European Parliament
2019-2024

Committee on Transport and Tourism

2023/0109(COD)

25.10.2023

OPINION

of the Committee on Transport and Tourism

for the Committee on Industry, Research and Energy

on the proposal for a regulation of the European Parliament and of the Council on Measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Rapporteur for opinion: Gheorghe Falcă

PA_Legam

SHORT JUSTIFICATION

Organizations affected by cyberattacks, including in the transport sector, rarely report them, especially private sector companies, since they tend to see them as 'bad publicity'. Most organizations prefer to deal with them internally and it is often the attackers who publicize them. In the EU, the good news is that the entry into force of Directive 2022/2555 on network security (known as the 'NIS2 Directive'), which Member States have until October 2024 to transpose, harmonises the incident reporting obligations across the Member States. Therefore, a better understanding of the nature and scale of the problem is likely to emerge in coming years.

The European Union Agency for Cybersecurity (ENISA) published a recent report[1] that provides information on cybersecurity threats in the transport sector, where it emphasizes that cybercriminals were responsible for more than half of the incidents observed in the 2022 reporting period (55%) and that the leading motivation behind these attacks was financial gain. It also notes that most cyber-attacks in the transport sector target IT systems, causing operational disruptions.

As regards preparedness and response to cybersecurity incidents, there is currently limited support at Union level and solidarity between Member States. The Council Conclusions of May 2022 highlighted the need to address these gaps, by calling for the Commission to present a proposal on a new **Emergency Response Fund for Cybersecurity**[2].

This Regulation implements the **EU Cybersecurity Strategy** adopted in December 2020 that announced the creation of a **European Cyber Shield**, reinforcing the cyber threat detection and information sharing capabilities in the European Union through a federation of national and cross-border Security Operations Centres (SOCs). The actions of this Regulation will be supported by **funding under 'Cybersecurity' Strategic Objective of DEP (Digital Europe Programme).**

The total budget includes an increase of EUR 100 million that this Regulation proposes to re-allocate from other strategic objectives of DEP. This will bring the new total amount available for cybersecurity actions under DEP to EUR 842.8 million.

Part of the additional EUR 100 million will reinforce the budget managed by the European Cybersecurity Competence Centre (ECCC) to implement actions on SOCs and preparedness as part of their work programme(s). Moreover, the additional funding will serve to support the establishment of the EU Cybersecurity Reserve. It complements the budget already foreseen for similar actions in the main DEP and Cybersecurity DEP Work Programme for the 2023-2027 period which could boost the total amount to 551 million for 2023-2027, while 115 million were dedicated already in the form of pilots for 2021-2022. Including Member States contributions, the overall budget could amount up to 1.109 billion euros.

[1] "Understanding Cyber Threats in Transport", ENISA, published March 21, 2023.
[2] Council conclusions on the development of the European Union's cyber posture of 23 May 2022, (9364/22).

Rapporteur's position

Your rapporteur welcomes the new proposal and believes that it will offer significant benefits to the various stakeholders. The rapporteur underlines the necessity for a deeper understanding of the cybersecurity needs and requirements of transportation, as well as for providing transport critical entities with access to proper funding for preparedness, response and solving incidents.

Your rapporteur endorses the 'transport cybersecurity toolkit', which aims at contributing to greater levels of cyber-awareness and cyber-hygiene, with a specific focus on the transport sector. It addresses transport organisations, regardless of their size and domain of activity, as well as taking into account transport critical infrastructure and military mobility, particularly having regards the war in Ukraine, especially but not limited to:

- Air carriers, airport managing bodies, core airports, air traffic management and air traffic control centres, the European Union Aviation Safety Agency and Eurocontrol;
- Infrastructure managers, railway undertakings and the European Rail Traffic Management System (ERTMS);
- Inland, sea and coastal passenger and freight water transport companies, managing bodies of ports, including their port facilities, entities operating works and equipment contained within ports, operators of vessel traffic services;
- Road authorities responsible for traffic management control, operators of Intelligent Transport Systems;
- Postal and courier services.

