Prepared Remarks of
Christopher Ross
Deputy Head of Unit for Security
European Commission Directorate-General for Mobility and Transport
"Seaport Security Issues"
Hazard Final Conference
Tallinn, Estonia
15 March 2019
(CHECK AGAINST DELIVERY)

Ladies and Gentlemen, distinguished participants to this Conference, I am delighted to be with you today and join this final conference of the Hazard Project. At the outset, I would like to congratulate you for all the good work achieved. It is impressive!

I have been asked to address "Seaport Security Issues", a topic on which I note the project has addressed via several seminars and events, including on cybersecurity in ports.

Against this solid background, I thought it might be useful to highlight a number of maritime security issues with a port nexus which are currently at the forefront of our work with Member States, as well as in close co-operation with the European Maritime Safety Agency.

Specifically, I would like to update you on (1) trends in maritime security inspections, (2) Ferry Security, (3) the growing importance of cybersecurity in maritime, and (4) the EU operational guidelines on Places of Refuge.

First, at the outset, we should recall the importance of maritime security in EU legislation. Of particular relevance is Directive 2005/65 on enhancing port

security and which complements the measures adopted in 2004 in Regulation 725 on enhancing ship and port facility security. The scope of the Regulation was limited to cover security measures on board ships and the immediate interface between ships and ports. Member States committed to these obligations as a priority, which essentially fall under the IMO ISPS (International Ship and Port facility Security) Code, before agreeing to implement further obligations as part of the adoption of the Directive. The Directive complements Regulation 725 by establishing a security system for all of the port area, in order to ensure a high and equal level of security for all European ports serving direct sea-going services.

The scope of application is significant: over 1 200 commercial maritime ports are operated along the 70 000 km of coastline in the European Union, one of the regions in the world with the largest number of ports. Around one thousands of these ports fall within the scope of the Directive, i.e. all ports housing one or more port facilities which are the subject of a security plan (approved under the Regulation).

The procedures for monitoring the implementation of the Directive are carried out during inspections by the Commission in accordance with Regulation (EC) No 324/2008.

1. Allow me to share with you some recent trends we observe from these maritime security inspections, both regarding national administrations and direct inspections of a sample of ports.

Overall, we see a significant improvement over the last years in the level of security coordination among local authorities, port operators and public law enforcement bodies in European ports. The introduction of security measures have also often led to a review of the organisation of ports, such as – for example – the movement and storage of goods, the control of access to different areas of the port or a definition of restricted areas within the port operational areas. These measures have proved to be important for making port activities more efficient in terms of security and protection of persons, goods and ships in port, in a highly competitive environment. The large number of port security inspections has also significantly contributed to this level of port security; and the findings are exchanged between Member States through the MARSEC Committee, including the exchange of best practices fostered.

Nevertheless, there is still a series of recurrent common issues regarding proper implementation at the level of Member States ports, including: additional efforts needed (despite the progress made) in improving port security coordination; the definition of port boundaries for security purposes; the periodicity in the review of port security assessments and port security plans; and discrepancies between port security assessments and port security plans.

Looking ahead, the Commission's multi-annual inspections work programme will continue to include detailed examinations of port security measures. For example, the implementation and application of procedures under the port security plans to be applied to passengers and vehicles to be loaded on ro-ro vessels (which are, by nature, particularly vulnerable) will continue to be the

subject of further examination and monitoring by the Commission inspection services.

2. **This brings me to the second area I would like to highlight today, which is our work on ferry security**.

We (DG MOVE) recently received the final report of a study we commissioned focusing on the security of ro-ro ferries.

The Study analysed the maritime security aspects and security measures in place across Europe and assessed the case for enhancing those measures through a risk-based approach. The scope covered 23 EU Coast Member States, and 8 case studies, including Helsinki-Tallinn and Stockholm-Turku. I should note that the Study focused on one main threat: attacks conducted by terrorist and/or violent extremist groups or individuals with criminal motives targeting ferries' passengers and crew, not goods.

The study identified a range of security gaps in the areas of pre-departure, port facility perimeter control, port facility access and boarding, on-board and disembarkation, as well as horizontal gaps (like background checks, access to ship layout plans, and security culture training).

Considering the vulnerabilities identified on the basis of risk assessment, the study collected and selected best and innovative practices to address these gaps, as well as conducted a cost-benefit analysis of those measures. The result is a series of recommendations of so-called quick wins to improve overall security. These include: actively promoting security culture and awareness

among port facility and ro-ro passenger ship staff and passengers; adopting security by design principles; sharing of security measures between port facilities and ro-ro passengers on a need to know basis; making design plans of ships readily available on request to allow intervention forces to better prepare their response to a terrorist attack; as well as use of sniffing dogs trained to detect explosives to check passengers on foot (and their luggage) and vehicles while they wait to access the port facility or board a ro-ro ferry.

