Parlamento Europeu
2019-2024

Comissão dos Transportes e do Turismo

2023/0109(COD)

25.10.2023

PARECER

da Comissão dos Transportes e do Turismo

dirigido à Comissão da Indústria, da Investigação e da Energia

sobre a proposta de regulamento do Parlamento Europeu e do Conselho que estabelece medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança
(COM(2023)0209 – C9-0136/2023 – 2023/0109(COD))

Relator de parecer: Gheorghe Falcă

PA_Legam

JUSTIFICAÇÃO SUCINTA

As organizações afetadas por ciberataques, nomeadamente no setor dos transportes, raramente os denunciam, sobretudo as empresas do setor privado, uma vez que tendem a considerá-los como «má publicidade». A maioria das organizações prefere tratá-los a nível interno e são frequentemente os atacantes que os divulgam. Na UE, a boa notícia reside no facto de a entrada em vigor da Diretiva 2022/2555 relativa à segurança da rede (conhecida como «Diretiva SRI 2»), que os Estados-Membros têm até outubro de 2024 para transpor, harmonizar as obrigações de notificação de incidentes em todos os Estados-Membros. Por conseguinte, é provável que nos próximos anos se compreenda melhor a natureza e a dimensão deste problema.

A Agência da União Europeia para a Cibersegurança (ENISA) publicou recentemente um relatório1 que fornece informações sobre as ameaças à cibersegurança no setor dos transportes, no qual salienta que os cibercriminosos foram responsáveis por mais de metade dos incidentes observados no período de referência de 2022 (55 %) e que a principal motivação para estes ataques foi o lucro financeiro. O relatório assinala igualmente que a maioria dos ciberataques no setor dos transportes visa os sistemas informáticos, causando perturbações operacionais.

No que diz respeito à preparação e resposta a incidentes de cibersegurança, existe atualmente um apoio limitado à escala da União e uma solidariedade limitada entre os Estados-Membros. As conclusões do Conselho de maio de 2022 salientaram a necessidade de colmatar estas lacunas, convidando a Comissão a apresentar uma proposta relativa a um novo **Fundo de Resposta de Emergência para a Cibersegurança**[2].

O presente regulamento aplica a **Estratégia da UE para a Cibersegurança**, adotada em dezembro de 2020, que anunciou a criação de um **ciberescudo europeu**, reforçando as capacidades de deteção de ciberameaças e de partilha de informações na União Europeia através de uma federação de centros de operações de segurança (SOC) nacionais e transfronteiriços. As ações do presente regulamento serão apoiadas por **financiamento concedido ao abrigo do objetivo estratégico «Cibersegurança» do Programa Europa Digital (PED).**

O orçamento total inclui um aumento de 100 milhões de EUR que o presente regulamento propõe reafetar a partir de outros objetivos estratégicos do PED. Deste modo, o novo montante total disponível para ações de cibersegurança no âmbito do PED ascenderá a 842,8 milhões de EUR.

Parte do montante adicional de 100 milhões de EUR reforçará o orçamento gerido pelo Centro Europeu de Competências em Cibersegurança (ECCC) para executar ações em matéria de SOC e de preparação no âmbito do(s) seu(s) programa(s) de trabalho. Além disso, o financiamento adicional servirá para apoiar a criação da Reserva de Cibersegurança da UE. Complementa o orçamento já previsto para ações semelhantes no programa de trabalho principal do PED e no programa de trabalho em matéria de cibersegurança do PED para 2023-2027, o que poderá elevar o montante total para 551 milhões para o período 2023-2027, ao passo que 115 milhões

[1] «Understanding Cyber Threats in Transport» [Compreender as ciberameaças nos transportes], ENISA, publicado em 21 de março de 2023.

[2] Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço de 23 de maio de 2022 (9364/22).

foram já afetados sob a forma de projetos-piloto para 2021-2022. Incluindo as contribuições dos Estados-Membros, o orçamento global poderá ascender a 1 109 milhões de EUR.