Your Rapporteur believes that the size of the budget for the functioning of the **Emergency Response Fund for Cybersecurity** (ERFC) will determine its success; therefore, it should be sufficiently large to support Member States in **preparing for, responding to and recovering from** significant and large-scale cybersecurity incidents. Support for incident response shall also be made available to institutions, bodies, offices and agencies of the Union.

The **European Cyber Shield** will improve the cyber threat detection capabilities of the Member States. The **Cyber Emergency Mechanism** will complement Member States' actions through emergency support for preparedness, response and immediate recovery/restoration of the functioning of essential services.

AMENDMENT

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

Amendment 1

Proposal for a regulation
Recital 2

Text proposed by the Commission	*Amendment*
(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy of the Union, and could even have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries.	(2) The magnitude, frequency and impact of cybersecurity incidents are increasing, including supply chain attacks aiming at cyberespionage, ransomware or disruption. They represent a major threat to the functioning of network and information systems***, as well as critical IT and physical infrastructure***. In view of the fast-evolving threat landscape, the threat of possible large-scale incidents causing significant disruption or damage to critical infrastructures demands heightened preparedness at all levels of the Union's cybersecurity framework. That threat goes beyond Russia's military aggression on Ukraine, and is likely to persist given the multiplicity of state-aligned, criminal and hacktivist actors involved in current geopolitical tensions. Such incidents can impede the provision of public services***, of public and private transport,*** and the pursuit of economic activities, including in critical or highly critical sectors, generate substantial financial losses, undermine user confidence, cause major damage to the economy of ***the Union as well as to mobility within*** the Union, and could even have health or life-threatening consequences. Moreover, cybersecurity incidents are unpredictable, as they often emerge and evolve within very short periods of time, not contained within any specific geographical area, and occurring simultaneously or spreading instantly across many countries.

Amendment 2

Proposal for a regulation
Recital 2 a (new)

Text proposed by the Commission	*Amendment*
	(2a) An increasingly serious cybersecurity threat is posed to the transport sector by state-sponsored actors, cybercriminals and hacktivists targeting authorities, operators, manufacturers, suppliers and service providers in aviation, maritime, railway and road transport. The European Union Agency for Cybersecurity (ENISA) has observed a 25% increase in the monthly average number of reported incidents affecting the transport sector in 2022, compared to 2021 levels. A majority of the attacks on the transport sector targets information technology (IT) systems, with possible operational disruptions occurring as a result[14a].
	[14b] ENISA (2023),ENISA threat landscape: Transport sector, pages 7 and 17.

Amendment 3

Proposal for a regulation
Recital 2 b (new)

Text proposed by the Commission	*Amendment*
	(2b) Russia's unprovoked invasion of Ukraine determined a significant increase of cybersecurity incidents, including distributed denial-of-service (DDoS) cyber attacks, targeting the transport sector in the EU and areas close to the EU, mainly airports, railways and transport authorities[14b]. This increase in attacks is highly likely to continue.

[14b] ENISA (2023),ENISA threat landscape: Transport sector, page 9.

Amendment 4

Proposal for a regulation
Recital 2 c (new)

Text proposed by the Commission	*Amendment*
	(2c) Cyberattacks target authorities and bodies in all transport subsectors, with railway undertakings and infrastructure managers as well as port operators being affected. As regards the road sector, original equipment manufacturers (OEMs), suppliers and service providers were targeted, along with public transport operators. In the aviation sector, the main targets were airlines and airport operators, followed by service providers, surface transport operators and the supply chain[14c].
	[14c] ENISA (2023),ENISA threat landscape: Transport sector, page 17.

