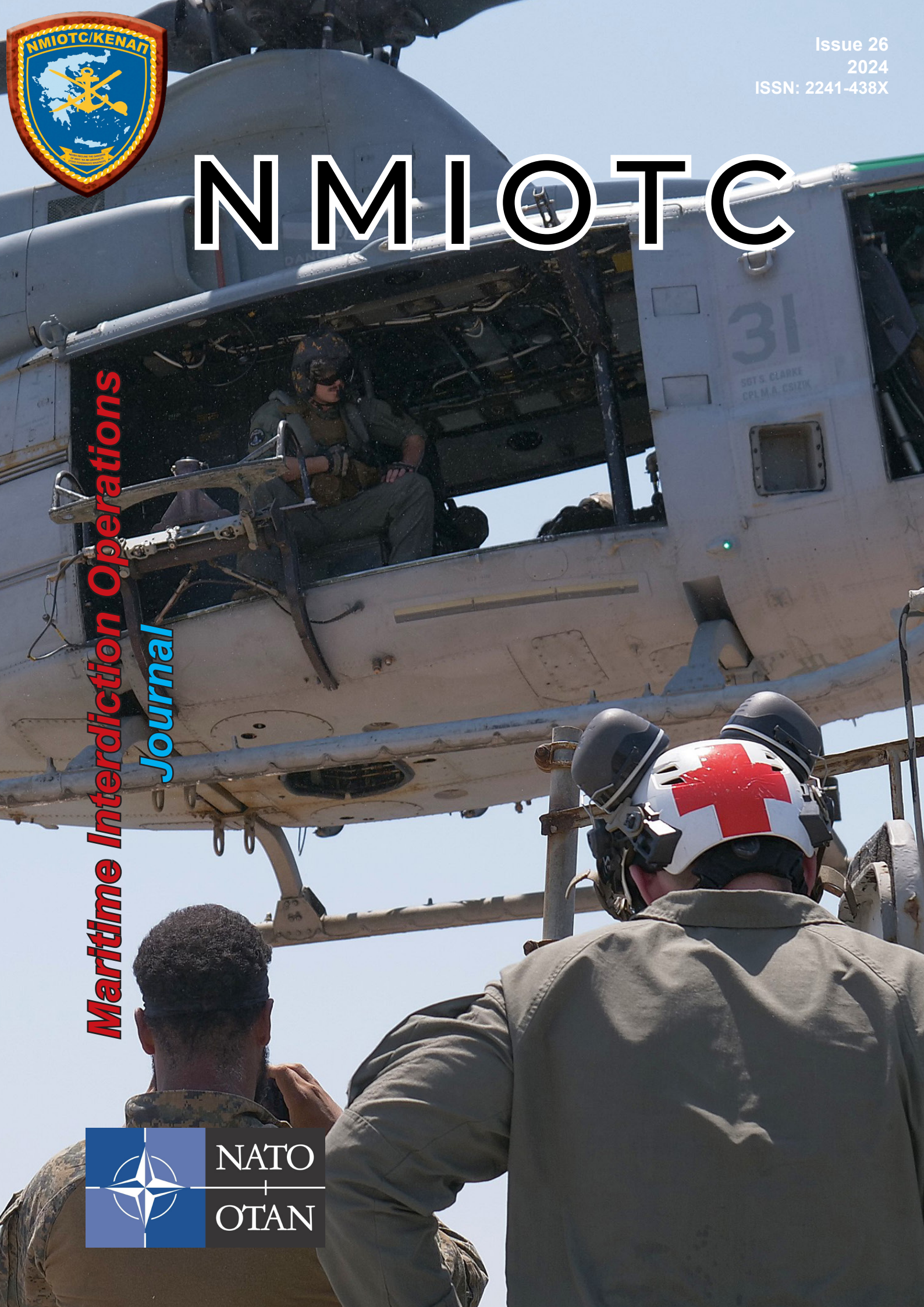
Issue 26
2024
ISSN: 2241-438X

NMIOTC

Maritime Interdiction Operations Journal



NATO
OTAN

NATO
Maritime Interdiction Operational Training Centre

SAVE THE DATES

16th NMIOTC Annual Conference
4 - 5 June 2025

""Steering into theFuture:
The Impact of Climate Change on Maritime Security"

9th Conference
on Cyber Security
in the Maritime Domain
24-25 September 2025

CONTENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Cdre E. Kyriakidis GRC (N)
Commandant NMIOTC

Executive Director
Cdr G. Finamore ITA (N)
Director of Training Support

Editor
Cpt G. Chaidemenakis GRC (N)
Head of Transformation Section

Layout Production
Lt Cdr I. Giannelis GRC (N)

Cover Photo:
Lt Cdr I. Giannelis GRC (N)

The views expressed in this issue reflect the opinions of the authors, and do not necessarily represent NMIOTC's or NATO's official positions.

All content is subject to Greek Copyright Legislation.

Pictures used from the web are not subject to copyright restrictions.

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

NMIOTC
Commandant's Editorial

Maritime Security: Adapting to a Transforming Landscape

By 2025, maritime security continues to be a vital foundation for global peace and prosperity, requiring constant vigilance and flexibility to tackle increasingly complex challenges. The shifting geopolitical, technological, and environmental dynamics highlight the need for comprehensive, multi-domain approach to protect freedom of navigation.

Central to these challenges is the safeguarding of Maritime Critical Infrastructure (MCI), encompassing energy platforms, pipelines, ports and undersea cables. These assets are crucial to the stability of global economies and are increasingly vulnerable to threats from both state and non-state actors. Ranging from cyber intrusions to physical sabotage, these hybrid and ever-changing threats underscore the necessity of enhancing resilience throughout the maritime sector.

Recent conflicts, such as the ongoing Russia-Ukraine war, have exposed the vulnerability of energy and maritime infrastructure to hybrid warfare tactics. This reality highlights the need for NATO and Allied Nations to counter these threats through unified and innovative strategies, including Multi-Domain Operations (MDO) that go beyond conventional military approaches. Cyber threats, in particular, present significant risks to navigation systems, logistical networks, and overall situational awareness. The integration of Artificial Intelligence (AI) into cyber defenses, including AI-driven exercises, has proven to be a valuable tool for improving response capabilities and situational clarity.

Moreover, intelligence and surveillance are now cornerstones of effective Maritime Interdiction Operations (MIO). Using cutting-edge technologies like satellite imagery, drones, and machine learning enables the precise identification and neutralization of illegal activities such as smuggling, piracy, and terrorism. However, the same technological advancements require robust safeguards against misuse by malicious actors.

Collaboration between military, civilian, and private entities is now more than just beneficial, it is indispensable. The fusion of resources and expertise from these domains can mitigate vulnerabilities and fortify maritime defenses. The future security landscape necessitates stronger partnerships, as demonstrated by initiatives like the EU's Maritime Security Strategy and the NATO-EU Task Force on Critical Infrastructure Resilience, which emphasizes on information-sharing and coordinated responses.
The integration of cyber resilience into maritime security is equally critical. The recent emphasis on multi-domain operations, has underscored the importance of maintaining operational superiority across all fronts. Cybersecurity measures must shift from reactive to proactive, employing predictive analytics and real-time intelligence to counter threats.

Contemporary Maritime Interdiction Operations
In that context, the contemporary Maritime Interdiction encompasses an expanded array of activities, from combating illicit trafficking to safeguarding marine ecosystems and addressing environmental challenges. Advances in technology, such as unmanned systems and sophisticated radar, have made MIO a cornerstone of maritime safety and stability.

Looking forward, education and training will be instrumental in preparing stakeholders to meet emerging challenges in a Multi-Domain Operations (MDO) context. NATO's Education and Training Facilities, like NMIOTC, play a pivotal role in bridging the gap between military and civilian sectors, promoting innovation, and incorporating emerging concepts into training. Tailored programs focusing on maritime infrastructure and energy security scenarios, cybersecurity exercises, and advanced interdiction methods will be essential to creating a robust maritime security framework.
The year 2025 represents not just a continuation of existing challenges but a call to adapt, innovate, and lead in overcoming adversity. Through collective effort, informed strategies, and unwavering commitment, we can ensure that the maritime domain remains a cornerstone of global stability and prosperity.

Efstathios Kyriakidis
Commodore GRC (N)
Commandant NMIOTC

NMIOTC
15th Annual Conference, 2024

Risks and Challenges in a Dynamic Maritime Domain: Strategy Adaptation, Technology Innovation, and the Operational Landscape of the Future

by Dinos Kerigan-Kyrou

* The author is very grateful to Gen. David Petraeus (U.S. Army, Ret.) Chair of the KKR Global Institute, former Director of the CIA, previously Commander ISAF and U.S. CENTCOM, for his invaluable correspondence in regard to the conclusions.

The following is an overview of the 15th NMIOTC Annual Conference of June 2024. The Conference focused on the developing risks and challenges in an ever-changing maritime environment. Crucially, the Conference focused on how we adapt to this environment with strategies and innovation for the changing operational landscape.

The definition of the 'maritime environment' is expanding. The surface and subsurface have long been considered the maritime environment. But it now also encompasses the entire logistical supply chain including ports, cyberspace, satellites, and space. Environmental considerations are now a central part of the maritime environment and relate directly to maritime security. The maritime environment also comprises Critical Maritime Infrastructure (CMI), including Underwater Critical Infrastructure (UCI). Indeed, NMIOTC has placed great emphasis - at its conferences, seminars, and training sessions - on how we protect our CMI. And this is vital; several months after the Conference wide attention was drawn to the critical importance of CMI. In November 2024 the C-Lion 1, a 1200 km subsea fibre-optic communications cable running from Helsinki, Finland to Rostock, Germany was severed. Germany's Defence Minister described the incident as a "hybrid" action. Low-intensity, continuous, difficult to attribute, hybrid warfare waged by nefarious actors against our Critical Infrastructure at sea, ashore, in the air, in cyberspace and possibly even in space, is likely to continue; Resilience will become increasingly central to Critical Infrastructure protection at sea and ashore. Indeed, the need for resilience, together with CMI and UCI, protection is central to NMIOTC's invaluable work.

Moreover, how we respond to asymmetric, ever-changing threats will now be a key factor of our maritime security. The August Houthi terrorist attack on the Greek oil tanker MV Sounion was the most prominent strike on commercial shipping of 2024. Nonetheless, there have been over 80 such attacks on ships in the Red Sea and Gulf of Aden. The incident led to a spill of approximately 150,000 tons of crude oil between Eritrea and Yemen. The entire crew was rescued by the EU mission EUNAVFOR ASPIDES. EU commanders also neutralized an Unmanned Surface Vessel (USV) that was heading for the tanker, and are currently helping to alleviate the effects of the attacks by preventing environmental damage. Likewise, NATO Operation Sea Guardian in the Mediterranean maintains a safe and secure maritime environment through maritime security capacity-building, situational awareness and counter-terrorism. NATO and EU close liaison and cooperation,

including the NATO-EU Task Force on the Resilience of Critical Infrastructure and through the critical work of NMIOTC, will be ever more crucial. And this cooperation is invaluable because the attack on Sounion is precisely the type of asymmetric event - combining state and non-state actors utilising low cost but widely available technology - that is increasingly targeting peaceful and legitimate maritime operations. Indeed it is now over 24 years since such asymmetric technology was utilised by al-Qaeda terrorists against the USS Cole while docked in Yemen. Since 2000, low-cost, highly adaptable technology has, unfortunately, been utilised by those with nefarious aims against us. To be direct: over the past nearly 25 years it has been nefarious actors wishing to cause us harm who have been particularly successful in utilising cyberspace and low-cost commercially available technology, adapting this technology to execute their actions and atrocities. Thankfully this situation is beginning to change. Key recommendations from this conference regarding how we should adapt to the operational landscape of the future are being applied, and we can all learn from them.
This summary will firstly recap the main synopsis from the Keynote Speakers' Session addressing the challenges we face - across NATO, the EU, our Partners and Allies - within the new dynamic maritime domain. The conference presentations and panel discussions will then be summarised, before drawing conclusions, including external reflections.

Keynote Addresses[1]

"What I fear is not the enemy's strategy but my own mistakes".

Gen. Pericles, 431 B.C.

The quote from the speech to the Athenians by Gen. Pericles highlights the 'fil rouge' followed by the distinguished session participants.

The critical role of academia and international organisations, as well as the shipping industry, for maritime security was emphasised. The many Houthi attacks affect not only shipping but also all of us all globally. Energy security and the protection of critical infrastructure is a central NATO concern. Hybrid warfare challenges today greatly shape NATO and national security; subsequently the need for cyber resilience in the maritime domain is paramount. Moreover, emerging technologies present both risks and opportunities for NATO Allies. Challenges come in many forms. For example, climate change is altering the security of the maritime environment in ways that we could not foresee; civil preparedness is therefore essential, as is the crucial necessity for NATO to maintain a technological edge in transformative technologies. The military and civilian sectors need to coordinate and work much more closely with one another; for example, multi-domain operations should be coordinated and integrated with civilian operations. NATO needs to be adaptable to a future landscape that is no longer only the 'traditional' maritime environment we have come to know over hundreds of years; it now comprises subsea sensors, Critical Maritime Infrastructure - (CMI, including energy pipelines, electricity and internet cables), unmanned water vehicles, satellites carrying data, and operations below and above the sea - in addition to 'regular' maritime assets. We must

[1] Keynote Speakers: Admiral (Ret'd) Panagiotis Chinofotis, Honorary Guest; Radm Placido Torresi, Allied Command Transformation, Deputy Chief of Staff, Joint Force Development; Vice Admiral Michael Utley, Commander of NATO's Allied Maritime Command (MARCOM); Alison Weston, Senior Coordinator for Maritime Security and Deputy to the Director at the European External Action Service (EEAS).

learn lessons from ongoing conflicts and use these lessons to address emerging security challenges. NATO needs to be a platform for these new technologies and training. In particular, NMIOTC will play a pivotal role in countering emerging threats. All stakeholders - civilian and military - need to adjust strategies and embrace technological innovation; this requires a coordinated effort between the military, government and industry. We must be able to Detect, Deter and Recover. It was highlighted that the Hellenic Armed Forces will continue to support NMIOTC to enable these crucial requirements.

The critical importance of the NATO 2022 Strategic Concept - which states that Maritime Security is the key to our prosperity and security - was stressed. This is particularly the case because the maritime domain provides a 'hiding place' for threats. In order to counter the now permanent threats of terrorism and supranational organised crime we must ensure collaborative responses. Moreover, NMIOTC's competence and capabilities bring substantial benefits to the Alliance.

Several of the keynote speakers mentioned that the global security situation has never been so complex. It was also stated that to respond to this complexity Command and Control must be agile, multi-domain, and multi-agency to achieve decision superiority. Artificial Intelligence (AI) is part of what can be called "the war of maths" - new ways of thinking. The technology needs to be utilised to make us more adaptable. We need to apply the technology to enable Decision Superiority. We need to be able to understand the deterrence we are delivering and when that deterrence becomes kinetic. And we must be adaptable and utilise technology and innovation; the maritime environment has become a network of networks. Situations over the past two years have highlighted that we must act right across government and agencies. Indeed, decisions need to be made with unity, thereby enabling the delivery of capabilities and readiness; it is important our adversaries clearly see this.

Moreover, agile command and control is vital. CMI security is an issue across the Area of Responsibility (AOR). However, the logistical infrastructure that NATO maritime forces have relied upon is outdated; we must be able to store and deliver complex systems; therefore a transformation is taking place across the AOR. We have to 'embrace the complex'; cyber enabled systems and AI are here to stay. We must stay ahead of our adversaries in cyberspace because if we do not we may not even be able to get out of a harbour [because our maritime systems will have been disrupted or shutdown online]. In order to fully utilise the benefits of these changes we need outside views; it is critical to learn lessons from others and adapt training accordingly.

The keynotes emphasised the critical importance of digitised fully Multi-Domain Operations, underscoring the importance of operational synchronisation. Crucially, this synchronisation requires intensified working with the non-military sector. We cannot work 'only' as the military any longer. Successful multi-domain operations are not only about different domains working together but also require much better connectivity than we presently have. In order to achieve this our hierarchies need to be much 'flatter' with better information-sharing. Different cultures with different languages across NATO and its Partners should learn from one another. We need better data-sharing within secure defence networks across our organisations with wide-spread digital awareness. While the army and air force are increasingly integrated we also need to also integrate maritime, space, and cyber operations. Our aim must be to make the adversary change their mind about their intended action. Utilising cyberspace and integrating operations is essential. Capabilities, especially logistical capabilities, are crucially important. When deploying forces we need to understand the lessons learnt previously and combine this with doctrine. Speed and scale are necessary to produce the full possible potential.

By mapping what is presently happening - and planning for the future - we are enabling 20 year horizon planning - analysing what our adversaries will do and where. We are also mapping what all our Partner Nations are doing including PfP, Mediterranean Dialogue, and all NATO Partnerships across the world. The NATO War-fighting Capstone Concept [which moves us beyond 'traditional' notions of conflict] aims to achieve cognitive superiority, layered resilience, and and cross-domain command - utilizing multi-domain defence creating influence and power projection.

In regard to the crucial role of the European Union it was underlined that security and defence for the EU is some-

thing that continues to develop and adapt. It is very much a 'work in progress' as we face increasing non-traditional security threats, including in the maritime domain and for EU Maritime Security Strategy (EUMSS). From this perspective, the EU has many tools and instruments to address these challenges. The importance of several crucial strategic documents in this respect was highlighted, including the EU 2014 Maritime Security Strategy, the 2022 EU Strategic Compass, and the Maritime Security Strategy and Action Plan (updated) 2023.

The EU Strategic Compass focuses on crisis management, capability development, resilience and partnerships. It underlines the importance of ensuring continued access to contested strategic domains - such as the maritime space - and upholding the international rules based order, including the UN Convention on the Law of the Sea. The Strategic Compass also underlines that global partnerships are key; not just in the military sphere but also with vital partners such as coastguards. The revised EU Maritime Security Strategy and its Action Plan, which includes actions for EU Member States as well as EU institutions and agencies, reinforces the EU's commitment in these areas. In the last few years we have seen a strong EU engagement in joint naval activities with partners, through European Naval Force Operation ATALANTA as well as in maritime domain awareness, such as the EU CRIMARIO project, helping to create maritime domain awareness.
The EU has developed an 'Integrated Approach' which aims to bring together different instruments to maximise impact. How to orchestrate this approach with partners, particularly NATO, is an area of significant development. It is important to continue to foster the already-close EU-NATO partnership, including in the maritime domain: there is no need to see this as a competition, there are enough challenges for both organisations to have a role to play, it was stated. Indeed, the EU has been engaged in maritime security operations for some years already and currently has three ongoing naval operations: EUNAVFOR ATALANTA, which has been underway for nearly 16 years contributing to the anti-piracy activities off the Horn of Africa and escorting World Food Programme ships. In support of UN resolutions, ATALANTA is also successfully countering illegal drug trafficking, most recently preventing Euro 57m trade in narcotics; EU Naval Force IRINI in the Mediterranean aims to implement the arms embargo on Libya, while also addressing human trafficking and illegal oil smuggling; Operation EUNAVFOR ASPIDES, the most recent naval operation, is playing a crucial role in protecting merchant shipping and their crews and in disturbing the Houthi terrorist activity against maritime trade in the Red Sea.
The EU has also designated two Maritime Areas of Interest (MAIs) in the Gulf of Guinea and in the North West Indian Ocean, where it applies its "Coordinated Maritime Presences" concept. This is a light-touch mechanism based on the voluntary coordination by EU Member States of naval assets deployed in a given MAI. This concept also provides a framework for a more active and consistent coordination of maritime security-related activities by EU bodies and Member States in the given MAIs, with a focus on supporting regional maritime security architectures. In line with the EU's strategic documents, such as the the revised Maritime Security Strategy, there is the ambition to do more in the maritime domain. In May 2024 the EU conducted its first Maritime Security exercise in Cartagena, led by the Spanish Navy with the participation of a number of other EU Member States and the relevant EU agencies (FRONTEX, EFCA, EMSA). This was also an opportunity to test the Common Information Sharing Environment (CISE). Further challenges remain in the maritime domain; for example, the protection of CMI is becoming an increasingly important topic. The EU already has a number of capability-related initiatives ongoing, for example through the European Defence Agency and through the Permanent Structured Cooperation framework (PESCO). It will continue to be crucial to establish and maintain an integrated approach across the EU and with the many different actors at the national level. It was highlighted that - just like NATO - the EU is only as strong as its Member States enable it to be. Moreover, an integrated approach focusing on all domains, combined with capacity building with world-wide partners, developing regional maritime security, together with EEAS diplomatic processes, can substantially help the EU contribute to maritime security on a global scale, the keynote session concluded.