Posição do relator

O relator acolhe com agrado a nova proposta e considera que a mesma trará benefícios significativos às várias partes interessadas. O relator destaca a necessidade de uma compreensão mais profunda das necessidades e dos requisitos em matéria de cibersegurança dos transportes, bem como de proporcionar às entidades críticas do setor dos transportes acesso a um financiamento adequado para a preparação, resposta e resolução de incidentes.

O relator apoia o «conjunto de ferramentas para a cibersegurança dos transportes», que visa contribuir para níveis mais elevados de sensibilização para a cibersegurança e de ciber-higiene, com especial destaque para o setor dos transportes. Dirige-se às organizações de transportes, independentemente da sua dimensão e domínio de atividade, e tem em conta as infraestruturas críticas de transportes e a mobilidade militar, em particular no que se refere à guerra na Ucrânia, em especial, mas não só:

- transportadoras aéreas, entidades gestoras de aeroportos, aeroportos principais, gestão do tráfego aéreo e centros de controlo do tráfego aéreo, a Agência da União Europeia para a Segurança da Aviação e a Eurocontrol;
- gestores de infraestruturas, empresas ferroviárias e o Sistema Europeu de Gestão do Tráfego Ferroviário (ERTMS);
- empresas de transporte de passageiros e de mercadorias por vias navegáveis interiores, marítimas e costeiras, entidades gestoras de portos, nomeadamente as suas instalações portuárias, entidades que gerem as obras e os equipamentos existentes dentro dos portos, operadores de serviços de tráfego marítimo;
- autoridades rodoviárias responsáveis pelo controlo da gestão do tráfego, operadores de sistemas de transporte inteligentes;
- serviços postais e de correio rápido.

O relator considera que a dimensão do orçamento para o funcionamento do **Fundo de Resposta de Emergência para a Cibersegurança** determinará o seu êxito; por conseguinte, deve ser suficientemente avultado para apoiar os Estados-Membros na **preparação** para incidentes de cibersegurança significativos e em grande escala, para dar-lhes **resposta** e **recuperar** dos mesmos. O apoio à resposta a incidentes deve também ser disponibilizado às instituições, órgãos e organismos da União.

O **ciberescudo europeu** melhorará as capacidades de deteção de ciberameaças dos Estados-Membros. O **mecanismo de ciberemergência** complementará as ações dos Estados-Membros através do apoio de emergência para a preparação, resposta e recuperação imediata ou restabelecimento imediato do funcionamento dos serviços essenciais.

ALTERAÇÃO

A Comissão dos Transportes e do Turismo insta a Comissão da Indústria, da Investigação e da Energia, competente quanto à matéria de fundo, a ter em conta o seguinte:

Alteração 1

Proposta de regulamento
Considerando 2

Texto da Comissão	*Alteração*
(2) A magnitude, a frequência e o impacto dos incidentes de cibersegurança estão a aumentar, incluindo ataques de ciberespionagem, sequestro por programas maliciosos ou perturbação da cadeia de abastecimento. Os referidos incidentes constituem uma grave ameaça ao funcionamento dos sistemas de rede e informação. Tendo em conta a rápida evolução do cenário de ameaças, a ameaça de eventuais incidentes em grande escala que causem perturbações ou danos significativos às infraestruturas críticas exige uma maior preparação a todos os níveis do quadro de cibersegurança da União. Esta ameaça vai além da agressão militar da Rússia contra a Ucrânia e é provável que persista, dada a multiplicidade de intervenientes associados ao Estado, criminosos e ativistas háquer envolvidos nas atuais tensões geopolíticas. Tais incidentes podem impedir a prestação de serviços públicos e o exercício das atividades económicas, incluindo em setores críticos ou altamente críticos, gerar perdas financeiras importantes, minar a confiança dos utilizadores, causar graves prejuízos à economia da União e até ter consequências para a saúde ou ser potencialmente fatais. Além disso, os incidentes de cibersegurança são imprevisíveis, dado que, muitas vezes, surgem e evoluem em prazos muito curtos, não se confinam a uma área geográfica específica e ocorrem em simultâneo ou alastram-se imediatamente por vários	(2) A magnitude, a frequência e o impacto dos incidentes de cibersegurança estão a aumentar, incluindo ataques de ciberespionagem, sequestro por programas maliciosos ou perturbação da cadeia de abastecimento. Os referidos incidentes constituem uma grave ameaça ao funcionamento dos sistemas de rede e informação***, bem como às infraestruturas físicas e informáticas críticas***. Tendo em conta a rápida evolução do cenário de ameaças, a ameaça de eventuais incidentes em grande escala que causem perturbações ou danos significativos às infraestruturas críticas exige uma maior preparação a todos os níveis do quadro de cibersegurança da União. Esta ameaça vai além da agressão militar da Rússia contra a Ucrânia e é provável que persista, dada a multiplicidade de intervenientes associados ao Estado, criminosos e ativistas háquer envolvidos nas atuais tensões geopolíticas. Tais incidentes podem impedir a prestação de serviços públicos***, de serviços de transporte públicos e privados*** e o exercício das atividades económicas, incluindo em setores críticos ou altamente críticos, gerar perdas financeiras importantes, minar a confiança dos utilizadores, causar graves prejuízos à economia da ***União e à mobilidade na*** União e até ter consequências para a saúde ou ser potencialmente fatais. Além disso, os incidentes de cibersegurança são imprevisíveis, dado que, muitas vezes, surgem e evoluem em prazos muito curtos,

países.	não se confinam a uma área geográfica específica e ocorrem em simultâneo ou alastram-se imediatamente por vários países.

Alteração 2

Proposta de regulamento
Considerando 2-A (novo)

Texto da Comissão	*Alteração*
	(2-A) O setor dos transportes enfrenta ameaças cada vez mais graves à sua cibersegurança por parte de intervenientes patrocinados por Estados, cibercriminosos e ativistas da pirataria informática dirigidas a autoridades, operadores, fabricantes, fornecedores e prestadores de serviços dos transportes aéreos, marítimos, ferroviários e rodoviários. A Agência da União Europeia para a Cibersegurança (ENISA) registou, em 2022, um aumento de 25 % da média mensal de incidentes comunicados que afetam o setor dos transportes em relação aos níveis de 2021. A maioria dos ataques contra o setor dos transportes visa os sistemas informáticos, o que pode provocar perturbações operacionais[14-A].
	[14-A] ENISA (2023),«ENISA threat landscape: Transport sector» [Panorama das ameaças em 2023 elaborado pela ENISA: o setor dos transportes], páginas 7 e 17.

Alteração 3

Proposta de regulamento
Considerando 2-B (novo)

Texto da Comissão	*Alteração*
	(2-B) A invasão não provocada da

	Ucrânia pela Rússia originou um aumento considerável de incidentes de cibersegurança, nomeadamente ciberataques distribuídos de negação de serviço (DDoS) dirigidos ao setor dos transportes da UE e de zonas próximas da União, sobretudo aeroportos, transportes ferroviários e autoridades de transportes[14-B]. É muito provável que este tipo de ataques continue a aumentar.
	[14-B] ENISA (2023),«ENISA threat landscape: Transport sector» [Panorama das ameaças em 2023 elaborado pela ENISA: o setor dos transportes], página 9.