Amendment 5

Proposal for a regulation
Recital 3

Text proposed by the Commission	*Amendment*
(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[16] , it is necessary to increase the resilience of citizens, businesses and entities operating critical infrastructures against the growing cybersecurity threats,	(3) It is necessary to strengthen the competitive position of industry and services sectors in the Union across the digitised economy and support their digital transformation, by reinforcing the level of cybersecurity in the Digital Single Market. As recommended in three different proposals of the Conference on the Future of Europe[16] , it is necessary to increase the resilience of citizens, businesses***, transport operators*** and entities operating critical infrastructures against the growing

which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents.

[16] https://futureu.europa.eu/en/

cybersecurity threats, which can have devastating societal and economic impacts. Therefore, investment in infrastructures and services that will support faster detection and response to cybersecurity threats and incidents is needed, and Member States need assistance in better preparing for, as well as responding to significant and large-scale cybersecurity incidents. The Union should also increase its capacities in these areas, notably as regards the collection and analysis of data on cybersecurity threats and incidents ***as well as on the state and the evolution of the cybersecurity labour market as it plays an instrumental role in providing the necessary detection and response services***.

[16] https://futureu.europa.eu/en/

Amendment 6

Proposal for a regulation
Recital 4

Text proposed by the Commission	*Amendment*
(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[17] , Commission Recommendation (EU) 2017/1584[18] , Directive 2013/40/EU of the European Parliament and of the Council[19] and Regulation (EU) 2019/881 of the European Parliament and of the Council[20] . In addition, the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant	(4) The Union has already taken a number of measures to reduce vulnerabilities and increase the resilience of critical infrastructures and entities against cybersecurity risks, in particular Directive (EU) 2022/2555 of the European Parliament and of the Council[17] , Commission Recommendation (EU) 2017/1584[18] , Directive 2013/40/EU of the European Parliament and of the Council[19] and Regulation (EU) 2019/881 of the European Parliament and of the Council[20]***as well as the proposal for a Regulation on guidelines for the development of the trans-European transport network, and the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act)***. In addition, the Council Recommendation on

public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

a Union-wide coordinated approach to strengthen the resilience of critical infrastructure invites Member States to take urgent and effective measures, and to cooperate loyally, efficiently, in solidarity and in a coordinated manner with each other, the Commission and other relevant public authorities as well as the entities concerned, to enhance the resilience of critical infrastructure used to provide essential services in the internal market.

---

[17] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

[18] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[19] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8).

[20] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

[17] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (OJ L 333, 27.12.2022).

[18] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises (OJ L 239, 19.9.2017, p. 36).

[19] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (J L 218, 14.8.2013, p. 8).

[20] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, p. 15).

Amendment 7

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) While welcoming the European Commission's Transport Cybersecurity Toolkit[2a], which contains basic information on threats that may affect transport organisations (malware diffusion, denial of service, unauthorised access and theft, and software manipulation) and lists good mitigating practices, transport operators should be provided with proper training on cybersecurity and with proper tools to prevent cyber threats. The Union budget should also cover the support, such as training, provided by ENISA to enable the effective implementation by transport operators of best mitigating practices included in the Toolkit.
	[1a] ENISA threat landscape: transport sector / ENISA, March 2023
	[2a] European Commission, (2021). Transport Cybersecurity Toolkit, available at https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en

Amendment 8

Proposal for a regulation
Recital 4 a (new)

Text proposed by the Commission	*Amendment*
	(4a) A Union-wide coordinated approach to strengthen the preparedness and resilience of critical infrastructure, such as transport infrastructure, is based on the Member States' capacity building. As acknowledged in the recent Communication from the Commission to the European Parliament and the Council on Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience[19a], the security of the EU

cannot be guaranteed without the EU's most valuable asset: its people.