Panel Discussion Summaries
'Academic and Regional Perspectives[2] - 'Current and Future Challenges in the Operational Landscape.[3]

[2] Academic and Regional Perspectives: Prof James Bergeron, Allied Maritime Command, UK and U.S., 'Net Assessment of the Transregional Crisis and Conflict 2024'; Prof Francois Vrey PhD and CAPT (ret'd) Mark Blaine RSA, SIGLA, Stellenbosch University, 'Maritime Security Threats off Africa'; Dr Christina Schori Liang, Geneva Centre for Security Policy, Switzerland, 'Cognitive Dominance, Influence and Disinformation Strategies'; Dr. Marios Panagiotis Efthymiopoulos, Neapolis University, 'A Holistic Approach to Strategic Security'. Moderator: Dr Panagiotis Efthymiopoulos, Neapolis University.

[3] Current and Future Challenges in the Operational Landscape: Rear Admiral Vasileios Gryparis GRC (N) EUNAVFOR Operation Aspides; 'Outline of EUNAVFOR Operation Aspides'; Brig Gen Nikolaos Makrygiannis GRC (AF) Integrated Air and Missile Defence (IAMD) COE, 'Train as You Fight Reinvented - Synthetic Environment Exploitation'; Rear Admiral Fabrizio Rutteri ITA (N) (NATO / EU), Plans and Policy Div, 'Italian Navy's Approach in Maritime Security Operations for Better Leveraging Sea Coordination and Cooperation Efforts'; Rear Admiral Ignacio Cuartero ESP (N) , 'Navigating Future Challenges: a Multi-Domain Approach to Maritime Security and Technological Innovation'. Moderator: CDRE Konstantinos Pitykakis, GRMARFOR HQ.

The panels emphasised a holistic approach to strategic and maritime security and the importance of an information-sharing environment to address new challenges. There will be increasing conflict over natural resources. Prof James Bergeron stated that many 'new' and 'emerging' problems have existed for centuries, but now present themselves in different forms.

It was emphasised that both 'traditional' and 'non-traditional' maritime security requires capacity building to remain in-step with a shifting threat landscape. Non-state actors successfully deploy anti-ship mines and drones. The conflicts waged by al-Shabaab in some regions of Africa utilise non-traditional means producing a hugely detrimental effect including economic loss, regional instability, food supply disruption, and threats to CMI. This enables foreign military footholds in Africa by nefarious state and non-state actors, it was explained.

Cognitive Dominance Influence and Disinformation Strategies as a critical threat to our trust ecosystems were discussed. Research presented by the Geneva Centre for Security Policy (GSCP) stated that Russia understands cognitive dominance; this is demonstrated by its influencing of decision-making, attempting to change the way we look at political situations and conflicts, and undermining our institutions. Disinformation spreads through social engineering, inauthentic amplification, micro-targeting, harassment, and abuse; Russia seeks to decrease support for Ukraine and wants people to lose trust and undermine public faith in information, it was stated. And while NATO and EU EEAS are combatting disinformation we need to think about how societies can become aware of cognitive dominance. Finland was mentioned as the world-leader in addressing these challenges, and we need to learn from what Finland is doing. The Finnish approach includes developing the ability for all of us to manage how media is understood and to build youth cyber-skills, it was mentioned. Work undertaken by the Intelligence College of Europe, a collective of EU / EEA and UK intelligence agencies, is a huge step in the right direction in achieving this. Moreover, the company Huawei and other Chinese telecom and IT companies are embedding theirdevices and systems into the critical communications and 5G infrastructure of some partner nations, creating potential major cybersecurity vulnerabilities, concluded the expert from GCSP.

The panels discussed the threat from Houthi terrorism comprising a combination of missiles and drones. Presentations argued that the greatest danger is in the straits and narrows and the Red Sea. The damage to economies from these attacks is substantial, it was posited. So far 150 ships have been protected by EU ASPIDES; 12 hostile UAVs and four USVs have been destroyed. There is excellent communication and cooperation with civilian shipping industry. The importance of simulation at IAMD was highlighted, - particularly important as many NATO nations are transiting from fourth [present] to fifth [AI] generation data capture systems. Space and cyber capabilities should be simulated within a synthetic environment [a highly realistic computer simulation environment - for example a full-motion flight simulator].

The success of the EU's current naval missions was emphasised, but it was put forward that we cannot ever accept the 'marginalisation' of the Mediterranean Sea. Moreover, new challenges are occurring not only on the sea but also under the sea. It was explained that proposals for the maritime environment should be based on technological possibilities. Indeed, hybrid threats and confrontations in cyberspace, space, and across the maritime environment are all essential concerns. A 'Digital Backbone' and technological innovation is necessary, it was argued. There is a great need for digitalisation, sensor network and data management requiring new distributed platforms and public-private collaboration, it was emphasised. Joint operations are key but must be part of the new paradigm. Leaders must cultivate an open and creative approach and the development of new multi-modal operations. We need adaptable and forward thinking strategies, the panel concluded.

'New Threats and Opportunities in the Maritime Environment'[4] - 'Solutions, Capabilities, and Technology Innovation for the New Operational Landscape'[5]

The panels emphasised the 'expanding maritime environment offensive surface'. Maritime risks - including forced migration, environmental pollution, and threats to communication, terrorism, sabotage, smuggling, and unauthorised access to ships and ports with malevolent intent - are growing in number. A Rules Based International Order is crucial to minimise challenges, it was claimed. Today, maritime transport is not only by ship - it also includes cables and pipelines; new maritime domains include cyber and space. The 'offensive surface' has expanded, it

[4] New Threats and Opportunities in the Maritime Environment: Cdr Theodore Bazinis GRC (N), 'Threats and Challenges in a Rapidly Changing Maritime Environment'; Capt Petar Dimitrov BGR (N) Bulgarian Navy Command, 'Current Operational Picture - How this is Impacting the Future Bulgarian Fleet'; Dr Iosif Progoulakis, Dept of Shipping, Trade and Transport, University of the Aegean, Chios, Greece, and Prof Nikitas Nikitakos, Sharjah Maritime Academy, UAE, 'Drone Attacks Against Ships: Security Assessment and Mitigation'. Moderator: Cdre (ret'd) Ioannis Kakavas Msse GRC (N).

[5] Solutions, Capabilities, and Technology Innovation for the New Operational Landscape: Anastasios-Nikolaos Kanellopoulos, Athens University of Economics and Business, 'Enhancing Maritime Security Adopting an Integrated Intelligence Strategy'; Jurgen Scraback, European Defence Agency EU Maritime Domain Capability Dev, 'New EU Capability Development Priorities and the Implementation Roadmaps'; CAPT (Ret'd) Ioannis Androulakis GRC (N) MANiBUS, 'Underwater Security Horizon Europe'; Lt Col Petros Tsirigotis GRC (A); NATO Special Operation HQ, Maritime Development Division, 'Operational Experimentation in the Maritime SOF [Statement of Facts] Environment'. Moderator: Dinos Kerigan-Kyrou, NATO DEEP / PfPC.

was affirmed. For example, the Bulgarian new coastal defence missile system is based around UAVs aboard ships and enhancing subsea surveillance capabilities. Recent exercises mentioned include Operation BREEZE in Bulgaria with 12 countries including the U.S. 6th Fleet, and the EU's European Maritime Safety Agency [focusing on explosive ordnance disposal (EOD), and unmanned underwater vehicles], and the NATO TRITON 2024 diving exercise on the Black Sea.

The panels discussed drones increasingly operating in a pattern of: observe, damage, disable, and destroy. Our militaries (NATO, EU, and Partners), are starting to develop counter-drone technology based on suppression of threat (avoiding the situation where possible), detection, response and engagement. Underwater and Seabed Warfare, naval combat. Maritime interdiction procedures are continually innovating and are priorities for EUMSS. Combined NATO and the EDA (European Defence Agency) maritime domain awareness, underwater security operations, and other cooperation is crucial, the conference delegates were informed.

'Challenges in the Maritime Domain - Practitioners' Views'[6]

Experts from Stellenbosch University presented on the critical importance of the maritime security of Africa; the nexus between geopolitical instability, the lack of maritime policy framework and lagging development in fragile states' regional maritime security was discussed. Addressing these risks requires a multilayered approach and adherence to international legal frameworks with regional cooperation. For example, the Djibouti Code of Conduct to combat piracy off the east coast of Africa and the Red Sea, and the Yaoundé Code of Conduct for the west coast can help progress security. Ensuring maritime security requires a holistic understanding of the complex dynamics of African geopolitics and the interplay and dependency of landlocked and coastal states, it was explained.

The Conference heard that since 2016 NATO Operation Sea Guardian has operated in the Mediterranean, enabling maritime security capacity building and supporting maritime situational awareness and maritime counter-terrorism. Since 2023 the U.S. led Operation Prosperity Guardian in the Red Sea Bab el-Mandeb Strait has sought to address many of the threats we face to shipping and CMI. This is crucial, it was argued, because Iranian backed Yemen based Houthis are a constant threat to Red Sea maritime traffic. It was specified that diverting shipping around the Cape of Good Hope adds 10% to fuel and 12 extra days of travel; a significant amount of traffic is now doing this. Moreover, the Somali piracy threat is rising, and the security situation off the Arabian peninsula not improving. The result is higher prices for all and increasing maritime and global security threats, the delegates at the Conference were told.

The Houthi attacks increased significantly following the October 2023 Hamas atrocities. The Houthis operate drones and missiles combined with gunmen on speedboats. There are also direct Houthi threats to Egypt and the Mediterranean Sea. Because of this we must use intelligence to avoid attacks but we must also think about how we join-up the data as we move to digital security combined with physical security it was posited. Nonetheless, we should not only be aware of maritime physical and cyber threats; globally, air pollution is the leading cause of premature deaths, it was explained. At sea we now have the highest ever boat-whale collision rate for reasons that are not clear. We have to also be mindful of the direct effect on food security arising from threats to the maritime environment. The threat to our environment is one of the greatest threats to maritime security, the panel affirmed.

Conclusions

The 15th NMIOTC Annual Conference concluded that the new operational environment requires new approaches. Multi Domain Operations require a connectivity of domains, working with the vital civilian sector and with critical Partners and Allies across the world, including the EU. Indeed, NMIOTC has been the leader in bringing-in the civilian sector - together with NATO's many global Partners and Allies - into its world-class training and education at Souda Bay and with the Mobile Education Training Teams (NMIOTC METTs). The new environment requires us to think differently because over the last three decades it has been those that wish to cause us harm who have been the most adept at utilising new, lost cost technology and acting in flatter, less hierarchical organisational structures. As the panellists and speakers made clear, we need to adapt and accelerate a new approaches to the maritime environment. Indeed, as Gen. David Petraeus recently stated:"We need to transition a fair amount of our military forces from a small number of large platforms...in-

[6] Challenges in the Maritime Domain - Practitioners' Views: Prof Aspasia Pastra, World Maritime University (WMU), 'Unmanned and Unbound: Drones Redefining the Maritime Sector and Naval Operations'; Vice Admiral (ret'd) Ioannis Pavlopoulos GRC (N) Hon Commander in Chief of the Hellenic Fleet, 'Consequences of the Red Sea Crisis for Global Commerce'; Nikos Georgopoulos, Diapllous Group, 'Digital Risk Management'; Dr. Konstantinos Galanis, Whale Safe, 'Creating Sustainable Maritime Operations'; Prof Michelle Nel and Andries Fokkens, SIGLA, Stellenbosch University, 'Geopolitical Risk of Landlocked Fragile States to Maritime Security - West and East African Dilemmas'; CDR Rafal Mietkiewicz PhD POL (N) Polish Naval Academy, 'Challenges of CMI Protection - Baltic Context'; Frederik Rogiers Hendrik, Gent University, 'Freedom of Navigation and EEZs [Exclusive Economic Zones]'; Capt. Panagiotis Tripontikas GRC (N) MARCOM/ACOS/N2, 'The Implications of Climate Change for the Maritime Security'. Moderators: Prof Dimitrios Dalaklis, WMU, and CAPT Spyridon Alexiou GRC (N) Athens Multinational Sealift Coordination Centre.

cluding major surface combatants...which are, to be sure, incredibly capable, but also heavily manned, exorbitantly expensive, and increasingly vulnerable. Because you can see everything on the surface of the water and up nowadays. And if you can see it, you can hit it; if you can hit it, you can kill it (if the defenses can penetrated, to be sure). We need to transition to a vast number of unmanned systems which are much smaller, and increasingly will not be even remotely piloted - but algorithmically piloted. We are going to have these below the surface of the water, on the surface, on the ground, in the air, in outer space and cyberspace."

Gen. Petraeus indicates that Ukraine is likely to be the country which has adapted most successfully to the asymmetric security situation - indeed, the security environment described at the NMIOTC Annual Conference. Moreover, we may need to speed-up this process. As Gen. Petraeus adds: "Ukraine is showing that we are not doing this fast enough; how does a country that has no meaningful navy (surface combatants, that is) sink a third of the Russian Black Sea ships? With aerial drones that find the Russian ships and maritime drones that sink them - drones produced by Ukraine - forcing the Russians to completely withdraw from the western Black Sea, including the centuries-occupied port of Sevastopol."[7]

It could be argued that Ukraine is doing precisely what was recommended at the NMIOTC Annual Conference: creating firm partnerships between the military and civilian sectors, rapidly utilising developments in technology (thereby avoiding long military procurement timescales), working closely with key organisations (including NATO and the EU), flattening outdated hierarchical structures, eliminating siloed working, and creating dynamic innovation.

Over two decades ago the late U.S. Defense Secretary CAPT (U.S. Navy, Ret.) Donald Rumsfeld produced an incredibly forward-looking analysis and recommendations document that became known as the 'Rumsfeld Doctrine'.[8] The Doctrine opened with a quote from President George W Bush to the United States Naval Academy, envisioning "..a future force that is defined less by size and more by mobility and swiftness - one that is easier to deploy and sustain, one that relies more heavily on stealth, precision weaponry and information technologies." The Rumsfeld Doctrine focused on transformation, integrating joint operations "..enabling the near-simultaneous synergistic employment and deployment of air, land, sea, cyber and space warfighting capabilities." The 2003 Rumsfeld Doctrine accurately foresaw the issues that were superbly discussed at the 15th NMIOTC Annual Conference. It is now perhaps time to take such measures forward. This may well be the way for NATO, the EU, and Partners and Allies across the world to adapt strategy and innovative technology to address the risks and challenges of the future operational landscape in a dynamic maritime environment.

Dinos Anthony Kerigan-Kyrou PhD CMILT AmRINA is a Cybersecurity and Hybrid Threats instructor on NATO DEEP (Defence Education Enhancement Programme), coordinated by NATO and the Partnership for Peace Consortium of Defence Academies (PfPC). Dinos assists at the DEEP eAcademy developing Advanced Distributed Learning (ADL) platforms for NATO and Partner nations. He is an editor of the PfPC journal Connections, and a visiting instructor at the EU European Security and Defence College. Dinos is a co-author of the NATO / PfPC Cybersecurity, and Hybrid Warfare and Hybrid Threats Curriculums. From 2017-2024 he led the Cybersecurity and Hybrid Threats education on the Irish Defence Forces Joint Command & Staff Course. He is a founding member of the cybersecurity committee of Royal Institution of Naval Architects, and a board member of Digital Business Ireland.

Dinos Kerigan-Kyrou PhD CMILT Dinos Anthony Kerigan-Kyrou PhD CMILT AmRINA is a Cybersecurity and Hybrid Threats instructor on NATO DEEP (Defence Education Enhancement Programme), coordinated by NATO and the Partnership for Peace Consortium of Defence Academies (PfPC). Dinos assists at the DEEP eAcademy developing Advanced Distributed Learning (ADL) platforms for NATO and Partner nations. He is an editor of the PfPC journal Connections, and a visiting instructor at the EU European Security and Defence College. Dinos is a co-author of the NATO / PfPC Cybersecurity, and Hybrid Warfare and Hybrid Threats Curriculums. From 2017-2024 he led the Cybersecurity and Hybrid Threats education on the Irish Defence Forces Joint Command & Staff Course. He is a founding member of the cybersecurity committee of Royal Institution of Naval Architects, and a board member of Digital Business Ireland.

[7] General David H. Petraeus: Comments from the Walker Webcast (September 2024), and expanded upon with further detail via correspondence with the author (October 2024).
[8] U.S. Dept of Defense, 'Transformation Planning Guidance', April 2003.

Contemporary Maritime Interdiction and the role of NMIOTC

by Commodore Efstathios Kyriakidis GRC - N

Maritime Interdiction refers to the efforts both by states and international organizations, to prevent illegal activities at sea. That includes measures to protect critical infrastructure (both at sea bed and on the surface), to counter terrorism, smuggling, piracy, trafficking, and illegal/unauthorized fishing. The concept encompasses a wide range of strategies, actions and operations, often involving cooperation and collaboration among multiple stakeholders, be it civilian or military.

Maritime Interdiction and the corresponding operations, are the main tool to ensure Maritime Security. The concept of Interdiction evolved in parallel with the context, the period and the threats and challenges at sea. By definition, Maritime Interdiction Operations (MIOs) during the war, are naval operations that aim to delay, disrupt, or destroy enemy forces or supplies enroute to the battle area, before they do any harm against friendly forces.

Maritime Interdiction through History

The practice of stopping, boarding, and inspecting ships to enforce laws or sanctions, has evolved significantly over time, shaped by changes in technology, international law, and geopolitical challenges. The first MIO that has been recorded, was the blockade of Aegina by the Athenian fleet during the first Peloponnesian Wars between the Ancient Greek city states, in 458 BCE.

In ancient and medieval times, maritime interdiction large-

ly took the form of combatting piracy or enforcing naval dominance. Strong maritime powers like Rome, Carthage, and later the British Empire, used their naval fleets to secure sea routes and protect their trade. Naval blockades and “letters of marque”, a government license that authorized a private person, to attack and capture vessels of a

nation at war, were common forms of authorized piracy to weaken adversaries or stop illegal trade. For example, in the Napoleonic Wars, Britain used blockades to prevent French ships from accessing their colonies.

The 19th century saw the formalization of international laws regarding maritime interdiction, particularly the rights to search and seize ships involved in slave trading, piracy, or unauthorized privateering. One of the key legal instruments that came out of this period was the Declaration of Paris in 1856, which sought to limit the practice of privateering and regulate the treatment of neutral ships during war.

Both World War I and II saw extensive use of maritime interdiction in the form of naval blockades. During these wars, belligerent nations sought to restrict the flow of materials and goods to their enemies. The British blockade of Germany in World War I and the German U-boat campaigns targeting Allied shipping in both wars were major examples. During these conflicts, advances in submarine technology and aircraft significantly altered the dynamics of maritime interdiction, making sea blockades more complex and dangerous.

The Cold War era saw the use of maritime interdiction to enforce embargoes, with a focus on non-military objectives like preventing arms smuggling and enforcing trade

sanctions. The U.S. and its allies frequently interdicted Warsaw Pact ships, suspected of carrying military supplies to nations like Cuba or Vietnam. One famous example is the Cuban Missile Crisis in 1962, when the U.S. Navy established a "quarantine" of Cuba to prevent Soviet ships from delivering nuclear missile components. This naval blockade, while termed a "quarantine" to avoid the legal implications of a blockade, became one of the most well-known instances of maritime interdiction.

