9th NMIOTC Conference on Cyber Security in the Maritime Domain
Lt Col (ret'd) Nollag Conneely,
Dinos Kerigan-Kyrou*

***The authors are very grateful to Tanja Geiss, NATO DEEP, Senior Instructional Designer DEEP eAcademy; Aoife Noone, Think Smart Cyber, Ireland; Capt (ret'd) Jamie Redfarn, British Army, The Life Guards Household Cavalry Regiment; Amy Stokes-Waters, The Cyber Escape Room Co. for their invaluable insights and analysis.**

2025 was a critical year for maritime cybersecurity. The vulnerability of military and civilian shipping to attacks from nefarious actors became increasingly apparent. What also became apparent is that cybersecurity - the security of cyberspace - is now directly connected to economic, political, and physical security. Cyberspace is a determining factor for the security of the maritime environment, which in turn impacts the security of NATO, the European Union, and our Allies and Partners across the world.

NMIOTC Commandant Periklis Piyis opened by highlighting NMIOTC's 17 years of excellence - NMIOTC actively supports NATO across the maritime security spectrum. Comdt Piyis stated that the Sea is the basis for prosperity and security; however, the nature of maritime threats evolves - cyber and hybrid threats are now paramount. NMIOTC today educates across *multiple* domains. NMIOTC's contributions include cybersecurity courses, working closely with ACT and SHAPE – scenarios-based training in a multidomain environment. AI [Artificial Intelligence], connected devices, and data are now the fuel of maritime power. The maritime domain is an integration of cyber, digital and maritime. The future requires us to exploit real-time intelligence; and these requirements are being incorporated into NMIOTC's expertise including with drones, emerging technology, and cyberspace situational awareness. Working with industry is vital going forward to ensure cybersecurity in the maritime environment, concluded Comdt Piyis.

Commodore Athanasius Dimitriou, Hellenic National Defence General Staff (HNDGS) stated that cyberspace is now one of the most crucial operational domains. However, reliance on digital systems creates vulnerabilities. Maritime cybersecurity concerns protecting global trade routes and creating resilience; but cyber attacks undermine collective security. To counter these threats cybersecurity education must be integrated with specialised training and knowledge sharing. NMIOTC is at the forefront of the efforts to develop cybersecurity resilience for the maritime environment. Bridging the gap in maritime cybersecurity between the strategic and operational levels is vital, concluded Cdre Dimitriou.

Governor of the National Cybersecurity Authority of Greece, Michail Bletsas emphasised that the Authority is Greece's single point of contact for regulation, compliance, and operations. The requirements of NIS2 [the EU's second Networks and Information Systems Directive] are now mandatory, and the domain is vast - 1,000 and 2,000 entities - anything where a cybersecurity incident causes disruption. (In Greece and the EU we are often efficient in drafting regulations but poor in application, Gov Bletsas stated). The first priority is establishing a clear threat landscape picture; we cannot improve something we can't measure. Most Greek cybersecurity victims are public sector entities; however, they lack specialised personnel. Cybersecurity is a 'team sport'; we have good cooperation between military and civilian sectors in Greece. However, losing staff to the private sector is a problem; we need core public sector cybersecurity expertise. Moreover, cybersecurity challenges are increasingly complex, and the asymmetry between attackers and defenders is growing. Specialised 'hackers' are no longer required to breach defences; anyone can be a cyber-criminal, spy, or saboteur; tools enabling capabilities without expertise - especially using AI - are widely

available online. Indeed, nefarious actors play a numbers game; a 10% success-rate is all that is required. Today we have scam farms in Burma sending persuasive and accurate SMS fraud messages using Large Language Models (LLMs) - even in perfect Greek. People's computers are constantly phished; criminals' targeting is getting extremely good. Indeed nefarious, actors aim to breach your personal email to survey and monitor you. LLMs [Large Language Models - AI that aims to understand large data sets] now generate code; and if LLMs fail they will simply invent! (Gov Bletsas gave examples of lawyers using AI for cases only to discover from the court's judge that their AI produced information is nonsense). Criminals are creating LLM malicious libraries. While AI does indeed help automation we must have humans 'in the loop' - and this is why cybersecurity skills are so vital. Greece is working with regional neighbours, as well as the US to help create a new cybersecurity framework. Flags of convenience make it difficult to ensure cybersecurity compliance, and a ship can be disabled online in the middle of the ocean. It is crucial the collaborative work continues, concluded Gov Bletsas.