[19a] Communication from the Commission to the European Parliament and the Council on Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy') COM(2023) 207 final

Amendment 9

Proposal for a regulation
Recital 12

Text proposed by the Commission	*Amendment*
(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union**,** including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European	(12) To more effectively prevent, assess and respond to cyber threats and incidents, it is necessary to develop more comprehensive knowledge about the threats to critical assets and infrastructures on the territory of the Union including their geographical distribution, interconnection and potential effects in case of cyber-attacks affecting those infrastructures**.** ***These critical assets and infrastructures include Intelligent Transport Systems, which, whilst essential for automated and multimodal mobility, operate on the basis of crucial exhanges of sensitive data***. A large-scale Union infrastructure of SOCs should be deployed ('the European Cyber Shield'), comprising of several interoperating cross-border platforms, each grouping together several National SOCs. That infrastructure should serve national and Union cybersecurity interests and needs, leveraging state of the art technology for advanced data collection and analytics tools, enhancing cyber detection and management capabilities and providing real-time situational awareness. That infrastructure should serve to increase detection of cybersecurity threats and incidents and thus complement and support

Parliament and of the Council[24] .

Union entities and networks responsible for crisis management in the Union, notably the EU Cyber Crises Liaison Organisation Network ('EU-CyCLONe'), as defined in Directive (EU) 2022/2555 of the European Parliament and of the Council[24] .

[24] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

[24] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (OJ L 333, 27.12.2022, p. 80).

Amendment 10

Proposal for a regulation
Recital 14 a (new)

Text proposed by the Commission	*Amendment*
	(14a) The transport sector is increasingly becoming one of the most lucrative businesses for cybercriminals, with customer data considered a highly valuable commodity and with the transport supply chain becoming more and more targeted. For this reason, transport infrastructure characterised by a cross-border nature or by data exchange through wireless technologies should be considered a pivotal object of analysis and monitoring for both national and, particularly, for Cross-border SOCs. For instance, the recent proposal revising the TEN-T Regulation requires greater solidarity and cooperation in sharing information on cross-border cyber threats that this transnational network might face. Similarly, Intelligent Transport Systems (ITS) are vital to make transport safer, more efficient and more sustainable, yet they make transport systems more vulnerable to cyber attacks

	that can create accidents, traffic jams or cause economic losses to both private and public operators. In order to safeguard the safety of passengers, the protection of users' and providers' data and to avoid financial damages, it is essential that the implementation programme of the revised directive on Intelligent Transport Systems includes provisions and tools to strengthen the collaboration among Member States to detect, prepare for and respond to cybersecurity threats and incidents.

Amendment 11

Proposal for a regulation
Recital 15

Text proposed by the Commission	*Amendment*
(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty.	(15) At national level, the monitoring, detection and analysis of cyber threats is typically ensured by SOCs of public and private entities, in combination with CSIRTs. In addition, CSIRTs exchange information in the context of the CSIRT network, in accordance with Directive (EU) 2022/2555. The Cross-border SOCs should constitute a new capability that is complementary to the CSIRTs network, by pooling and sharing data on cybersecurity threats from public and private entities, enhancing the value of such data through expert analysis and jointly acquired infrastructures and state of the art tools, and contributing to the development of Union capabilities and technological sovereignty. ***In this regard, in order to strengthen the Union's autonomy in the cyber field and with reference to Article 47 (4) of the proposal for a Regulation on guidelines for the development of the trans-European transport network (COM(2021)0812), it is also necessary to prevent access to data leading to cyber threats by enforcing a robust regulatory framework that governs foreign***

ownership and investments in critical infrastructure, like in transport.

Amendment 12

Proposal for a regulation
Recital 21

Text proposed by the Commission	*Amendment*
(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative.	(21) While the European Cyber Shield is a civilian project, the cyber defence community could benefit from stronger civilian detection and situational awareness capabilities developed for the protection of critical infrastructure. Cross-border SOCs, with the support of the Commission and the European Cybersecurity Competence Centre ('ECCC'), and in cooperation with the High Representative of the Union for Foreign Affairs and Security Policy (the 'High Representative'), should gradually develop dedicated protocols and standards to allow for cooperation with the cyber defence community, including vetting and security conditions. The development of the European Cyber Shield should be accompanied by a reflection enabling future collaboration with networks and platforms responsible for information sharing in the cyber defence community, in close cooperation with the High Representative. ***It should also enable synergies with the Action Plan on Military Mobility 2.0. A well-functioning military mobility network needs to be resilient, including in the context of cyber and other hybrid threats that could affect critical nodes in the transport system that are dual-use. For instance, a cyber-attack on systems used in airports, harbours or railroads or a cyber-attack on military assets could have major consequences. Thus, digitalising processes and procedures, including for the necessary civilian and military cooperation, will require the strengthening of computer information systems (CIS) against cyber***

threats.