In the '90s, Maritime Interdiction was used to impose the UN Security Council resolutions. As an example a multinational task force conducted MIO both at the Straits of Hormuz and at the Gulf of Aqaba before and after the Desert Storm Operation in 1991. Similarly, NATO and Western European Union (WEU) vessels conducted MIO in the Adriatic Sea (1993-1996) during the war in former Yugoslavia. Those operations involved the stopping and boarding of any ship transiting the aforementioned areas, to search for oil and weapons.

In the 21st Century, maritime interdiction has become a critical tool in combating piracy, particularly off the coast of Somalia in the 2000s. International naval coalitions, such as the EU's Operation ATALANTA and NATO's Operation Ocean Shield, have worked to secure one of the world's busiest shipping lanes, the Gulf of Aden.

Nowadays Maritime Interdiction, has become a comprehensive, complex and cross domain concept that refers to a broad spectrum of actions, to preserve maritime security. It addresses both traditional and emerging threats and leverages technological advancements to enhance global maritime security. These operations involve the proactive measures taken by naval forces and other maritime security agencies to gather and analyze

intelligence, intercept, board, inspect, divert or even seize vessels suspected of engaging in illegal activities. The objectives of MIO also include preventing the trafficking of weapons, drugs, and people, enforcing sanctions, combating piracy, and protecting marine resources.

In addition, maritime interdiction has been transformed by technology. The use of satellite surveillance, advanced radar, unmanned aerial vehicles (UAVs), and modern communication systems has enhanced the ability of navies and coast guards to track and intercept suspect vessels over vast areas. Warships and patrol vessels today are equipped with boarding teams trained for specialized missions, including counterterrorism and anti-piracy operations.

Therefore, the key difference between historical and current Maritime interdiction could be summarized as

follows:

a. Scope: Historically, maritime interdiction focused on naval dominance, piracy suppression, and wartime blockades. Modern interdiction is broader, addressing everything from anti-piracy, counterterrorism, and sanctions enforcement to humanitarian efforts and environmental protection.

b. Technology: In the past, maritime interdiction was limited by the range of ships and basic communication tools. Today, advanced sensors, satellite systems, and drones enable interdictions over vast ocean areas with greater precision.

c. International Cooperation: While earlier maritime interdiction was often unilateral or confined to individual empires or nations, today's operations are largely multilateral, involving coalitions of nations and governed by international law.

Contemporary Maritime Interdiction

MIO are conducted by both Naval Forces and Coast Guards. Their roles depend on the various national legislations; however the main tasks remain the same: They conduct patrols, board and inspect vessels, and apprehend those involved in illegal activities. Moreover, training programs and capacity-building initiatives help strengthen the capabilities of navies and coast guards, particularly in developing countries. These programs often involve exercises, simulations, and knowledge sharing.

Those kind of operations require a robust legal framework, to legitimize actions at sea and ashore. Today, the United Nations Convention on the Law of the Sea (UNCLOS), provides the legal basis for maritime interdiction, despite

the fact that it has not been ratified by all countries. However, even those countries evoke its provisions on the basis of customary law. The legal framework also includes agreements and protocols, like the Proliferation Security Initiative (PSI), which also facilitates cooperative efforts. In addition, successful interdiction includes not only the apprehension of suspects, but also their prosecution. This requires, apart from the strong legal framework, judicial cooperation to ensure that those involved in illegal activities are held accountable.

Moreover, effective interdiction relies on robust intelligence and surveillance systems. Technologies like satellite imagery, drones, and automatic identification systems (AIS) help monitor maritime traffic and detect suspicious activities. In the same vein, advances in technology, including artificial intelligence, machine learning, and unmanned systems, enhance the capabilities of maritime interdiction operations. These technologies improve detection, tracking, and response times.

Given the global and transnational nature of maritime threats, maritime interdiction relies on international cooperation. Organizations such as NATO, the European Union, and regional coalitions like the Combined Maritime Forces (CMF), coordinate efforts to enhance maritime security.

The main elements of MIO include, but are not limited to, the following:

a. Detection and Monitoring: Utilizing a range of surveillance tools, including radar, satellite imagery, and maritime patrol aircraft, to monitor vessel movements and identify suspicious activities.

b. Interception: Deploying naval or coast guard vessels to intercept suspicious ships. This requires fast, agile naval/ coast guard units, that can approach and immobilize the target vessel.

c. Visit, Board, Search and (if necessary) seizure: Boarding teams, often composed of special operation forces (SOF), conduct inspections to verify the ship's documentation, cargo, and crew. These teams are prepared to handle potentially hostile situations.

d. Intelligence gathering and analysis: Collecting and analyzing information from various sources to support interdiction efforts. This includes signals intelligence (SIGINT), human intelligence (HUMINT), biometric data collection and open-source intelligence (OSINT).

Some examples of current operations related to Maritime Interdiction are:

a. Operation ATALANTA: Launched by the European Union Naval Force (EU NAVFOR SOMALIA), this operation focuses on combating piracy off the coast of Somalia. It involves patrolling the region, protecting vulnerable ships, and conducting interdiction operations against pirate vessels.

b. Operation IRINI: Launched by the European Union Naval Force (EU NAVFOR MED), the maritime interdiction operations are primarily focused on enforcing arms embargoes. The United Nations Security Council has authorized these operations to implement the arms embargo on Libya. Additionally, there are significant efforts to intercept and return migrant and refugee boats attempting to cross the Mediterranean Sea.

c. Combined Maritime Forces (CMF): A multinational coalition operating in the Middle East and surrounding waters. CMF conducts a variety of MIO,

including counter-piracy, counter-terrorism, and counter-narcotics operations. Task Force 150, for example, focuses on maritime security and interdiction in the Gulf of Aden and the Indian Ocean.

d. Operation Sovereign Borders: An Australian government operation aimed at preventing illegal maritime arrivals and combating human smuggling. The operation includes patrols, interdictions, and the return of intercepted vessels to their points of origin.

e. US Coast Guard Operations: The US Coast Guard regularly conducts interdiction operations to combat drug trafficking in the Caribbean and Eastern Pacific. Operation MARTILLO involves the U.S. Coast Guard and partner nations drug law enforcement agencies conducting boardings, searches, seizures, and arrests. Another significant effort is the SOUTHCOM Enhanced Counter Narcotics Operations, which deploys additional naval and air assets to the Caribbean Sea and Eastern Pacific Ocean to disrupt the flow of drugs.

f. Aegean Activity: The Standing NATO Maritime Group 2 (SNMG2) contributes to the international efforts to stem illegal trafficking and illegal migration in the Aegean Sea through intelligence, surveillance and reconnaissance. The maritime force is cooperating with the European Union's border management agency Frontex, in full compliance with international law and the law of the sea.

NATO's approach to Maritime Interdiction

Maritime security is one of the most popular topics in international relations. There are various interrelated domains that constitute the broad spectrum of the Challenges in the maritime domain: There are political ones, such as Delineation of Borders, the Exploitation of Resources and the Resource management. The military ones, like the conventional Asymmetric terrorism that incorporates all the non-nuclear threats. The economic challenges, such as the smuggling and trafficking of goods and humans and last but not the least the environmental ones, mainly related to the climate crisis and the oil and chemical spillovers.

Major actors in maritime policy, ocean governance and international security – including first and foremost NATO, have in the past decade started to include maritime security in their mandate or reframed their work in such terms. Core dimensions of maritime security involves the concept of blue economy, food security and the resilience of coastal populations.

The Allied Maritime Strategy sets out, the ways that maritime power could help resolve critical challenges facing the Alliance now and in the future, and the roles - enduring and new - that NATO forces may have to carry out in the maritime environment. It aims to maintain stability in the global maritime environment by ensuring freedom of navigation, protecting critical infrastructure, and preventing disruptions to international trade, in order to contribute to Deterrence and collective defence, Crisis management and Cooperative security through partnerships, dialogue and cooperation, the core tasks of the Alliance as described in NATO's Strategic Concept (2022).

Similarly, NATO's Maritime Security Policy is an integral part of its broader security strategy, reflecting the alliance's commitment to ensuring stability, safety, and the protection of vital sea lanes. Given the importance of maritime routes for trade, energy supplies, and military mobility, NATO prioritizes the safeguarding of international waters against various threats.

Some of the tasks of the naval forces in the context of the Allied Maritime Strategy could be summarized as follows:

a. Maritime Situational Awareness (MSA): The Alliance has to ensure continuous monitoring of maritime activities through intelligence sharing, surveillance, and reconnaissance to identify potential threats.

b. Counter-Piracy and Counter-Terrorism: It is of utmost importance to defend international shipping routes against piracy and potential terrorist acts. NATO has led missions to counter piracy off the coast of Somalia (e.g., Operation Ocean Shield) and monitors for terrorist activities in the Mediterranean.

c. Protection of Sea Lines of Communication (SLOCs): SLOCs are critical for NATO's own supply chains, as well as for global economic stability; therefore securing key maritime trade routes and ensuring the free

flow of goods and energy resources is in the epicenter of the Maritime Strategy.

d. Energy Security: It is essential for NATO to protect the critical energy infrastructure at sea, such as undersea cables, pipelines, and offshore installations, which are increasingly vulnerable to sabotage or cyber-attacks.

e. Cybersecurity in the Maritime domain: Recognizing the increasing digitization of maritime operations, there is a need to defend against cyber threats targeting naval assets, maritime infrastructure, and communication networks.

For the implementation of the Allied Maritime Strategy, NATO conducts the Operation Sea Guardian. It is a flexible, enduring maritime security operation in the Mediterranean Sea. It focuses on three core areas: maritime situational awareness, counter-terrorism at sea, and capacity building with partner nations. Sea Guardian enables NATO to detect and deter illegal activity while protecting vital shipping lanes. Therefore, the second Standing NATO Maritime Group (SNMG 2) is permanently deployed and ready for rapid response. Along with SNMG 1, they patrol and conduct various operations to ensure maritime security across NATO waters.

In addition, NATO has previously engaged in anti-piracy missions (e.g., off the Horn of Africa) to protect vessels from pirate attacks and improve the capacity of local navies. The relevant Operation Ocean Shield, was terminated in 2016.

Finally, NATO's maritime security efforts are bolstered by partnerships with other international organizations and non-NATO nations, such as the UN and EU. As global maritime threats evolve, NATO continually adapts its policies to meet new challenges. This includes addressing hybrid threats, such as a mix of cyber-attacks, disinformation, and conventional military actions that could target maritime interests.

Maritime Interdiction and the Multi Domain Operations

NATO has adopted the concept of Multi-Domain Operations (MDO), a military strategy that seeks to integrate and synchronize operations across multiple domains, namely land, sea, air, space, and cyberspace, to achieve military objectives from the strategic to the tactical level. The concept reflects the evolving complexity of warfare, where the traditional boundaries between domains are increasingly blurred due to advancements in technology, communications, and the capabilities of both state and non-state actors.

MDO emphasizes the integration of military actions across all five domains and involves joint operations and combined operations (among allied nations) to create a cohesive and mutually supportive operational plan. The goal is to leverage the unique advantages of each domain to maximize overall effectiveness and to complicate the adversary's ability to defend.

The main characteristic of MDO is the ability to act simultaneously across all domains, creating multiple dilemmas for the adversary. This involves rapid decision cycles, where forces across domains communicate and adapt in real-time, creating a dynamic and unpredictable operating environment for the enemy. The use of disruptive technologies such as artificial intelligence (AI), advanced data analytics, robotics, autonomous systems, data analytics, machine learning and space-based surveillance systems to enhance situational awareness, is critical in MDO, as these technologies enable faster processing of vast amounts of data, improving situational awareness and accelerating decision-making. As an example, disrupting enemy networks and communication systems, while protecting one's own assets from cyberattacks and electronic interference plays a crucial role in the theater of operations.

Beyond the five domains, NATO also recognizes the importance of the information and cognitive domains, where the goal is to shape public perception, influence decision-makers, and counter adversary narratives. Information warfare, including disinformation campaigns and psychological operations, plays a significant role in MDO. However these domains do not constitute another MDO dimension.

On the other hand, there are significant challenges and considerations related to MDO. One of the greatest challenges is to ensure that systems and forces across all five domains are interoperable and can effectively communicate. This requires a high degree of coordination among different services, nations, and systems. In addition, MDO is heavily reliant on advanced technology. This also makes it vulnerable to cyberattacks and electronic warfare. Moreover, MDO seeks to create dilemmas for adversaries, but those adversaries are also evolving and developing countermeasures. Peer competitors are also investing in A2/AD capabilities, hypersonic weapons, and cyber technologies that can challenge MDO approaches. Another challenge is the complexity of logistical challenges, especially in terms of maintaining supply chains, repair capabilities, and the movement of forces in contested environments. Finally, operations in domains such as space and cyber, raise legal and ethical questions regarding sovereignty, rules of engagement, and collateral damage, particularly when actions could have far-reaching consequences for civilian infrastructure.

The future of Maritime Interdiction is closely related to MDO. That relation is rooted in the growing complexity of modern warfare, where success often depends on the integration of capabilities across various domains. Both maritime interdiction and MDO reflect strategies aimed at achieving dominance or control in contested environments.

Maritime interdiction operations require multi-domain coordination. For instance, naval forces conducting interdiction missions may rely on cyber operations to disable enemy communications, space-based intelligence for real-time situational awareness, and air power for reconnaissance and protection from aerial threats. In an MDO framework, maritime interdiction is an integral part of a broader campaign. For example, to enforce a blockade effectively, joint forces might need to operate across domains—cyber assets to disrupt logistics, air forces to provide surveillance and cover, and land-based missile systems to deter reinforcements.

As maritime interdiction forces may have to operate in contested waters, MDO helps navigate and counter enemy efforts to deny access. This could involve cyber operations to disable enemy defenses or air power to neutralize anti-ship missile batteries. Moreover, the speed of operations in MDO is essential, and interdiction at sea requires real-time decision-making, often informed by intelligence from multiple domains. The integration of cyber, space and air assets helps commanders make faster, more informed decisions during maritime interdiction missions.

A characteristic example is the anti-piracy operations or counterterrorism: Maritime interdiction relies on real-time data from drones (air domain), satellite imagery (space domain), and cybersecurity to track and block financial flows (cyber domain). These interdiction missions benefit from MDO to act swiftly against agile and adaptive threats. Similarly, during blockade Enforcement in crisis, air power may be needed to establish aerial dominance, space assets for constant surveillance, and cyber capabilities to undermine the enemy's ability to communicate or coordinate relief efforts.

In that vein, Maritime Interdiction can be seen as one of the tactical actions within the broader strategic framework of multi-domain operations, leveraging capabilities across various domains to achieve specific objectives. This integrated approach is key to modern military effectiveness and adaptability.

References

1. 'Understanding Maritime Interdiction Operations: A Comprehensive Guide', July 6, 2024, https://militarysphere.com/maritime-interdiction-operations/
2. Stephanie Smart, 'Maritime Interdiction Operations'. U.S. Military Operations: Law, Policy, and Practice. Oxford University Press, December 3, 2015.
3. Martin Fink, 'Maritime Interception and the Law of Naval Operations', Springer, Asser Press, 2018.
4. NATO HQ, 'Alliance Maritime Strategy', March 18, 2011 https://www.nato.int/cps/en/natohq/official_texts_75615.htm
5. NATO SACT, 'Multi-Domain Operations in NATO – Explained' October 5, 2023. https://www.act.nato.int/article/mdo-in-nato-explained/

"Enhancing Maritime Security: Adopting an Integrated Intelligence Strategy in the Shipping Sector"

Anastasios-Nikolaos Kanellopoulos, PhD candidate, Athens University of Economics and Business
Anthony Ioannidis, Assistant Professor of Management, Athens University of Economics and Business

Introduction

In the dynamic and intricate global business landscape, industries, particularly those with significant revenue and geopolitical implications, such as the Shipping industry, encounter diverse challenges that necessitate strategic approaches. This paper presents a unified Intelligence C2I Model designed specifically for the Shipping Industry, amalgamating Competitive Intelligence (CI) and Counterintelligence (CI) to address offensive and defensive capabilities crucial for sustained competitiveness. Acknowledging the inherently international and information-rich nature of the Shipping industry, the proposed framework integrates these intelligence processes to enable informed decision-making while bolstering internal defenses against adversarial actions.

Concurrently, maritime sectors worldwide face security challenges that threaten Shipping operations. This article examines the complexities of ensuring Shipping security, delving into issues like conflict, maritime terrorism, and cyber threats to critical infrastructure. It underscores the importance of regional collaboration and technological advancements in countering piracy and enhancing maritime security through initiatives like joint patrols, intelligence sharing, and advanced surveillance technologies.

By synthesizing insights from the proposed C2I Model and global Shipping security challenges, this paper offers a comprehensive view of the risks and hurdles encountered by the Shipping industry. It underscores the pivotal role of Competitive Intelligence, Counterintelligence, collaborative endeavors, and technological innovation in safeguarding maritime trade routes. Ultimately, this framework contributes to a deeper comprehension of the strategic imperatives necessary for addressing regional risks and challenges within the Shipping industry in the broader context of global trade.

Security Challenges in the Shipping Industry

Regional Conflicts

Geopolitical tensions and regional conflicts cast a long shadow over the global Shipping industry, creating tangible challenges in key maritime zones. The South China Sea, for example, grapples with competing territorial claims that generate legal ambiguities and navigational hazards for Shipping companies. The presence of military forces and heightened regional tensions necessitate stringent security protocols to protect Shipping operations (Jenner and Tran, 2016).

Similarly, conflicts and geopolitical friction in the Persian Gulf, particularly involving Iran and its neighbors, have serious consequences for trade routes and maritime security (Insights to the Global Shipping, trade, and global ports, 2018). The Strait of Hormuz, a vital passageway for global oil transport, becomes a focal point of concern during periods of escalated tensions, forcing Shipping companies to proceed with caution and potentially absorb higher insurance premiums to offset the risk of disruption (Maaike Warnaar and Aarts, 2016).

Beyond these specific regions, the conflict in Ukraine and its ripple effects on the Black Sea exemplify how broader trade disruptions can reverberate across global markets (Weaver, 2016). The uncertainties engendered by such conflicts and political instability can discourage investment in Shipping infrastructure and restrict access to critical ports, ultimately hindering the smooth flow of goods and commodities within the global marketplace.

Piracy, Armed Robbery and Terrorism

The resurgence of maritime security threats, including piracy, armed robbery, and terrorism, presents a significant challenge to the global Shipping industry, impacting operations far beyond any single region. While traditionally associated with the open ocean, piracy has expanded its reach from known hotspots like the Gulf of Aden to encompass areas such as the South China Sea, the Indian Ocean, and the Gulf of Guinea (Geiss and Petrig, 2011; Haywood, 2013). In these regions, heavily armed pirate groups target vessels, disrupting vital trade routes and forcing Shipping companies to divert ships around high-risk zones, leading to increased operational expenses and delays.

Armed robbery poses a persistent threat as well, particularly in congested port areas across the globe. These incidents, often occurring during loading and unloading operations, involve armed groups seizing cargo and jeopardizing the safety of crews and the integrity of vessels. Reports of armed robbery have surfaced in ports throughout Southeast Asia and South America, underscoring the need for robust security protocols and comprehensive crew training to mitigate risks and ensure safe operations (Geiss and Petrig, 2011). Furthermore, terrorism remains a global menace to maritime security, with incidents reported in regions like the Gulf of Aden, the Indian Ocean, the Arabian Sea, and Southeast Asia. Terrorist organizations, aiming to disrupt trade and inflict economic harm, often target vessels and critical infrastructure (Murphy, 2013).

The consequences of these security threats extend far beyond financial implications, profoundly impacting the safety and well-being of maritime personnel worldwide. Incidents of piracy, armed robbery, and terrorism can lead to physical harm, emotional trauma, and even loss of life. This grim reality underscores the critical need for ongoing investment in crew training and security measures to protect the industry's most valuable asset: its people.

