as a strategic enabler of climate adaptation. For NATO to remain fit for purpose, it must put climate foresight, civil-military cooperation, and inclusive governance at the heart of its maritime security agenda.

2. Climate Impacts on Maritime Security: Direct and Indirect Threats

The climate-security nexus in the maritime domain is increasingly visible in both direct and indirect forms[2]. Direct effects include sea level rise, which threatens to inundate coastal infrastructure such as naval bases, ports, and logistical hubs. For example, rising waters have already led to regular flooding at naval installations in Norfolk, Virginia, the largest naval base in the world[3]. Similarly, Caribbean Island states face increasing difficulty in maintaining maritime infrastructure in the face of more frequent hurricanes and coastal erosion.

The maritime domain includes not only open seas but also coastal zones, estuaries, and riverine environments, all of which are deeply affected by climate change[4]. Sea-level rise is reshaping coastlines, while saltwater intrusion affects freshwater availability. Fisheries are being disrupted by ocean warming and acidification, the growing frequency and severity of storms, cyclones, and hurricanes is causing operational disruption and physical destruction of infrastructure including roads, bridges, and power grids, with cascading effects on both militaries and civilians. During Hurricane Maria in 2017, the destruction of Puerto Rico's infrastructure delayed emergency assistance, disrupted maritime aid, and required intervention by the U.S. Army Corps of Engineers.[5] In 2024, Cyclone Chido devastated Mayotte, leaving the island accessible only by sea after its airport and critical infrastructure were destroyed. Reconstruction is being organized as a humanitarian military operation under a former French army general, illustrating France's capacity to integrate military expertise into large-scale civil recovery.

Indirect threats, meanwhile, are no less severe. Climate change is rendering entire regions uninhabitable due to saltwater intrusion, extreme heat, and resource scarcity. These changes drive displacement and create climate refugees, increasing the strain on national and international governance systems. In the Sahel and Horn of Africa, the combined effects of drought and conflict have already contributed to mass displacement and instability that ripple into coastal areas[6]. Moreover, loss of access to essential resources such as water and fisheries can heighten tensions, exacerbate inequality, and provide fertile ground for recruitment into criminal and extremist groups[7]. Public health is also affected, as climate change contributes to the spread of tropical diseases into previously unaffected regions. In addition to heat, these pose new health risks for military personnel.

In the Gulf of Guinea, these dynamics are already visible. The degradation of fish stocks due to illegal, unreported, and unregulated (IUU) fishing has driven artisanal fishermen into poverty, un-

[2] Hans-Otto Pörtner et al., eds., Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. (2022).
[3] "On the Front Lines of Rising Seas: Naval Station Norfolk, Virginia | Union of Concerned Scientists," accessed June 30, 2025, https://www.ucs.org/resources/front-lines-rising-seas-naval-station-norfolk-virginia.
[4] R J Nicholls and T Wilson, 5. INTEGRATED IMPACTS ON COASTAL AREAS AND RIVER FLOODING, n.d.
[5] "Hurricane Maria Disaster Response," accessed June 30, 2025, https://www.usace.army.mil/About/History/Historical-Vignettes/Relief-and-Recovery/154-Hurricane-Maria/.
[6] "What the Data Tells Us – and Doesn't Tell Us – about the Costs of Climate Change in the Sahel and Horn of Africa," SPARC, December 2, 2024, https://www.sparc-knowledge.org/news-blog/news/data-gaps-loss-damage.
[7] "Climate Change Is Fueling Recruitment into Armed Groups - Our World," accessed June 30, 2025, https://ourworld.unu.edu/en/climate-change-is-fueling-recruitment-into-armed-groups.

dermining coastal traditional economies and increasing the risk of parallel economy structures run by criminal[8] organizations. Similar patterns are seen off the coast of Somalia, where foreign exploitation of fishing grounds and diminished livelihoods contributed to the resurgence of piracy. The confluence of environmental degradation and economic deprivation creates fertile conditions for instability, exploitable by both criminal and state-based adversaries.

Climate change is also transforming the strategic geography of maritime trade. Chokepoints such as the Strait of Hormuz, where warming seas and shifting salinity threaten ecosystems while regional tensions jeopardize tanker traffic; the Suez Canal, hit by extreme weather, droughts reducing Nile flows, and incidents like the 2021 Ever Given blockage; and the Panama Canal, where El Niño–driven droughts have restricted shipping amid global trade rivalries, all face mounting stress from the combined impacts of climate change and geopolitical pressures.[9] Emerging corridors in the Mozambique Channel and Gulf of Guinea, vital for energy exports, are exposed to piracy, illegal fishing, and coastal erosion. Infrastructure projects such as the Niger-Benin pipeline require protective security architectures and climate-sensitive risk planning. In the Philippines and the South China Sea, large-scale dredging to build militarized artificial islands has destroyed coral reefs, threatening marine biodiversity and the fisheries that sustain coastal livelihoods. This environmental damage is a consequence of and a contributor to intensifying security competition, as the fortified islands serve as strategic military outposts while the loss of natural resources deepens local economic vulnerabilities and geopolitical tensions[10].

For NATO and its partners, the challenge lies in building strategic foresight and operational readiness to manage both the security risks, changing operating environment, and the humanitarian consequences of these shifts.

3. From Risk to Resilience: A Holistic Approach to Maritime Security and Governance

To effectively respond to these complex challenges, NATO must broaden its approach to security beyond traditional notions of deterrence and sea control. A holistic approach recognizes that maritime security encompasses military preparedness, economic resilience, and environmental sustainability. It must also be rooted in strong governance frameworks that empower both coastal communities and regional institutions[11].

3.1. Strategic adaptation – governance and norms

First, there needs to be recognition that maritime security is not solely a military matter, but at the same time economic, social and environmental. It is inseparable from the protection of sea lines of communication vital to global trade, from the sustainable management of marine ecosystems, and from the capacity to respond to climate-related disasters. NATO militaries are increasingly called upon to aid in natural disasters, monitor ecological threats, and support civilian institutions during complex emergencies[12]. This evolving landscape demands more than tactical adjustments; it requires systems thinking that acknowledges the interdependence between environmental resilience, human security, and strategic stability. For the Alliance, this entails a conceptual evolution, underpinned by integrated planning across defense, development, and environmental sectors. It also calls for investment in outreach, awareness-raising, and trust-building efforts within the Alliance, with partners and local communities, ensuring that military engagement in non-traditional

[8] "Context and Stakeholder Analysis of Maritime Security and Justice in the Gulf of Guinea | DCAF – Geneva Centre for Security Sector Governance," accessed June 30, 2025, https://www.dcaf.ch/context-and-stakeholder-analysis-maritime-security-and-justice-gulf-guinea.

[9] United Nations Conference on Trade and Development, Review of Maritime Transport 2024 (Overview) (2024), https://unctad.org/system/files/official-document/rmt2024overview_en.pdf.

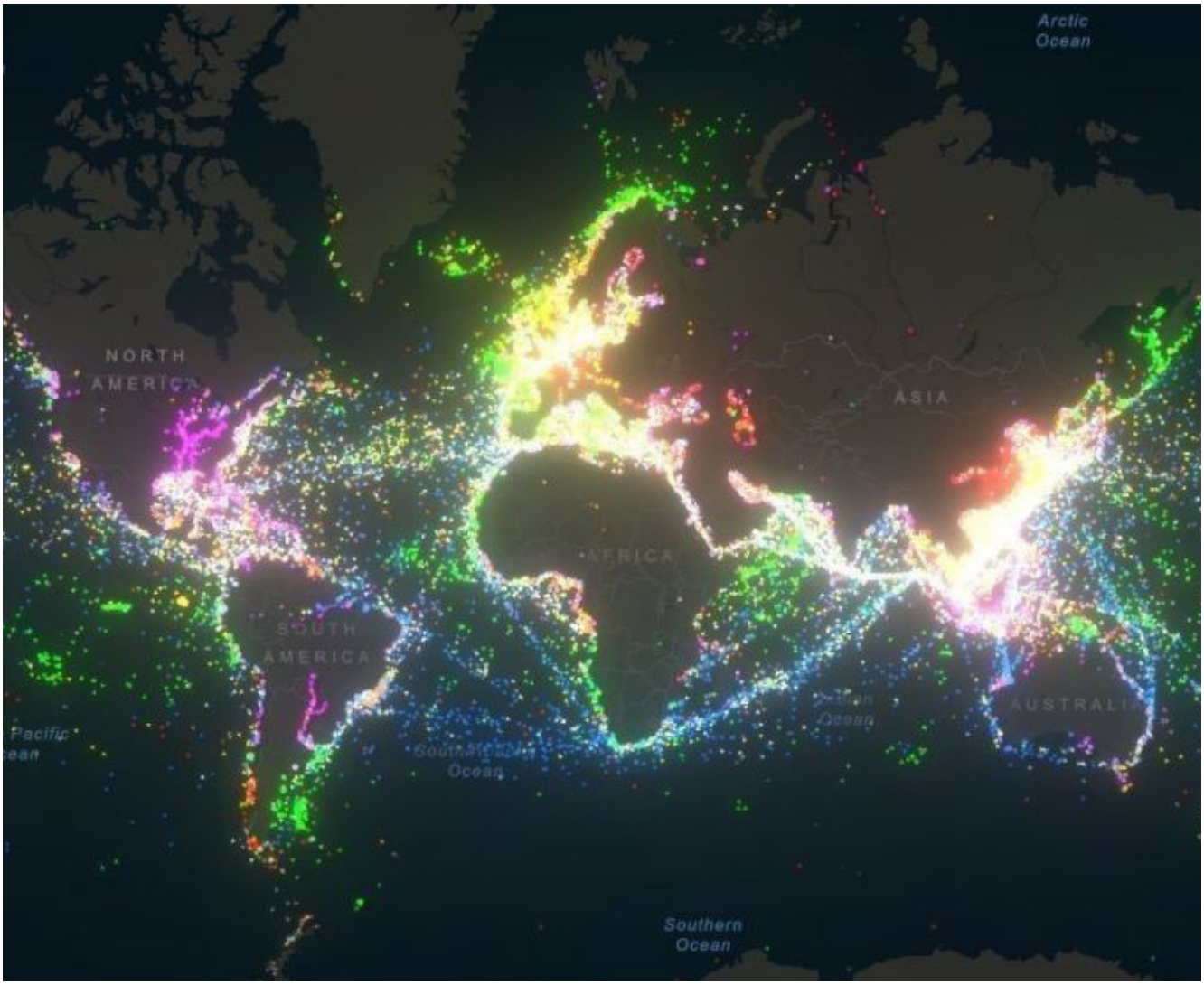
[10] Karen Lema, "China Denies Philippine Report of 'Artificial Island' in Disputed Waters," Asia Pacific, Reuters, May 13, 2024, https://www.reuters.com/world/asia-pacific/philippine-coast-guard-wont-allow-china-reclamation-disputed-shoal-official-says-2024-05-13/.

12 Viola Csordas et al., "Protecting People, Planet and Peace: Shaping the Future of the Security Sector | DCAF – Geneva Centre for Security Sector Governance," accessed June 30, 2025, https://www.dcaf.ch/stocktaking-security-sector-roles-climate-and-environmental-security-chapeau-report. 11 "Maritime Security Sector Governance and Reform | DCAF – Geneva Centre for Security Sector Governance," accessed June 30, 2025, https://www.dcaf.ch/maritime-security-sector-governance-and-reform.

roles reinforces, rather than substitutes, legitimate governance structures.

Supporting maritime trade resilience is one such area where joint action is critical. Recent NATO initiatives, such as the NATO 2025 Summit's multinational agreement on the joint acquisition and management of critical defense raw materials, underscore how supply chain resilience—including the maritime transport of lithium, titanium, and rare earths—is now viewed as a strategic security priority. This reflects a broader shift toward systems-based security thinking, integrating climate, trade, and geopolitical risk into Alliance planning.

Secondly, strengthening maritime governance is essential to ensuring long-term regional stability, sustainability, and effective crisis response in the maritime domain. This requires a dual effort: reinforcing international legal frameworks, such as the United Nations Convention on the Law of the Sea (UNCLOS), and fostering inclusive, multi-level coordination among a broad range of actors. Effective maritime governance cannot rely solely on national capacity or military presence; it depends on strong cooperation between civilian authorities, regional bodies, and international partners. Institutions such as the International Maritime Organization (IMO), the African Union, ASEAN, and the European Union play vital roles in setting norms, facilitating information sharing, and harmonizing practices. To address complex transboundary threats like piracy, IUU fishing, or pollution, NATO must engage with both member and non-member countries through strategic partnerships that enable burden sharing and coordinated action. A multi-level governance approach, spanning national governments, regional maritime coordination centers, and international actors, can help ensure that roles are clearly defined, resources are effectively allocated, and responses are timely and legitimate. In the Gulf of Guinea, for example, cooperation among coastal states under the Yaoundé Code of Conduct has contributed to a measurable decline in piracy and maritime crime by promoting joint surveillance, operational coordination, and shared early warning systems. In Somalia, SSR initiatives



such as the FAO-supported biometric registration of fishermen[13], EUCAP Somalia's[14] training and equipping of maritime police and coast guards, and UN-assisted policy and payroll reforms – together with EU NAVFOR operations[15] - have strengthened governance, accountability, and maritime law enforcement, despite persistent challenges. These experiences highlight the importance of embedding NATO efforts within locally owned and regionally anchored governance frameworks, while also promoting norms of accountability, transparency, and inclusive security provision.