Marco Criscuolo, NATO Digital Staff stated that cyber and digital threats are now a key focus for multidomain operations, including for research into autonomous shipping with NATO Task Force X. We operate in a complex, dynamic and contested environment where emerging and disruptive technologies integrate into Command, Control, and Communications. 'Traditional' security for people, processes and technologies is no longer effective. Cybersecurity can never be 100% and aiming for this can be dangerous, concluding that 'perfect cybersecurity' should not become 'the enemy of good'.

Santiago Encabo, Head of Unit at the EU Maritime Safety Agency (EMSA), stated that cybersecurity is a growing concern and a reality directly affecting everyone. Cooperation is essential, as those coordinating attacks are advanced and persistent. Main objectives are: learning, awareness, and implementation of state-of-art solutions. EMSA has developed a cybersecurity taskforce. Every ship should have a cyber plan; however, EMSA inspections reveal this is often not the reality. Regarding autonomous ships - EMSA dislikes the term 'autonomous', preferring 'ships with high degrees of automation / autonomy' [i.e. it is unlikely ships will be fully autonomous]. EU is studying security of increasing navigation automation resulting from increased connectivity. EMSA uses the risk assessment for unmanned aircraft systems as a reference for this process.

Evangelos Ouzounis, ENISA stated that while cybersecurity is the new reality of maritime, many challenges exist. Ports have inadequate numbers of people and insufficient policies to manage cybersecurity. Supervision and resilience challenges are further complicated by low maritime cybersecurity awareness, with ICT [Information and Computer Technology] SCADA [hardware and software to control processes], and IoT [Internet of Things - devices with sensors exchanging data online] complexity. Maritime environment governance is fragmented. Moreover, direct economic incentives to implement effective cybersecurity are lacking (ENISA NIS360 2024 was recommended as a critical document regarding cybersecurity maturity of the maritime sector). Threats are broad including ransomware, ‘hacktivists’ / activists [such as extreme environmentalists], criminals, and nefarious states. Their targets include operators, logistics, ports, ferry operators, and yacht manufacturers. Cyber Europe 2026 - engaging national authorities and cybersecurity Incident Response Teams - is helping cyber-resilience. It is crucial to develop coordinated frameworks for managing EU large-scale cyber incidents. If systems at a port such as Rotterdam are breached, worldwide supply-chains are hugely impacted; cooperation and information sharing between the private sector, governments, and the EU is now essential, due to the evolving, sophisticated threat landscape. Moreover, building cybersecurity skills is vital. ENISA, at the Commission’s request, is working with relevant stakeholders to establish a certification scheme for Managed Service Providers (MSPs). And the European

Cyber Security Challenge to attract more workers and students promotes skill development, collaboration and cybersecurity careers. The Cyber Solidarity Act enables a faster process to engage contractors - due in part to the new Russian threats we face. Private sector collaboration is critical.

Brig Gen Konstantinos Kokodroulis, Assistant Chief of Staff, J6,SHAPE stated Cyberspace Operations are core to Joint, and Multi-Domain Operations. Cyberspace is deeply integrated into all aspects of modern military operations, and can both influence and be influenced by activities in land, sea, air and space (playing a critical role in coordinated military strategies across all areas). In parallel, Cyberspace is not only a military operations domain but deeply integrated into critical national infrastructure functions, economic activities, governance, and national security. Four key activities represent NATO's core areas of Cyberspace Operations:

a. Comms and Info Systems Operations (CISOPS).
b. Cyber ISR (Intelligence, Surveillance, and Reconnaissance).
c. Defensive Cyberspace Operations (DCO)
d. Offensive Cyberspace Operations (OCO).