Human, Drugs Trafficking, and Arms Smuggling

The global Shipping industry faces a multifaceted challenge from human trafficking, drug trafficking, and arms smuggling, all of which exert a significant influence on maritime operations worldwide. These illicit activities, often intertwined and facilitated by criminal networks, exploit the vast and complex web of sea routes that crisscross the globe (Otto, 2020).

Drug trafficking, particularly originating from South American countries like Colombia, Peru, and Venezuela, is closely linked to maritime trade routes leading to Europe through the Mediterranean. Criminal organizations utilize a variety of vessels, including cargo ships and fishing boats, to transport narcotics such as cocaine, marijuana, and synthetic drugs across the Atlantic Ocean. The Shipping industry faces direct consequences as a result, including vessel seizures and reputational damage, leading to financial losses for Shipping companies (International Chamber of Shipping, 2017).

Adding to the complexity is the informal money transfer system known as Hawala, which poses a distinct challenge for the Shipping sector. Hawala facilitates the covert movement of funds through maritime channels, enabling criminal organizations to launder money and finance illicit activities, including drug and arms smuggling. Human smuggling has also emerged as a major concern within global maritime operations, as refugees and migrants seek passage from conflict-ridden nations to Europe and North America. While not directly involved in smuggling operations, the Shipping industry faces indirect challenges related to search and rescue efforts, compliance with international maritime safety regulations, and potential operational delays stemming from humanitarian crises.

Furthermore, the Shipping industry has become a focal point for arms smuggling, with weapons originating from South America and African countries finding their way into illicit maritime routes (Cragin and Hoffman, 2003). Arms are often concealed within legitimate cargo or transferred clandestinely, fueling conflicts, insurgencies, and terrorism.

Cybersecurity Threats

In an era of increasing digitalization, the global Shipping industry faces a growing array of cybersecurity threats that extend beyond geographical borders and impact maritime sectors worldwide. These threats, encompassing a range of malicious activities, pose significant risks to operations, sensitive data, and vessel safety.

Malware and ransomware attacks are persistent and widespread concerns for Shipping companies operating globally Cybercriminals and state-sponsored actors employ tactics such as phishing emails and malicious software downloads to infiltrate corporate networks and onboard ship systems The consequences of such attacks can be severe. For instance, in 2017, the Maersk Group was targeted by the NotPetya ransomware attack, resulting in widespread disruptions to its global operations and substantial financial losses (Gruner, 2021).

Cyberattacks on the maritime Shipping business are becoming more common, and organized criminal networks and hostile nations are now targeting all actors in the digital value chain, including Shipping companies, vessels, and their shore-side facilities (Giannakopoulou et al., 2016; Akpan, 2022). This example highlights the growing threat of cyberattacks in the maritime industry and their potential to cause significant disruption and financial damage. To mitigate these risks, Shipping companies must prioritize cybersecurity measures, including robust network security, employee training on cyber threats, and incident response planning.

Intelligence Operations Threats

Intelligence operations within the maritime industry have undergone significant transformations, reflecting advancements in technology and the increasing digitalization of global Shipping infrastructure (Alcaide & Llave, 2020). Today, information warfare poses a substantial threat to maritime operations, manifested through state-sponsored and corporate espionage aimed at acquiring sensitive Shipping data (Barnea, 2019). These operations are carried out by foreign governments and rival firms to obtain crucial information about cargo, routes, and operational strategies, which can confer strategic advantages or economic benefits (Emmanuelides & Tsavliris, 2019).

A primary motivation behind such espionage is economic gain. Given the vast quantities of goods handled by Shipping companies and the complexities of the global supply chain, access to detailed cargo information, shipment schedules, and route plans can provide significant advantages (Sodhi & Tang, 2014). Malicious actors can exploit this data to predict market trends, target valuable cargo, or exploit pricing disparities, potentially destabilizing market conditions and causing financial harm to legitimate industry players (Grammenos, 2010).

Geopolitical interests also drive intelligence operations in the maritime sector. The crucial role of the maritime industry in global trade underscores its strategic importance, as control over Shipping routes and cargo can influence international trade dynamics (The Hague Centre for Strategic Studies, 2019). State actors, particularly those with vested geopolitical interests, may engage in intelligence activities to monitor foreign vessels and leverage gathered information to advance their national security objectives (Van Cleave, 2007). For example, China's substantial investment in global port infrastructure under the Belt and Road Initiative illustrates how such investments can serve both commercial and intelligence-gathering purposes (Russel & Berger, 2020; European Parliament, 2023). Control over port facilities provides China with valuable insights into global trade and logistical operations (Calatayud, 2023; Van der Putten, 2019).

Competitive Intelligence in the Shipping Industry

Competitive Intelligence is a fundamental driver of success in the Shipping industry, operating within a complex and dynamic global environment. Across diverse maritime regions, Shipping companies are continuously exploring strategies to gain competitive advantages, mitigate risks, and optimize profitability through Competitive Intelligence practices (Cloutier, 2013). Competitive Intelligence activities encompass a broad spectrum of efforts focused on gathering, analyzing, and leveraging information to inform strategic decisions and maintain competitiveness in the market (Bose, 2008).

In any operational setting, Competitive Intelligence is essential for monitoring market trends, geopolitical shifts, regulatory developments, and security challenges (Cavallo et al., 2020). For instance, in maritime regions with strategic significance, vigilance over energy dynamics influences Shipping routes and commercial opportunities. Similarly, tracking evolving state relationships and territorial disputes aids in anticipating potential disruptions and security risks, essential for informed decision-making.

Moreover, route optimization and logistics management are critical aspects of Competitive Intelligence in dynamic maritime environments. Factors like port congestion, weather variations, and non-state actor activities necessitate real-time data analysis to facilitate efficient decision-making. Competitive Intelligence tools enable companies to adjust routes, schedules, and cargo handling procedures promptly, ensuring timely deliveries while minimizing operational costs and fuel consumption, ultimately enhancing competitiveness and environmental sustainability. In addition, effective cargo operations management relies heavily on Competitive Intelligence to navigate the diverse cargo types transported through maritime regions, including legal and illegal shipments. Gathering and analyzing data on cargo movements, regulations, and compliance with international laws are essential for mitigating risks associated with cargo security, customs procedures,

and adherence to legal frameworks.

Intelligence for Counterintelligence and Counterterrorism in the Shipping Industry

The contemporary security landscape of the global Shipping industry demands a strategic deployment of intelligence to counter intelligence operations and terrorism threats (Thai, 2014). Leveraging intelligence is pivotal to mitigating risks, enhancing security measures, and safeguarding the flow of maritime trade worldwide. The interplay between Counterintelligence and Counterterrorism activities is critical, given the multifaceted challenges faced by Shipping companies across different operational environments.

Counterintelligence involves the systematic acquisition and analysis of information to detect and neutralize intelligence and espionage activities that may pose internal and external threats (Prunckun, 2019). In regions with geopolitical complexities and economic interests, such as the maritime sector globally, state-sponsored espionage remains a significant concern. Shipping companies must vigilantly monitor for signs of espionage, assess vulnerabilities, and implement countermeasures to protect sensitive information, trade routes, and technological assets. Counterintelligence efforts may include Open-Source Intelligence (OSINT) monitoring, tracking of suspicious entities or vessels, and stringent background checks on personnel to mitigate insider threats. Additionally, robust cybersecurity measures are essential to safeguard digital assets from state-sponsored cyberattacks aimed at breaching Shipping company networks and accessing critical information.

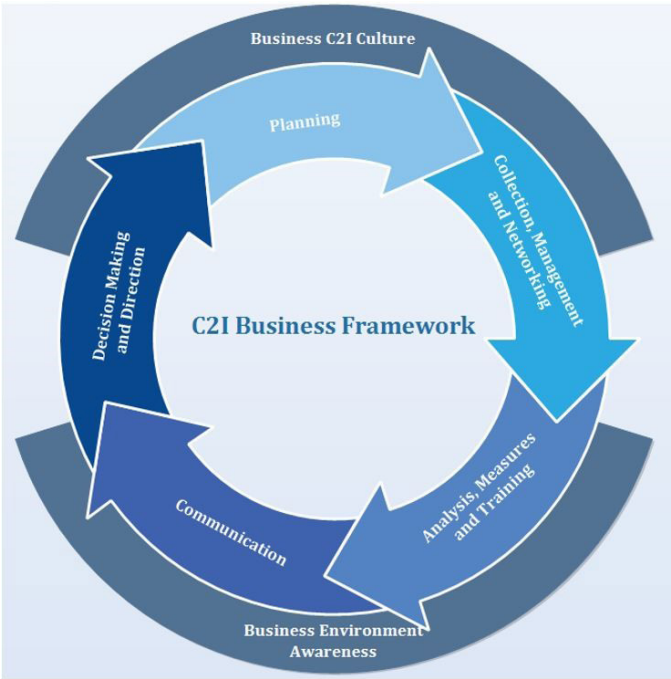
Moreover, counterterrorism plays a crucial role in addressing non-state threats posed by terrorist organizations and criminal networks operating within the global Shipping industry. Intelligence is indispensable in preempting and countering such threats. Counterterrorism intelligence involves continuous monitoring and analysis of known terrorist organizations and emerging threats, along with understanding operational tactics employed by these groups (Cilluffo et al., 2012). Effective counterterrorism may necessitate intelligence-sharing with national and international security agencies, fostering collaboration to compile comprehensive threat assessments and preemptive measures.

Discussion over a recommendation on Enhancing Maritime Security through Intelligence

The imperative need for an innovative business intelligence management system, "C2I: Competitive Intelligence and Counterintelligence," is unmistakable in light of the evolving landscape of Shipping Security, Counterintelligence, and Counterterrorism on a global scale. The maritime industry faces an array of increasingly complex challenges, from cyber threats to piracy and terrorism, necessitating a departure from traditional approaches. C2I represents a groundbreaking solution that will serve as a cornerstone in enhancing the safety and security of international waters and maritime trade routes worldwide.

The C2I Business Framework

The C2I model is structured around a comprehensive business framework designed to ensure systematic planning, collection, analysis, communication, and decision-



(C2I Business Framework)

making.

Planning: The initial step focuses on transforming strategic directions into operational actions. Maritime security managers play a crucial role in interpreting strategic goals and implementing them as actionable plans.

Collection, Management, and Networking: This phase emphasizes the gathering of information through OSINT and internal sources. The data is managed using robust databases, while networking activities incorporate both internal and external human intelligence (HUMINT).

Analysis, Measures, and Training: Collected data undergoes rigorous scrutiny, including market analysis, profiling, and social network analysis. Following this, measures are implemented to protect internal intelligence, and ongoing training programs are conducted to enhance internal protection protocols.

Communication: Effective communication is vital. The C2I manager is responsible for conveying intelligence insights to the CEO or the Shipping company owner, ensuring clarity and understanding.

Decision Making and Direction: The final step involves the CEO making informed decisions based on the provided intelligence and directing strategic initiatives accordingly.

Conclusions

The evolving global business landscape, especially in the Shipping industry, demands innovative solutions to complex challenges. The C2I Model presented in this paper offers a comprehensive approach tailored to the maritime sector's unique needs. By integrating Competitive Intelligence and Counterintelligence, the C2I Model enables maritime businesses to address both offensive and defensive challenges, ensuring competitiveness and security. Eventually, the C2I Model enhances decision-making and internal defenses, emphasizing proactive intelligence gathering and strategic responses.

References

Akpan, F., G., Bendiab, S., Shiaeles, S., Karamperidis, & M., Michaloliakos (2022). 'Cybersecurity challenges in the Maritime Sector'. Network, 2(1), 123–138. https://doi.org/10.3390/network2010009

Alcaide, J., & R. G., Llave (2020). 'Critical infrastructures cybersecurity and the Maritime Sector'. Transportation Research Procedia, 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.

Barnea, A. (2019) 'Big Data and counterintelligence in Western countries', International Journal of Intelligence and Counterintelligence, 32(3), 433–447. doi:10.1080/08850607.2019.1605804.

Bose, R. (2008). Competitive intelligence process and tools for intelligence analysis. Industrial Management & Data Systems, 108(4), 510–528. https://doi.org/10.1108/02635570810868362.

Calatayud, L. (2023). The complex relationship between Europe and Chinese investment: The case of Piraeus. Lau China Institute. King's College London, Available at: https://www.kcl.ac.uk/lci/assets/china-in-focus-piraeus-paper-final.pdf. (Accessed 22/07/2024).

Cavallo, A., Sanasi, S., Ghezzi, A., & Rangone, A. (2020). Competitive intelligence and strategy formulation: Connecting the dots. Competitiveness Review: An International Business Journal, 31(2), 250–275. https://doi.org/10.1108/cr-01-2020-0009.

Cilluffo, F. J., Clark, J. R., Downing, M. P., & Squires, K. D. (2012). Counterterrorism Intelligence.

Cloutier, A. (2013). Competitive Intelligence Process Integrative Model based on a scoping review of the literature. International Journal of Strategic Management, 13(1), 57–72. https://doi.org/10.18374/ijsm-13-1.7.

Cragin, K., & Hoffman, B. (2003). Arms Trafficking and Colombia. Rand Corporation.

Emmanuelides, G., & P., Tsavliris (2019). Winning shipping strategies. theory and evidence from leading shipowners. Economia Publishing

European Parliament (2023). In-Depth Analysis, Security implications of China-owned critical infrastructure in the European Union. Available at: https://www.europarl.europa.eu/RegData/etudes/IDAN/2023/702592/EXPO_IDA(2023)702592_EN.pdf (Accessed 22/07/2024).

Geiss, R., & Petrig, A. (2011). Piracy and armed robbery at sea: the legal framework for counter-piracy operations in Somalia and the Gulf of Aden / Piracy and armed robbery at sea: the legal framework for counter-piracy operations in Somalia and the Gulf of Aden. Oxford University Press.

Giannakopoulou, E. N., E. I., Thalassinos, & T. V., Stamatopoulos (2016). 'Corporate governance in shipping: an overview'. Maritime Policy & Management, 43(1), 19-38. https://doi.org/https://doi.org/10.1080/03088839.2015.1009185.

Grammenos, C. T. (2010). The Handbook of Maritime Economics and Business. Lloyd's List.

Greenberg, A. (2018, August 22). The untold story of Notpetya, the most devastating cyberattack in history. Wired. Retrieved Available at: https://cyber-peace.org/wp-content/uploads/2018/10/The-Untold-Story-of-NotPetya-the-Most-Devastating-Cyberattack-in-History-_-WIRED.pdf (Accessed 22/07/2024).

Gruner, J. (2021). Digital Transformation in Shipping: The Hapag-Lloyd Story. In: Seebacher, U.G. (eds) B2B Marketing. Management for Professionals. Springer, Cham. https://doi.org/10.1007/978-3-030-54292-4_23.
Haywood, R., & Spivak, R. (2013). Maritime Piracy. Routledge.
International Chamber of Shipping. (2017). Drug trafficking and drug abuse on board ship: guidelines for owners and masters on preparation, prevention, protection, and response. Witherby Publishing Group Ltd.
Jenner, C. J., & Tran Truong Thuy. (2016). The South China Sea. Cambridge University Press.
Maaike Warnaar, Zaccara, L., & Aarts, P. (2016). Iran's Relations with the Arab States of the Gulf: Common Interests over Historic Rivalry. Gerlach Press.
Murphy, M. N. (2013). Contemporary Piracy and Maritime Terrorism. Routledge.
Otto, L. (2020). Global Challenges in Maritime Security. Springer Nature.
Prunckun, H. W., (2019). Counterintelligence theory and practice. London: Rowman et Littlefield.
Russel, D., & B., Berger (2020). Weaponizing the Belt and Road Initiative. Asia Society Policy Institute. Available at: https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf (Accessed 22/07/2024).
Sodhi, M. M. S., & C. S., Tang (2014). Managing supply chain risk. Springer.
Thai, V. V. (2014). Solving the Security-Trade Puzzle. Journal of Applied Security Research, 9(3), 305–327. https://doi.org/10.1080/19361610.2014.913235
The Hague Centre for Strategic Studies (2019). Geopolitics and Maritime Security. Available at: https://hcss.nl/wp-content/uploads/2021/01/Geopolitics-and-Maritime-Security-web.pdf (Accessed 22/07/2024).
Van Cleave, M. K. (2007). Counterintelligence and national strategy. https://doi.org/10.21236/ada471485. Available at: https://apps.dtic.mil/sti/pdfs/ADA471485.pdf. (Accessed 22/07/2024).
Van der Putten, F-P. (2019). 'European seaports and Chinese strategic influence'. Clingendael Institute. Available at: https://www.jstor.org/stable/pdf/resrep21415.4.pdf (Accessed 22/07/2024).
Weaver, C. (2016). The Politics of the Black Sea Region. Routledge.

Anastasios-Nikolaos Kanellopoulos is a PhD candidate of the Athens University of Economics and Business, holds a Master in International Relations, Strategy and Security from the University of Neapolis Pafos in Cyprus and a Bachelor in Business Administration from the Athens University of Economics and Business. In addition, he is a certified Security Risk Analyst from FRONTEX and the Hellenic Ministry of Citizen Protection. His research interests include Competitive Intelligence and Counterintelligence frameworks application in modern Business environment.

Dr. Anthony Ioannidis is an Assistant Professor of Management at the Department of Business Administration, Athens University of Economics and Business, Greece. He has previously taught at the University of Patras, Greece, University of La Verne California, and Baruch College - City University of New York. He holds a B.S. from the University of Athens, Greece, and, an M.B.A., an M.Phil., and a Ph.D. from Baruch College - City University of New York. Dr. Ioannidis also possesses working experience as management consultant with leading consultancy firms in the United States and Greece, in the areas Telecommunications, Media and Technology. His current research interests include strategy formation, organizational design, public-private partnerships and entrepreneurship.

8th NMIOTC Conference on Cyber Security in the Maritime Domain, 2024

by Dinos Kerigan-Kyrou

* The author is very grateful to Brenda van Rensburg (B.Sc., LLB, Grad Cert AI) for her invaluable contributions to the conclusions.

The following is a summary of the 8th NMIOTC Maritime Cybersecurity Conference. The keynote speeches will be highlighted before summarising the panel discussions, and then drawing final conclusions.

One of the key messages from the conference is that cybersecurity concerns us all. Cybersecurity must move from the siloed 'IT only' domain to a situation where the safety of our people in our military and civilian organisations becomes the central focal point of our cybersecurity polices and strategies. Because it is the people within our organisations - and within our partners such as supply chains - who are being targeted by nefarious states, terrorists and criminal actors (and increasingly a combination of all three). IT based cybersecurity solutions - no matter how good they are - do not solve this problem. The critical theme of the conference is how we need to adapt our approach to cybersecurity - thinking and operating holistically.

Keynote Speeches[1]

It was stated to the conference that oceans have become a new battleground in cyberspace. And this is especially true because cybersecurity extends beyond technical concerns.

Attempts to compromise maritime systems, and attacks on ports, are just two examples of the cyber threats we face. For example, AI cyber enabled attacks in the future may combine with cyber physical attacks and information warfare against us with the aim of aim of disrupting our decision-making processes. To defeat this we must work with partners and allies. In Greece new legislation has been enacted for cyber defence. A specialised body has been set-up to act in a unified, holistic way for the for Greek army, navy and air force; it will be responsible for continually evaluating cyberspace holistically, looking at the whole evolving security and threat landscape.

The delegates were told about the new National Cybersecurity Authority (NCSA) for Greece. The mission of the NCSA is to be the main coordination point for cyberse-

[1] Keynote speakers: Maj Gen E. Fragoulopoulos, GRC, Director, Informatics Directorate Hellenic National Defence General Staff; Michail Bletsas, Director of Computing, MIT Media Lab, and Director of the General National Cybersecurity Authority (NCSA); Despina Spanou, Head of the Cabinet of European Commission Vice President Margaritis Schinas, European Union; Dr Mart Noorma, Director of NATO Cooperative Cyber Defence Centre Of Excellence (CCDCOE); Lt Cdr (Ret'd) Chronis Kapalidis of the EU European Maritime Safety Agency (EMSA).

curity. Considerable recent cybersecurity developments in the EU were highlighted; the first Network Information Security Directive ['NIS1' - on the cybersecurity of critical infrastructure] was ineffective because enforcement was, essentially, 'voluntary'; it was left to the Member States to apply the legislation with no EU level penalities and very little oversight, it was posited. Conversely 'NIS2' - with strong oversight and penalities - will play a far bigger role in the protection of critical infrastructure cybersecurity.