3.2. Operational adaptation – capabilities and civil military cooperation

On the one hand, NATO doctrine and capabilities must adapt to the realities of climate risk and develop robust resilience measures. Enhanced maritime domain awareness (MDA) must go beyond vessel tracking and encompass the monitoring of environmental changes and disaster risks. Information sharing should be broadened to include civilian and humanitarian actors for non-classified data, enabling a common operating picture and a timely response during crises. Contingency planning should address scenarios ranging from large-scale migration to critical infrastructure failure. NATO's Climate Change and Security Action Plan[16] provides an important milestone for this operational integration but could be further improved especially with regards to much integrated capacities for emergency response within the alliance and with partners. This consists of capacity building and training that could be extended to non-traditional roles such as disaster management and environmental protection. France[17] started to establish civil protection units within their armed forces in 1964 and last year the 4th Civil protection training and intervention Regiment (4éme Régiment d'Instruction et d'Intervention de la Sécurité Civile - RIISC) was created in Libourne (South-west of France). France now has a Civil Security Brigade, part of the armed forces, but deployable by the Ministry of the Interior, and the Marseille Marine Fire Battalion (Bataillon de Marins-Pompiers de Marseille - BMPM), whose resources and experts can be mobilized for crises affecting sea fronts. Operation Taquari II in Brazil illustrates further what might be required from militaries in the future[18]: over 20,000 military personnel supported civilian authorities during massive floods in 2024, deploying amphibious vehicles, helicopters, and warships for rescue operation and the transport of relief and medical goods. An integrated command structure facilitated coordination between defense and civilian agencies, demonstrating a model for effective civil-military disaster response.

This also highlights the increasingly important role for dual-use equipment, such as UAVs, satellite systems, and AI-driven platforms offering critical dual applications in surveillance, environmental monitoring and emergency operations. Riverine operations in the Amazon[19] and Sahel show how military presence can deter trafficking and support state outreach in hard-to-reach areas. These examples can also help NATO shape its maritime investment strategies and partnerships.

Finally, partnerships are at the center of climate proofing NATO's maritime security. As climate impacts cross institutional, geographic, and sectoral boundaries, they require an integrated response that goes beyond traditional military cooperation. Some allies' joint training

[13] A Rapid Analysis of the Fisher Folk Registration Data in Puntland State of Somalia (FAO, 2014), https://openknowledge.fao.org/server/api/core/bitstreams/dfc56666-1a62-4116-94c1-fe2a76b8fc10/content.
[14] "Strengthening Somalia's Maritime Governance: EUCAP Somalia and UNTMIS Deliver Joint Training on Vessel Traffic Management & Information System | EEAS," accessed August 12, 2025, https://www.eeas.europa.eu/eucap-som/strengthening-somalia%E2%80%99s-maritime-governance-eucap-somalia-and-untmis-deliver-joint-training-vessel_en?s=332.
[15] "Home | EUNAVFOR," accessed June 30, 2025, https://eunavfor.eu/.
[16] NATO, "NATO Climate Change and Security Action Plan," NATO, accessed June 30, 2025, https://www.nato.int/cps/en/natohq/official_texts_185174.htm.
[17] "Les Formations Militaires de La Sécurité Civile | Ministère Des Armées," accessed July 1, 2025, https://www.defense.gouv.fr/terre/nos-unites/niveau-divisionnaire/commandement-terre-territoire-national/formations-militaires-securite-civile.
[18] Viola Csordas, Effectiveness of the Security Sector in Preparation, Adaptation, Mitigation and Response to the Impacts of Climate Change: Report on the May 2024 Floods in Rio Grande Do Sul, Brazil, Internal report (EU SSG Facility, 2025).
[19] "Stocktaking of Security Sector Roles in Climate and Environmental Security - Brazil | DCAF – Geneva Centre for Security Sector Governance," accessed June 30, 2025, https://www.dcaf.ch/stocktaking-security-sector-roles-climate-and-environmental-security-report-brazil.

and capacity building with partners[20], particularly in climate-vulnerable regions such as the Philippines, now incorporates humanitarian assistance, disaster response, and environmental protection. However, to implement a truly systems-based approach, these partnerships must also bridge defense, economic, social, and development perspectives.

Civil-military cooperation is essential in this regard. Anticipating crises by determining in advance who is responsible for what, who has authority over the State's resources and what financial resources are immediately available to react in an emergency is often decisive in the response to a crisis. Any poorly managed civil security crisis very quickly risks becoming a political crisis, an increasingly likely scenario in the context of proliferating climate disasters. Military actors can bring logistical expertise, early warning capabilities, and operational reach to support civilian authorities and humanitarian responders, but they must do so in a manner that strengthens, not supplants, local governance and social cohesion. Establishing pre-agreed coordination protocols with local civilian actors, including insurance companies, interoperable communications systems, and shared training – using jointly developed training curricula – can improve trust, coherence, and effectiveness across the civil-military interface.

Above all, to be effective, NATO's climate-resilient maritime strategy must be aligned with broader regional and multilateral frameworks - from the EU's Global Gateway initiative to UN disaster risk reduction efforts and World Bank-supported coastal development programs. Particularly within the framework of NATO-EU cooperation on maritime security[21], there is space to further develop joint early warning systems, coordinated investment in climate-resilient maritime infrastructure, and integrated capacity-building programs that link security, development, and environmental governance in vulnerable coastal regions.

By embedding wider social and economic resilience agendas within its security concerns, NATO can help safeguard the maritime commons in a way that supports peace, prosperity, and shared responsibility.

4. Conclusion: A Forward-Looking Maritime Alliance

Climate change is reshaping the maritime domain, driving cross-border and multi-sectoral risks that destabilize coastal communities and disrupt global trade. For NATO, this demands a decisive shift toward a systems-oriented maritime posture, one that embeds climate foresight, civil-military cooperation, and multi-level governance at its core.

The Alliance has a critical opportunity to lead by example. A future-ready NATO maritime strategy must be climate-informed in doctrine, resilient in infrastructure, and interagency in execution. It must build interoperability not just among naval forces, but across humanitarian, environmental, and development actors.

Equally important is acknowledging the security sector as a key enabler of climate adaptation. Armed forces are no longer peripheral actors in this space; they are central to prevention, preparedness, and recovery. From Brazil's flood response to emerging civil protection units within European militaries, the strategic value of dual-use assets and whole-of-society engagement is becoming clear. NATO must now institutionalize these insights through planning, training, and partnership frameworks.

Looking ahead, the Alliance must grapple with forward-looking questions that cut to the heart of future maritime stability. What is the status and legal protection of climate-displaced persons, many of which use maritime transport routes and arrive in littoral areas? How will NATO and its partners engage with hybrid risks where climate threats and environmental degradation are weaponized? What responsibilities do security and defense forces bear in contributing not just to crisis response but to long-term societal resilience? And how can civil-military cooperation be enhanced in practice to support whole-of-society adaptation?

Ultimately, the maritime domain is not only a space of contestation but also one of cooperation. By adopting a systemic approach to the realities of climate change - and by recognizing security institutions as integral to adaptation - NATO can ensure it remains a stabilizing force in a rapidly changing world.

[20] Viola Csordas et al., "Stocktaking of Security Sector Roles in Climate and Environmental Security - the Philippines | DCAF – Geneva Centre for Security Sector Governance," accessed June 30, 2025, https://www.dcaf.ch/stocktaking-security-sector-roles-climate-and-environmental-security-philippines.
[21] "Factsheet EU-NATO Cooperation on Maritime Security," accessed July 1, 2025, https://www.eeas.europa.eu/sites/default/files/factsheet_-_eu-nato_maritime_cooperation.pdf.

Climate change, maritime crimes and anti-money laundering legislation[1]

*By **Dr. Iliana Christodoulou Varotsi,***
Senior Legal Consultant & Lead Industry Trainer

Abstract

Despite the lack of consensus on the definition of maritime security, neither its importance nor its evolving nature can be challenged or overstated. Suffice it to recall that according to various sources more than 95% of international data traffic is carried by submarine cables. The frequency and intensity of phenomena associated with global warming are growing and the effects of climate change go far beyond coastal and maritime areas, thus they become a question of national security. The paper takes note of the fact that climate change contributes to an increase in maritime crime, such as environmental offences, illegal fishing, and trafficking in human beings. The deterioration of the living conditions of communities directly affected by climate change can lead to poverty-related crimes at sea or exacerbate pre-existing trends; at the same time, the elements of an offence may be related both to marine and terrestrial areas and may be of interest to several jurisdictions. Based on the observation that maritime crimes are not expected to occur in a vacuum and may be associated with more than one offence, including money-laundering, the paper examines the legal relationship between climate change-related maritime crime under international law and anti-money laundering legal framework; it explores the possibilities offered by anti-money laundering regulations to deal with maritime crimes, thus contributing to the discussion as to whether the existing legal regime is adequate, including in the case where we are in the presence of new anti-social and harmful behaviours related to global warming.

[1] This article is based on a presentation made by the author at the 16th NATO Maritime Interdiction Operational Training Centre (NMIOTC) Conference in Souda Bay, Greece (4-5 June 2025).

Introduction

Climate change is at the heart of the work of policymakers and legislators in many parts of the world. It is widely acknowledged that climate change contributes to poverty and poverty-related crimes, thus putting pressure on security. In general, studies suggest that there is a link between temperature and the incidence of crime[2]; climate change also contributes to an increase in maritime crimes[3]. While there is no single, universal definition for maritime crimes[4], it is pertinent to consider that maritime crimes are criminal acts committed at sea that are prohibited by national or international law[5]. While climate change attracts a lot of attention today, especially in public consciousness, including in the shipping industry, climate change is not a novel phenomenon.

The impact of climate on humans has been a matter of great interest to ancient Greeks. Both the poet Hesiod and the physician and philosopher Hippocrates had studied the climate of specific regions, respectively of Boeotia and Thasos island[6]. From past to present, according to research findings published in 2025 which had examined ice-rafted rocks in Iceland and the effects of rapid cooling, climatic cooling in the 6th century is likely to have contributed to mass migrations and to the collapse of the Roman Empire[7].

It is of essence to understand and address the exacerbation of existing harmful behaviours that are contrary to public policy because of climate change stressors. Elements of offences centered around climate change may be of interest to more than one jurisdiction. Thus, maritime crimes may be associated with more than one offence, including money laundering offences.

Within its limited confines, the purpose of this paper is to contribute to the launch of a multi-disciplinary discussion on the adequacy of existing legal mechanisms in addressing maritime crimes associated with climate change with the emphasis on the possible legal avenues offered by anti-money laundering legislation.

Are there any climate change offences per se?

On this point, a logical question arises. Strictly speaking, are there any climate change offences per se? Contrary to the legal qualification of environmental crimes such as improper collection, transport, recovery or disposal of waste, which appears to be straightforward in several jurisdictions, the definition of climate change offences raises a few questions.

It should be noted from the outset that generally, criminal law is not the main channel for tackling climate change[8]. According to the United Nations Office on Drugs and Crime (UNODC) and the World Wild Fund for Nature (WWF), there are almost no climate-related cases that use criminal law as the vast majority of cases is based on constitutional or administrative law. The United Nations Environment Programme (UNEP) and other stakeholders point out that "Classification of crimes and links with climate change poses another challenge. Many cases involving illegal deforestation or crimes affecting the marine environment will not reference climate change explicitly and are therefore not

[2] M. J. Lynch & Others (2022) 'The Climate Change – Temperature – Crime Hypothesis: Evidence from a Sample of 15 Large US Cities, 2002 to 2015', 66(4) International Journal of Offender Therapy and Comparative Criminology 430, cited in 'Criminal law and climate change', website of the Hughes Hall Centre for Climate Engagement, University of Cambridge (last access on 7 September 2025).

[3] As noted by Peter Schwartzstein in 'Climate Change & Crime – A big, bad largely overlooked nexus', briefer edited by Tome Ellison and Francesco Femia and published by the Center for Climate & Security (Briefer No. 67, 17 October 2024), "climate change is leaving its mark on almost every category of crime" and "climate impacts aggravate [...] the other forces that at least partly underlie lawbreaking [...]".

[4] The challenge posed by legal definitions can be seen, for example, in the Suppression of Unlawful Acts (SUA) treaties, which are concerned with maritime crimes such as maritime terrorism and piracy. None of the terms 'maritime crime', 'maritime terrorism' or 'piracy' are defined in the articles of the SUA Convention 1988.

[5] However, the United Nations Convention on the Law of the Sea (UNCLOS), which was adopted in Montego Bay in 1982 and is the international instrument of reference on ocean management and navigational freedoms with the force of customary international law, defines piracy (Article 101).