Ladies and Gentlemen, these are some of the recommendations. I will not outline them all. We discussed the outcome of this Study at our last Maritime Security Committee with the Member States just a few weeks ago, as well as with maritime stakeholders in the Stakeholders Advisory Group for Maritime Security. The ferry security study, together with a cruise ship security study finalised in 2017, will inform our work on possible actions at EU level in the course of the coming months. This will be done in close contact with MS and industry. Watch this space.

3. A third area of increasing importance is cyber security. Over the past couple of years, we all saw a number of cyber-attacks that hit the headlines and negatively affected transport companies. Ransomware attacks such as 'Wannacry' and ‘NotPetya’ were particularly serious. They led to important disruptions of transport supply chains, resulting in significant costs. We all know the example of Maersk. While these attacks are bad for business, they can also compromise the safety of transport operations with even dire consequences, measured in accidents and loss of human life. As a transport sector, it is therefore our collective responsibility to ensure that our system is both able to deter attacks and to show resilience should they occur.

Just over a year ago - in November 2017 – some of us in this room participated here in Tallinn in Digital Transport Days, organised jointly by DG MOVE and the then Estonian Council Presidency. Cybersecurity was one of the topics on the agenda, and the final declaration read, *"Transport must adapt to evolving challenges such as cyber-attacks which threaten lives and businesses, by inter alia raising awareness and by collaborating and exchanging information".*

Much has happened since then, notably at EU level, with the implementation of the Directive on Security of Network and Information Systems (NIS Directive) and the work on the new Cybersecurity Act. The NIS Directive is a game-changer for cybersecurity in Europe. But will it be enough to address the specificities of transport and specificities of different modes? I would argue that the NIS Directive lays some solid foundations for better cybersecurity. This being said, consideration is being given at some levels to additional sector-specific rules, covering one or several modes of transport. This is clearly visible in the aviation sector, where the International Civil Aviation Organization (ICAO) has adopted new standards on cybersecurity, which need to be translated in the EU Aviation Security legislation.

In the maritime domain, cyber security is progressing well with good international cooperation through the IMO. In June 2017 IMO adopted a Resolution which encourages administrations to ensure that cyber risks are appropriately addressed in the safety management system of companies as of 1 January 2021. In July 2017 IMO further adopted a set of guidelines providing recommendations on maritime cyber risk management. And of course, industry is actively producing helpful best practices, for example the Guidelines for

Cyber Security on Board Ships developed by BIMCO and others. IMO, however, is not addressing the issue beyond the port-ship interface.

As DG MOVE, we are bringing the different transport communities together to share their experiences, including with respect to NIS implementation. Just this past January, we supported the EU Agency for Network and Information Security (ENISA) in the organisation of the first ever transport cybersecurity conference, which took place at EMSA headquarters with the participation of all the transport agencies (EMSA, EASA, ERA). There were over 170 participants from national administrations and industry. It was a unique opportunity to share experiences and best practices across modes and across entities, including different regulators in the Member States.

It will continue to be the policy aim of DG MOVE to raise the overall level of awareness and preparedness to cyber-risks while also supporting Member State administrations in their efforts. In this respect a central challenge in closing security gaps must consider non-regulatory actions, focusing notably on the 'end-user' who is often described as the weakest link in the cybersecurity chain. We see far too often that many employees do not feel concerned by cybersecurity, which they perceive as an issue for the IT services only. More efforts are needed in raising the basic cyber-skills among staff.

4. Finally, while not strictly a security issue, but certainly related to risk assessment, I would like to say a few words on an issue managed by my safety colleagues in DG MOVE, which are the **EU Operational Guidelines on Places of Refuge.**

These guidelines are rooted in the lessons learned from the MSC Flaminia incident in 2012. The guidelines' principles and methods are established under article 20.3 of the VTMIS Directive, the effective use of all available information sources and data platforms (hosted in EMSA), the application of risk assessment, and seeking industry involvement and expert input.

They were developed because of an identified need for co-operation and coordination among competent authorities and industry actors involved in an incident and to provide a user-friendly manual for implementation of existing rules. Perhaps above all, they seek to change attitudes towards ships in need of assistance.

An important principle in these guidelines is that each State involved in an operation should examine the ability to provide a place of refuge. In principle, and unless deemed unsafe, there should be "no rejection without inspection."

I am pleased to report that EU Member States together with all concerned industry stakeholders successfully made a submission to IMO MSC100 (Dec 2019) where the issue of revisions to IMO guidelines has now been put on the agenda. This work, at international level, will draw inspiration from the work done at EU level!

Ladies and gentlemen, let me close by thanking the project once again for its good work, and each of you here today. You have all contributed and played a part in protecting our citizens. It has been a pleasure to be in your company and I look forward to further exchanges!