We all have to be aware of and involved with cybersecurity, stated the Director. The measure of success will be the speed we establish this very 'cybersecurity ecosystem'. We have to change the mentality - from 'nodes and firewalls' to a situation involving everyone. Compartmentalising cybersecurity - which has been done for many years - is the very worst thing that can be done. Information-sharing is critical; we can no longer have people 'hiding behind security' as the excuse for not sharing information.

In Greece there's been a big increase in DDoS attacks [a distributed denial-of-service, DDoS - where the bandwidth of a targeted system, usually a web server, is deliberately overwhelmed by a nefarious actor]. Security comprises a chain; and that chain is only as strong as its weakest part. Threat actors are developing hybrid threats; for example, the race riots in the UK were incited with disinformation and fake news online. We have to think holistically and share information. We have to be concerned about the Supply Chain. In Greece there is good cooperation between the military and civilian sectors this cooperation will increase. However, we have to start thinking of cybersecurity in the same way we think of the immune system; i.e. we have to be able to quickly detect and mitigate threats. The threats are always there. Indeed, there are two types of organisations: Those that have been hacked, and and those who don't know they've been hacked, the Conference was told.

Despina Spanou, Head of the Cabinet of European Commission Vice President Margaritis Schinas, European Union began by stating the NMIOTC Cybersecurity Conference is an annual 'landmark' point in the cybersecurity calendar. Moreover, the conference came this year at a very opportune moment, with the next European Commission soon to take office.

Over the past five years the European Commission has taken significant steps to address cybersecurity, providing solid foundations for the next five years, by: boosting the resilience of critical infrastructure (CI); improving supply chain and product security; strengthening cybersecurity solidarity between EU Member States; and enhancing the ability to detect, prepare for and respond to cyberattacks. Covering a much broader range of critical infrastructure (including manufacturing of certain critical products such as medical devices as well as public administration), the revised NIS2 Directive strengthens the level of cybersecurity requirements for operators of critical entities and sets up reporting obligations. Enforcement is also substantially enhanced, with the possibility to impose fines for breaches of cybersecurity management and reporting obligations. By the end of 2024, the Cyber Resilience Act will bolster resilience of all products that have digital components, making it the first piece of legislation of this type anywhere in the world. Moreover, the Cyber Solidarity Act will create: a European Cybersecurity Alert System to enhance coordinated detection and situational awareness capabilities; a Cybersecurity Emergency Mechanism System, which will include the creation of an EU Cyber Reserve; and a Cyber Incident Review Mechanism to evaluate large-scale and significant cybersecurity incidents. Nonetheless, the cybersecurity skills gap remains a major issue, with an estimated shortfall of at least 260,000 cybersecurity professionals in Europe. The establishment of the EU Cybersecurity Skills Academy is a very important milestone in

addressing this lack of cybersecurity expertise, which is essential not only to respond to cyber threats, but also to implement all of these new EU cybersecurity rules.

In regard to the maritime cybersecurity environment - the revised EU Maritime Security Strategy provides a framework for effective tools for the EU to address maritime cybersecurity challenges. This is necessary because risks are multiplying - hybrid and cyber threats, threats to offshore CI and Critical Maritime Infrastructure (including renewable energy platforms), underwater threats, pipelines and cables - all require greatly increased resilience.

Cooperation between the EU and its partners, such as NATO, is paramount in that regard. Addressing hybrid threats and strengthening resilience is among the most dynamic areas of EU-NATO cooperation, with a newly-established dedicated EU-NATO Task Force on the resilience of critical infrastructure. Head of EU Cabinet Despina Spanou concluded by saying that we will have to work hard over the coming years to implement this new set of EU legislation and ensure that Europe is better prepared and equipped to respond to these emerging threats.

The Conference was told about the excellent history of cooperation between NMIOTC and CCDCOE - the NATO Cooperative Cyber Defence Centre Of Excellence. CCDCOE's main challenge in cyberspace is to try and deter the adversary and to ensure a safe and secure internet - essential for our economies. Cybersecurity now concerns the political, diplomatic, legal, information and cognitive environments. The attacks on us all are continuos, it was stated. All 39 nations at CCDCOE [32 NATO plus seven PfP and Partner Nations] are continuously occupied addressing these threats and simultaneously preparing for future cybersecurity challenges. We cannot only look at previous cybersecurity events; education and training is critical to support future capabilities. All staff and colleagues need to be trained to understand cyber threats. And we must stop talking about 'people being the weakest link'. Every single person has a role as a defender - in addition to their own particular role in their organisation. All officers must be cyber commanders, it was stated.

Many of us are placing increasing trust in AI. In the military environment enabling AI within weapons systems is a considerable challenge. AI has raised questions regarding systems which may be unmanned for months on end, such as unmanned underwater vehicles (UUVs). Moreover, we are rapidly approaching a post-quantum environment for cryptography. This raises questions such as how do our navies recognise the huge change that a post-quantum environment will create for our maritime cybersecurity? Regarding the legal environment, CCDCOE is firmly of the view that existing laws already preclude nefarious activities online. Indeed, NATO and its Partner Nations obey the laws - very different to the actions of nefarious states such as Russia who break laws regularly. Nonetheless, it is because we obey the law our response to those who break the law is far more restricted. Thus, in order to defeat our adversaries we must work together in a like-minded way as Allies and Partners.

In regard to the role of the EMSA - the EU's European Maritime Safety Agency - and cybersecurity, the delegates were told about EMSA's key role supporting safety, security, and sustainability. EMSA has established a Cyber Task Force with the aim to provide support to the European Commission and EU Member States in the development, identification and exchange of best practices and cross-sectoral cooperation on cybersecurity for the maritime environment, as well as to contribute to European inter-agency cooperation on maritime cybersecurity issues. EMSA supports EU naval operations; EU maritime reconnaissance and surveillance is becoming increasingly vital for the security of the EU. Frontex is the EU agency responsible for the EU's border security, and EMSA plays an ever more important role in assisting Frontex in its surveillance and data collection roles. EMSA has established an Academy to develop and enhance maritime skills, including the course 'Concepts in Maritime Cybersecurity' which introduces participants to the central role cybersecurity plays in the maritime environment. The keynote sessions concluded with an emphasis on the importance of a Common Information Sharing environment for maritime cybersecurity information and learning.

Summary of Panel Discussions

'Anchoring Security: Enhancing Cyber Resilience in Maritime Industry'[2]

The changing nature of cybersecurity in the cruise line industry was explained; while a modern ship may have several thousand passengers it can be crewed by only 10 people. Moreover, the distinction between ashore and aboard in a digital environment is becoming increasingly less. Cybersecurity is a huge issue for cruise line operators. However, there is a radical transformation in the maritime industry, especially moving on from legacy IT systems. Many factors are increasing maritime cybersecurity complexity. We must consider the entire supply chain, where there are real and substantial security challenges, as a single entity to increase the security level of

[2] Anchoring Security - Enhancing Cyber Resilience in Maritime Industry: Sylvain Rodenburg, Naval Group, 'Cyber Capacities On-Board, Toward New Warship Operational Performance'; Teresa Spadafora and Fabio Cocurullo, Leonardo, 'Cyber Operations Dimension in the Maritime Domain'; Simone Fortin, MSC Cruises, 'Cybersecurity Marine Supply Chain Transformation: Complexities and Challenges'. Moderator: Joffrey Guerry, Oledcomm.

the maritime industry. Each ship is becoming a 'smart city' involving multiple complex cyber enabled capabilities for the vessels' systems, in addition to the accommodation and all the other aspects affecting passengers' cybersecurity.

All the panellists emphasised the complexities and challenges that occur through the digitalisation of systems. Threats include keeping information gateways secure, as well as evolving cyber-enabled threats, including drones. The crew needs to be able to deal with cyber attacks even if they are not specialists. Vessels should be designed to operate with no cyber specialists aboard. Indeed, it was emphasised that a cyber attack can be equivalent to a conventional weapons attack.

Emerging and disruptive technologies are altering the character of conflicts. Cyber threats are evolving rapidly. Moreover, maritime cyber protection is not only about vessels but also the cables and Critical Maritime Infrastructure (CMI) that transmits 99% of our information. Multi-domain operations introduce a vulnerability as the enemy can hide within networks.

In the past we have 'air gapped' security [where we attempt the physical separation of both IT and OT (Operating Technology) from the online environment]. However, air gapping no longer works because of the need for connectivity of systems. Moreover, we need to be able to detect internal threats; cyber 'resilience by design' is crucial going forward. Our long-running approach of 'classified' and 'non-classified information is becoming increasingly redundant. Traditionally we tried to protect the classified systems from the 'known threats'. But our objective now has to switch from 'protecting against threats' to "protecting the mission." We have to move on from seeing a single threat at a single time. This requires a Cyber Resilience approach, and we must assume that we are always under attack from Advanced Persistent Threats (APTs)

'Navigating the Waters: Addressing Cyber Threats and Challenges in Maritime Security'[3]

The panel opened with the statement: "If you can dream it, someone has likely already done it - so expect the unexpected." We need a clear understanding of the cyber threats. To do this we must no longer think 'in lists' of the threats we face. Threat hunting must be proactive and we must assume that our networks are already compromised. The importance of sharing cyber threat intelligence was emphasised, as was redefining our understanding of what constitutes the threat perimeter - it is now everywhere, so we must share information and work proactively.

The importance of civil-military cooperation was emphasised, including the huge importance of civilian transport and other infrastructure for the military, and of civilian companies' criticality throughout the military supply chain. Indeed, there is increasing outsourcing to civilian companies, who are in turn becoming targets for adversaries. Vessel spoofing is becoming an increasing concern. Moreover, all surface vessels can be tracked using open source intelligence (the websites 'MartimeTraffic' 'or VesselFinder', for example), social media, and a variety of online data, including live webcams around the world.

[3] Navigating the Waters - Addressing Cyber Threats and Challenges in Maritime Security: Captain Spyridon Papageorgiou, Hndgs/e5-Director Cyber Defense Directorate, 'Hunting Cyber Security Operations'; Captain Pawel Wolinski, Cybersecurity Division Poland, 'Civil-Military Cooperation on Maritime Cybersecurity'; Captain Yann Bozec (Fra-n) MARCOM Acos N6/cyberspace, 'Cybersecurity Marine Supply Chain Transformation: Complexities and Challenges', Moderator: Cdr Phd Adam Stojałowski, Polish Naval Academy.

Cyber attacks on port infrastructure are being combined with other nefarious activities; indeed, many of these attacks are not reported in the media. In order to counter this, cyber threat intelligence sharing is critical. The military can help the civilian sector in this regard by helping to conduct their cybersecurity assessments. Much of the threat at sea is similar to the threat emanating from land including GPS jamming, cyberattacks against control systems, data exfiltration, and psychological operations (PSYOPs).

'Building Cyber Defenders'[4]
The panel raised the importance of moving away from a siloed approach toward a multi-disciplinary strategy that emphasises resilience. Moreover, cybersecurity should be much more integrated within social sciences to produce a cybersecurity educational environment that is both technical and non-technical.

The successful role of the EU's European Security and Defence College (ESDC) was emphasised, particularly its cybersecurity education and training, development of curricula, and its working with the Hybrid Centre of Excellence. [Hybrid COE is a joint EU-NATO facility in Helsinki that researches, advises, and trains on hybrid threats and challenges]. ESDC education increasingly combines leadership development, crisis management, hybrid threats, and cybersecurity. Between 2023 and 2024 over 5300 people were involved in over 200 ESDC educational activities. ESDC's aim is to develop a 'defence culture' for the EU addressing multifaceted security risks. ESDC also has a crucial diplomatic role developing strategic partnerships; its outreach and education includes a special focus on Ukraine, the western Balkans, and recently, the Indo-Pacific and the Middle East North Africa (MENA) regions. The EU is seeing an increasing demand for skills in cybersecurity and emerging technologies. Advanced Distributed Learning (ADL) is ever-more central to ESDC's work with the Cyber ETEE (Training, Evaluation and Exercise) Platform. AI and digital transformation will develop the learning experience. ESDC and NATO are increasingly working with one another, especially with NATO DEEP. Work is also developing on possible cooperation between ESDC and NATO CCDCOE.

'AI-Driven Horizons: Revolutionizing Maritime Cyber Security'[5]
The panel explored both the legislative and operational aspects of AI in the maritime cybersecurity environment. Moreover, it looked at the social and 'human in the loop' factors of AI, in addition to the technical aspects.

At the EU level the AI Act will oblige operates of AI to meet certain expectations in all environments including CI and supply chains, and essential services such as law enforcement and the administration of justice - as well as the maritime environment. We have an expectation for AI to be trustworthy, including aboard ships and all aspects of maritime activities. On ships AI is increasingly being used within smart systems and will thus be affected directly by the new EU legislation. Platforms need to be usable by everyone. Moreover, we need conformity assessments of trustworthiness. We also need cybersecurity and AI certification, with manufacturers using a harmonized standard, the Conference was told.

'Fortifying Maritime Frontiers: Leveraging Advanced Cyber Intelligence for Enhanced Security'[6]
The panel emphasised that the importance of gathering information and how we leverage cyber intelligence is critically important. This includes identifying phishing, analysing threat actors' profiles, preventing ransomware, and helping victims.

There are methods we can use to identify potential threat actors. For example, an analogy of the Q-ships in WW1 was made, where allied ships were deliberately located to provide a decoy in order to lure submarines away from key targets. Similar situations can be used in the maritime environment as a 'honey pot' in order for us to learn more about adversaries' strategies, the panel concluded.

'Strengthen Foundations: Cyber Security and the Protection of Critical Infrastructure'
The panel discussed the growing number of available targets for our adversaries in the maritime environment as a result of increasing connectivity. For example, there are cybersecurity threats to CMI. Furthermore, Multi-Domain Operations increasingly comprise Joint All-Domain Command and Control (JADC2). Because of this, the

[4] Building Cyber Defenders: Giuseppe Zuffanti, ESDC, European External Action Service, EU, 'The Key Role of the European Security and Defence College (ESDC), Implementing Cyber Security and Cyber Defence EU Policy'; Dr Dries Putter, Dr Susan Henrico, Stellenbosch University, 'Cybersecurity Education at the Faculty of Military Science, Stellenbosch Professional Cyber Course'; Dr Theodoros Karvounidis, University of Piraeus, 'Professional Cybersecurity Education in the Maritime Sector'. Moderator: Ourania Stavropoulou, Ministry of Migration And Asylum, Greece.
[5] AI-Driven Horizons - Revolutionizing Maritime Cyber Security: Lt Françoa Taffarel, Brazilian Navy, 'Enhancing Cyber Situational Awareness in Maritime Military Operations Through Artificial Intelligence-Driven Cyber Exercises'; Prof. Nineta Polemi, University of Piraeus, 'Cyber Security Certification of AI Systems'; Mr Giuseppe Laurenza, E-phors, 'Naval Cyber Security (NACYSE)'. Moderator: Professor Nikitas Nikitakos, University Of The Aegean.
[6] Fortifying Maritime Frontiers - Leveraging Advanced Cyber Intelligence for Enhanced Security: Andreas Sfakianakis, University Of Crete, 'CTI [Cyberthreat Intelligence] In The Age of AI'; Arne Asplem, Norma Cyber, 'The "Norwegian Mode" For Collaborative Maritime Cyber Defence'; LtCol Mathieu Couillard, Canadian Special Operations Forces Command, Dr Britta Hale, NPS, 'DRACO - Deceptive Resistance to Adversary Cyber Operations'. Moderator: Dr Britta Hale, US Naval Postgraduate School (NPS), Monterey, California.

panel discussed advanced cybersecurity protection in the military and commercial environments. Examples of such advanced cybersecurity protection include in-depth vulnerability assessments of container shipping systems. Such assessments need to become much more widely available than they are presently in both the military and civilian environments.

The 2023 Balticconnector incident [where damage to a gas pipeline and two telecom cables between Estonia, Finland and Sweden occurred when the anchor of a Chinese registered ship was dropped] highlighted the risk of deliberate or grossly negligent damage caused to Underwater Critical Infrastructure (UCI). (For example, the perpetrator can claim "an accident" caused damage to UCI, but their real motives would remain unclear). Until robust, resilient and effective protection systems are developed, UCI will continue to remain vulnerable to attacks aimed at disrupting economies, communication and energy transit. UCI protection is urgent, requiring technology, R&D, and substantial investment.

Like the previous panel it was stated that attempting to 'Air Gap' UCI and CMI from the internet is inherently unsafe. Instead of air-gapping we need communication systems, networks, sensors and servers combining underwater unmanned and autonomous assets operating with a mesh connection [where infrastructure nodes connect directly, dynamically and non-hierarchically], thereby providing increased resilience.

Conclusions

Brenda van Rensburg, advisor to the Australian government, financial services, and the Australian mining industries states: "According to Sun Tzu, the greatest victory is that which requires no battle. As such, when it comes to disrupting the maritime environment both physical and cyberspace are important. Cables, towers, servers, hardware, and satellites are just as important as network infrastructure, user interface, and integration of applications. The effort to protect all of this does not rest on one person or entity; it is a shared responsibility that stems from the service providers to us all. We all play a part in this security. Taking responsibility for updating our own security on personal devices, responsibility for responding to news online, and for our online safety and wellbeing are all critical. Cybersecurity disruptions, including online disinformation can directly affect maritime infrastructure, including ports and the whole maritime environment. It is therefore vital we all play a vital part in its security. Only when we join forces can we make a difference; increasing our capability to reduce maritime disruptions will secure the maritime environment holistically." The presentations, talks and discussions of the 8th NMIOTC Cybersecurity Conference entirely concur with this excellent analysis.

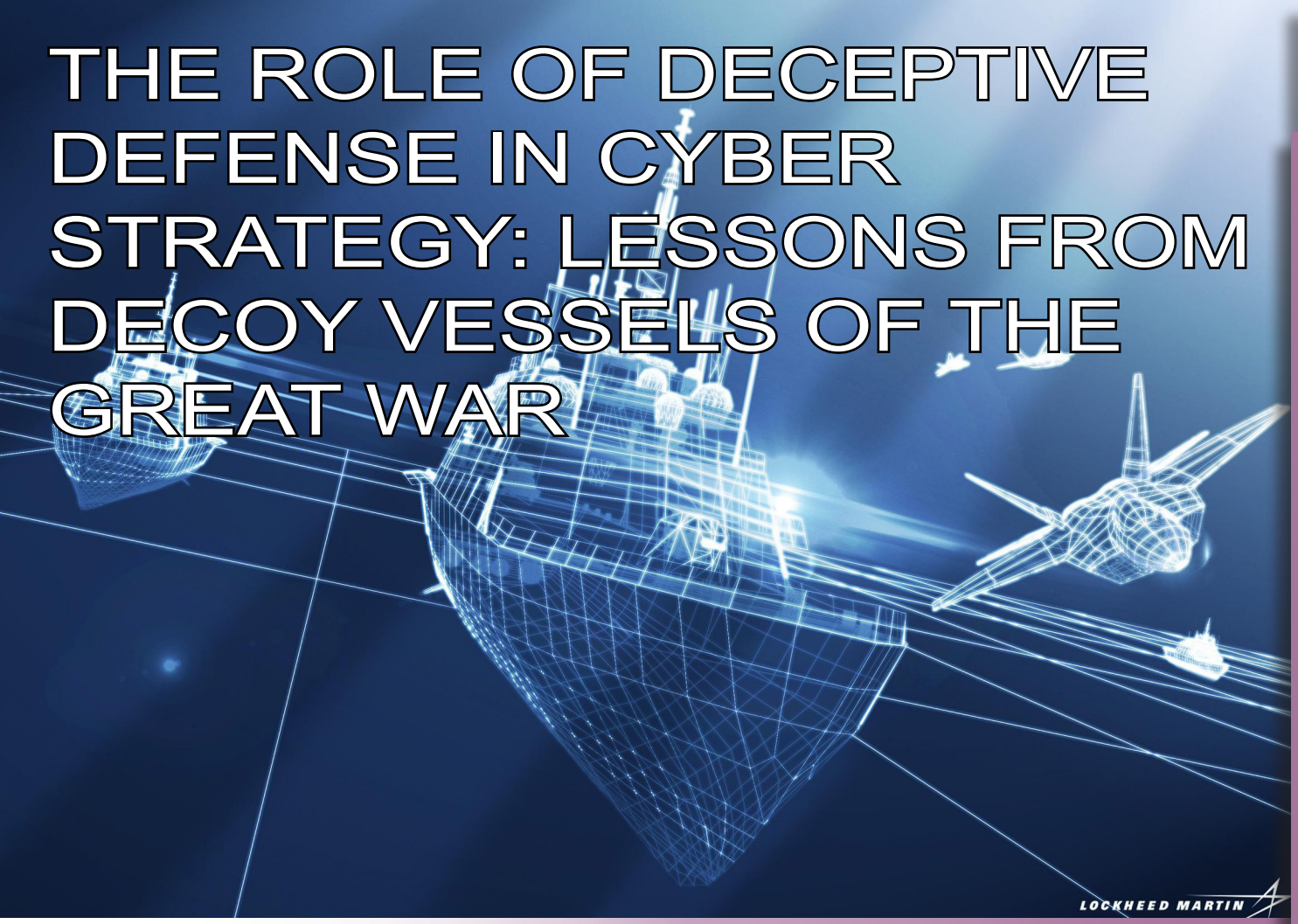
While cybersecurity in the maritime environment can never be completely perfect, we have a duty to make it as good as it can possibly be. As the NCSA of Greece stated at the Conference: We all have to be aware of and involved with cybersecurity. We have to change the mindset - "from 'nodes and firewalls' to involving everyone".