[6] Jacques Jouanna (2018) Subir et penser le climat: Essai de comparaison entre Hésiode et Hippocrate, Publications de l'Académie des Inscriptions et Belles-Lettres, no 29 (Thématique Vie et Climat d'Hésiode à Montesquieu), pp. 1-28.

[7] Christopher J. Spenser, Thomas M. Gernon, Rose N. Mitchell (2025) Greenlandic Debris in Iceland Likely Tied to Bond Event 1 Ice Rafting in the Dark Ages, Geology, 53/7, pp. 572-575. DOI: doi.org/10.1130/G53168.1; cited in Oguz Buyukildirim (11 April 2025) 'New Research Links Climate Crisis to the Fall of the Roman Empire, Arkeonews.

[8] 'Criminal law and climate change', website of the Hughes Hall Centre for Climate Engagement, University of Cambridge (last access on 7 September 2025).

considered or 'labelled' as climate-related cases. Climate change litigation requires that a case explicitly raises issues of law or fact regarding climate change"[9].

In the general acceptance of the term maritime crime, maritime crimes which may have a link with climate change may cover illegal, unreported and unregulated fishing but it is very unlikely to consider associated crimes such as the use of fraudulent documents, tax evasion, etc. as falling under the scope of maritime crimes. Arguably, one may expect to see new forms of anti-social and harmful behaviours against public policy triggered by or related to climate change that are not regulated or where the law is weak. It is very unlikely to qualify the offences relating to net zero transition and decarbonization in shipping (one may think of fraud) as maritime crimes. However, the nascent link between climate-related frameworks and fraud (e.g. in the context of emissions trading schemes) cannot be ignored[10].

Against this background, does anti-money laundering legislation offer any legal avenues in the presence of anti-social and harmful behaviours centered around climate change when laws are absent or weak? The suggested reasoning helps us to critically revisit the scope of maritime crimes as well as the risks entailed by climate change; such risks have the potential to contribute to new forms of illegal behaviours that represent a threat to maritime security.

How does anti-money laundering legislation come into play?

To the extent that climate change contributes to the increase of maritime crimes, money laundering linked to maritime crimes should reasonably be expected to be on the rise[11]. Is the current legal regime adequate to address this situation?

Anti-money laundering legislation consists of national, regional and international provisions which aim at preventing criminals from exploiting the financial system to launder illicit proceeds[12]. Anti-money laundering legislation, which is intertwined with the standards to counter the financing of terrorism, encompasses a wide range of mechanisms including customer due diligence by the obliged entities such as banks, transaction monitoring, risk assessments, internal controls and audits. National legislations vary in their approach. Without exhausting the subject, the United Nations Convention against Transnational Organized Crime and the Protocols thereto (2000) contains provisions, amongst others, on money laundering. On the regional level, i.e. the European Union (EU) level, the 6th Anti-Money Laundering Directive (often referred to as 6AMLD)[13], aims to strengthen the legislation of EU Member States on anti-money laundering and anti-terrorism-financing via measures such as the requirements relating to certain service providers and to the granting of residence rights in exchange of investment, checks on the beneficial owners of certain obliged entities, etc. Like any EU Directive, EU Member States are required to transpose EU provisions in their national legislations, which is achieved via the adoption of primary or secondary legislation.

The usual legal mechanisms include[14] the following, namely: freezing, which is a temporary prohibition to use, transfer, etc. the relevant property; conviction-based confiscation, which is the final deprivation of property following a court decision; non conviction-based confiscation (e.g. in case of death of the suspected or accused person); confiscation of instrumentali-

[9] United Nations Environment Programme (UNEP) and Sabin Center for Climate Change Law cited in UNODC, Crimes that Affect the Environment and Climate Change, ddu, p. 19).

[10] See Mary Alice Young and Deborah Adkins (2022) 'The Ascent of Green Crime: Exploring the Nexus Between the Net Zero Transition and Organized Crime', 29(3), Journal of Financial Crime 789 cited in cited in 'Criminal law and climate change', website of the Hughes Hall Centre for Climate Engagement, University of Cambridge (last access on 7 September 2025).

[11] Money-laundering, tax evasion, corruption and trafficking of persons are connected with illegal behaviours along the fisheries value chain (UNODC (ddu) 'Tackling Crimes that Affect our Ocean', p. 2).

[12] On 30 May 2024, an instrument adopted by the European Union (EU) set out a new anti-money laundering authority called AMLA. MONEYVAL, is a permanent monitoring body of the Council of Europe which assesses compliance with anti-money laundering treaties.

[13] This is Directive (EU) 2024/1640 of the European Parliament and of the Council of 31 May 2024 on the mechanisms to put in place by Member States for the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Directive (EU) 2019/1937, and amending and repealing Directive (EU) 2015/849 (Text with EEA relevance) (OJ L, 2024/1640, 19.6.2024).

[14] These generic definitions are based on EU anti-money laundering legislation.

ties; confiscation of proceeds; extended confiscation, which refers to the confiscation, either wholly or in part, of the property of the convicted person which stems from criminal conduct; value confiscation, which entails a pecuniary liability realizable against the assets of the individual; and additional sanctions set out by national legislations such as monetary fines and/or imprisonment.

One way in which national legislation can be structured is by setting out prescribed offences that comprise laundering and predicate offences. If we take as an example that of the law of the Republic of Cyprus, which is a Member State of the EU and of the Council of Europe, Cypriot legislation[15] provides for prescribed offences[16], which encompass laundering offences, i.e. the offences of laundering income from illegal activities,[17] as well as predicate offences. The wrongdoer must be aware of ("knows or ought to have known") the property constituting proceeds from the commission of illegal activities; when he/she carries out certain activities such as acquiring, possessing, using or transferring the property to conceal its illegal origin, he/she commits a laundering offence. A list of acts constituting laundering offences in this context is set out by the law. A predicate offence is any offence defined as criminal offence under national law. One can easily see that the wording of this legislation potentially leads to an all-embracing approach to money laundering. In this vein, it is reasonable to consider that in the presence of a new harmful behaviour rooted in climate change that is not grasped by a robust provision in national law, anti-money laundering legislation could be, under conditions, relevant.

This approach is not new. It is observed that, in general, domestic anti-money laundering legislations may be used to strengthen the legal basis used in the proceedings. For example, in the case of a vessel that was taken by pirates in the exclusive economic zone of Côte d'Ivoire, as Nigeria at that time had not finalised its piracy law, trying the pirates for piracy was not possible. As a result, the pirates were charged with other offences such as conspiracy, unlawful possession of arms and money laundering[18].

On this point it is useful to remember that the assumption for the purposes of this paper was that there may be new anti-social and harmful behaviours rooted in climate change which are subject to weak legal provisions. In domestic legislations structured as in the example above, the provisions on money laundering may be useful to the extent that there is at least one offence covered by the law (not necessarily related to climate change). Subject to the particularities of each national system, while this approach cannot remedy the problem of legal gaps, it can be of interest to the judiciary in case of weak provisions punishing a new or complex situation.

Against this background, the above-mentioned 6th Anti-Money Laundering Directive, which became effective in December 2020, expanded the list of the original crimes the laundered money

[15] Prevention and Suppression of Money Laundering and Terrorist Financing, Law 188(I)/2007, as amended.
[16] Section 3 of Law 188(I)/2007, as amended.
[17] Provided in Section 4 of Law 188(I)/2007, as amended.
[18] This is the case of the M/T MAXIMUS cited in UNODC (2019) Maritime Crime: A Manual for Criminal Justice Practitioners, Second edition, p. 170.

stems from and set out 22 different predicate (underlying) offences, including environmental crimes, which constitute money laundering. The list of the 22 predicate offences includes participation in an organised criminal group, terrorism, trafficking in human beings, sexual exploitation, illicit trafficking in narcotic drugs, illicit arms trafficking, illicit trafficking in stolen goods, corruption, fraud, counterfeiting of currency, cybersecurity, environmental crime, murder, kidnapping, robbery or theft, smuggling, counterfeiting and piracy of products, tax crimes, extortion, forgery, piracy and insider trading.

Would legislating 'climate change offences be a pertinent approach?

In general, legislating 'climate change' offences per se does not appear to be the approach selected by legislators and concepts such as environmental crimes are the reference at present. However, in the context of the broader reflection on the new parameters introduced by climate change[19], including in relation to maritime and associated crimes, it is reasonable to question how advisable it would be to legislate in this direction. This would presuppose identifying legal gaps, i.e. which new behaviours rooted in climate change are not adequately covered by existing provisions; the conducts to be prohibited constitute the physical element. The mental element would need to consider the required culpability. Defences, burden of proof, personal scope and penalties would also need to be identified. On this point, it is worth considering if civil society is ready to legislate in this direction and how civil society could be further involved, including, wherever relevant, via synergies between the civil and military spheres.

Concluding remarks

The interest of the cross-professional dialogue on climate change, including in relation to the adequacy of the legal regime when it comes to maritime and associated crimes, points to the need to revisit existing provisions and consider the dynamics of anti-money laundering legislation to strengthen the legal basis in case new harmful behaviours rooted in climate change are not adequately covered. The above discussion was intended as an introduction to a proposed public debate on the advisability of legislating offences relating to climate change and showcased some of the dynamics and limitations.

About the author

Dr Iliana Christodoulou Varotsi is a senior legal consultant in private practice (member of the Athens Bar Association) based in Greece. She is a lecturer and shipping industry trainer with international experience, specialising in international maritime law, shipping regulations, and EU law and policies. She obtained her PhD in Law with the highest distinction from the Law Faculty of Paris Sorbonne University at the age of 27. She has extensive experience in law drafting in view of the accession of the Republic of Cyprus to the EU. She provides specialised consultancy services as a subcontractor to the EU on projects including legal studies, compliance assessments, reporting and training. She has exposure to numerous aspects of EU and international law, including economic sanctions, the criminalisation of firearms, anti-money laundering legislation, illicit drug trafficking and maritime safety law. She delivers training on shipping regulations to international groups of learners via the world's largest professional development providers. She has provided training services to shipping companies, shipyards, banks and navies, amongst others, via Lloyd's Maritime Academy (Informa Connect). She is a visiting lecturer at ALBA Graduate Business School The American College of Greece and at the Hellenic Naval Academy/University of Piraeus inter-institutional post graduate programme. Honorary visiting fellow at the Institute of Maritime Law, University of Southampton. Guest speaker at the IMO Institute of Maritime Law (IMLI), Malta. Author of five books with international publishers and of numerous papers in academia and shipping industry press.

The European Union and Cybersecurity

the Critical Importance of a Holistic Approach

By Giuseppe Zuffanti

Why is a holistic approach to cybersecurity crucial for the maritime environment and the security of Europe? For too long, cybersecurity has been seen as an issue concerning computers, networks, and access to information. While this is clearly a critical component of cybersecurity, it is only one element. Cybersecurity encompasses international relations, law, and business. It also concerns disinformation, online social engineering, and deception - from terrorists, extremists, nefarious states, and all types of criminality. Nefarious actors use cyberspace to conduct and facilitate their harmful activities. Cybersecurity concerns how we secure ourselves in cyberspace from those who wish to cause harm. Understanding this is crucial to our security in the EU, NATO, and indeed across the world.

And it is because of this that the European Union has embraced a holistic approach to cybersecurity, recognising that the cyber domain encompasses all aspects of security, including defence, diplomacy, and the protection of critical infrastructure - including Critical Maritime Infrastructure. The European Security and Defence College (ESDC), an autonomous EU entity, plays a vital role in promoting EU peace and security efforts by providing training and education in the Common Security and Defence Policy (CSDP) framework, which is an integral part of the Common Foreign and Security Policy (CFSP). Through close cooperation with key partners, including NATO - particularly its Defence Education Enhancement Programme (DEEP) - as well as strategic regions such as Ukraine, the Eastern Partnership, the Western Balkans, the Indo-Pacific, and the Middle East and North Africa (MENA), the ESDC fosters mutual understanding and capacity building, thereby enhancing the EU's contribution to global security.