Amendment 13

Proposal for a regulation
Recital 21 a (new)

Text proposed by the Commission	*Amendment*
	(21a) In case of a cybersecurity crisis, an effective exchange of information is pivotal to ensure situational awareness among the military and civilian transport sectors. This exchange of information should also stimulate cooperation between relevant sectoral authorities responsible for transport, competent cybersecurity authorities, SOCs and CSIRTs.

Amendment 14

Proposal for a regulation
Recital 29

Text proposed by the Commission	*Amendment*
(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality'). The coordinated testing exercises should be based on common risk scenarios and	(29) As part of the preparedness actions, to promote a consistent approach and strengthen security across the Union and its internal market, support should be provided for testing and assessing cybersecurity of entities operating in highly critical sectors identified pursuant to Directive (EU) 2022/2555 in a coordinated manner. For this purpose, the Commission, with the support of ENISA and in cooperation with the NIS Cooperation Group established by Directive (EU) 2022/2555, should regularly identify relevant sectors or subsectors, which should be eligible to receive financial support for coordinated testing at Union level. The sectors or subsectors should be selected from Annex I to Directive (EU) 2022/2555 ('Sectors of High Criticality')***. Specific attention should be given to the transport sector and its subsectors (air,***

methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[29] . The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

rail, water, road), as they incorporate critical infrastructure where cyber incidents and attacks could severely undermine the safety of passengers and operators. The coordinated testing exercises should be based on common risk scenarios and methodologies. The selection of sectors and development of risk scenarios should take into account relevant Union-wide risk assessments and risk scenarios, including the need to avoid duplication, such as the risk evaluation and risk scenarios called for in the Council conclusions on the development of the European Union's cyber posture to be conducted by the Commission, the High Representative and the NIS Cooperation Group, in coordination with relevant civilian and military bodies and agencies and established networks, including the EU CyCLONe, as well as the risk assessment of communications networks and infrastructures requested by the Joint Ministerial Call of Nevers and conducted by the NIS Cooperation Group, with the support of the Commission and ENISA, and in cooperation with the Body of European Regulators for Electronic Communications (BEREC), the coordinated risk assessments to be conducted under Article 22 of Directive (EU) 2022/2555 and digital operational resilience testing as provided for in Regulation (EU) 2022/2554 of the European Parliament and of the Council[29] . The selection of sectors should also take into account the Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.

[29] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014,

[29] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014,

Amendment 15

Proposal for a regulation
Recital 30 a (new)

Text proposed by the Commission	*Amendment*
	(30a) With a view to the criticality of the sector and to the implications of cyberthreats on mobility and, in consequence, on human lives of passengers and pedestrians, the transport sector should be prioritised with regards to the coordinated preparedness testing of entities.

Amendment 16

Proposal for a regulation
Recital 35 a (new)

Text proposed by the Commission	*Amendment*
	(35a) In view of the increased tasks and responsibilities given to ENISA by this proposal as well as by the proposal on the on Cyber Resilience Act, the adoption of the ENISA Amending budget 1/2022 for the Pilot Implementation of a Cybersecurity Support Action is necessary. Moreover, in view of the Union interests at stake, additional financial and human resources should be allocated to ENISA.