The cybersecurity threat landscape will continually adapt and change. Those who wish to cause us harm will find ever more novel ways of disrupting maritime cybersecurity. New methods will increasingly include AI and its utilization to disrupt our legitimate and lawful maritime activities. We need to continually improve and indeed use AI to help protect our cyberspace. AI will increasingly be combined with cyber enabled capabilities - including drones on the water, under the water and in the air - facilitating cyber enabled attacks on Critical Maritime Infrastructure as well as our vessels and ports. Moreover, the maritime environment will now and always comprise multiple levels of IoT (Internet of Things) on vessels, at ports, and within CMI, including Underwater Critical Infrastructure. We need to be increasingly cautious regarding the supply chain concerning the use of components and the IoT manufactures, with particular attention to the critical components and systems made by companies that create security risks for NATO and the EU.

We need to address cybersecurity holistically by placing our people - all of the people who work with our organisations, companies, and militaries - at the heart of the continual process of developing the cybersecurity of our maritime environment.

Dinos Anthony Kerigan-Kyrou PhD CMILT AmRINA is a Cybersecurity and Hybrid Threats instructor on NATO DEEP (Defence Education Enhancement Programme), coordinated by NATO and the Partnership for Peace Consortium of Defence Academies (PfPC). Dinos assists at the DEEP eAcademy developing Advanced Distributed Learning (ADL) platforms for NATO and Partner nations. He is an editor of the PfPC journal Connections, and a visiting instructor at the EU European Security and Defence College. Dinos is a co-author of the NATO / PfPC Cybersecurity, and Hybrid Warfare and Hybrid Threats Curriculums. From 2017-2024 he led the Cybersecurity and Hybrid Threats education on the Irish Defence Forces Joint Command & Staff Course. He is a founding member of the cybersecurity committee of Royal Institution of Naval Architects, and a board member of Digital Business Ireland.

THE ROLE OF DECEPTIVE DEFENSE IN CYBER STRATEGY: LESSONS FROM DECOY VESSELS OF THE GREAT WAR



by Lieutenant-Colonel Mathieu Couillard
& Dr. Britta Hale

Sun Tzu stated, "All warfare is based on deception," and cyber conflict poses no exception to this aphorism. Cyber threat actors exploit human and technical vulnerabilities to penetrate even the most secure and sensitive networks. Once inside, attackers gain a foothold and silently pivot across the network, employing yet more deceptive tradecraft to cloak themselves beneath the noise of network traffic. Notably, a 2022 report from IBM found that on average, network breaches were only detected 212 days after the initial compromise.0F In many cases, the ambiguity of the cyber domain enables the attacker to thwart punishment, as the ultimate attribution of cyber attackers' identities is a costly and imperfect process.

In the same way that deception can enable the cyber offense, deception can elevate current efforts to deter or detect cyber attacks. Defenders utilize cyber deception through many techniques, including one widely known as the honeypot. This article explores the profound impact that deceptive defense can have on cyber strategy by presenting a historical case study of Q-ships—anti-submarine warships disguised as commercial vessels during the First World War. The lessons gleaned from this case study are then applied to the cyber domain to illustrate potential effects and strategies.

CASE STUDY: Q-Ships

Background: The U-Boat Campaign

On October 20, 1914, the German U-boat U-17 fired a shot across the bow of SS Glitra, a British merchant ship sailing off the coast of Norway.80F In accordance with naval tradition, U-17 ordered the crew to escape before scuttling the 866-ton ship.81F SS Glitra was the first trade vessel to be sunk by a U-boat during the First World War. When U-20 torpedoed the British commercial liner RMS Lusitania in May 1915, the crew and passengers were not so lucky: nearly 1,200 men, women, and children lost their lives.82F The incident caused massive global outrage, reducing Germany's moral standing and energizing the war movement in the United States.83F Nonetheless, U-boats continued to attack commercial ships. Acting on

promises from the Imperial German Navy that the U-boat campaign could "starve Britain into submission," the German Chancellor even resumed "unrestricted submarine warfare" in January 1917.84F Over the course of the war, U-boats would attack thousands of allied and neutral ships, sending more than 11 million gross tons of shipping to the bottom of the ocean.85F

With the tragedy of RMS Lusitania arose an opportunity. After the sinking of the commercial liner, the Kaiser directed a moderation of the U-boat campaign to avoid further angering the United States and other neutral countries.86F Remaining in accordance with "prize rules," U-boats would surface near trading vessels to give the passengers a chance to evacuate before scuttling the ship, as they had with the SS Glitra.87F While the U-boats were a deadly and silent threat to any ship when submerged, they were far more vulnerable when surfaced. Admiral Karl Dönitz, who captained a U-boat during the First World War and rose to high command during the Second World War, wrote that surfaced U-boats were "slow" and "low in the water with a restricted field of vision," leaving them ill-suited for a direct confrontation.88F U-boats also lacked armor, such that a single shot could "sink or at least prevent the ship from diving."89F The British, who were desperate to find solutions to the German raids, looked for new ways to exploit this weakness.

Q-ships

Naval officers had already proposed the idea of decoys to the British Admiralty in the autumn of 1914.90F Winston Churchill, First Lord of the Admiralty at the time, instructed the Commander-in-Chief to proceed with arming "small to moderate sized steamers" to "trap the German submarine" and "sink her with gunfire."91F The Royal Navy had a working prototype in the form of SS Vittoria, refitted from commercial trawler.92F SS Vittoria and other early decoy ships were not impactful, as shipping losses inflicted by the U-boats rose to 1.4 million gross tons by the end of 1915.93F An updated concept saw the British deploy a trawler, USS Taraniki, paired with the submarine C-24. On June 23, 1915, the USS Taraniki spotted a German submarine and promptly informed C-24 via underwater cable. C-24 positioned itself to attack and sank U-40 with a single torpedo, killing all but three members of the crew. Decoy vessel tactics gained momentum in the summer of 1915. In the aftermath of the German sinking of RMS Lusitania, the British strove to better coordinate the deception campaign.94F The Royal Navy launched new decoy ships in Queenstown, Ireland, where they became known as Q-ships. Vice-Admiral Gordon Campbell, who commanded a Q-ship during the war, detailed improvements to their "disguises," including false cargo and neutral colors according to their itinerary.95F Vice-Admiral Andreas Michelsen, Commander of the German Submarine Forces starting in June 1917, reported that "even a visitor on board … could not recognize [their] true character, and a careful examination through the periscope would fail to reveal anything suspicious."96F Q-ship crews were dressed as civilians (even as women) and trained to simulate commercial crews in every aspect, including the nomination of a "panic crew," which would abandon the ship in a false demonstration of vulnerability.97F

Efforts to improve the deceptive effectiveness of Q-ships were soon rewarded. On July 26, 1915, the HMS Prince Charles spotted a U-boat to the north of Scotland.98F The Q-ship waited for the submarine to engage, at which time it stopped its engines and lowered the boats to simulate an evacuation. When U-36 exposed its broadside in its approach, the crew of HMS Prince uncovered their guns and fired on the U-boat. U-36 was the first German submarine to be sunk by a Q-ship, but two more U-boats were lost to the decoy vessels by the end of 1915. As German knowledge of the Q-ship stratagem spread, the Royal Navy adapted by increasing the armor and armament of the decoy ships.99F However, one of the last Q-ship engagements featured the opposite approach: HMS Stockforce was a small (360-ton) steamer commanded by Lieutenant Harold Auten.100F German U-boats found it more difficult to fire effectively on smaller ships and would be forced to surface.101F In July 2018, HMS Stockforce sank UB-80 in a dramatic engagement that won Aulen a Victoria Cross.102F

Q-ships had a significant impact on the U-boat campaign during the First World War. Over the next years, their numbers soared as the Royal Navy commissioned up to 180 vessels.103F Actively hunting U-boats, they saved countless commercial vessels and the lives of their crews simply by drawing U-boats away from vulnerable targets. Estimates on the total number of U-boats sunk by Q-ships range from 11 to a "couple of dozen," with up to 80 U-boats damaged and sent for repairs.104F Beyond the tangible cost of replacing and repairing U-boats, decoy ships may have inflicted a moral effect on the German submarine crews, who suffered a "great wariness" when approaching any vessel.105F Such a change in U-boat tactics is indicative of the impact that Q-ships had in the war.106F

The used of Q-ships eventually declined, as any military technology naturally does. Critics have claimed that the U-boat campaign may have become more ruthless because of the Q-ship stratagem.107F Raiding submarines eventually became reluctant to surface, thus removing any opportunity for the crews of civilian ships to evacuate. Yet, President Woodrow cited "unrestricted submarine warfare," in the U.S. declaration of war in April 1917.108F Q-ships and other anti-submarine measures contributed to the reduced effectiveness of the U-boat campaign under "prize rules," which Germans concluded would be insufficient to starve Britain.109F Thus, the Q-ship (along

with other anti-submarine measures) may have indirectly contributed to the United States joining the war. Other critics have wisely noted that the decline in the success rate of U-boats was surely due to a combination of factors, including mines and naval convoys, and cannot be solely attributed to the Q-ship.110F Some scholars have also debated the legality of deception, possibly creating a perception of moral equivalency between U-boat raids and Q-ships.111F The nuances between perfidy and ruse may be subtle, but at least the British ordered Q-ships to change their colors just before opening fire, as international law required.112F

Cyber Q-ships?

Q-ships illustrate some potential effects of deceptive cyber defense. Decoy vessels lured the stealthy U-boats to a position of vulnerability when surfaced, allowing for the identification of threats. In the same way, an effective defensive cyber deception may compel the adversary to an engagement on the defender's terms. By offering a target of opportunity, Q-ships and deceptive cyber defense misdirect the adversary, drawing them away from their intended targets. The ultimate purpose of Q-ships was to destroy or disable U-boats, and they did so through deceptive defense, in retaliation for an initial engagement by the U-boat. Current cyber response practice is analogous to launching an anti-submarine ship to search for a U-boat that had sunk a defenseless ship a few months earlier. With Q-ships, as with deceptive cyber defense, retaliation can occur immediately after an adversarial attack.

Lessons from the employment of Q-ships can be applied to the operationalization of deceptive cyber defense. No analogy is perfect, beginning with the violence and other hardships that the crews of Q-ships needed to contend with. Nonetheless, the bravery and genius of the men who served on these decoy vessels demonstrates that effective deception results from creativity, attention to detail, and operational security. As the deceptive quality of Q-ships improved in 1915, so did the stratagem's results. To achieve analogous effects in the cyber domain, defenders must optimize every aspect of deceptive cyber defense. The Royal Navy regularly modified the characteristics of the decoy ships throughout the Great War, extending the useful lifetime of the stratagem. Only once the U-boats fundamentally shifted their tactics did the direct threat of Q-ships abate, and by then, other means of anti-submarine warfare were available to compensate.

Effect Descriptions

Identification

Identification provides a general understanding of the cyber threat environment and the specific detection and characterization of adversarial attacks. The former can inform a network's internal defensive measures. As discussed in Chapter II, researchers have long employed deception to characterize emerging threats. In a recent example, scholars utilized honeypots to study the "log4j" attacks.113F Defenders can also leverage the information gained through deceptive cyber defense. For instance, malicious internet addresses can be detected on an external honeypot and blocked from the network potentially faster than they can be identified and indexed by a threat intelligence provider. In addition, these malicious addresses may represent a more relevant asset than a generic blacklist.

Deceptive cyber defense supports the detection of attacks by luring the adversary to an engagement on the defender's terms. For instance, a defender can configure a deceptive asset in a way which negates any possibility of legitimate communication. Thus, an actor's mere engagement with the asset constitutes an indicator of compromise. In this sense, deceptive cyber defense serves as an enabler to threat-hunting operations. With additional traffic and attack activity from the adversary, the defender may even observe multiple stages of the attacker's infrastructure (i.e., the initial compromise may be conducted via a botnet while more advanced exploitation through a more permanent channel), facilitating attribution.114F Similarly, deception may also yield insight into the types of malicious activities adversaries are undertaking and their goals.

Misdirection

In the context of deceptive cyber defense, misdirection primarily aims to keep the adversary away from one's own valued resources. Many cyber threat actors strike targets of opportunity: they look for assets that are vulnerable to exploits that are available to them. Consequently, a simple deception that mirrors a known vulnerability may be enough to occupy the adversary long enough for the defender to counter the attack. Delay tactics could extend the duration of the effect. For instance, the LaBrea Tarpit responds to traffic destined for unused addresses, purposely delaying incoming connections.115F

A cognitive-level misdirection effect can be achieved when the defender leaves false or misleading information on a deceptive enclave of a network. Such a stratagem may not tactically improve network defense but could strategically alter the balance of information in favor of the defender. The defender could follow the trail of misinformation to gain information about the adversary or simply benefit from the effect of this misinformation on the decision processes of the adversary. In certain applications, the defender could simply ask the target of the deception to provide information, as the Dutch police did in the case of the AlphaBay decoy.116F

Retaliation

In retaliation, the roles are flipped: the defender wants to take the offensive to disrupt or dismantle a threat actor, as the U.S. National Cybersecurity Strategy suggests. Normal (non-deceptive), targeted offensive cyber operations are much more difficult to conduct than opportunistic attacks that cybercriminals and other cyber threat actors routinely conduct. Rather than match a network to a given exploit as the opportunistic attacker would, a discriminate attacker (e.g., the U.S. government when seeking to disrupt a specific cyber threat actor) must identify a vulnerability on a given network and match it to an exploit to gain access. Thus, without the valuable context potentially provided by defensive operations, offensive planners begin with a blank slate and must scan the adversarial network perimeter to gain access. Erica Borghard and Shawn Lonergan explain that the task of gaining access to an adversarial network is complex and resource intensive.117F Deceptive cyber defense can also enable retaliation by bridging offensive and defensive cyber operations. Offensive and defensive cyber operations are often planned in isolation, through different structures, processes, and people. By collaborating closely, defensive and offensive planners can take advantage of opportunities created by deceptive cyber defense. Within the deceptive enclave, offensive teams can plant canaries which would generate alerts when files are open, backdoors to establish a persistent presence within the adversarial network, or a combination of malware to achieve the desired effect. Deceptive cyber defense thus presents a possibility to bypass the complex task of gaining access to an adversarial network.

Conclusion

Deceptive cyber defense, like the Q-ships of the past century, can enable an active posture to detect threats and misdirect the adversary. Most importantly, deception can allow the defenders to regain the initiative in cyber conflicts by bridging offensive and defensive cyber operations. However, to be truly effective, deception must be carefully tuned to specific threats and objectives, as it is not a universally applicable solution. Just as the Q-ships required ongoing modifications to maintain their effectiveness against evolving U-boat strategies, modern cyber defenders must innovate to enhance deceptive effectiveness while managing security risks. Advancing the practice of deceptive cyber defense is imperative for overcoming current challenges and enhancing defensive capabilities. By integrating deception more fully into cybersecurity strategies, defenders can achieve a more proactive and resilient posture, effectively countering sophisticated cyber threats and regaining the strategic initiative.

References

[1] "Cost of a Data Breach," IBM, 2022, 14, https://www.ibm.com/reports/data-breach.
[2] Lawrence Sondhaus, German Submarine Warfare in World War I: The Onset of Total War at Sea (Lanham, MD: Rowman & Littlefield, 2017), 5–6.
[3] J. Ashley Roach, "The Law of Naval Warfare at the Turn of Two Centuries," The American Journal of International Law 94, no. 1 (2000): 73–74, https://doi.org/10.2307/2555231.
[4] Diana Preston, Lusitania: An Epic Tragedy (New York, NY: Bloomsbury Publishing USA, 2002).
[5] Thomas A. Bailey, "The Sinking of the Lusitania," The American Historical Review 41, no. 1 (1935): 73, https://doi.org/10.2307/1839355.
[6] Dirk Steffen, "The Holtzendorff Memorandum of 22 December 1916 and Germany's Declaration of Unrestricted U-Boat Warfare," The Journal of Military History 68, no. 1 (2004): 215–24.
[7] R. H. Gibson and Maurice Prendergast, The German Submarine War 1914–1918 (Cornwall, UK: Periscope Publishing Ltd., 2002), 380–82.
[8] Gerd Hardach, The First World War, 1914–1918 (Oakland, CA: University of California Press, 1981), 41.
[9] Andreas Michelsen, The Submarine Warfare, 1914–1918 (Washington, DC: U.S. Government Publishing Office, 1926), 51.
[10] Karl Dönitz, Memoirs Ten Years and Twenty Days (Chicago, IL: Frontline Books, 2012), 10.
[11] Richard Compton-Hall, Submarines at War 1914–1918 (Cornwall, UK: Periscope Publishing Ltd., 2004), 91.
[12] Edward Keble Chatterton, Q-Ships and Their Story (Boston, MA: Sidgwick and Jackson, Limited, 1922), 7–8.
[13] Tony Bridgland, Sea Killers in Disguise: The Story of the Q-Ships and Decoy Ships in the First World War (Annapolis, MD: Naval Institute Press, 1999), x.
[14] Chatterton, Q-Ships and Their Story, 7.
[15] Gibson and Prendergast, The German Submarine War 1914–1918, 380.
[16] Bridgland, Sea Killers in Disguise, 6.
[17] Gordon Campbell, My Mystery Ships (Garden City, New York: Doubleday, Doran & Company, 1929), 43–47.
[18] Michelsen, The Submarine Warfare, 1914–1918, 70.
[19] Mary T. Hall, "False Colors and Dummy Ships: The Use of Ruse in Naval Warfare," Naval War College Review 42, no. 3 (1989): 60, https://www.jstor.org/stable/44636917.