The ESDC's Cyber Education, Training, Exercise, and Evaluation (ETEE) platform has been instrumental in establishing strong partnerships with key EU entities in the cyber ecosystem and in promoting a comprehensive approach to cyber defence, cybercrime, network and information security (NIS), and cybersecurity, aligning with the European Cybersecurity Skills Framework (ECSF) established by the European Union Agency for Network and Information Security (ENISA). The ECSF provides a framework for identifying and addressing cybersecurity skills gaps, and the ESDC has been actively working to support its implementation.AAWhy is a holistic approach to cybersecurity crucial for the maritime environment and the security of Europe? For too long, cybersecurity has been seen as an issue concerning computers, networks, and access to information. While this is clearly

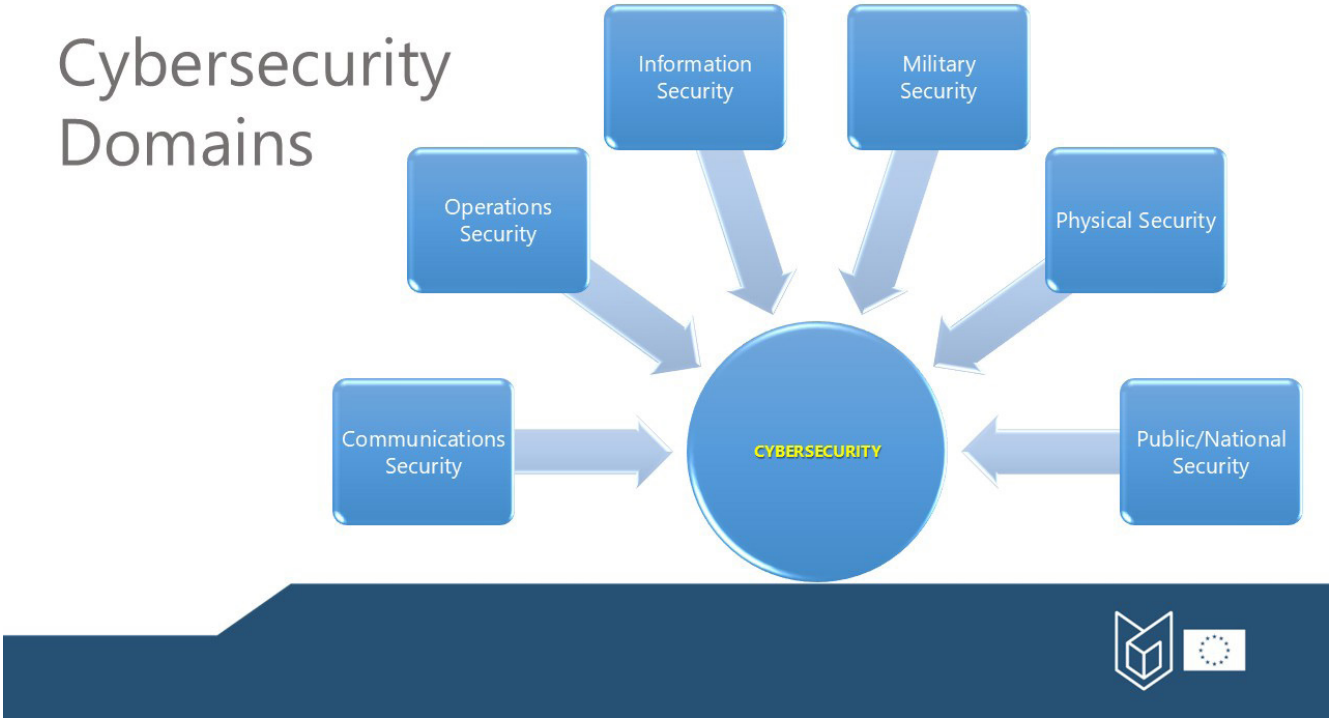
a critical component of cybersecurity, it is only one element. Cybersecurity encompasses international relations, law, and business. It also concerns disinformation, online social engineering, and deception - from terrorists, extremists, nefarious states, and all types of criminality. Nefarious actors use cyberspace to conduct and facilitate their harmful activities. Cybersecurity concerns how we secure ourselves in cyberspace from those who wish to cause harm. Understanding this is crucial to our security in the EU, NATO, and indeed across the world.

And it is because of this that the European Union has embraced a holistic approach to cybersecurity, recognising that the cyber domain encompasses all aspects of security, including defence, diplomacy, and the protection of critical infrastructure - including Critical Maritime Infrastructure. The European Security and Defence College (ESDC), an autonomous EU entity, plays a vital role in promoting EU peace and security efforts by providing training and education in the Common Security and Defence Policy (CSDP) framework, which is an integral part of the Common Foreign and Security Policy (CFSP). Through close cooperation with key partners, including NATO - particularly its Defence Education Enhancement Programme (DEEP) - as well as strategic regions such as Ukraine, the Eastern Partnership, the Western Balkans, the Indo-Pacific, and the Middle East and North Africa (MENA), the ESDC fosters mutual understanding and capacity building, thereby enhancing the EU's contribution to global security.

The ESDC's Cyber Education, Training, Exercise, and Evaluation (ETEE) platform has been instrumental in establishing strong partnerships with key EU entities in the cyber ecosystem and in promoting a comprehensive approach to cyber defence, cybercrime, network and information security (NIS), and cybersecurity, aligning with the European Cybersecurity Skills Framework (ECSF) established by the European Union Agency for Network and Information Security (ENISA). The ECSF provides a framework for identifying and addressing cybersecurity skills gaps, and the ESDC has been actively working to support its implementation.

In line with the EU Cybersecurity Strategy 2020-2030, the ESDC has focused on building resilience, advancing a global and open cyberspace, and developing operational capacity to prevent, deter, and respond to cyber threats. The ESDC's cyber training and education initiatives have been designed to support these goals, with a particular emphasis on enhancing cooperation and collaboration between the EU and its partners.

As a high priority, in support of Ukraine's security and defence efforts, the ESDC has established a strong partnership with 16 Ukrainian training institutions, with over 700 Ukrainian officials having participated in ESDC programmes since 2020, including cyber courses to bolster collective resilience against cyber threats.



Looking ahead, the ESDC will continue to enhance its cooperation with Ukraine, NATO, and other key partners to promote a comprehensive approach to cybersecurity and support the development of a more stable and secure Europe. The ESDC will also continue to work closely with ENISA to support the implementation of the ECSF and promote cybersecurity skills development across the EU, including continuing to focus on emerging technologies such as deep learning and artificial intelligence, supporting and contributing to the EU Cyber Skills Academy, and enhancing EU-NATO cooperation on cyber training.

Overall, the ESDC's holistic approach to cybersecurity and cyber defence, combined with its strong partnerships and cooperation with key EU entities and international partners, including across the whole maritime environment, has positioned it as a leader in promoting a comprehensive and coordinated approach to training and education in the cyber domain across the EU.

Giuseppe Zuffanti is the coordinator for cybersecurity, cyberdefence and hybrid threats education at the EU's European Security and Defence College (ESDC). Giuseppe has served for over 30 years in the Italian National Police, including senior posts within the Ministry of the Interior, before joining the ESDC in 2020. Giuseppe holds advanced degrees in computer science and engineering from the universities of Turin and Naples. Giuseppe has a long-standing interest in cybersecurity, cyber defence, and AI, and how they affect our security in Italy, Europe, and across the world.with the European Cybersecurity Skills Framework (ECSF) established by the European Union Agency for Network and Information Security (ENISA). The ECSF provides a framework for identifying and addressing cybersecurity skills gaps, and the ESDC has been actively working to support its implementation. AAWhy is a holistic approach to cybersecurity crucial for the maritime environment and the security of Europe? For too long, cybersecurity has been seen as an issue concerning computers, networks, and access to information. While this is clearly a critical component of cybersecurity, it is only one element. Cybersecurity encompasses international relations, law, and business. It also concerns disinformation, online social engineering, and deception - from terrorists, extremists, nefarious states, and all types of criminality. Nefarious actors use cyberspace to conduct and facilitate their harmful activities. Cybersecurity concerns how we secure ourselves in cyberspace from those who wish to cause harm. Understanding this is crucial to our security in the EU, NATO, and indeed across the world.

And it is because of this that the European Union has embraced a holistic approach to cybersecurity, recognising that the cyber domain encompasses all aspects of security, including defence, diplomacy, and the protection of critical infrastructure - including Critical Maritime

Infrastructure. The European Security and Defence College (ESDC), an autonomous EU entity, plays a vital role in promoting EU peace and security efforts by providing training and education in the Common Security and Defence Policy (CSDP) framework, which is an integral part of the Common Foreign and Security Policy (CFSP). Through close cooperation with key partners, including NATO - particularly its Defence Education Enhancement Programme (DEEP) - as well as strategic regions such as Ukraine, the Eastern Partnership, the Western Balkans, the Indo-Pacific, and the Middle East and North Africa (MENA), the ESDC fosters mutual understanding and capacity building, thereby enhancing the EU's contribution to global security.

The ESDC's Cyber Education, Training, Exercise, and Evaluation (ETEE) platform has been instrumental in establishing strong partnerships with key EU entities in the cyber ecosystem and in promoting a comprehensive approach to cyber defence, cybercrime, network and information security (NIS), and cybersecurity, aligning with the European Cybersecurity Skills Framework (ECSF) established by the European Union Agency for Network and Information Security (ENISA). The ECSF provides a framework for identifying and addressing cybersecurity skills gaps, and the ESDC has been actively working to support its implementation.

In line with the EU Cybersecurity Strategy 2020-2030, the ESDC has focused on building resilience, advancing a global and open cyberspace, and developing operational capacity to prevent, deter, and respond to cyber threats. The ESDC's cyber training and education initiatives have been designed to support these goals, with a particular emphasis on enhancing cooperation and collaboration between the EU and its partners.

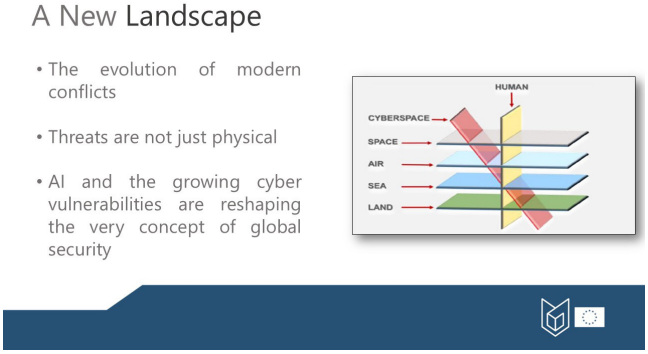
As a high priority, in support of Ukraine's security and defence efforts, the ESDC has established a strong partnership with 16 Ukrainian training institutions, with over 700 Ukrainian officials having participated in ESDC programmes since 2020, including cyber courses to bolster collective resilience against cyber threats.

Looking ahead, the ESDC will continue to enhance its cooperation with Ukraine, NATO, and other key partners to promote a comprehensive approach to cybersecurity and support the development of a more stable and secure Europe. The ESDC will also continue to work closely with ENISA to support the implementation of the ECSF and promote cybersecurity skills development across the EU, including continuing to focus on emerging technologies such as deep learning and artificial intelligence, supporting and contributing to the EU Cyber Skills Academy, and enhancing EU-NATO cooperation on cyber training.

Overall, the ESDC's holistic approach to cybersecurity and cyber defence, combined with its strong partnerships and cooperation with key EU entities and international partners, including across the whole maritime environment, has positioned it as a leader in promoting a comprehensive and coordinated approach to training and education in the cyber domain across the EU.

About the author

Giuseppe Zuffanti is the coordinator for cybersecurity, cyberdefence and hybrid threats education at the EU's European Security and Defence College (ESDC). Giuseppe has served for over 30 years in the Italian National Police, including senior posts within the Ministry of the Interior, before joining the ESDC in 2020. Giuseppe holds advanced degrees in computer science and engineering from the universities of Turin and Naples. Giuseppe has a long-standing interest in cybersecurity, cyber defence, and AI, and how they affect our security in Italy, Europe, and across the world.



The role of Emerging and Disruptive Technologies (EDT) in NATO cyberdefense

Authors (in alphabetic order):
Ilias Athanasopoulos, *University of Cyprus, athanasopoulos.elias@ucy.ac.cy*
Christos Douligeris, *University of Piraeus, cdoulig@unipi.gr*
Theodoros Karvounidis, *University of Piraeus, tkarv@unipi.gr*
Kitty Kioskli, *trustilio B.V, kitty.kioskli@trustilio.com*
Christos Ntrikogias, *Logstail, cn@logstail.com*
Constantinos Patsakis, *University of Piraeus, kpatsak@unipi.gr*
Nineta Polemi, *University of Piraeus, dpolemi@unipi.gr*
Ioannis Stamatiou, *University of Patras, stamatiu@ceid.upatras.gr*

1. Introduction

The maritime domain is rapidly transforming through the integration of Emerging and Disruptive Technologies (EDTs), which are reshaping NATO's approach to naval cybersecurity and operational dominance. Technologies such as quantum computing, artificial intelligence (AI), Internet of Things (IoT), 5G/6G networks, blockchain, and cloud computing offer NATO fleets new capabilities in Cyber Threat Intelligence (CTI), risk and incident management, decision-making, and mission secure coordination. EDTs are a double-edged sword: while they can strengthen NATO's cyber defense capabilities, they may also be exploited by adversaries to launch catastrophic attacks. Naval operations are particularly exposed due to their dependence on mobile, bandwidth-constrained environments and interconnected digital systems. As NATO platforms - from ships and submarines to unmanned maritime vehicles - rely more heavily on data-driven operations and edge-to-cloud communications, safeguarding these networks becomes critical to mission assurance. Furthermore, the human factor remains central to effective cyber defense, with trust, interpretability, and operational readiness influencing how EDTs are adopted and secured. This paper examines how NATO can integrate EDTs into its maritime cybersecurity practices, presenting specific use cases to enhance its resilience. It outlines technological opportunities, identifies

risks, and provides strategic recommendations aligned with NATO's cyber defense functions – namely: prevent, detect, defend, respond, recover, planning, C2 (command & control) and situational awareness - to ensure resilient and secure operations at sea.