Offensive effects are offered by Nations voluntarily, through SCEPVA [Sovereign Cyber Effects Provided Voluntarily by Allies]. In Multi-Domain Operations, all four activities are integrated with one another and with other domains (i.e. not 'standalone'). Cyberspace Situational Awareness (CySA) and Electromagnetic Operations (EMO) support and enable NATO's cyberspace operations. SHAPE J6 will continue to support all training linked with Cyberspace, concluded Brig Gen Kokodroulis.

Panel Discussions

Cyber Resilience in the Maritime Sector: Anchoring Security in an Evolving Threat Landscape.[1]

The panel emphasised that naval threats are now hybrid, and cyber monitoring aboard is crucial. Cyber resilience must be integral to processes, people, systems, and fleet management. Thales emphasised that in the new digital battlespace cyberattacks can cripple ships and missions - without a shot fired. In 2024 over 1,800 ships were targeted. The results of these attacks are visible (e.g. a direct attack on a ship or its systems), and 'invisible' (i.e. long-term and not immediately apparent), including adversary access to classified information and long-term security consequences to the EU, and NATO. Thales emphasised that enabling technology is key to identifying and managing these threats.

Navigating Maritime Cybersecurity: Confronting Emerging Threats and Operational Challenges.[2]

The panel clarified the difference between GPS spoofing - where GPS is mimicked - and jamming - where 'noise' is created. The example given was the MSC *Antonia* where system spoofing caused grounding near the Eliza Shoals off Jeddah. The security, military, and economic threats and consequences of such incidents can be catastrophic. Belgium's maritime security as an 'energy island' was emphasised, comprising critical shipping lanes and pipelines. Threats originate from organised crime, state actors, terrorists and extreme protestors. It is critical to develop partnerships and information sharing between the civilian and military.

1 Ioannis Kechaoglou, Naval Group 'Building Cyber-Ready Naval Forces'; Stephanie Tonneau, Thales, 'Cyber Resilience in Naval Digital Transformation: Securing Maritime Defense Ecosystems'; Giuseppe Laurenza, E-Phors, 'Maritime Cybersecurity Platforms'. Moderator: Dinos Kerigan-Kyrou, NATO DEEP.

2 CDR Georgios Lykos, NATO ACT, 'Strengthening NATO’s Maritime Cyber Security Training'; Ioannis Pantazis, NCI Academy, Capt Yann Bozec, MARCOM, 'Operationalising maritime cyberspace'; Peter Schellaert, Belgian Cyber Command 'Belgian Maritime Cybersecurity landscape'. Moderator: CDR Adam Stojałowski PhD, Polish Naval Academy.

'TTEX Maritime' - a programme assessing civil-military resilience - is a positive example of this development.

Human Capital in Cybersecurity: Building Competence through Training, Education, and Accreditation.[3]

NATO DEEP emphasised holistic cybersecurity. Nefarious actors - criminals, hostile states (such as Russian actions against NATO, the EU, Ukraine and Partner Nations - or indeed by nefarious states harming their own people, such as Myanmar against the Rohingya), utilise cyberspace, directly targeting people. In other words, cybersecurity is about the security of the whole of cyberspace; the failure to understand this and to see cybersecurity only as an 'IT' issue has been detrimental to the online wellbeing and safety of our militaries, governments and people across our Allies and Partners.

The European Security and Defence College (ESDC) stated it employs a holistic approach to cybersecurity, integrating defence and critical infrastructure protection, consistent with the EU Cybersecurity Strategy. Its Cyber Education, Training, Exercise, Evaluation (ETEE) platform advances comprehensive cyber strategies, aligning with ENISA's European Cybersecurity Skills Framework (ECSF) addressing skills gaps. ESDC builds resilience, collaborates with NATO DEEP and global partners, prioritising support for Ukraine's security. A vital partnership with 16 Ukrainian institutions facilitated cybersecurity training for over 700 Ukrainian officials since 2020, significantly bolstering collective cyber threat resilience. Future efforts implementing ECSF will enhance EU-NATO cooperation.

