European Parliament
2019-2024

Committee on Transport and Tourism

2020/0359(COD)

30.4.2021

DRAFT OPINION

of the Committee on Transport and Tourism

for the Committee on Industry, Research and Energy

on the proposal for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148
(COM(2020)0823 – C9-0422/2020 – 2020/0359(COD))

Rapporteur for opinion: Jakop G. Dalunde

PA_Legam

SHORT JUSTIFICATION

The transport sector is increasingly vulnerable to and affected by cybersecurity threats. Due to the sector's particular features, it is also subject to a range of distinct vulnerabilities. The amendments in this draft opinion, although general in nature, are therefore proposed with these particularities in mind. My proposals are relevant to transport for the following reasons:

- Transport is often an international enterprise in which many entities fall under the jurisdiction of several Member States. The sector is therefore strongly impacted by excessive disparity in the cybersecurity risk management and reporting obligations between Member States;

- The transport sector relies on the safe data exchange between various actors. Due to the interconnected nature of logistics, insufficient cybersecurity in one entity could endanger the entire system and lead to serious consequences for the operations of other entities;

- Transport is a labour-intensive sector and therefore especially sensitive to cybersecurity threats targeting employees;

For these reasons, the amendments focus on the following subjects: assessing the degree of divergence between Member states in terms of cybersecurity obligations, fostering the alignment of these obligations through non-legislative means, promoting staff training and knowledge of cyber security risks.

In addition to these general points, it is worth noting that the transport sector increasingly uses remote sensors capable of connecting to the internet in the provision of services, and that vehicles themselves are increasingly digitised. Although not necessarily part of the wider information systems, these devices may require specific security assessments.

AMENDMENTS

The Committee on Transport and Tourism calls on the Committee on Industry, Research and Energy, as the committee responsible, to take into account the following amendments:

Amendment 1

Proposal for a directive
Recital 15 a (new)

Text proposed by the Commission	*Amendment*
	(15a) The increased digitalisation of key economic sectors, like transport, needs to be done in a secure way, with built in resilience to ensure that the whole supply chain responds adequately to risks and threats. There is therefore a need for a coordinated approach ensuring a minimal level of security for connected devices, especially when present in sectors like transport and included in vehicles, and deploying end-to-end encryption by default.

Or. en

Amendment 2

Proposal for a directive
Recital 33

Text proposed by the Commission	*Amendment*
(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations to be addressed through better implementation of existing rules.	(33) When developing guidance documents, the Cooperation Group should consistently: map national solutions and experiences, assess the impact of Cooperation Group deliverables on national approaches, discuss implementation challenges and formulate specific recommendations***, particularly on facilitating alignment in the transposition of this Directive among Member States,*** to be addressed through better implementation of existing rules.

Or. en

Justification

Connected to amendment on Article 12.

Amendment 3

Proposal for a directive
Recital 37 a (new)

Text proposed by the Commission	*Amendment*
	(37a) Excessive disparity in the cybersecurity risk management and reporting obligations in Member States' transposition of this Directive could put the common level of cybersecurity within the Union at risk. ENISA should therefore, in cooperation with the Commission, evaluate the degree of divergence in cybersecurity risk management and reporting obligations among Member States in its biennial report on the state of cybersecurity in the Union.

Or. en

Justification

Connected to amendment on Article 15.

Amendment 4

Proposal for a directive
Article 12 – paragraph 4 – point a

Text proposed by the Commission	*Amendment*
(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive;	(a) providing guidance to competent authorities in relation to the transposition and implementation of this Directive***, particularly with the aim of facilitating alignment of the cybersecurity risk management and reporting obligations within the Union***;

Or. en

Justification

Excessive disparity in the cybersecurity risk management and reporting obligations in Member States' transposition of this Directive could put the common level of cybersecurity within the Union at risk. That is especially pertinent to transport, which is often an international enterprise, where many entities will fall under the jurisdiction of several Member States. The Cooperation Group could therefore act as a facilitator in aligning the obligations within the Union through non-legislative means, in order to alleviate that risk, without prejudice to Article 3.

Amendment 5

Proposal for a directive
Article 15 – paragraph 1 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) the degree of disparity of cybersecurity risk management and reporting obligations between Member States, and to what extent it is affecting the common level of cybersecurity within the Union.

Or. en

Justification

Further to the amendment on Article 12, the biennial report could present an opportunity to evaluate the degree of divergence in cybersecurity obligations for entities among Member States. Conclusions on this subject in the biennial report could inform further alignment of national standards following the entry into force of the Directive, and provide Member States with clear information on how to voluntarily align their national legislation.

Amendment 6

Proposal for a directive
Article 18 – paragraph 2 – point e

Text proposed by the Commission	*Amendment*
(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	(e) security in network and information systems***, including mobile elements such as vehicles and remote sensors, their*** acquisition, development and maintenance, including vulnerability handling and

disclosure;

Or. en

Justification

Using remote sensors that are capable of connecting to the internet in the provision of e.g. transport services is becoming increasingly common. Examples include real-time location tracking, fuel consumption tracking and data, temperature tracking in refrigeration systems etc. Including specific provisions on assessing cybersecurity risk in these devices is therefore important. The same is true for vehicles themselves: they are becoming increasingly digitised.

Amendment 7

Proposal for a directive
Article 18 – paragraph 2 – point g a (new)

Text proposed by the Commission	*Amendment*
	(ga) policies and procedures to ensure that employees have reasonable knowledge to apprehend cybersecurity risks.

Or. en

Justification

Staff not having adequate knowledge of cybersecurity risks constitutes a danger to the level of cybersecurity in any entity. Practices such as phishing continues to be a serious problem in many sectors, not least in labour-intensive operations such as transport and manufacturing. Entities should be required to provide their staff with a reasonable degree of knowledge in the field of cybersecurity.

Amendment 8

Proposal for a directive
Article 18 – paragraph 6 a (new)

Text proposed by the Commission	*Amendment*
	6a. In order to ensure an efficient policy and facilitate its implementation, the Commission shall organise structured consultations with entities designated as essential and important, especially with regard to adopting the delegated acts

referred to in paragraph 6.

Or. en

Justification

Article 36(4) states that the Commission shall consult experts designated by the Member States before adopting delegated acts in accordance with Article 18(6). They should also be, at a minimum, required to consult any number of experts designated by those entities that will be subject to the delegated acts.