1. Artificial Intelligence: The Battle of Algorithms

AI stands at the forefront of the technological arms race, utilized for both incident management and the coordination of autonomous systems.

1.1 AI-Enabled Cyber Defense vs. Adversarial AI

In the context of general cyber defense, AI systems are essential for automated monitoring, user reporting, and incident management. However, the integration of AI creates a dynamic where NATO functions are mirrored by adversarial adaptations.

Prevention and Detection: NATO utilizes AI for predictive analytics and continuous vulnerability scanning to preemptively identify weak points. Conversely, adversaries use AI-generated scans to simulate NATO infrastructure for targeted attacks. To counter this, NATO must deploy deception networks to confuse adversarial scans. While AI improves anomaly detection via real-time correlation, adversaries develop AI-generated polymorphic malware to evade conventional detection.

Defense and Response: Automated threat scoring and triage are enhanced by AI, but this requires continuous stress-testing via red-teaming to maintain integrity against adversarial machine learning (ML) techniques. Furthermore, while AI speeds up containment and countermeasures, the dynamic nature of AI-generated payloads complicates forensics.

Strategic Planning and C2: AI assists in simulating adversarial tactics for optimized defense plans. However, adversaries may use AI to predict NATO responses, necessitating deception-based planning to deny them reliable predictive data. In Command and Control (C2), AI supports real-time orchestration, but this reliance creates vulnerabilities to misinformation or spoofed commands, requiring multi-factor authentication and commander override authority.

1.2 AI-Coordinated Swarm Drones

The deployment of AI in Intelligence, Surveillance, and Reconnaissance (ISR) through drone swarms illustrates the physical manifestation of these cyber threats.

Operational Security: AI-coordinated drones can predict flight risks and secure communication channels, yet they face adversarial probing attempting signal spoofing. Defense strategies must include adaptive anti-spoofing protocols and "secure boot" measures to prevent pre-mission tampering.

Resilience and Recovery: Drone swarms must autonomously adjust mesh networks when jammed. Adversaries may attempt to override C2 links or launch jamming attacks, which requires hardened encryption and frequency agility. Post-attack, swarms must be able to re-synchronize channels and reload trusted AI models, as adversarial interference can corrupt logic or delay telemetry recovery.

2. Cloud Computing: Simulation and Navigation

Cloud computing offers scalability for training and real-time operations but introduces significant data integrity risks.

2.1 Cloud-Enabled Military Training Simulations

Cloud infrastructure (CI) is pivotal for realistic simulations that test detection, response, and recovery capabilities.

Vulnerabilities: The primary threat is the compromise of the cloud to steal sensitive information or the injection of fake information into Command and Control (C2) systems.

Mitigation: It is recommended to use private cloud implementations with open protocols, multiple communication channels, and standard hardening techniques. To protect against data leakage, "honey data" should be used to detect leaks, and sensitive data should be excluded from simulated trainings where possible.

2.2 Real-Time Navigation of Unmanned Devices

For unmanned ships, CI assists in real-time navigation and routing decisions that thin clients cannot process independently.

The Hijacking Threat: Adversaries may attempt to hijack the communication channel or send fake geolocation data to misguide devices.

Defensive Routing: Defending these systems requires establishing secondary communication channels for trusted geolocation data and using sensors on the device to inform the cloud of discrepancies. If a device is hijacked, the cloud must be capable of overwriting routing with fresh updates or utilizing alternative routings to avoid specific attack vectors.

3. Quantum Technologies: The Cryptographic Horizon

3.1 The Quantum Threat

Quantum technologies pose an existential threat to current cryptographic standards while offering new methods for securing communications. The emergence of Shor's and Grover's algorithms threatens to break public-key encryption (RSA, ECC) and erode symmetric strength. The most immediate danger is "Harvest-now, decrypt-later," where adversaries store current encrypted traffic to decrypt it once quantum capabilities mature. Maritime environments face specific challenges, such as exposure points in ship-to-shore links and increased risk of side-channel attacks due to harsh operational conditions.

3.2 Quantum Key Distribution (QKD)

To counter these threats, NATO is exploring QKD-enabled strategic fiber backbones.

Prevent and Detect: Deployment requires strong classical authentication and physical protection of conduits. Detection involves monitoring Quantum Bit Error Rates (QBER) and correlating them with maintenance schedules to identify anomalies or eavesdropping attempts.

Defend and Recover: Defense mechanisms include automatic re-keying or rerouting upon anomaly detection and implementing Software-Defined Wide Area Network (SD-WAN) failover policies. Recovery protocols demand the purging of affected key material and the enforcing of minimum crypto levels to prevent rollback to weaker modes.

4. 5G/6G: Digital Twins and Tactical Connectivity

Next-generation networks provide the bandwidth and low latency required for advanced operations but expand the attack surface.

4.1 The Digital Twin Sandbox

NATO is integrating complex systems like IoT and autonomous vehicles, which creates risks if deployed without rigorous testing.

Solution: A 5G/6G-enabled "digital twin" sandbox—a secure virtual environment that replicates battlefield conditions, including network congestion and jamming.

Operational Use: This environment allows AI and IoT systems to be subjected to simulated cyberattacks to identify vulnerabilities. It enables the testing of "mission abort" plans and self-healing network nodes.

Counter-Adversarial Measures: Adversaries may use their own sandboxes to find zero-day exploits; therefore, NATO must test all third-party products in the sandbox prior to integration. Additionally, the sandbox itself must be protected by Zero Trust Architecture (ZTA) to prevent enemies from hacking the test environment to alter results.

4.2 Private "Network-in-a-Box"

For forward-deployed units in remote areas with compromised communications, a portable 5G/6G "network-in-a-box" offers a solution.

Capabilities: This kit establishes a high-speed local bubble using Mobile Edge Computing (MEC) for local forensic analysis, avoiding reliance on weak satellite links.

Security via Slicing: Network slicing creates isolated virtual networks for different functions, such as quarantining infected devices while maintaining C2 traffic.

Risks: Threats include supply chain attacks on the kit and jamming of C2 channels. Mitigations involve scanning firmware pre-deployment, using directional antennas, and requiring digital signatures for commands.

5. Blockchain and the Human Element

5.1 Blockchain Limitations

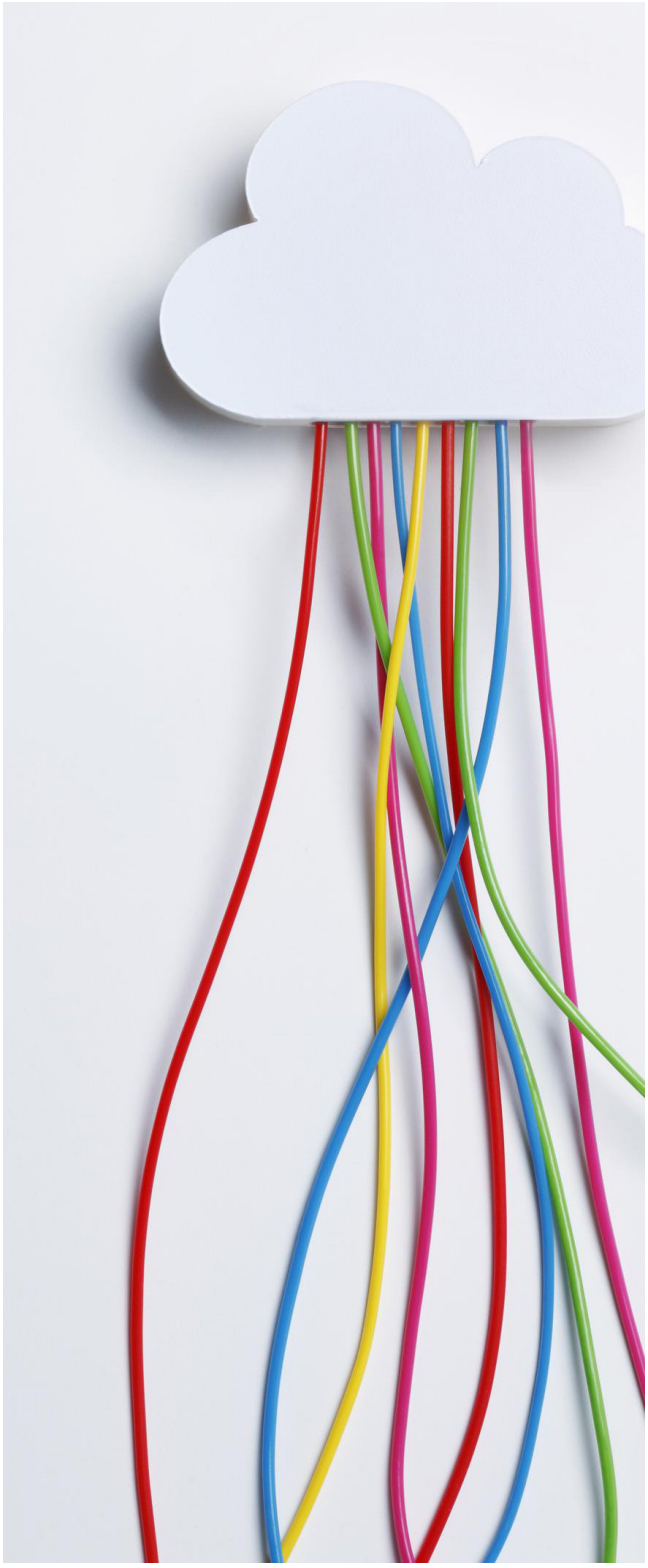
While often touted for integrity, blockchain faces hurdles in NATO operations. It is not developed for DDIL (Denied, Disrupted, Intermittent, and Limited) environments where bandwidth is constrained. Furthermore, most blockchains are not quantum-secure, and cryptocurrencies like Bitcoin and Monero are frequently abused for criminal purposes.

5.2 Human Factors

Despite technological advancements, human factors remain a critical vulnerability.

Risks: Social engineering, phishing, and insider threats persist, exacerbated by cognitive overload, automation bias, and reduced situational awareness.

Recommendations: To build resilience, NATO must deploy robust identity management and use simulation-based exercises with realistic, human-centered threat scenarios. Personnel must be specifically prepared for denied or degraded environments where human judgment becomes the last line of defense.



6. Conclusions

The integration of EDTs into NATO's maritime cyberdefense is an opportunity masked as a threat—and vice versa. Whether through the deployment of AI drone swarms, QKD backbones, or 5G digital twins, the imperative remains consistent: NATO must adopt a posture of "Prevent, Detect, Defend, Respond, and Recover," ensuring that technological innovation is always aligned with robust human capability and rigorous security protocols.

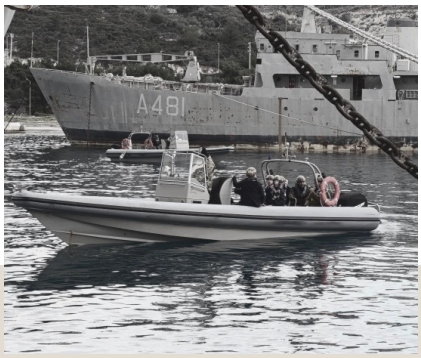
NMIOTC
Courses & Activities

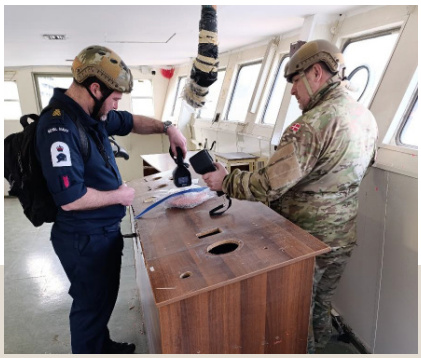
Course 28000 – "Radiological Search in Maritime Environment"

From 10th to 14th of February 2025, an additional iteration of Resident Course 28000 "Radiological Search in Maritime Environment" was conducted at the NMIOTC premises, utilizing the wide range of NMIOTC training facilities and capabilities. The Course is one of the pillars of the Office of Nuclear Incident Policy and Cooperation at the U.S. National Nuclear Security Administration (NNSA's NIPC) and NATO's training effort in Europe.

In total, twenty-four (24) participants and ten (10) Subject Matter Experts (SMEs) from five (5) NATO nations [Denmark (3), Germany (1), Greece (9), United Kingdom (2), and USA (9 students +10 instructors)] participated in the Course.

The U.S. Department of Energy (DOE) and the Naval Criminal Investigative Service (NCIS) supported the course with their SMEs, equipment and know-how.





Course 30000 “NATO Identity Intelligence Analyst in a Complex Environment”

From 10th to 14th of February 2025, NMIOTC conducted the Resident Course 30000 “NATO Identity Intelligence Analyst in a Complex Environment”.