The panel emphasised that cybersecurity also needs to be classified as a maritime safety issue. Finally the panel emphasised the importance of cybersecurity education - e.g. open with Massive Open Online Courses, and utilising technology including Advanced Distributed Learning (ADL) developed by US Dept of Defence and utilised by NATO and PfPC.

Leveraging Advanced Cyber Intelligence to Strengthen Maritime Security Frameworks.[4]

The panel stressed the importance of cyber threat intelligence, documenting challenges and learning from previous cybersecurity experiences. South Korea's CYTUR highlighted growing cybersecurity threats due to the integration of IT and OT (Operating Technology), in naval architecture. The need for a Defense in Depth strategy, and a lifecycle-based approach was emphasised - from initial design to operation. By applying threat modeling techniques to commercial container vessels, 'secure-by-design' principles must be embedded into ship systems, ensuring resilience against evolving cyber threats throughout its decades' long service-life.

Reinforcing the Cybersecurity Framework: Protecting Vital Infrastructure Assets in the Digital Age.[5]

The criticality of the sub-sea cable environment around Africa was underscored. Security challenges increasingly include fragmented governance and foreign interference. Regulatory and complex approval

3 Giuseppe Zuffanti, European Security and Defence College, 'Enhancing Cyber Resilience: The Pivotal Role of the European Security and Defence College'; Dinos Kerigan-Kyrou, NATO DEEP, 'The Misunderstanding of Maritime Cybersecurity - What We Can Learn from NMIOTC and NATO DEEP for a Safer Maritime Environment'; Prof. Yvon Kermarrec, École Navale, 'Maritime cybersecurity 'MOOCs; Dr. Edwin Armistead, Peregrine, 'Cybersecurity Training for Maritime Environment'. Moderator: Luc Hellebooge, Skyline.

4 Arne Asplem, Nordic Maritime Cyber-Resilience Centre, 'Maritime Cyber Intelligence'; Andreas Sfakianakis, ThreatIntel, 'Cyber-Threat Intelligence'; Alexandros Lyginos, Cygnus, 'Enhancing Maritime Cyber-Resilience'; Hyoseok Lim, CYTUR, 'Secure by Design for Naval Ships'. Moderator: Dr. Christina Schori Liang, Geneva Centre for Security Policy.

5 Drs. Susan Henrico, Dries Putter, Stellenbosch University, 'Submarine Cable Security, South Africa Implications'; Prof. Nineta Polemi, Dr Theodoros Karvounidis, University Piraeus, 'EDTs in Maritime Cybersecurity'; Duncan Woodbury, Maritime Hacking Village, 'Hacking Maritime Systems'. Moderator: Rick Siebenaler, Maritime Cybersecurity Institute.

processes for renewing infrastructure decrease security. Critical infrastructure skills, 'smart' cable upgrades, better security at the cable landing sites, and improved regional and global cooperation are needed. The panel discussed opportunities and threats from Emerging Disruptive Technologies (EDTs), including quantum, IoT, AI, 6G networks, and cloud computing, with human factors as the critical determinant of EDT security. Finally, voluntary 'collective' maritime systems hacking was proposed as an effective method to progress and enhance maritime cybersecurity.

Revolutionizing Maritime Cybersecurity through advanced applications: Trends, Risks, and Strategic Integration.[6]

The panel stated that the maritime attack surface increases exponentially, now including above, on, and under the sea, as well as ashore. Cyber-attacks are increasingly sophisticated; however existing tools are reactive - unable to assess threats without disrupting maritime operations. Today 'Decision Dominance' is key; a commander's ability sensing, assessing, comprehending, deciding and acting faster, more effectively than adversaries. Agentic AI - where AI conducts complex tasks with minimal human intervention - was presented as a potential cybersecurity advancement. However, today's AI limitations were highlighted, and it was suggested that active human intervention is likely to be essential for the safety and effectiveness of future AI systems.

Conclusions

A key conference finding is the multi-domain nature of cybersecurity. Cyberspace intrinsically links the maritime environment with air, space, and land.

