Position of the European Sea Ports Organisation on the proposal for a Directive on measures for high common level of cybersecurity across the Union (COM (2020)0359)

10 March 2021

The European Sea Ports Organisation (ESPO) welcomes the Commission's proposal for a Directive on measures for high common level of cybersecurity across the Union (NIS 2.0), published on 16 December 2020. The proposal is the result of a revision process of the Directive on security and network of information systems ((EU)2016/1148). The NIS 2.0 proposal again identifies ports as essential entities, setting obligations for port managing bodies, their port facilities and entities operating works and equipment in the port.

European ports are well aware that the increased use of digital solutions both within the port as well as in the broader transport and logistics chain, and the economy as such, comes with cyberthreats and -attacks. They also understand that the cyberthreat landscape is evolving fast, and additional measures might be needed to ensure a safe and secure use of digital solutions both within the port as well as in the broader transport and logistics chain.

Developing an EU cybersecurity policy that protects business continuity and mitigates the risks of cyberattacks, without curtailing the rapid pace of digital innovation, is a top priority for European ports. In this context, ESPO would like to raise a number of concerns on the NIS 2.0 proposal as well as propose a number of suggestions in order to better protect ports, as well as the broader transport and logistics chains in which they operate.

1. Limiting the NIS 2.0 to those ports that need high levels of protection

The NIS 2.0 proposal extends the scope of the previous Directive by dividing entities respectively into "essential" and "important" categories and by introducing an additional number of sectors. Port managing bodies, their port facilities and entities operating works and equipment in the port have been designated as "essential", and therefore are subjected to a number of obligations in order to enhance their cybersecurity and -resilience.

In order to harmonise its implementation, the NIS 2.0 proposal introduces a size cap in order to determine which entities in the sectors covered by the proposal would be subjected to the requirements of the NIS 2.0. More precisely, the proposal determines that all medium and large companies within selected sectors fall under the scope of the Directive, while the proposal also leaves flexibility for Member States to identify smaller entities with a high security risk profile.

European port managing bodies welcome the further harmonisation in the identification of essential entities that would fall under the NIS 2.0 Directive. At the same time, ESPO believes that guidelines should serve as a basis to define which ports in a given Member State should be designated as essential entities, as it is unclear how the medium and large companies size cap for entities that should be subjected to the NIS 2.0 will be translated to port managing bodies, and which port managing bodies would be considered smaller entities with a high security risk profile. Those guidelines should be developed by the Commission in close cooperation with the Member States and the stakeholders and should take into account the diverse nature of European ports, as they vary in size and in activities performed, and as their strategic importance in a given Member State may vary.

2. The focus should lay on the port ecosystem

The Annex of the NIS 2.0 proposal identifies which entities are considered essential, and as a consequence should take measures to comply with the obligations set by the proposal. Managing bodies of ports (referred to in point of Article 3 of Directive 2005/65/EC), including their port facilities (referred to in point 11 of Article 2 of Regulation 725/2004/EC), and entities operating works and equipment contained within ports, are designated as essential.

Ports are complex ecosystems with many different stakeholders, ranging from public authorities (such as customs) to private entities (such as terminals or various types of industries). The focus should therefore be on the protection of the entire port ecosystem, including the various actors involved in the port. In implementing the previous NIS Directive, Member States had different approaches as to which aspects of the ports should fall under the Directive. Given that in the NIS 2.0 proposal the same definition is used as in the previous NIS Directive, European ports believe that guidelines developed by the Commission in close cooperation with the Member States and the stakeholders and defining which aspects of the port should be designated as essential could be useful in ensuring that the relevant parts of the port are protected, and that Member States will implement the Directive in a harmonised way. In this context, the responsibility for complying with the NIS 2.0 should lie with the respective stakeholders in the port ecosystem, and not with the port managing body.

3. Protecting the entire transport and logistics chain

European ports also believe that there should be more focus on the protection of the entire transport and logistics chain. The NIS 2.0 proposal currently identifies individual essential entities and defines their obligations on an individual basis. Transport and logistics chains are however made up of a large number of interlinked actors and systems, where goods are being transported in an intermodal fashion using road, rail, inland waterways and maritime transport. This process requires swift and reliable exchange of data between the various links of the transport and logistics chain through various interfaces. However, a chain is only as strong as its weakest link.

To achieve the optimal transport and delivery of goods across the EU, communication and exchange between various actors needs to be safe and secure. If one of the actors in the transport and logistics chain, or any of the interfaces they use for data exchange, is compromised by a cyber incident, this could have a serious negative impact on the operations of the other players involved in moving the goods. Due to the interconnected nature of the various links in the chain, insufficient cybersecurity risks to endanger the functioning of the entire chain through domino effects created by a cyber incident in one or several parts of the transport and logistics chain. Furthermore, there are great

disparities in terms of cybersecurity awareness and capabilities of the various actors and the interfaces they use to exchange data.

4. Supporting ports when implementing the NIS 2.0 Directive

European ports foresee considerable costs to implement the NIS 2.0 proposal as it stands, especially for smaller ports and those ports that were previously not identified as essential entities. Investments in both cybersecurity infrastructure as well as skilled workforce are expensive, and will be needed in order to implement the NIS 2.0 proposal. In this context, ESPO believes that the transport envelope of the Connecting Europe Facility, both the modernisation pillar (actions relating to smart, interoperable, sustainable, multimodal, inclusive, accessible, safe and secure mobility), as well as the military mobility pillar, should be used to enhance the resilience of Europe's port infrastructure to cybersecurity threats. Given the limited budget of the Connecting Europe Facility, it is essential that Member States strengthen the cyber resilience of the port sector in their national Recovery and Resilience Plans as part of the EU's digital transition objective.

The European Sea Ports Organisation (ESPO) represents the port authorities, port associations and port administrations of the seaports of 22 Member States of the European Union and Norway at political level. ESPO has also observer members in Iceland, Israel, Ukraine and the United Kingdom. ESPO is the principal interface between the European seaport authorities and the European institutions. In addition to representing the interests of European ports, ESPO is a knowledge network which brings together professionals from the port sector and national port organisations. ESPO was created in 1993.