The aim of the course is to develop NATO analysts who can leverage identity intelligence (I2) to enhance analysis and production in order to inform command decisions in NATO Joint Operations Areas. This I2 Analyst Course is also intended for sharing lessons learned and develop analytical techniques.

In total, nine (9) experts from Greece, The Netherlands, Romania and USA contributed as lecturers in the Course. Course. Eighteen (18) trainees coming from eleven (11) Nations (Belgium, Czech Republic, France, Greece, Latvia, The Netherlands, Spain, Sweden, Slovenia, United Kingdom and USA) attended and successfully completed the training.

Courses 2000 & 3000 “Boarding Team Theoretical & Practical Issues”

From 10th to 21st of February 2025, the Resident Courses 2000 “Boarding Team Theoretical Issues” and 3000 “Boarding Team Practical Issues” were conducted in tandem at NMIOTC premises.

Course “2000” provided theoretical training to Boarding Teams in order to better plan and conduct Boarding Operations. Course “3000”, which followed, focused on the associated practical training for safe and effective Boarding Operations.

In total, twenty three (23) trainees from seven (7) NATO and Partner countries (Greece, Kuwait, Latvia, Lithuania, Poland, Ukraine and the USA) attended both courses.

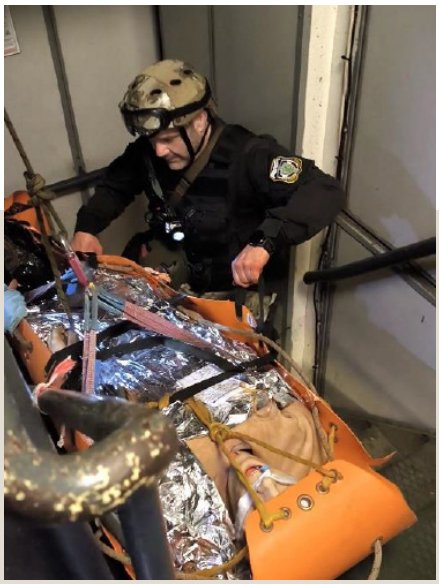
Course 26000 “Tactical Combat Casualty Care (TCCC)/ Combat Lifesaver (CLS) in Maritime Operations”

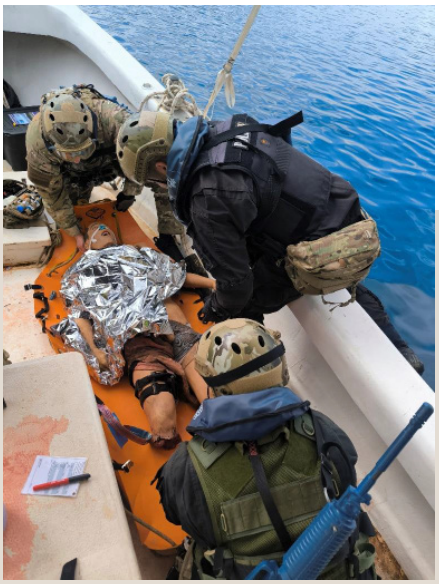
From 24th to 28th of February 2025, the Resident Course 26000 “Tactical Combat Casualty Care / Combat Lifesaver in Maritime Operations” was successfully conducted at the Centre’s premises.

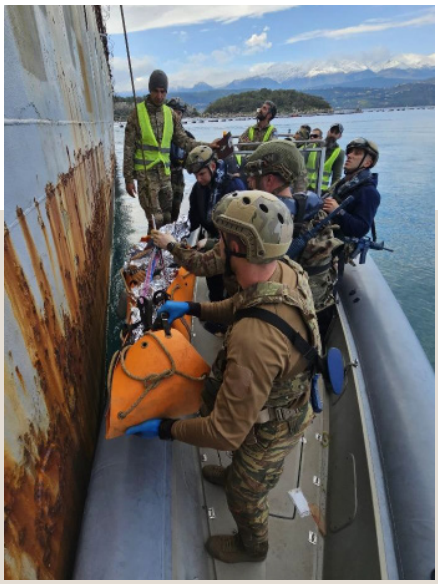
The course aims to provide to all combatants and first responders (SOF and conventional personnel), involved in Maritime Operations, basic knowledge and skills in delivering necessary pre - hospital care with limited equipment and in confined spaces. Furthermore, critical and essential skills are taught so as first responders are able to assist medical personnel to provide more complicated medical assistance and deal effectively with a mass casualty situation.

Subject Matter Experts from NMIOTC, the 31 Search & Rescue Operations Squadron, HAF, the Hellenic Police, the Chania Fire Department and U.S. NSA Souda Bay - certified as NAEMT instructors - delivered training to sixteen (16) participants, coming from three (3) Countries (Germany, Greece and Switzerland).

NMIOTC has been the first NATO Education and Training Facility (NETF) to receive the National Association of Emergency Medical Technicians (NAEMT) certification that is eligible to provide TCCC Courses.







NMIOTC's METT in IMX25, in Aqaba, Jordan

From 10th to 21st of February 2025, NMIOTC supported, with a Mobile Education & Training Team (METT), the International Maritime Exercise (IMX) 2025, in Aqaba, Jordan. The Centre deployed two (2) Sea Trainers/Instructors to deliver Underwater C-IED Disposal and Tactical Combat Casualty Care (TCCC) training to IMX25 participants.

Photos above by Sgt. Thomas Brown, U.S. Army, captured moments of the training and a Casualty Evacuation (CASEVAC) practice on February 11th and 19th.

IMX25 was a major multinational training event in the Middle East, led by U.S. Naval Forces Central Command (NAVCENT), which involved 5,000 personnel from more than 30 Nations and International Organizations, aiming at strengthening regional maritime security cooperation.

NMIOTC Course 6000 “WMD in MIO”

From 31st of March to 4th of April 2025, the NMIOTC Course 6000 “Weapons of Mass Destruction in Maritime Interdiction Operations (WMD in MIO)” was conducted at the Centre’s premises.

In total, eighteen (18) trainees coming from eleven (11) countries (Algeria, Azerbaijan, Jordan, Georgia, Greece, Italy, Lithuania, Netherlands, Poland, United Kingdom and USA) attended the course.

Instructors from U.S. Defense Threat Reduction Agency, the Naval Criminal Investigative Service (NCIS) and the Joint CBRN Defence CoE provided invaluable support to the course with their expertise and equipment, in addition to the Centre’s Instructors and assets.

National Security School, Hellenic Police Academy at NMIOTC

On Wednesday, April 2nd, 2025, the 28th Senior Course of the National Security School, Hellenic Police Academy, paid a formal visit to NMIOTC, in the context of their educational trip to Crete. The Senior Officers attending this National Security School's Course, were led by the School's Commandant, Police Colonel Anastasia Mylona.

The visitors were thoroughly informed about the Centre's mission, and had a productive conversation with NMOTC Chief of Staff and NMIOTC Director of Education & Training.

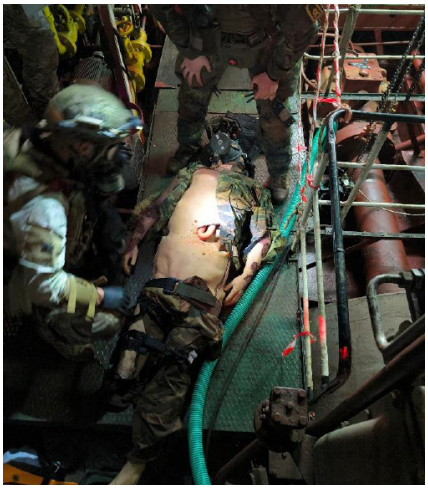
Course 21000 “Medical Combat Care in Maritime Operations”

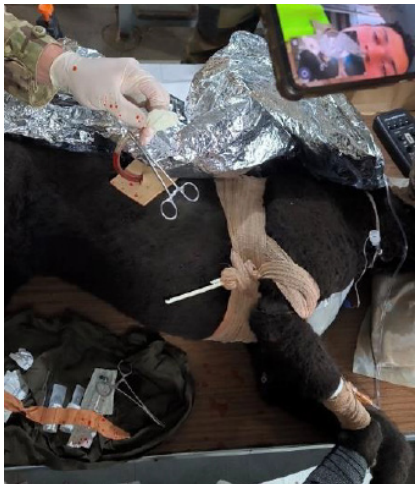
From the 31st of March to 11th of April 2025, the Resident Course 21000 “Medical Combat Care in Maritime Operations” was conducted at the NMIOTC’s premises.

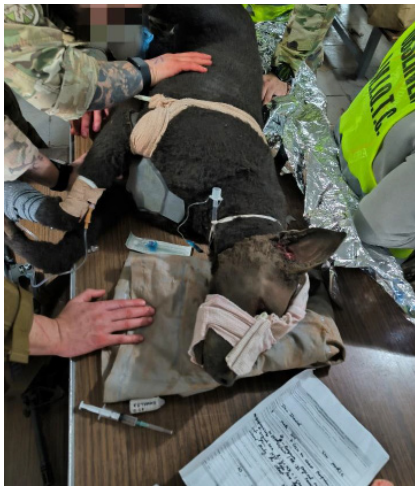
The goal of this course was to transfer knowledge and create & enhance trainees’ skills so as to provide pre-hospital emergency medical assistance from the point of injury in the mission/theatre until the final transfer to the closest Medical Treatment Facility is accomplished.

In this iteration, in collaboration with the U.S. 64 Medical Detachment Veterinary Service Support, a pilot module pertaining to K9 TCCC was presented to students for the first time. The module received exceptional feedback, highlighting its significance and fostering high engagement.”

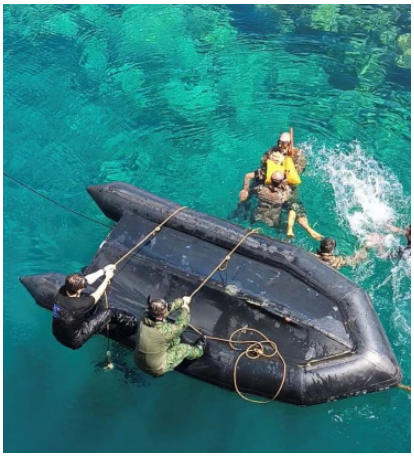
In total, seventeen (17) participants from nine (9) Countries (Germany, Greece, Hungary, Latvia, Malta, Poland, Singapore, Spain, and USA) attended the course. Training was delivered from Subject Matter Experts certified as NAEMT (National Association of Emergency Medical Technicians) instructors and augmenters specialized in extraction from confined spaces and prolonged field care.









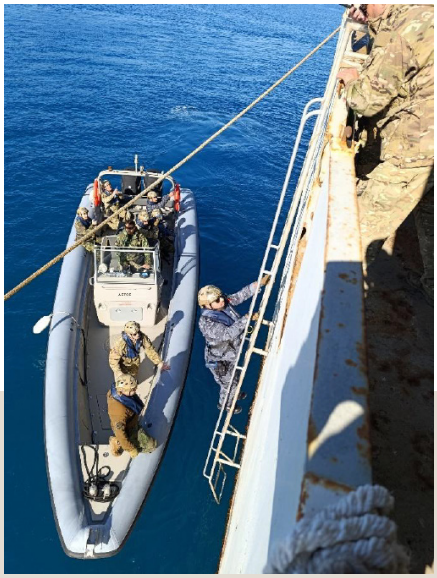


Course 29000 “Detection and Identification of WMD (CBRN Materials) in Maritime Interdiction”

From 7th to 11th of April 2025, the Course 29000 “Detection and Identification of WMD (CBRN Materials) in Maritime Interdiction” was successfully conducted at the NMIOTC premises.

Seventeen (17) trainees coming from eight (8) NATO and Partner Nations (Czech Republic, Denmark, Greece, Italy, Jordan, Kuwait, Netherlands and Poland) attended the course. Subject Matter Experts from US Defense Threat Reduction Agency (DTRA), Naval Criminal Investigative Service (NCIS), Institute for Maritime Operations Training (IMAF), Austrian and Finnish Army, supported the course as augmenters and instructors.





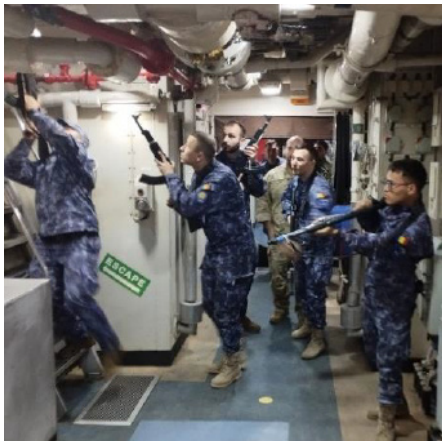
NMIOTC Presence at Military Strategic Partnership Conference 2025

From Monday 7th to Friday 10th April 2025, NMIOTC, as a NATO Education and Training Facility (NETF) and continuum member of Military Strategic Partnership (MSP), participated with a three-staff-officer delegation in the Military Strategic Partnership Conference for 2025 (MSPC 25), organized and conducted by NATO SHAPE Partnership Directorate (PD), in Doha, Qatar.

