INTRODUCTION speech :

Mr Peter Claeyssens : Director General Shipping of the Belgian Maritime Authority

Federal Public Service of Mobility and Transport

WG on Cyber Security of the ECGFF (European Coast Guard Functions Forum)

CYBER THREATS in the Maritime Sector

Dear experts of the Member States, Chairman, members of the affiliated entities :

I welcome you on behalf of the Belgian Maritime Authority in our capital Brussels and hope you had some networking opportunities and good fun through our ice breaker yesterday evening.

Dear colleagues, my name is Peter Claeyssens and I am the director-general for maritime shipping within the Federal Public Service (or ministry) for Mobility & Transport. As such I am also president of the National Authority for Maritime Security also acting as sectoral authority for the NIS-directive in Belgium.

The maritime mobility is crucial for the wellbeing of Europe's economy and every European citizen. Belgium is together with the Netherlands the logistical linchpin of Europe. The impact of a "relatively small" disruption in the maritime chain is immediate and far reaching as we have seen with recent events like the blockage of the Suez canal. Needless to say that we are very concerned about the possible impact of cybersecurity actions in the maritime sector by organized crime syndicates, terrorist and let's not forget state actions. It is probably that last one that is the most concerning in the form of digital warfare or espionage.

It goes without saying that Cyber threats are on the rise , more and more sectors are being targeted by organized crime as potential victims . The Maritime sector , being rather specific business , came later but non the less is a high potential victim for the perpetrators.

A very recent example being DNVGL attacked by ransomware which resulted in nearly 70 shipping Companies and a 1000 ships being victim of ransomware and having to shift from their Ship Management software to fully manual operating.

Although ransomware is not the only form of attack (hacktivism and terroristic attacks remain possible) it remains the most common one and represents the majority of 85% of the cases (depending on source and region).

At the International Maritime Organization (IMO), cyber threats and cybersecurity are now considered as an important part of the ship security and have to be included in the ship security plans. Ship need to access different port systems all over the world because of the evolution towards more and more single window approach and the digitalization. Ships also become more and more controlled or monitored from their on-shore companies with different levels of autonomy. Therefor a permanent link with the shore is always established. An awareness needs to be created that ships and shipping companies are becoming more and more vulnerable to cyberthreats and hacking because of these evolutions.

Although the maritime private sector understands the need for investing in protection against cyberattacks, it is important that we as governments are aware of our responsibilities as well and take the necessary actions to protect the shipping industry and the maritime sector or infrastructure as a whole against cyberattacks

It is therefore that intelligence sharing and the application of this knowledge remains of vital importance to counteract the newest evolutions in the area of cybercrime in order to make are networks more robust , to make our users more aware

and our information more secure.

The actors we will present you in our Working Group will be representative for the Belgian and European landscape in this fight .

On the last day of the conference their will also be the election for a new chairman of this WG , we wish the potential candidates good luck.

I wish you all a fruitful meeting and a safe cyber environmenta