“Charting a New Course: Overcoming Maritime Challenges”
Parklane Resort and Spa – Limassol, Cyprus 27/11/2025

Dear Commissioner of Communications, Mr. George Michaelides,
Dear Ambassador of the State of Israel,
Dear Director General of the Israel National Cyber Directorate,
Distinguished guests,

I am pleased to be here today to address this event that focuses on the recent cybersecurity challenges, opportunities, and technological enhancements that emerge in the maritime domain. The event is co-organised by the Commissioner of Communications and the Shipping Deputy Ministry in collaboration with the Israeli National Cyber Directorate.

Maritime transport is the backbone of global trade since almost 90% of the world’s goods are transported by ships. It is therefore imperative to ensure that all infrastructures that directly or indirectly affect the operations of the shipping industry and the overall supply chain enjoy the highest level of protection. One of the major challenges that the maritime domain is currently facing is the prevention of the continuously increasing cyber aggression and the protection of all its critical infrastructures. I think it is widely recognized that the maritime transport sector is one of the largest and most important international critical infrastructure industries.

Digital technologies are an integral part of the management and operation of numerous systems, critical to ship and port operations, including the functioning and navigation of the ship itself as well as the use of electronic systems to store, process and transmit information to and from ships. However, the use of electronic systems and electronic exchange of information is not limited to the operations and communications between ships, ports, port terminals and ship management companies but is extended to the services provided by the various competent authorities of the states.

Undoubtedly, in our days industries of any type become more vulnerable to cyberattacks as they incorporate more digital technologies in their operations – and the shipping industry cannot be an exception. The growing reliance of modern vessels on automation and the increased usage of electronic systems for navigation and exchange of information between authorities is inevitably exposed to cyber threats. Moreover, maritime companies ashore face increased exposure to cyber-attacks due to their global nature and the wide range of clients, partners,

suppliers, and contractors all over the world that utilize various digital systems forming a complex maritime ecosystem.

Recent cybersecurity studies that focused on the maritime industry showed a significant increase in cyberattacks targeting maritime companies and vessels. It is worth noting that during the last decade we have witnessed many incidents of high profile cyberattacks with severe costs that have highlighted the need for stronger cybersecurity measures.

The secure development of digital infrastructures is therefore essential so that stakeholders and investors can gain the necessary confidence in developing their operations. Appropriate security controls should be implemented to protect information and data pertaining to a ship, its crew, passengers and cargo, as well as company operations. The reason is very simple. The consequences of cyber-attacks can be devastating. I think a sign I see on my way to work every day almost says it all: data leaks can sink ships. And not only. The financial impact can be enormous. Operations could be blocked.

Considering the challenges and the needs of the industry, the Digital Security Authority and the Shipping Deputy Ministry in collaboration with the Israeli National Cyber Directorate took the initiative to organize this event, aiming to bring together the shipping industry of Cyprus and the relevant authorities to discuss about actions that can be taken to protect our industry from cybercrime.

The proposal to explore possible collaborations to establish a regional Maritime Cybersecurity Center of Excellence (MCCE) is completely aligned with our Deputy Ministry's mission to safeguard and further develop Cyprus shipping as a safe, socially responsible and sustainable industry. The proposed collaboration focuses on four main pillars:

- To establish a Maritime Regional Security Operations& Threat Intelligence Center (MRSOC), which will provide services to the maritime industry
- To create an Innovation Center to drive research, innovation, and excellence in the maritime industry
- To establish a training center to provide capacity building
- Cooperation of governmental organizations, cybersecurity, and maritime stakeholders on cyber issues

Ladies and Gentlemen,

The shipping industry realizes the importance of ensuring a high level of protection against cybercrime. At the same time, as regulators, we do acknowledge our duty and responsibility to act proactively to facilitate and support a high level of digital security, thus contributing to the development of the required market environment and trust, to enable progress in the sector. The active implementation of the national strategy on Cybersecurity shows the government's determination to work closely with all stakeholders, to support the maritime sector and to promote positive change and smooth transformation to the new norms.

Concluding, I would like to wish you fruitful and productive discussions that will contribute positively towards building successful collaborations in our maritime ecosystem.

Thank you.