Amendment 17

Proposal for a regulation
Recital 38 a (new)

Text proposed by the Commission	*Amendment*
	(38a) The development of skills and competences should therefore receive

centre stage, across all sectors, not least to those that are vulnerable to cybersecurity threats, such as staff working on mass transit or critical infrastrucures, including train control systems and digital transport planning tools for all modes of transport. The introduction and further development of the cybersecurity culture is therefore paramount to the success of implementing this regulation for both citizens´ awareness and specialists' knowledge across all critical infrastructure sectors.

Amendment 18

Proposal for a regulation
Article 1 – paragraph 2 – point a

Text proposed by the Commission	*Amendment*
(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;	(a) to strengthen common Union detection and situational awareness of cyber threats and incidents thus allowing to reinforce the competitive position of industry***, transport infrastructure*** and services sectors in the Union across the digital economy and contribute to the Union's technological sovereignty in the area of cybersecurity;

Amendment 19

Proposal for a regulation
Article 1 – paragraph 2 – point b

Text proposed by the Commission	*Amendment*
(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, including by making Union cybersecurity incident response support available for third countries associated to the Digital Europe	(b) to reinforce preparedness of entities operating in critical and highly critical sectors across the Union and strengthen solidarity by developing common response capacities against significant or large-scale cybersecurity incidents, ***with particular attention to critical IT and physical infrastructure,*** including by making Union cybersecurity incident response support

Programme (‘DEP’);	available for third countries associated to the Digital Europe Programme (‘DEP’);

Amendment 20

Proposal for a regulation
Article 1 – paragraph 2 – point c a (new)

Text proposed by the Commission	*Amendment*
	(ca) to strengthen the Union’s preparedness, cooperation and efficacy in protecting transport infrastructure and services in Member States from cybersecurity incidents, to ensure the transport sector’s continuous functioning, the integrity of supply chains and Union-wide mobility.

Amendment 21

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 1 – point c

Text proposed by the Commission	*Amendment*
(c) contribute to better protection and response to cyber threats***;***	(c) contribute to better protection and response to cyber threats***, including for transport infrastructure characterised by a cross-border nature, such as the TEN-T, or by data exchange through wireless technologies, like Intelligent Transport Systems.***

Amendment 22

Proposal for a regulation
Article 3 – paragraph 2 – subparagraph 2

Text proposed by the Commission	*Amendment*
It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173.	It shall be developed in cooperation with the pan-European High Performance Computing infrastructure established pursuant to Regulation (EU) 2021/1173. ***It shall enable collaboration, via dedicated***

protocols and standards, with the cyber defence community, to ensure the development of stronger civilian detection and situational awareness capabilities for the protection of critical infrastructure. In this regard, synergies shall be developed also with the Action Plan on Military Mobility 2.0, and an effective exchange of information shall be ensured to provide situational awareness among the military and civilian transport sectors.

Amendment 23

Proposal for a regulation
Article 8 – paragraph 2 a (new)

Text proposed by the Commission	*Amendment*
	2a. The Commission shall involve the European Cyber Shield, in particular the cross-border SOCs, in its opinion to Member States in the framework of the proposal for a Regulation on the trans-European transport network (COM(2021)0812) whenever the participation of or contribution of any kind by a natural person of a third country or an undertaking of a third country is likely to affect the cybersecurity of cross-border critical infrastructure, such as the TEN-T.

Amendment 24

Proposal for a regulation
Article 10 – paragraph 1 – point a

Text proposed by the Commission	*Amendment*
(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union;	(a) preparedness actions, including the coordinated preparedness testing of entities operating in highly critical sectors across the Union***, with specific attention to transport infrastructure and its subsectors included in Annex I to Directive (EU)***

2022/255;

Amendment 25

Proposal for a regulation
Article 18 – paragraph 2

Text proposed by the Commission	*Amendment*
2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.	2. To prepare the incident review report referred to in paragraph 1, ENISA shall collaborate all relevant stakeholders, including representatives of Member States, the Commission, other relevant EU institutions, bodies and agencies, managed security services providers and users of cybersecurity services. Where appropriate, ENISA shall also collaborate with entities affected by significant or large-scale cybersecurity incidents***, including transport operators***. To support the review, ENISA may also consult other types of stakeholders. Consulted representatives shall disclose any potential conflict of interest.