[20] Bridgland, Sea Killers in Disguise, 10.
[21] Campbell, My Mystery Ships, 308.
[22] Bridgland, Sea Killers in Disguise, 135.
[23] Michelsen, The Submarine Warfare, 1914–1918, 70.
[24] Harold Auten, "Q" Boat Adventures: The Exploits of the Famous Mystery Ships (London: H. Jenkins, 1919).
[25] Chatterton, Q-Ships and Their Story, 136.
[26] Bridgland provides context to the varying estimates here: Bridgland, Sea Killers in Disguise, 147; Chatterton reports "over eighty" damaged U-boats here: Chatterton, Q-Ships and Their Story, 137.
[27] Gibson and Prendergast, The German Submarine War 1914–1918, 156.
[28] Richard W. Smith, "The Q-Ship—Cause and Effect," U.S. Naval Institute Proceedings 79, no. 3 (1953), https://www.usni.org/magazines/proceedings/1953/may/q-ship-cause-and-effect.
[29] Campbell, My Mystery Ships, 304.
[30] Woodrow Wilson, "Joint Address to Congress Leading to a Declaration of War Against Germany (1917)," National Archives, April 2, 1917, https://www.archives.gov/milestone-documents/address-to-congress-declaration-of-war-against-germany.
[31] Steffen, "The Holtzendorff Memorandum of 22 December 1916 and Germany's Declaration of Unrestricted U-Boat Warfare."
[32] Chatterton, Q-Ships and Their Story, 270.
[33] Matthew G. Morris, "'Hiding Amongst a Crowd' and the Illegality of Deceptive Lighting," Naval Law Review 54 (2007): 256, https://apps.dtic.mil/sti/citations/ADA476997.
[34] Chatterton, Q-Ships and Their Story, 8.
[35] Shreyas Srinivasa, Jens Myrup Pedersen, and Emmanouil Vasilomanolakis, "Deceptive Directories and 'Vulnerable' Logs: A Honeypot Study of the LDAP and Log4j Attack Landscape," in 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), 2022, 442–47, https://doi.org/10.1109/EuroSPW55150.2022.00052.
[36] David D. Clark and Susan Landau, "The Problem Isn't Attribution: It's Multi-Stage Attacks," in Proceedings of the Re-Architecting the Internet Workshop (Conference on emerging Networking EXperiments and Technologies, Philadelphia, PA: Association for Computing Machinery, 2010), 1–6.
[37] Tom Liston, "LaBrea – The Tarpit," accessed April 19, 2023, https://labrea.sourceforge.io/Intro-History.html.
[38] Barniuk, Chris, "AlphaBay and Hansa Dark Web Markets Shut Down," BBC News, July 20, 2017, https://www.bbc.com/news/technology-40670010.
[39] Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," Strategic Studies Quarterly 13, no. 3 (2019): 125, https://www.jstor.org/stable/26760131.

Lieutenant-Colonel Mathieu Couillard is the J6 and Chief Information Officer of the Canadian Special Operations Forces Command (CANSOFCOM). He held a variety of technical leadership positions within CANSOFCOM, including multiple deployments. He also served as a regimental signals officer within the Canadian Army (CA), and as a major capital project manager, overseeing the renewal of the CA's tactical radio fleet. Lieutenant-Colonel Couillard holds a Bachelor of Computer Engineering from Université Laval and two Master of Science degrees from the U.S. Naval Postgraduate School—one in Computer Science (Cyber Operations) and another in Defense Analysis (Irregular Warfare). He is a distinguished graduate of the U.S. Marine Corps Command and Staff College.

Dr. Britta Hale currently serves as the Director of the Implementing Technological Change program and leads Applied Cryptologic Engineering (ACE) at the Naval Postgraduate School under the U.S. Department of Defense, in addition to serving as a researcher and Associate Professor within Computer Science. Her research areas include cryptography, quantum resilience, unmanned system security, space system security, and security within constrained and denied environments. In addition to her work in cryptography, Dr. Hale has published multiple articles on security in systems engineering, and her work on critical infrastructure security includes facilitating training exercises in many countries. Prof. Hale holds a PhD from the Norwegian University of Science and Technology. She is an active member of the Internet Engineering Task Force (IETF) and has previously served on the Board of Directors for the International Association of Cryptologic Research.

The psychosocial-technical security challenges of the Maritime -Space Surveillance (MSS)

by Bruno BENDER[1], Kitty Kioskli[2] and Nineta Polemi[3]

Abstract

In this short paper, we review some of the new challenges and we provide proposals regarding the security of the Maritime Space Surveillance Systems (MSS). The enhanced MSS as AI systems bring new challenges, which are not only technical but also cognitive, behavioural and social that have catastrophic impact to maritime operations and naval warfare. Existing MSS-AI products are assessed, their limitations are identified and proposals for further enhancement are provided in this paper based on behaviour modelling and enrichment of data sources. Human AI Interaction (HAI) challenges in the maritime surveillance operations are also presented.

Introduction

Maritime surveillance plays a crucial role in various areas such as military operations, pollution prevention, combating illegal fishing, search and rescue (SAR) operations, and detecting illegal activities. These operations heavily rely on space-based technologies, information, and services. The primary source of data is the Automatic Identification System (AIS), which is supplemented by radar, imagery, and electromagnetic interceptions:

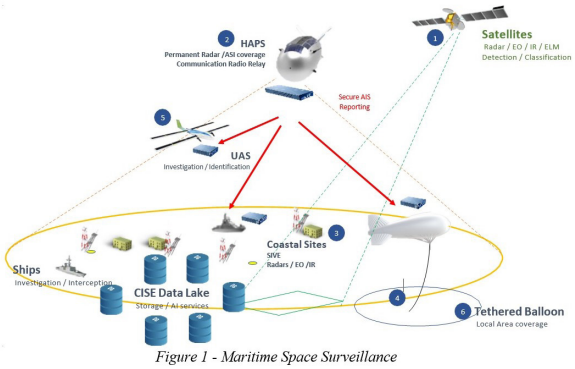


Figure 1 - Maritime Space Surveillance

[1] Athanor Engineering, 21 rue Bargue, 75016 Paris, France
[2] trustilio B.V., Amsterdam, Netherlands
[3] Department of Informatics, University of Piraeus, Piraeus, Greece

However, space is threatened by a variety of threats, e.g. cyber, physical, technological (AI, IoT, satellite) , environmental, business (e.g. espionage), human (see Fig. 1) with catastrophic impact to the maritime surveillance efforts and consequently to the security of the maritime ecosystem.
The attacks in the maritime space surveillance technologies (e.g. GNSS-R, Sat-AIS, GPS, navigation satellite systems) and services (e.g. Galileo) are emerging, especially after the Ukraine war.
It is most important. as outlined in the European Union Maritime Security Strategy (EUMSS), the security of the maritime space surveillance systems since the threat landscape is complex:

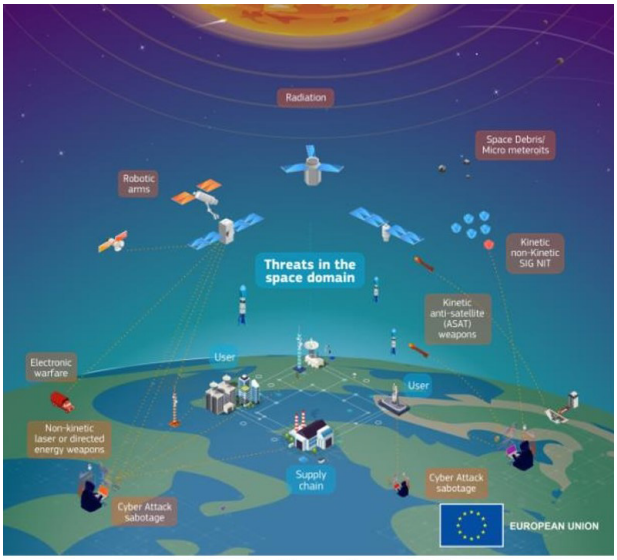


Figure 2 - Space threats [1]

The complexity and interconnection of various entities (e.g. critical infrastructures, space vessels, control centers) in the space environment reveal supply chain threats that propagate in the space domain.

Policies and Initiatives

Since 2010 The European Maritime Security Agency (EMSA) as a key user of satellite data, including AIS and the European Space Agency (ESA) as the key satellite data provider have set an agreement for ensuring the safety of the European maritime ecosystem. In 2021 EMSA and ESA deepened their collaboration for ensuring cyber resilience and strengthen their collaboration with all EU cybersecurity stakeholders e.g. ENISA, Eurocontrol, EDA. National EU efforts are increasing in space security e.g. in 2022, the German Federal Office for Information Security (BSI) published recommendations online on the subject of “Cyber Security for Air and Space Applications”.

There are various civilian standards (e.g. ISO2700x series, NIST 800-30, IMO-BIMCO) and research tools (e.g. CYSM, MITIGATE, CYRENE) for assessing and managing maritime cybersecurity risks. However, these efforts need to be adopted to maritime space surveillance systems and develop risk management tools addressing the requirements and specificities of these systems. In fact, innovative tools are needed for assessing, testing and validating the security of the maritime space surveillance systems against all types of threats and attacks; to provide a dynamic threat intelligence repository, a bundle of configurable risk and conformity assessment methodologies and a collaborative environment for information sharing.
The advanced risk management systems need to be compliant with cybersecurity standards (e.g. ISO 27001, ISO27005, ISO18045, ISO 15408), space and maritime standards and policies (e.g.EU Space Strategy for Security and Defence) imposed by various organisations (e.g. EDA, ESA, IMO, ENISA, EMSA). Additionally, automated workflows need to be designed and implemented encapsulating existing vulnerability assessment and penetration testing tools that will inspect the security and quality of space and maritime software. Enhanced methodologies and routines need to be combined in an effective and efficient manner providing integrated and transparent self-management capabilities as a service, which will be fully customizable depending on the maritime space surveillance technology provider. Training to maritime and space operators, practitioners and stakeholders is necessary to ensure secure communications and trustworthy surveillance capabilities and to accommodate technological advancements to manage security incidents in the cyberspace that impact the maritime operations.

Challenges and Proposals

The evolution of the maritime-space surveillance systems (MSS) is to become AI -systems that their trustworthiness needs to be ensured i.e. they need to behave within specified norms, as a function of the following characteristics: Technical (e.g. accuracy, robustness, reliability) Socio-technical (e.g. explainability, managing bias, transparency, security, privacy), and Guiding Principles (e.g. accountability, reliability, environmental well-being, diversity, fairness, traceability). Holistic risk assessment methodologies are needed and new scales and measurements for estimating socio-technical threats, vulnerabilities and risks.
The requirements to enhance MSS by applying algorithms for Behaviour Analysis is recognised in naval warfare. Multiple companies and countries have already developed solutions encompassing the needs of Navies, maritime security agencies and private companies.
We propose the use of the most advanced algorithms developed and used for maritime surveillance based on geographic, analytical and cognitive/psychological learning models to support the fusion, modelling and implementation of pattens of life and behavioural analysis; This encompasses:

- The review of OSINT data sources and existing

cross-sectorial databases;
- A layered approach allowing unlimited patterns of activities to be implemented as multiple sources interacting together;
- The possibility to store, to extract and to display key operational information and anomalies (in particular due to spoofing or jamming).

Our methodology proposes to detail an innovative and disruptive development based on the exploitation of weak signals and discrepancies with the well-known patterns of activities observed normally. The next Figure summarizes main steps that our proposed methodology follows based on data modelling and analysis:

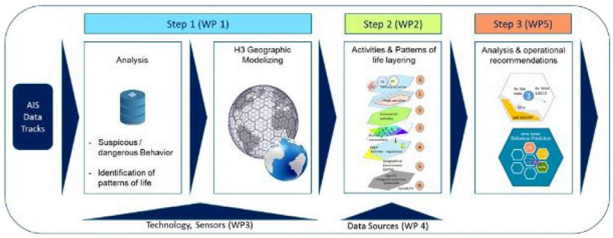


Figure 3 - Methodology

Interviews with OSINT specialists operating on the Ukrainian conflict, vendors and end-users (e.g. MARCOM, EMSA, EFCA, FRONTEX, SATCEN) could complement this methodology and improve the quality of the recommendations on tools allowing to detect incidents on GNSS and AIS contributing to situational awareness.

A documentary research has already identified sources and products (Annex A). For each of them, it will detail the operational added value and compare them to identify the leading products. However, these products are limited in using only declarative data (AIS data presently) and expensive satellite data. Indeed, today maritime stakeholders are mostly limiting themselves to non-reliable AIS and limited imagery data in their artificial intelligence (AI) developments to manage situational awareness. Even though extending its range to satellite imagery or radars, new sensors operated by future platforms (e.g. robotised "Cubesats") should allow end-users to extend their information capacities and improve the level of reliability and cybersecurity.

Further challenges in this AI era include: testing the cognition and perceptions aspects of how maritime operators can use AI tools (e.g., robots, downs) to improve maritime surveillance, cybersecurity practices and cybersecurity defenses. Human AI Interaction (HAI) in the maritime surveillance operations need to be further studied. The efficiency of the decision-making tasks when various HAI factors take place during an incident is one of the issues to be studied. For example, operators switching tasks with the AI system/robots, integration of information, belief of replacing their jobs, confidence that the infrastructures are appropriate, situational awareness HAI issues, social acceptance (when operators and AI systems need to communicate with more people), automation bias, level of trust between the teammates (operators and robots).

Behavioral change processes to improve the effectiveness and acceptance of HAI interaction are often neglected even though research has shown that behavioral

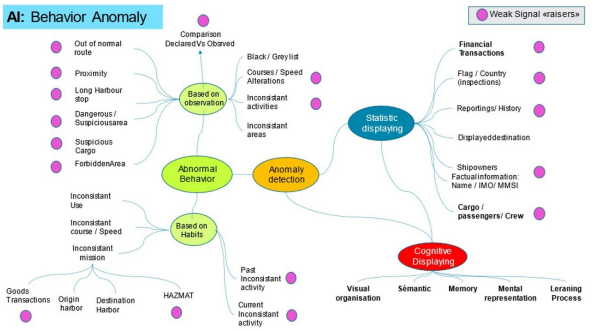


Figure 4 - Behaviour Anomalies Map

interventions are useful in meeting long-term goals. The cause of the avoidance of behavioral change processes lies on the facts that they are considered value-driven and are not easily implemented in models, compared to technological advancements. The following Figure is a taxonomy of anomaly behavior patterns:
We need to further study specific behavioral patterns, psychological, physical, societal and cognitive characteristics, capabilities and motives of the attackers in the maritime surveillance sector. Appropriate psychosocial-technical mitigation actions need to be identified according to the type of attackers in order to influence the attacker's decision-making during the attack and increase the effort and resources necessary to conduct attacks.

Conclusions

The MSS systems have entered a new phase, gradually implementing AI algorithms and models. Technical, behavioral and socio-technical challenges need to be resolved in order the MSS-AI systems to enhance the effectiveness, safety and reliability of the maritime operations and naval warfare.

Annex A. – List of identified solutions and vendors

Data / AI solution Vendors

- Vesselfinder
- Earthcube /Pregilens/Unseenlabs/Hawkeye 360
- MarineTraffic / FleetMon / Vessel Finder / CruiseMapper / VesselTracker
- Global Fishing Watch
- Windward
- AdrenaShip
- Cencoos
- Sea-Routes
- Shone
- Seavision

Vendor	Type	Country	Data sources (satellite constellations)
Preligens	Analyse de données	France	Multiple aquisitions / Copernicus
Astro Digital Inc.	Analysis	USA	Landmapper-BC 1 (Corvus-BC, Perseus-O), Landmapper-BC 2 (Corvus-BC, Perseus-O), Landmapper-BC 3 (Corvus-BC-C, Perseus-O), Landmapper-BC 3v2 (Corvus-BC, Perseus-O, Corvus BC3), Landmapper-BC 4v2 (Corvus-BC4 v2, Perseus-O), PALISADE, Landmapper-BC 5 (Corvus BC5, Corvus-BC, Perseus-O)
BlackSky Global	Analysis	USA	BlackSky Global
Deimos Imaging	Analysis	Spain	Multiples, voir source
Hexagon Geospatial	Analysis	USA	Sentinel 1 (Sentinel-1A, Sentinel-1B) et Sentinel 2 (Sentinel-2A, Sentinel-2B)
SI Imaging Services (SIIS)	Analysis	South Corea	Korean Multi-Purpose SATellite (KOMPSAT-2, -3, -3A, -5, -6, -7)
HEAD Aerospace Group	Analysis	USA	Multiples "Skylwalker constellation" : Superview (4 x VHR EO), Jilin-1 (19 x VHR EO, 2 x MRO, 1 x VideoSat), GaoFen (3 x VHR EO, 5 x MRO, 1 x C-Band SAR, 1 x Geo EO, 1 x Hyperspectral), CBRERS (1 x MRO), ZY Tri-Strereo (2 x MRO)
Beijing Space View Technology Co., Ltd. / SpaceWill	Analysis	China	GF-2, GF-1, ZY-3, HJ-1A & B, SuperView 1A, 1B, 1C, D, WorldView-1, -2 , -3 ; GeoEye-1 ; QuickBird ; Ikonos ; Korean KOMPSAT-2, -3, 3A, -5 ; ALOS ; Deimos-1, -2 ; KazEOSat-1
Beijing Space Eye Innovation Technology Co., Ltd	Analysis	China	Tianhui TH-01 (1A, 1B, 1C) et TH-02 (TH 2-01A, TH 2-01B) ; ZY-3, GF-1, GF-2
Descartes Labs	Analysis	USA	SPOT 6&7, Pleiades A&B, NAIP, Texas Orthoimagery Program
Planet	Analysis	USA	Flock, RapidEye, SkySat

Airbus DS Geo)	Data provider	Europe	Pléiades
Satellogic	Data provider	Argentina	Aleph-1 (ÑuSat)
Axelspace	Data provider	Japan	GRUS
IcEye	Data provider	Finland	ICEYE-X1 à X-10
DINAMIS (commercial : ADS)	Data provider	Europe	SPOT 6 & 7
EOS	Data provider	USA	Pléiades 1 (1A,1B), SPOT-5, SPOT 6,7, KOMPSAT-3/3A/-2, SUPERVIEW-1
Maxar (DigitalGlobe)	Data provider	USA	Early Bird, Quick Bird, World-View 1 à 4, WorldView-Scout (2019) & Legion (2021)
Hera Systems	Data provider	USA	Hera-1 (1HOPSat TD, IHOPSAT-TD, 1st-generation High Optical Performance Satellite)
Planet Labs	Data provider	USA	Planetscope (144), SkySat (21)
RESTEC (Remote Sensing Tech Center)	Data provider	Japan	ALOS-2 / PALSAR-2
Int. Space Tech CJSC	Data provider	Biéolorussia/Russia	BelKa 1, 2 (2023)
21st Century Aerospace Tech Co. Ltd	Data provider	China	Beijing-1, TripleSat Constellation (3)

EU projects

- EFFECTOR (2020 - Ongoing) - End to end Interoperability Framework For MSA at StrategiC & TacTical OpeRations
- TENSOR (2016) - Retrieval & Analysis of Heterogeneous Online Content for Terrorist Activity Recognition
- CLOSEYE (2013) – Exploitation of Satellite imagery
- PERSEUS (2011) - Protection of EU seas & borders through intelligent use of surveillance

As current reserve officer and independent expert, Bruno BENDER acted as national cybersecurity coordinator for the Maritime sector in France as the chairman of the EU Coastguards Functional Forum Cybersecurity working group and is currently Chairman of the NATO maritime C3 capability team (MC3CaT).
On behalf of the Prime Minister he managed a global project from 2018 to 2020 conducting to develop a maritime cybersecurity strategy and installing a coordinated governance between pub-lic administrations and private actors in the maritime domain. In 2019, he contributed to imple-ment a national cybersecurity governance and shared capacities to the benefits of the maritime actors.

Dr. KittyKioskli holds a B.Sc. in Social Anthropology from Panteion University, an M.Sc. in Health Psychology from City, University of London, and a Ph.D. in Health Psychology from King's College London. Her Ph.D. was fully funded through a nationally competitive fellowship from Diabetes UK. Currently, Dr. Kioskli works as a Research Fellow at the University of Essex and as a Project Manager at Gruppo Maggioli, focusing on digital health and cybersecurity. Additionally, she is the CEO of 'trustilio,' a start-up consultancy providing services in cybersecurity, behaviour change, business, and research innovation. Dr. Kioskli is a certified lead auditor on Information Security Management Systems (ISO 27001:2022).