Capt (ret'd) Jamie Redfarn, who was twice targeted by cyber operations during military deployments (both directly and against the operation), says that direct targeting of people is the primary way nefarious actors breach militaries: "The most successful line of aggression that proficient cyber attackers use is human social engineering. The cyberattacks I witnessed involved blackmail and attempted exploitation of relatives and close friends. With this in mind, it's essential to educate family and those close to you on how to discern what's authentic and what's deception." Technology advances and AI make this challenge more difficult, adding "With increasing voice and video deepfakes this ability is becoming more challenging, and is why human security must be the strongest pillar of cybersecurity." So, not only are military and civilian maritime personnel targeted directly - but also their friends and family are targeted by nefarious actors. These *direct to person cyber threats* have been underestimated in cybersecurity threat assessments; nonetheless, they represent the vast majority of maritime cybersecurity challenges. Aoife Noone, Ireland's leading authority for children and teenagers' online safety agrees stating "Cyber threats - such as sextortion, deepfakes, and online blackmail - increasingly target children as well as adults, and are almost identical in nature. Developing cybersecurity awareness and resilience from an early age is critical. Weak platform controls and technology misuse exacerbate these challenges, making structured cyber-education and mindset training an urgent priority." Therefore *how* we conduct cybersecurity education is critical. Amy Stokes-Waters of The Cyber Escape Room Co. states "The 'phishing training' which we've all had to endure not only doesn't work - it's counterproductive, harming cybersecurity and resilience," adding "Interactivity - where people 'learn by doing' - is essential for effective cybersecurity education and training." Indeed, NATO DEEP - focusing on Professional Military Education with Partner Nations' military academies - combines pedagogy and didactics

6 Dr. Fulvio Arreghini, INFODAS, 'Decision dominance'; Daniele Mancini, Fortinet, 'Proactive Cybersecurity'; Prof. Tejas Patel, DARPA, 'CASTLE'; Prof Angelos Stavrou, Virginia Tech University, 'Agentic AI'. Moderator: Prof. Nikitas Nikitakos, University of Aegean.

(the methods and processes of teaching and learning), with its cybersecurity and hybrid threats education. DEEP's Tanja Geiss states "Different active learning and teaching methods allow military instructors to engage classes in discussions. Different didactical processes allow us to teach cybersecurity - and all military subjects - from multiple perspectives. The use of modern education techniques and training keeps students more engaged in the whole process, making learning more meaningful."

As both NATO NMIOTC and EU EEAS emphasise, maritime cybersecurity threats need to be addressed holistically. Outdated notions of cybersecurity as something that involves only information and computer networks must change. Everyone who works in the maritime environment or its supply-chains is a direct target for nefarious actors online who are increasingly vociferous in their malign activities. Partnerships and multidisciplinary projects are crucial. Maritime cybersecurity and hybrid threats training needs to be continual and interactive - involving everyone in the maritime environment. The 9th NMIOTC Maritime Domain Cybersecurity Conference was an invaluable step forward in achieving these objectives.

Lt Col (ret'd) Nollag Conneely is Director of CompleteGRC, Ireland. Nollag has over 24 years' experience in the Irish Defence Forces serving on intelligence and operational roles in the Middle East, Africa, and the Balkans on UN, NATO, and EU missions. He is a coauthor of the NATO Hybrid Threats and Hybrid Warfare Curriculum, and a graduate of the Irish Defence Forces Joint Command and Staff Course.

Dinos Kerigan-Kyrou, NATO DEEP, Senior Advisor DEEP eAcademy is a Professional Military Education instructor with DEEP serving in central and eastern Europe, the Balkans, and Africa. Between 2017 and 2024 he was responsible for cybersecurity and hybrid threats training on the Irish Defence Forces Joint Command & Staff Course. Dinos is on the Partnership for Peace Consortium (PfPC) Marshall Center Academic Publications Board, and is a founding member of the Cybersecurity Taskforce of the Royal Institution of Naval Architects. He is a NATO Cybersecurity Curriculum coauthor, a consultant at CompleteGRC Ireland, and an advisory board member of the Cyber Escape Room Co. He lives in Co Leitrim, Ireland.