NMIOTC's SEA SHIELD Mobile Education and Training Team (METT)

From 5th to 6th April 2025, NMIOTC delivered Visit Board Search and Seizure (VBSS) tailored training with a Mobile Education and Training Team (METT) to the participants of Exercise SEA SHIELD 25, in Constanța, Romania.

In total, nineteen (19) participants received training [ROU Navy (9), ROU SOF (5) and Bulgarian Navy Boarding Team (5)].



NMIOTC instructor in SOFCOM Medical Instructor Development Course

From 14 to 18 April 2025, NMIOTC supported the SOF "Medical Instructor Development and Tactical Combat Casualty Care Instructor Course" with one (1) Subject Matter Expert (SME) as an instructor. The course was conducted in Riga, Latvia, and led by the Allied Special Operations Forces Command (NATO SOFCOM)'s Medical Mobile Training Team.

The training aimed to equip students with essential knowledge and skills related to SOF medical training, including requirements analysis, instructional design, skill acquisition in non-permissive environments, scenario-based training, and various debriefing techniques critical for SOF medical personnel.

NMIOTC remains at the forefront of NATO medical training excellence, being the first NATO Education and Training Facility (NETF) to receive certification from the National Association of Emergency Medical Technicians (NAEMT). As an Authorized NAEMT Training Centre, NMIOTC is qualified to deliver Tactical Combat Casualty Care (TCCC) Courses.

Looking ahead, in November 2025, NMIOTC will conduct the second annual iteration of Course 21000 "Medical Combat Care in Maritime Operations", followed later that month by Course 26000 "Tactical Combat Casualty Care (TCCC)/Combat Lifesaver (CLS) in Maritime Operations".

Defence Planning Practitioners Forum (DPPF) at NMIOTC

From 14th to 15th of May, 2025, NMIOTC hosted ACT's Defence Planning Practitioners Forum (DPPF) at its premises in Marathi, Souda Bay. The DPPF replaces the previously held Multinational Solutions Conference and is a newly ACT established initiative to provide participants an annual forum to connect, share expertise, solve problems and build a collaborative network to support the

planning and execution of NATO Defence Planning Process (NDPP) cycles.

The Assistant Chief of Staff - Strategic Plans & Policy NATO ACT, Commodore Ruud Schoonen NLD (N), the Director Staff Element Europe/Deputy Assistant Chief of Staff Defense Planning HQ SACT, Brigadier General Frédéric Gauthier FRA (A), Deputy Chief of the Swedish Navy, Brigadier General Patrik Gardesten SWE (Amf) and the Assistant Chief of Staff - Strategic Development of Forces, NATO SHAPE Brigadier General Marc Lobel FRA (A) paid office calls to the NMIOTC Commandant, with whom they discussed the Centre's mission, role, educational and transformational capabilities.

Course 13000
Command Team Issues in Maritime Interdiction Operation in Support of International Efforts to Manage the Migrant and Refugee Crisis at Sea

Resident Course 13000 "Command Team Issues in Maritime Interdiction Operation in Support of International Efforts to Manage the Migrant and Refugee Crisis at Sea" was conducted from 19th to 23rd of May 2025 at the NMIOTC premises.

Course objective was to deliver the appropriate knowledge to the Command Teams of naval units in order to prepare them to fulfil the unit's specific tasks related to operations to assist law enforcement agencies with the refugee and migrant crisis at sea.

In total sixteen (16) trainees coming from ten (10) countries (Belgium, Bulgaria, Estonia, Germany, Greece, Ireland, Portugal, Slovenia, Spain and Türkiye) attended the course. In this iteration, we had also the pleasure to receive trainees from FRONTEX.

Subject Matter Experts from respected authorities such as Hellenic Navy, Hellenic Coastguard and Military Medical Academy provided support to the course as Augmenters, in addition to the Centre's Instructors and Lecturers.

NSO 'NATO Maritime Operational Law Course' in NMIOTC

The NATO School Oberammergau (NSO) "Maritime Operational Law Course" was conducted from 26 to 30 May 2025 at our Centre's premises, in cooperation with the United States Naval War College (USNWC) and the NATO's Centre of Excellence for Operations in Confined and Shallow Waters (CSW CoE).

This NATO-approved Course aims to provide education and individual training to military/civilian Legal Advisors and Naval Officers in legal considerations pertaining to NATO maritime operations and public international law as it applies to peacetime operations and armed conflict at sea.

UPX "Underwater Post Blast Exploitation Training"

The Underwater Post Blast Exploitation Training (UPX) was conducted from 26th to 30th of May 2025, at NMIOTC premises.

Training objective was to provide comprehensive knowledge in investigating maritime terrorism incidents. The training included Diving Operations and Technical Exploitation of detonated improvised explosive devices found in a maritime environment.

Subject Matter Experts from the FBI's Explosives Unit and Critical Incident Response Group – Counter IED Section (USA), the Belgian EOD Batlajon DOVO-SEDEE, the French GPD Manche and the Hellenic Navy Special Operations Command provided support to the course.

NATO Defence Capacity Building (DCB) for Mauritania – Maritime Security Initiative

From 19th to 30th May 25, a two-week Tailored Training package in the field of Maritime Interdiction was provided to fifteen (15) members of the Mauritanian (MRT) Navy, in support of NATO's DCB for MRT. The modular structure of the activity included theoretical and practical training on Visit Board Search and Seizure (VBSS), Tactical Sweep, MEDEVAC, Breaching, Boarding Under multiple Threats (BUMPT), RHIB insertion and other related to MIO topics. On the occasion of the training, Mr. Leonardo Scanavino, NATO's Staff Officer Counter-Terrorism Section Operations Division (OPS), payed an office call to NMIOTC Commandant, to discuss future opportunities for NMIOTC engagement to DCB for MRT. In addition, Mr Scanavino witnessed first-hand the practical training modules of the MRT team.

16th NMIOTC Annual Conference 2025

From 4th to 5th June of 2025, the 16th NMIOTC Annual Conference titled: “Steering into the Future: The Impact of Climate Change on Maritime Security” took place at the NMIOTC premises. It was attended by more than 120 participants from 25 Nations, as well as representatives of NATO Command Structure, National and International Organizations, academic community and also from the shipping and defence industry.

NMIOTC Commandant, Commodore Periklis Piyis GRC (N), gave the welcome address to the attendees, followed by the Deputy Chief of the Hellenic National Defence General Staff, Commodore Ioannis Stratogiannis GRC (N), who commenced the Conference with the Host Nation opening remarks. Keynote Speakers were, Professor James Bergeron, Political Advisor to the Commander, NATO Allied Maritime Command (MARCOM), Dr Harry T. Conway, Chair of the Marine Environment Protection Committee (MEPC), International Maritime Organization (IMO) and Dr Alison Weston, Senior Coordinator for Maritime Security in the Security and Defence Policy Directorate of the European External Action Service (EEAS).

On the second day, Lieutenant General Michael Klouvas GRC (A), Commander of the Command of Constructions and Natural Disasters Relief, presented the Host Nation’s plans and measures to mitigate the Impact of Climate Change on the Safety of Maritime Facilities.

NSA Souda Bay tailored training

From 16th to 18th June of 2025, NMIOTC provided a three-day cooperative tailored training to fifty-three (53) U.S. Navy personnel of Naval Support Activity (NSA) Souda Bay. NSA Souda Bay participants took part part in training on topics related to Maritime Interdiction Operations, NATO membership, leadership, and team building.

During leadership lessons, Commodore Periklis PIYIS HN, Commandant NMIOTC delivered a lecture on resilience in NATO, followed by Captain Stephen STACEY USN, Commanding Officer, NSA Souda Bay, who briefed trainees on the importance of an organization's mission and vision.

NMIOTC and NSA Souda Bay personnel participated in a final team building exercise, which assembled teams of diverse backgrounds to accomplish various tasks and perform physically demanding exercises.

Italian Naval College “F. Morosini” Visits NMIOTC

On Friday, June 20th, students from the 2nd Class “Uranos” of the Italian Military Naval College “Francesco Morosini”, led by the Commanding Officer of the class, and the Commanding Officer of ITS MIMBELLI, paid a visit to NMIOTC during their summer educational campaign.

The CO ITS Mimbelli, Captain Luca CAPOBIANCO ITA-N, and the CO of the Naval College class, LtCdr Francesco MERCONE, had an office call with NMIOTC Commandant, with whom they discussed the Centre’s educational programs, training activities and transformational capabilities.

Course 7000 “Maritime Interdiction Operations in Support to Counter Piracy And Armed Robbery at Sea Ops”

From 7th to 11th of July 2025 the Resident Course 7000 “Maritime Interdiction Operations in Support to Counter Piracy and Armed Robbery at Sea Operations” was conducted at the NMIOTC premises.

This Course included theoretical and practical training for military personnel in terms of planning and execution of Operations aimed at fighting against piracy & armed robbery at sea.

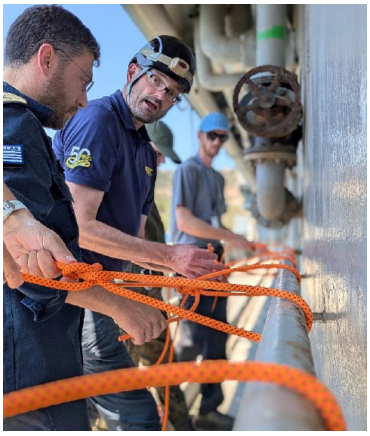
In total, twelve (12) participants from four (4) Nations (Bulgaria, Croatia, Greece and USA) successfully completed the Course. Lectures and practical drills were delivered by NMIOTC Sea Trainers and Instructors, in cooperation with augmenters from IMAF (Institut für Maritime Einsatzaus und Fortbildung).

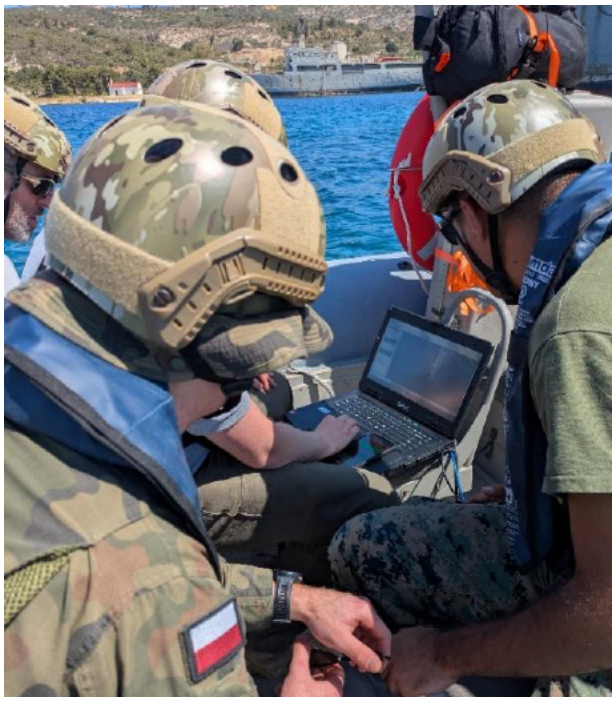
Course 28000 – "Radiological Search in Maritime Environment"

From 14th to 18th of July 2025, the Resident Course 28000 "Radiological Search in Maritime Environment" was conducted at the NMIOTC premises, utilizing a wide range of the Centre's training facilities.

Twenty-two (22) participants and twelve (12) Subject Matter Experts (SME) from eight (8) NATO nations (Belgium, Czech Republic, Greece, Italy, Poland, Romania, United Kingdom and USA) took part in the course.

The U.S. Department of Energy (DOE), Defense Threat Reduction Agency (DTRA), National Nuclear Security Administration (NNSA), and Naval Criminal Investigative Service (NCIS) supported the course with SMEs, equipment and 'know-how'.





Course 16000 “Maritime Aspects of Joint Operations”

From 8th to 12th of September 2025, NMIOTC’s Resident Course 16000 “Maritime Aspects of Joint Operations” was conducted at the Centre’s premises, with support from NATO MARCOM HQs, HNDGS and HNGS.

The objective of the course is to familiarize Staff Officers of various professional backgrounds with maritime aspects of Joint Operations.

In total, seven (7) trainees from six (6) NATO Nations (Czech Republic, France, Germany, Latvia, Poland & USA) attended the Course.

9th NMIOTC Cyber Security Conference in Maritime Domain

On 25 September 2025, the 9th NMIOTC Conference on Cyber Security in the Maritime Domain successfully concluded after two days of high-level discussions at the Centre's premises in Souda Bay, Greece.

The event gathered more than 130 participants from 30 nations, including representatives of national and international organizations, the academic community, and the maritime private sector and shipping industry.

The Commandant of NMIOTC welcomed all participants and highlighted the Center's contributions to cybersecurity training, as well as its future plans to develop a Digital Transformation concept in support of Maritime Interdiction Operations (MIO).