Amendment 26

Proposal for a regulation
Article 19 – paragraph 1 – point 1 – point b
Regulation (EU) 2021/694
Article 6 – Paragraph 2a (new)

Text proposed by the Commission	*Amendment*
	2a. In view of the Union interests at stake, in relation to its responsibilities for the preparation of candidate certification schemes pursuant to Regulation (EU) 2019/881, its responsibilities to review and assess cyber threats, vulnerabilities and mitigation, prepare an incident review report for Cybersecurity Incident Review Mechanism, as well asto provide training against cyber attacks and incidents to operators of critical infrastructure and in light of its newly assigned responsibilities

	in the framework of the Proposal on the Cyber Resilience Act, ENISA shall be provided with the necessary resources under the Union budget in accordance with the applicable legislation.

Amendment 27

Proposal for a regulation
Article 19 – paragraph 1 – point 1 a (new)
Regulation (EU) 2021/694
Article 7 – paragraph 1 – point ca (new)

Text proposed by the Commission	*Amendment*
	(1a) Article 7 is amended as follows:
	(a) paragraph 1 is amended as follows:
	(1) the following point (ca) is inserted:
	(ca) support high-quality training to transport operators and transport critical infrastructure's managers and workforce, also with the aim to effectively share and implement mitigating practices in face of cyber attacks or incidents to critical infrastructure, such as the ones provided by the Transport Cybersecurity Toolkit.

PROCEDURE – COMMITTEE ASKED FOR OPINION

Title	Laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cybersecurity threats and incidents
References	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Committee responsible Date announced in plenary	ITRE 1.6.2023
Opinion by Date announced in plenary	TRAN 1.6.2023
Rapporteur for the opinion Date appointed	Gheorghe Falcă 7.7.2023
Date adopted	25.10.2023
Result of final vote	+: 38 –: 0 0: 0
Members present for the final vote	Magdalena Adamowicz, Andris Ameriks, José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Karolin Braunsberger-Reinhold, Karima Delli, Anna Deparnay-Grunenberg, Gheorghe Falcă, Carlo Fidanza, Jens Gieseke, Elsi Katainen, Elena Kountoura, Bogusław Liberadzki, Peter Lundgren, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Tilly Metz, Cláudia Monteiro de Aguiar, Caroline Nagtegaal, Jan-Christoph Oetjen, Rovana Plumb, Thomas Rudner, Massimiliano Salini, Vera Tax, Barbara Thaler, István Ujhelyi, Achille Variati, Petar Vitanov, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Substitutes present for the final vote	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

38	+
ECR	Carlo Fidanza, Peter Lundgren, Dorien Rookmaker
ID	Roman Haider
PPE	Magdalena Adamowicz, Karolin Braunsberger-Reinhold, Gheorghe Falcă, Jens Gieseke, Elżbieta Katarzyna Łukacijewska, Marian-Jean Marinescu, Colm Markey, Cláudia Monteiro de Aguiar, Ljudmila Novak, Massimiliano Salini, Barbara Thaler, Elissavet Vozemberg-Vrionidi, Lucia Vuolo
Renew	José Ramón Bauzá Díaz, Izaskun Bilbao Barandica, Pierre Karleskind, Elsi Katainen, Caroline Nagtegaal, Jan-Christoph Oetjen
S&D	Andris Ameriks, Sara Cerdas, Josianne Cutajar, Bogusław Liberadzki, Rovana Plumb, Thomas Rudner, Vera Tax, István Ujhelyi, Achille Variati, Petar Vitanov
The Left	Elena Kountoura
Verts/ALE	Karima Delli, Anna Deparnay-Grunenberg, Pär Holmgren, Tilly Metz

0	-

0	0

Key to symbols:
+ : in favour
- : against
0 : abstention