Nineta Polemi is a cybersecurity professor at the University of Piraeus in the Department of Informatics and CTO/Co-Founder of trustilio BV. She served (2017-2020) as a Programme Manager and Policy Officer in the European Commission DG (CONNECT H1 Unit entitled 'Cybersecurity Technologies and Capabilities'). Her cybersecurity expertise includes maritime security, operational risk/conformity assessment, security management, supplychain security, threat intelligence, and AI trustworthiness. She obtained her Ph.D. from The City University of New York (Graduate Center). She held teaching and research positions at The City University of New York (Queens & Baruch Colleges), State University of New York (Farmingdale), Technical University of Denamark, and Université Libre de Bruxelles (ULB)-Solvay Brussels School.

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

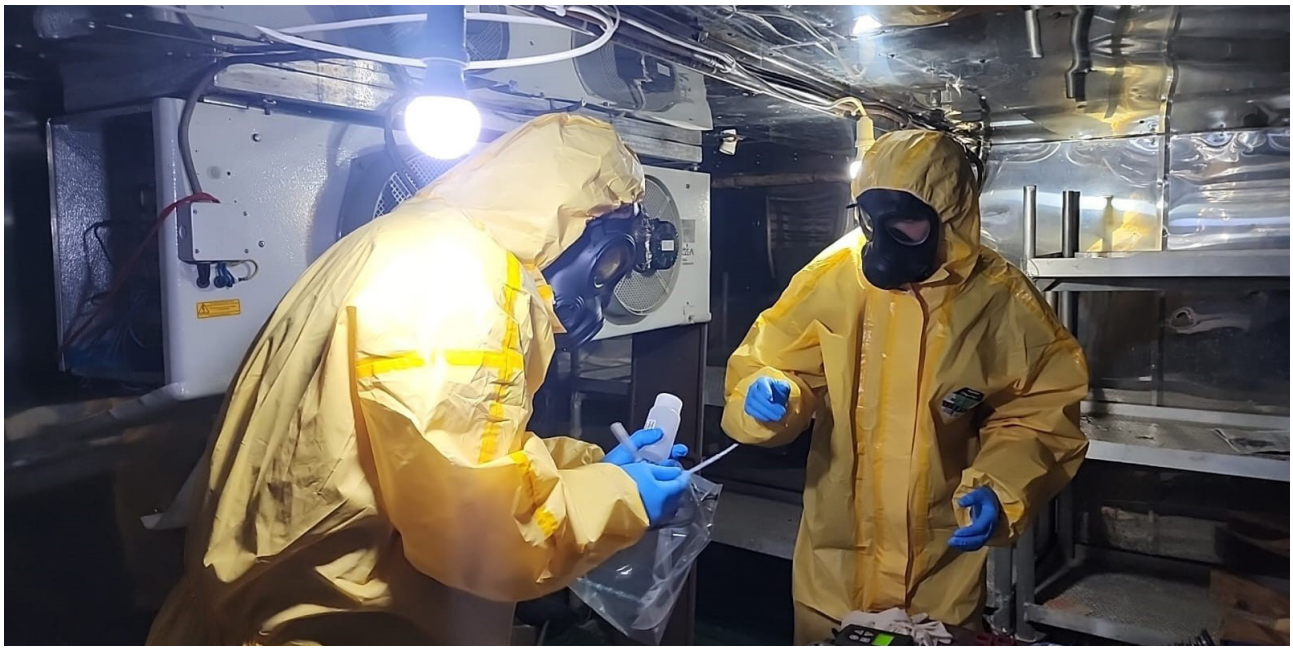
From 12th to 23rd of February 2024 the Resident Courses 2000 “Boarding Team Theoretical Issues” and 3000 “Boarding Team Practical Issues” were conducted in tandem at NMIOTC premises.

Visit of Austria and Greece MoD Delegations to NMIOTC

On Thursday, March 24th, 2024, a delegation from the General Directorate of National Defence Policy and International Relations (GDNDPIR) headed by H.E. Ambassador Michel Spinellis, General Director of National Defence Policy & International Relations (GDNDPIR), Hellenic Mod and a delegation from the Federal Ministry of Defence of Austria headed by Dr Arnold Kammel, Secretary General & Defence Policy Director, Austria MoD, visited NMIOTC.

Course 6000 “WMD in MIO”

From 1st to 5th of April 2024, the NMIOTC Course 6000 “Weapons of Mass Destruction in Maritime Interdiction Operations (WMD in MIO)”, was conducted at NMIOTC premises.



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

From 8 to 12th of April 2024, the Course 29000 “Detection and Identification of WMD (CBRN Materials) in Maritime Interdiction” was successfully conducted at the NMIOTC premises.

Course 27000 “Maritime Sniper Course”

From 8th to 19th April 2024, the NMIOTC Maritime Sniper Course was conducted at the Centre’s premises and in the broader area of Chania, Crete.

NSO ‘NATO Maritime Operational Law Course’ takes place at NMIOTC

The NATO School Oberammergau (NSO) “Maritime Operational Law Course” was conducted from 27th to 31st of May 2024 at the NMIOTC premises, in cooperation with the United States Naval War College (USNWC), the NATO’s Centre of Excellence for Operations in Confined and Shallow Waters (CSW CoE) and the NMIOTC.

JCBRND-CDG / Training and Exercise Panel Spring Meeting

From 10th to 14th of June 2024, NMIOTC hosted the Spring Joint Chemical, Biological, Radiological and Nuclear Capability Development Group / Training and Exercise Panel (JCBRND-CDG/TEP Meeting.

Visit of American Hellenic Institute Foundation (AHIF)

On Friday 21st of June 2024, a delegation from the American Hellenic Institute Foundation (AHIF), consisting of the President Mr. Nick Larigakis, twelve students and three escorts, visited NMIOTC during their 16th Annual College Student Foreign Policy trip to Greece.

2nd Meeting of theMilitary Committee Maritime Standardization Board (MCMSB) 2024

From Tuesday, July 2nd to Thursday, July 4th, Military Committee Maritime Standardization Board's (MCMSB) 2nd (away) Meeting 2024, chaired by NSO (NAVAL) and hosted by Hellenic Navy, was held at the Centre's premises.

8th NMIOTC Conference on Cyber Security in Maritime Domain

From 18th to 19th September of 2024, the 8th NMIOTC Conference on Cyber Security in Maritime Domain took place at the Centre's premises. It was attended by more than 120 participants from 30 Nations, representatives of National and International Organizations, academic community, the maritime private sector and shipping industry.

JCBRND-CDG / Training and Exercise Panel Spring Meeting

From 10th to 14th of June 2024, NMIOTC hosted the Spring Joint Chemical, Biological, Radiological and Nuclear Capability Development Group / Training and Exercise Panel (JCBRND-CDG/TEP Meeting.

Course 16000 “Maritime Aspects of Joint Operations”

From 7th to 11th of October 2024, the NMIOTC Resident Course 16000 ““Maritime Aspects of Joint Operations”, with support from MARCOM HQs, HNDGS, NRDC-GR and the Hellenic Navy, was conducted at the Centre’s premises.

Course 25000 “Drafting Production and Maintenance of NATO Standards”

From 7th to 11th of October 2024, the NMIOTC Resident Course 25000 “Drafting Production and Maintenance of NATO Standards”, with support from NATO Standardization Office, Allied Command Transformation, HNDGS and Defense Standardization Advice, was conducted at the Centre’s premises.

Course 31000 “Harbour Protection and its relation to MIO”

From 7th to 11th of October 2024, the pilot iteration of the Course 31000 “Harbour Protection and its relation to MIO”, with support from Bundeswehr Technical Center for Ships and Naval Weapons, Maritime Technology and Research (WTD-71) and NATO CoE CSW, was conducted at the NMIOTC premises.

Pilot Course 24000 “Building Up Interoperable Capabilities for NATO Ops & the Role of MIO”

From 14th to 18th of October 2024, the pilot iteration of the Course 24000 “Building Up Interoperable Capabilities for NATO Ops and the Role of MIO” was conducted at the NMIOTC premises.

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

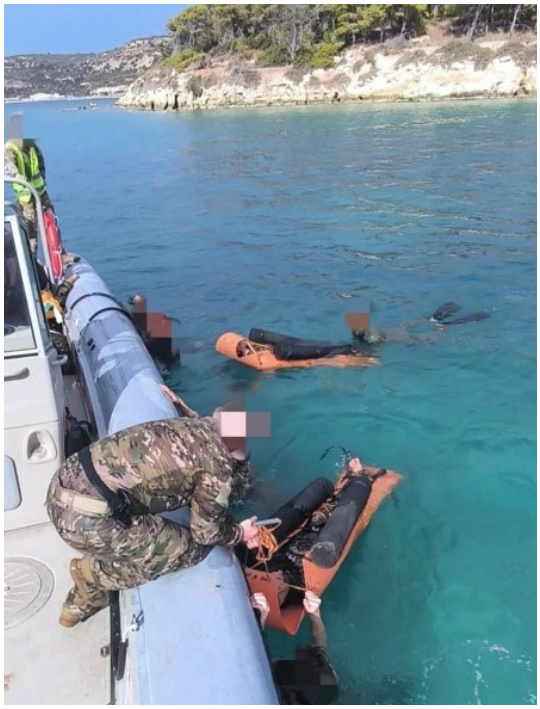
From Mon 21 Oct to Fri 08 Nov 24 a three (3) week Tailored Training package in the field of Contemporary Maritime Interdiction, was provided to 19 members of the Mauritanian (MRT) Navy, in support of NATO’s DCB for MRT. The modular structure of the activity included theoretical and practical training on Visit Board Search and Seizure (VBSS), countering Weapons of Mass destruction (WMD), Countering Improvised Explosive Devices (IEDs), First Aid / Medic in a Combat environment, fundamentals on biometrics and other relevant related topics. The Maritime Security Initiative has the aim of enhancing Mauritania’s Maritime Security Capacity, in a whole-of-government approach, to protect Maritime borders from various threats, including Counter Terrorism and Irregular Migration.

Activation of NMIOTC Training Platform HS LYKOUDIS

NATO Maritime Interdiction Operational Training Center proudly announces the activation of its latest training platform HS LYKOUDIS, with the invaluable support of the Hellenic Navy General Staff and the Souda Naval Base. Along with 2 new classrooms (isoboxes) in the adjacent training area, with a capacity of 18 persons each, the new platform will enhance NMIOTC's capabilities to deliver cutting-edge training for maritime interdiction, in support of global security efforts.

Course 21000 "Medical Combat Care in Maritime Operations"

From the 4th to 14th of November 2024, the Resident Course 21000 "Medical Combat Care in Maritime Operations" was conducted at the NMIOTC's premises.



Training of SNMCMG2
26 - 27 February 2024

JALLC LL POCs Course
16 - 18 July 2024

USMC training in NMIOTC, during Exercise KRAKEN
22 - 23 July 2024

Training of DEU K9 Dogs
7 July 2024

Training of 546 Airborne Battalion GRC Army
21 - 25 October 2024

Training of RS F221 Regele Ferdinand
4 - 8 November 2024

Visit ofCOM SNMG2, Rear Admiral Pascuale Esposito
19 January 2024

Visit of Supreme Allied Commander Transformation (SACT),
General Philippe Lavigne
11 March 2024

Visit of European Union Ambassadors
19 April 2024

Visit of the Defence Attache of Australia
23 May 2024

Visit of the Diplomatic Academy
11 June 2024

Visit of the Defence Attaché of India
9 September 2024

Visit of U.S. Congress STAFFDEL
12 October 2024

Visit NATO Parliamentary Assembly
15 October 2024

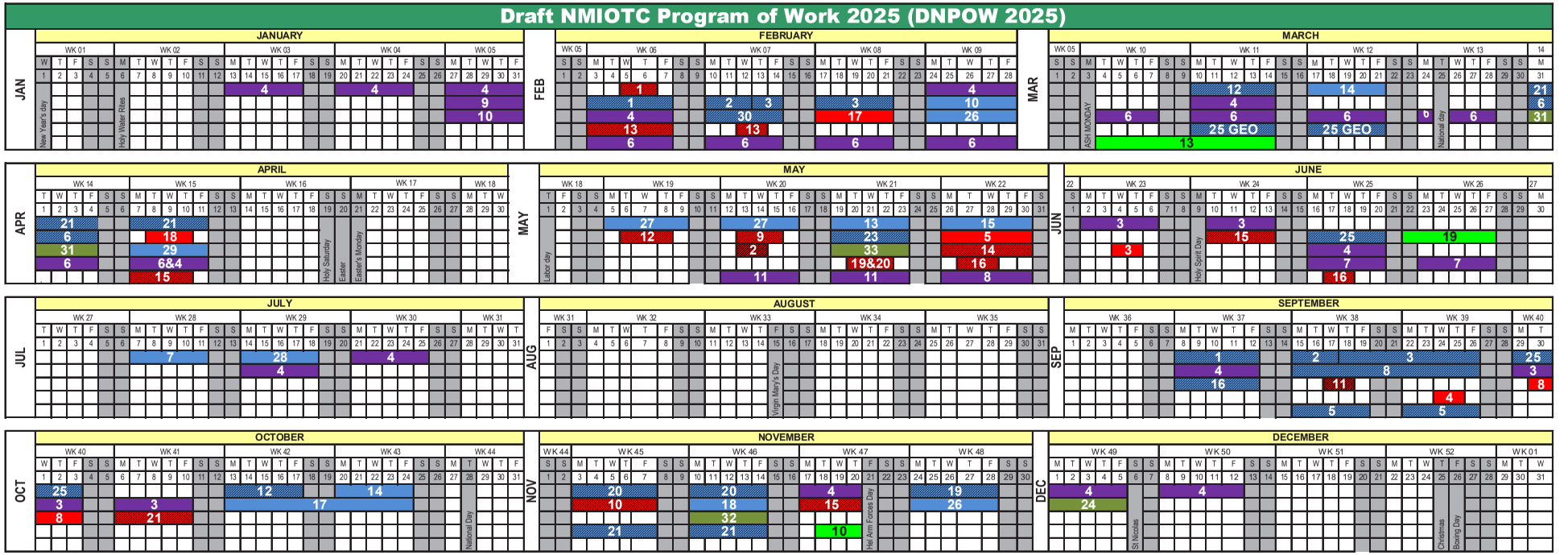
COM NMIOTC in American University in The Emirates
12-13 November 2024

Visit of NAC Political Committee
22 November 2024

COM NMIOTC participation in 'NATO Talk' in NIRC - Kuwait
8-9 December 2024

Visit of the Chief of the Naval Staff of the Royal Saudi Naval Forces (RSNF)
18 December 2024

Draft NMIOTC Program of Work 2025 (DNPOW 2025)



COURSES (ETOC ID.)

1. Course 1000 - Command Team MIO Issues (MOP-MO-31201)
2. Course 2000 - Boarding Team Theoritical Issues (MOP-MO-51203)
3. Course 3000 - Boarding Team Practical Issues (MOP-MO-41205)
4. Course 4000 - MIO Final Tactical Exercise (MOP-MO-41207)
5. Course 5000 - Maritime Operational Terminology Course (MOP-MO-11208)
6. Course 6000 - Weapons of Mass Destruction in MIO (MOP-MO-31209)
7. Course 7000 - MIO in support of Counter Piracy and Armed Robbery at Sea Ops (MOP-MO-41210)
8. Course 8000 - C-IED Considerations in Maritime Force Protection (IED-ED-31679)
10. Course 10000 - MIO in Support of Countering Illicit Trafficking at Sea (MOP-MO-32012)
12. Course 12000 - C-IED in MIO (IED-ED-31904)
13. Course 13000 - Command Team Issues in MIO in support of International Efforts to Manage the Migrant and Refugee Crisis at Sea (MOP-MO-3215)
14. Course 14000 - Maritime IED Disposal (IED-ED-32008)
15. Course 15000 - Migrant Handling Team Issues in MIO in support of International Efforts to Manage the Migrant and Refugee Crisis at Sea (MOP-MO-36
16. Course 16000 -Maritime Aspects of Joint Operations (MOP-MO-22078)
17. Course 17000 - Train the Trainers Technical Instructor (ETE-IT-34432)
18. Course 18000 - Maritime Biometrics Collection and Tactical Forensic Site Exploitation (MOP-MO-22
19. Course 19000 - Cyber Security Aspects in Maritime Operations (COP-CD-22104)
20. Course 20000 - MIO in Support of Managing Perilous Security Incidents on Coastal Critical Sites (SC
21. Course 21000 - Medical Combat Care in Maritime Operations (MED-MS-34411)
23. Course 23000 - WIT Supplement in Maritime Operations (IED-ED-35437)
24. Course 24000 - Building Up Interoperable Capabilities in support of MIO
25. Course 25000 - Drafting, Production and Maintenance of NATO Standards Course (ETE-IT-35477)
26. Course 26000 - Tactical Emergency Care for Maritime First responders in Maritime Operations (MED-MS-35537)
27. Course 27000 - Maritime Sniper Course (SOF-SO-35603)
28. Course 28000 - Radiological Search in Maritime Environment (WMD-CD-35614)
29. Course 29000 - Detection and Identification of Weapons of Mass destruction (CBRN materials) in Maritime Interdiction (WMD-MD-35660)
30. Course 30000 - NATO Identity Intelligence Analyst in a Complex Environment Course (TBD)
31. Course 31000 - Harbor Protection and Its Relation to Maritime Interdiction Operations
32. Course 32000 - Maritime Interdiction Operations in Maritime Oil and Gas Assets
33. Course 33000 - Counter Terrorism at Sea with MIO

EVENTS

1. NAB (NMIOTC)
2. NCB (HNGS)/ACT
3. NMIOTC Annual Conference
4. NMIOTC Cyber Security Conference
5. UPX Training
6. Cyber Operations Annual Discipline Conference
7. Cyber Gordian Knot (TBD)
8. ACTF meeting
9. Multinational Solution and Synchornization Conference
10. Steadfest Interest-26-2 Humint Part-CPTA-M
11. IAMD COE Conference
12. 2025 NATO Enterprise Cybersecurity Conference
13. Re-Accreaditation Process
14. NATO Maritime Operations Law Course
15. IAMD COE CET-P 2025
16. MARCOM MACA Conference
17. CTRC MEETING TBC
18. ASAB meeting 8 - 10 April 2025 **TBC**
19. NOSP 25 - MPC
20. IC WG
21. MILMED COE **LLIB TBC**

EXERCISES / METTs

1. CUTLASS EXPRESS METT (TBC)
2. SEA SHIELD METT (TBC)
3. ADRION METT (TBC)
4. SEA BREEZE METT (TBC)
5. BREEZE METT (TBC)
6. EXERCISE MARSEC (TBC)
7. NORTHERN SPIRIT (TBC)
8. PHOENIX EXPRESS METT (TBC)
9. OSG FOCOPS METT (TBC)
10. NIRIIS (TBC)
11. DYNAMIC MESSENGER (TBC)
12. NIRC (TBC)
13. ARIADNI
14. NOBLE DINA (TBC)
15. MAURITANIA METT (TBC)
16. ADRION CAX (TBC)
17. AEOLUS CBRNEX (TBC)
18. EXERCISE OBANGAME EXPRESS (TBC)
19. TOXIC BAY-25 (TBC)

TAILORED TRAININGS

1. US Teams
2. HCG Teams (TLCC)
3. DEU Teams
4. GRC Teams
5. GRC Naval Units
6. MFEA USV Course
7. BEL TT
8. US MARINES BALTOPS TT
9. CAN ANTU TT
10. C6F Cert PKN
11. NLD FMS

Updated 27 Nov 2024

Training Courses | Tailored Trainings | NATO Events | Exercise / MTTs | Trial Courses | Events | Naval Unit Training | National Holidays | Available Period for Training | Evaluation of Courses / Maintenance

NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

Phone: +30 28210 85710
Email: studentadmin@nmiotc.nato.int
nmiotc_studentadmin@navy.mil.gr

Webpage: https://nmiotc.nato.int/