Opening remarks were delivered by Commodore Dimitrios Athanasiou GRC-N, from the Hellenic National Defence General Staff (HNDGS). The Conference's Keynote speakers were:

Mr Michail Bletsas, Governor of the Hellenic National Cybersecurity Authority (NCSA)

Mr. Marco Criscuolo, Acting Deputy Assistant Secretary General / Director Strat. & Policy, Cyber & Digital Transformation at NATO HQ

Brigadier General Konstantinos Kokodroulis, ACOS J6 at NATO SHAPE

Mr. Santiago Encabo Head of Unit Safety and Security at European Maritime Safety Agency

Dr. Evangelos Ouzounis, Head of Capacity Building at the European Union Agency for Cybersecurity (ENISA)

The Conference panels included distinguished experts coming from HNDGS, NATO Allied Command Transformation, NCI Academy, NATO Maritime Command, NATO DEEP eAcademy, European Security & Defence College (ESDC), Polish Naval Academy, Belgian Cyber Command, Stellenbosch University, IMT Atlantique / French Navy Academy, University of Piraeus, University of the Aegean, University of Wisconsin-Madison, Maritime Hacking Village, Naval Group, Leonardo, E-phors/ Fincantieri, Nordic Maritime Cyber Resilience Centre, CYTUR Inc., CYGNUS, Peregrine Technical Solutions, LLC, Thales and ThreatIntel.

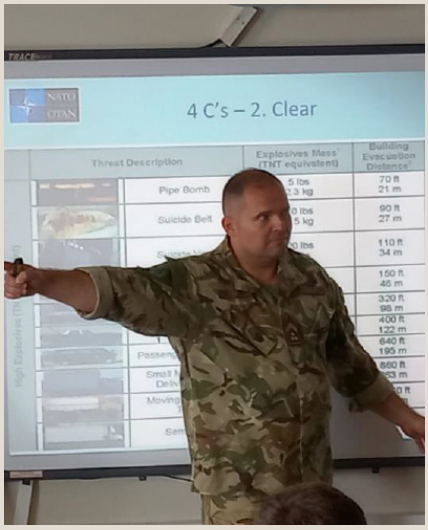


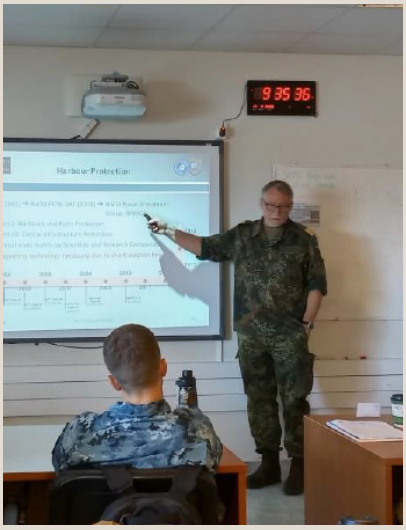


Course 8000 “C-IED Considerations in Maritime Force Protection”

From 15th to 26th of September 2025, the Resident Course 8000 “C-IED Considerations in Maritime Force Protection” was conducted at the NMIOTC premises.

The aim of the course was to educate and train students in NATO practices and procedures regarding operational and tactical dimensions of mitigating Improvised Explosive Device (IED) Threat in Maritime Force Protection. In total, sixteen (16) participants from ten (10) countries (Al-





geria, Azerbaijan, Belgium, Egypt, Italy, Pakistan, Poland, Portugal, Slovenia and Ukraine) attended the Course.

NMIOTC Sea Trainers and Instructors in cooperation with augmenters from the Centre of Excellence for Operations in Confined and Shallow Waters (CSW CoE), the HUN NCO Academy, the Hellenic Police Bomb Disposal Squadron, the Hellenic Army and the Institute for Maritime Operations Training – [Military and Law Enforcement MIO] delivered lectures and practical drills focused on C-IED aspects in Maritime Force Protection.

NMIOTC Course 25000

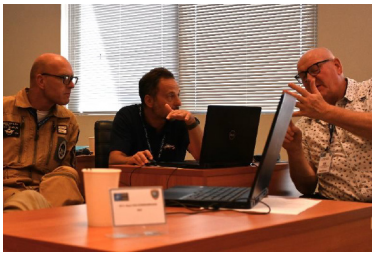
From September 29th to October 03rd, 2025, the NMIOTC's NATO-Approved Course 25000 "Drafting, Production & Maintenance of NATO Standards", was conducted at the Centre's premises, with support from Hellenic National Defence General Staff (HNDGS), NATO Standardization Office (NSO), NATO Allied Command Transformation (ACT) and DEFSTAND.

The aim of the course is to provide comprehensive knowledge to facilitate understanding of the procedures for development, production and maintenance of NATO standardization documents, including doctrines.

The training focused on the fundamental principles of drafting operational and materiel standards, and covered multiple practical examples with thorough contextual explanation. In this context, a live demo on a case study of standardization procedures was carried out at the Hellenic Air Force (HAF) 115 Combat Wing in Souda Air Base.

In total, twenty-six (26) trainees and six (6) instructors from twelve (12) NATO Nations & Partners (Australia, Canada, Colombia, Denmark, Finland, Greece, Italy, The Netherlands, Norway, Poland, Spain, Ukraine and United Kingdom) attended the course.





Course 17000
"Train the Trainers - Technical Instructor"

From 13th to 24th October 2025 the Course 17000 was conducted through a combination Advanced Distributed Learning (ADL) and in-person attendance at NMIOTC's premises.

The aim of the course was to provide a comprehensive training package which included theoretical and practical presentation of educational knowledge to enhance the participants' presentation and teaching skills.

Ten (10) trainees from five (5) countries (Bahrain, Greece, Italy, Poland and USA) participated in the course.


Multinational Exercise 'NIRIIS-25' hosted at NMIOTC

From 02 to 08 November 2025, NMIOTC provided support to Exercise "NIRIIS 25". The "NIRIIS" exercise is a multinational naval INVITEX (Invitation Exercise) conducted by the Hellenic Navy annually. Its purpose is to train participants in procedures for common naval warfare and modern threat scenarios, focusing on maritime security issues.

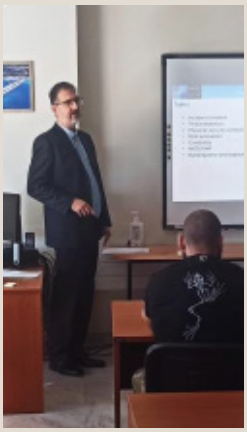
NMIOTC facilitated the Exercise Control (EXCON) cell, and hosted exercise syndicate meetings, the "Pre Sail Conference" (PSC) and the "Hot Wash Up" (HWU), proudly receiving at the Centre's premises the Deputy Commander in Chief of the Hellenic Fleet, Rear Admiral Leonidas Anagnostopoulos HN.

In the context of NIRIIS-25, NMIOTC provided Tailored Training to fifty (50) members of the participating Hellenic Navy warships' crew, focusing on VBSS skills and procedures.

Course 32000 "MIO in Maritime Oil and Gas Assets"

From 10th to 14th of November 2025, NMIOTC conducted the 1st iteration of Course 32000 "MIO in Maritime Oil and Gas Assets". The aim of this course is to train security and MIO planners to understand and assess security threats to offshore oil and gas assets and to support the effective planning of MIO, considering operational, technical and safety characteristics of oil and gas assets while applying advanced security assessment methodologies.

The course was attended and successfully completed by sixteen (16) trainees coming from five (5) Nations (Belgium, Greece, Malta, Romania and USA).



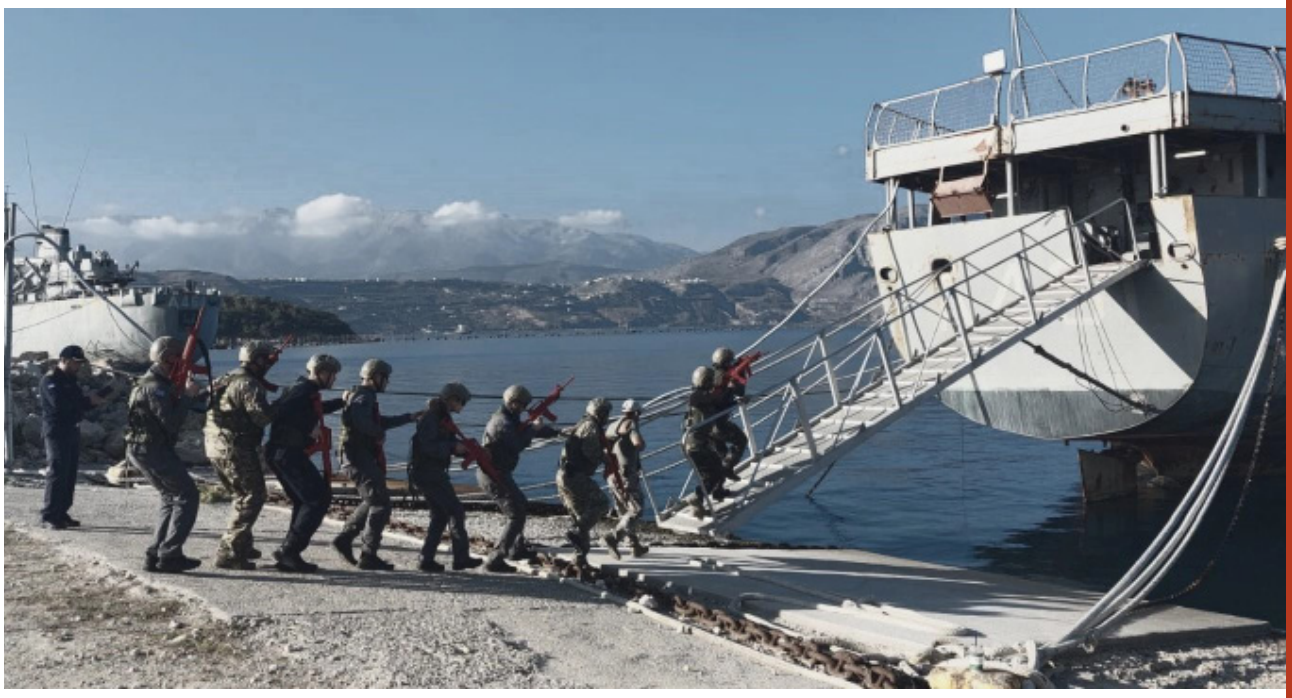
NMIOTC
Training

Belgian Marine Infantry Corps trained at NMIOTC (7 - 18 July)

NMIOTC's Mobile Education
and Training Team (METT) Exercise "BREEZE 25" (12 - 13 July)

Training of German Navy Boarding Team MOC 1 (29 September - 10 October)

Training of RNLN Maritime Security Squadron Group 2
(29 September - 3 October)



NMIOTC Course 12000 “C-IED in Maritime Interdiction Operations” (13 - 17 October)

Course 14000 “Maritime IED Disposal (M-IEDD)” (20 - 24 October)

Tailored Training to ITS CARABINIERE Boarding Team (14 November)

Course 26000 “Tactical Combat Casualty Care (TCCC)/
Combat Lifesaver (CLS) in Maritime Operations” (24 - 28 November)

NMIOTC
High Visibility Events

NMIOTC in Special Operations Medical Association (SOMA) 2025 (15 May)

HQ Supreme Allied Commander Transformation
Directorate of Multi-Domain Force Development
Norfolk, Virginia | USA

Quality Assurance Accreditation Certificate

The core processes and procedures of the NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE (NMIOTC) were reviewed and identified as being aligned with NATO Quality Standards. Therefore, the Institution qualifies for:

NATO ACCREDITED EDUCATION & TRAINING FACILITY

UNCONDITIONAL ACCREDITATION

Certificate ACT/MDFD/ETPP/TT-0584/SER:NU227

Effective: ***31 May 2025*** Expires: ***30 May 2031***

The *NATO Maritime Interdiction Operational Training Centre* 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

NMIOTC Re-Accreditation by ACT

Visit of the Hellenic Navy War College (16 May)

Maritime Air Coordination Agencies (MACA) Conference (11 - 12 June)

American Hellenic Institute Foundation Visits NMIOTC (26 June)

NATO Medical Lessons Learned Sharing Conference 2025 (6 - 8 October)

South Africa Maritime Security Conference
(30 September - 3 October)

Training Needs Analysis (TNA) Working Group (8 - 10 October)

NATO Infrastructure Conference (NIC) hosted in NMIOTC
(20 - 24 October)

U.S. Congress STAFFDEL visited NMIOTC (13 November)

Workshop on Non-Proliferation of Weapons of Mass Destruction t
Non-State Actors (21 November)

10th International Senior Course of Hellenic National Defence College: "Contemporary Maritime Security Threats" Module (4 December)

NMIOTC Training in NATO-Istanbul Cooperation Initiative Regional Centre (NIRC), Kuwait (30 November - 4 December)

NMIOTC
Souda Bay 732 00 Chania, Crete, GREECE

Phone:
+30 28210 85710

Email:
studentadmin@nmiotc.nato.int
nmiotc_studentadmin@navy.mil.gr

Webpage:
nmiotc.nato.int

Social media: