17th NMIOTC Annual Conference Summary Report

The 17th NMIOTC Annual Conference, titled **"Blue Resilience 360°: Securing Maritime Infrastructure in the Era of Multi-Domain Operations,"** convened a diverse assembly of academic, industry, military, and governmental leaders at the Centre's facilities in Souda Bay. In his opening address, the NMIOTC Commandant, Commodore Pavlos Angelopoulos, argued that maritime resilience is no longer a supporting concept but a strategic imperative. This resilience is increasingly contingent upon the ability of NATO and its partners to protect critical maritime infrastructures within a highly evolving and adaptive threat environment.

Within this landscape, the oceans are recognized as layered operational environments extending from seabed to the outer space. This multidimensional reality directly aligns with the doctrine of Multi-Domain Operations (MDO), formulated by Allied Command Transformation, which requires the simultaneous orchestration and real-time fusion of capabilities across five distinct domains: Land, Maritime, Air, Space, and Cyber. By transitioning from traditional service cooperation to this synchronized cross-domain approach, NATO can generate the asymmetric advantages and decisional superiority needed to secure critical maritime infrastructure.

Modern maritime practitioners must now become conversant with the 4th Industrial Revolution, where unmanned systems, artificial intelligence, cybersecurity, and data literacy have become essential components of naval competence. The technical shift in maritime operations is moving from isolated sensor cues toward a persistent "Detect-Fuse-Decide-Act-Exploit" cycle. This evolution is supported by edge technologies, including quantum applications for cryptography and sensing, as well as autonomous vessels operating on all domains. Strategic efforts have already moved from theoretical discussion to practical implementation, exemplified by the establishment of the NATO Maritime Centre for the Security of Critical Undersea Infrastructure in MARCOM. This Centre has achieved a comprehensive mapping of European subsea assets and utilizes MAINSAIL, an AI-based cloud platform, to merge heterogeneous multi-domain data for real-time situational awareness.

For infrastructure resilience, the framework of the 4Ds—Detect, Deter, Defend, Destroy—is coupled with the 2Rs—Redundancy and Repair. Recognizing that approximately 200 subsea cable incidents occur annually, the capacity to repair damage is as critical as the effort to prevent it. Simultaneously, the EU Action Plan on Cable Security focuses on a whole-of-resilience cycle and the establishment of regional hubs, such as the Baltic hub led by the Finnish Coast Guard, to aggregate data across civilian and military sectors.

A significant challenge remains the rise of hybrid threats and the "shadow fleet"—substandard, often flagless vessels that operate outside international rules and can serve as vehicles for environmental damage or covert sabotage. Addressing these threats requires wider cooperation, collective resolve, enhanced technical forensics, improved intelligence fusion, and the ability to attribute hostile actions with confidence.

Building resilient maritime ecosystems requires a genuine partnership model where industry is treated as an essential security partner from the outset. As most critical infrastructure is commercially owned and operated, security in the modern era will be "co-produced" through trust, joint exercises, and shared accountability. Furthermore, NATO's

roadmap toward 2030 aims to institutionalize Cross-Domain Command (CDC), requiring commanders to develop an adaptive leadership style capable of orchestrating military activities in synchronization with non-military activities at scale and speed. Building resilience depends also on educating and continuously training personnel across all domains relevant to the protection of maritime critical infrastructure.

In order for this multi-domain operational dialogue to flourish, it is essential that NATO and all stakeholders sustain continuous and constructive engagement. Discussions emphasized that the complexity and volatility of the international security landscape can only be addressed through the sharing of information and objectives. This collaboration must encompass Allies, intergovernmental agencies, European institutions, international organizations, academia, and the private sector. Such mutual support leads to a better alignment of objectives and the synergy that significantly enhances NATO's capabilities. Furthermore, universal adherence to the United Nations Convention on the Law of the Sea remains the cornerstone of maritime security. By establishing clear jurisdictional boundaries, UNCLOS reduces the legal "grey zones" that bad actors exploit to target infrastructure with impunity. Ultimately, collective intelligence and resolve will determine the ability of nations to safeguard the flows of energy, commerce, and information upon which modern societies depend.