Alteração 4

Proposta de regulamento
Considerando 2-C (novo)

Texto da Comissão	*Alteração*
	(2-C) Os ciberataques visam as autoridades e os organismos de todos os subsetores dos transportes, afetando as empresas de transporte ferroviário e os gestores de infraestruturas, bem como os operadores portuários. No que diz respeito ao setor rodoviário, foram visados fabricantes de equipamento de origem, fornecedores e prestadores de serviços, bem como operadores de transportes públicos. No setor da aviação, os principais alvos foram as companhias aéreas e as entidades gestoras dos aeroportos, seguidas dos prestadores de serviços, dos operadores de transportes terrestres e da cadeia de abastecimento[14-C].
	[14-C] ENISA (2023),«ENISA threat landscape: Transport sector» [Panorama das ameaças em 2023 elaborado pela ENISA: o setor dos transportes], página

17.

Alteração 5

Proposta de regulamento
Considerando 3

Texto da Comissão	*Alteração*
(3) É necessário reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Tal como recomendado em três propostas diferentes da Conferência sobre o Futuro da Europa[16], é necessário aumentar a resiliência dos cidadãos, das empresas e das entidades que operam infraestruturas críticas contra as ameaças crescentes à cibersegurança, que podem ter impactos societais e económicos devastadores. Por conseguinte, é necessário investir em infraestruturas e serviços que apoiem uma deteção e uma resposta mais rápidas a ameaças e incidentes de cibersegurança, e os Estados-Membros necessitam de assistência para se prepararem melhor para incidentes de cibersegurança significativos e em grande escala, bem como para dar resposta aos mesmos. A União deve também aumentar as suas capacidades nestes domínios, nomeadamente no que diz respeito à recolha e análise de dados sobre ameaças e incidentes de cibersegurança.	(3) É necessário reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e apoiar a sua transformação digital, reforçando o nível de cibersegurança no mercado único digital. Tal como recomendado em três propostas diferentes da Conferência sobre o Futuro da Europa[16], é necessário aumentar a resiliência dos cidadãos, das empresas***, dos operadores de transportes*** e das entidades que operam infraestruturas críticas contra as ameaças crescentes à cibersegurança, que podem ter impactos societais e económicos devastadores. Por conseguinte, é necessário investir em infraestruturas e serviços que apoiem uma deteção e uma resposta mais rápidas a ameaças e incidentes de cibersegurança, e os Estados-Membros necessitam de assistência para se prepararem melhor para incidentes de cibersegurança significativos e em grande escala, bem como para dar resposta aos mesmos. A União deve também aumentar as suas capacidades nestes domínios, nomeadamente no que diz respeito à recolha e análise de dados sobre ameaças e incidentes de cibersegurança***, bem como ao estado e à evolução do mercado de trabalho no domínio da cibersegurança, uma vez que este desempenha um papel fundamental na prestação dos serviços de deteção e de resposta necessários***.
[16] https://futureu.europa.eu/en/	[16] https://futureu.europa.eu/en/

Alteração 6

Proposta de regulamento
Considerando 4

Texto da Comissão	*Alteração*
(4) A União já tomou uma série de medidas para reduzir as vulnerabilidades e aumentar a resiliência das infraestruturas e entidades críticas contra os riscos de cibersegurança, nomeadamente a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[17], a Recomendação (UE) 2017/1584 da Comissão[18], a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho[19] e o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[20]. Além disso, a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas convida os Estados-Membros a tomarem medidas urgentes e eficazes, bem como a cooperarem leal e eficientemente, de forma solidária e coordenada, entre si, com a Comissão e com outras autoridades públicas competentes a fim de reforçar a resiliência das infraestruturas críticas utilizadas para prestar serviços essenciais no mercado interno.	(4) A União já tomou uma série de medidas para reduzir as vulnerabilidades e aumentar a resiliência das infraestruturas e entidades críticas contra os riscos de cibersegurança, nomeadamente a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[17], a Recomendação (UE) 2017/1584 da Comissão[18], a Diretiva 2013/40/UE do Parlamento Europeu e do Conselho[19] e o Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[20]***, bem como a proposta de regulamento relativo às orientações da União para o desenvolvimento da rede transeuropeia de transportes e a proposta de Regulamento relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais (ato legislativo sobre a ciber-resiliência)***. Além disso, a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas convida os Estados-Membros a tomarem medidas urgentes e eficazes, bem como a cooperarem leal e eficientemente, de forma solidária e coordenada, entre si, com a Comissão e com outras autoridades públicas competentes a fim de reforçar a resiliência das infraestruturas críticas utilizadas para prestar serviços essenciais no mercado interno.
[17] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (JO L 333 de 27.12.2022).	[17] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (JO L 333 de 27.12.2022).
[18] Recomendação (UE) 2017/1584 da	[18] Recomendação (UE) 2017/1584 da

Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

[19] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, (JO L 218 de 14.8.2013, p. 8).

[20] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

Comissão, de 13 de setembro de 2017, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala (JO L 239 de 19.9.2017, p. 36).

[19] Diretiva 2013/40/UE do Parlamento Europeu e do Conselho, de 12 de agosto de 2013, relativa a ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, (JO L 218 de 14.8.2013, p. 8).

[20] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

Alteração 7

Proposta de regulamento
Considerando 4-A (novo)

Texto da Comissão	*Alteração*
	(4-A) Embora os operadores de transporte acolham com agrado o conjunto de ferramentas para a cibersegurança dos transportes da Comissão Europeia[2-A], que inclui informações de base sobre ameaças suscetíveis de afetar empresas de transporte (difusão de software malicioso, negação de serviço, acesso não autorizado e roubo e manipulação de software) e enumere boas práticas de atenuação, devem ser facultados aos operadores de transporte uma formação adequada em matéria de cibersegurança e instrumentos adequados para prevenir ciberameaças. O orçamento da União deve igualmente abranger apoios, nomeadamente formação, fornecidos pela ENISA a fim de permitir a execução eficaz das boas

práticas de atenuação incluídas no conjunto de ferramentas por parte dos operadores de transporte.

[1-A] ***«ENISA threat landscape: transport sector / ENISA» [Panorama das ameaças elaborado pela ENISA: o setor dos transportes/ENISA], março de 2023.***

[2-A] ***Comissão Europeia, (2021). Conjunto de ferramentas para a cibersegurança dos transportes, disponível em https://transport.ec.europa.eu/transport-themes/security-safety/cybersecurity_en.***

Alteração 8

Proposta de regulamento
Considerando 4-A (novo)

Texto da Comissão	*Alteração*
	(4-A) Uma abordagem coordenada à escala da União para reforçar a preparação e a resiliência das infraestruturas críticas, designadamente as infraestruturas dos transportes, baseia-se no reforço das capacidades dos Estados-Membros. Tal como reconhecido na recente comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Colmatar o défice de talentos no domínio da cibersegurança para reforçar a competitividade, o crescimento e a resiliência da UE»[19-A], a segurança da UE não pode ser garantida sem o ativo mais valioso da União: os seus cidadãos.

[19-A] ***Comunicação da Comissão ao Parlamento Europeu e ao Conselho intitulada «Colmatar o défice de talentos no domínio da cibersegurança para reforçar a competitividade, o crescimento e a resiliência da UE» («Academia de Competências de Cibersegurança»), COM(2023) 207 final.***

Alteração 9

Proposta de regulamento
Considerando 12

Texto da Comissão	*Alteração*
(12) Para prevenir, avaliar e responder de forma mais eficaz às ciberameaças e ciberincidentes, é necessário desenvolver um conhecimento mais aprofundado sobre as ameaças a ativos e infraestruturas críticos no território da União, incluindo a sua distribuição geográfica, interligação e potenciais efeitos em caso de ciberataques que afetem essas infraestruturas. Deve ser implantada uma infraestrutura de SOC de grande escala na União («ciberescudo europeu»), composta por várias plataformas transfronteiriças interoperáveis, cada uma agrupando vários SOC nacionais. Essa infraestrutura deve servir os interesses e necessidades nacionais e da União em matéria de cibersegurança, tirando partido de tecnologias de ponta para ferramentas avançadas de recolha e análise de dados, reforçando as capacidades de deteção e gestão da cibersegurança e proporcionando um conhecimento da situação em tempo real. Essa infraestrutura deve servir para aumentar a deteção de ameaças e incidentes de cibersegurança e, assim, complementar e apoiar as entidades e redes da União responsáveis pela gestão de crises na União, nomeadamente a Rede de Organizações de Coordenação de Cibercrises da UE («UE-CyCLONe»), tal como definida na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[24].	(12) Para prevenir, avaliar e responder de forma mais eficaz às ciberameaças e ciberincidentes, é necessário desenvolver um conhecimento mais aprofundado sobre as ameaças a ativos e infraestruturas críticos no território da União, incluindo a sua distribuição geográfica, interligação e potenciais efeitos em caso de ciberataques que afetem essas infraestruturas. ***Os referidos ativos críticos e infraestruturas críticas incluem sistemas de transporte inteligentes, que, embora sejam essenciais à mobilidade automatizada e multimodal, se baseiam em intercâmbios cruciais de dados sensíveis.*** Deve ser implantada uma infraestrutura de SOC de grande escala na União («ciberescudo europeu»), composta por várias plataformas transfronteiriças interoperáveis, cada uma agrupando vários SOC nacionais. Essa infraestrutura deve servir os interesses e necessidades nacionais e da União em matéria de cibersegurança, tirando partido de tecnologias de ponta para ferramentas avançadas de recolha e análise de dados, reforçando as capacidades de deteção e gestão da cibersegurança e proporcionando um conhecimento da situação em tempo real. Essa infraestrutura deve servir para aumentar a deteção de ameaças e incidentes de cibersegurança e, assim, complementar e apoiar as entidades e redes da União responsáveis pela gestão de crises na União, nomeadamente a Rede de Organizações de Coordenação de Cibercrises da UE («UE-CyCLONe»), tal como definida na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[24].

[24] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

[24] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

Alteração 10

Proposta de regulamento
Considerando 14-A (novo)

Texto da Comissão	*Alteração*
	(14-A) O setor dos transportes está a tornar-se, cada vez mais, uma das atividades mais lucrativas para os cibercriminosos, uma vez que os dados dos clientes são considerados uma mercadoria muito valiosa e a cadeia de abastecimento é um alvo cada vez maior. Por este motivo, as infraestruturas de transporte de natureza transfronteiriça ou que procedam ao intercâmbio de dados através de tecnologias sem fios devem ser consideradas um elemento fundamental de análise e de acompanhamento para os SOC nacionais e, sobretudo, para os SOC transfronteiriços. Por exemplo, a recente proposta de revisão do Regulamento RTE-T exige uma maior solidariedade e cooperação na partilha de informações sobre ciberameaças transfronteiriças que esta rede transnacional pode ter de enfrentar. Do mesmo modo, os sistemas de transporte inteligentes (STI) são essenciais para tornar os transportes mais seguros, eficazes e sustentáveis, embora tornem os sistemas de transporte mais vulneráveis a ciberataques que podem dar origem a acidentes, engarrafamentos ou provocar perdas económicas, tanto para operadores públicos como privados. A fim de garantir a segurança dos passageiros, a proteção dos dados dos utilizadores e

dos fornecedores e de evitar prejuízos financeiros, é essencial que o programa de execução da diretiva revista sobre os sistemas de transporte inteligentes inclua disposições e instrumentos que reforcem a colaboração entre os Estados-Membros para proceder à deteção de ameaças e incidentes de cibersegurança, à preparação para os mesmos e à resposta a dar-lhes.

Alteração 11

Proposta de regulamento
Considerando 15

Texto da Comissão	*Alteração*
(15) A nível nacional, a monitorização, a deteção e a análise das ciberameaças são normalmente asseguradas pelos SOC de entidades públicas e privadas, em combinação com as CSIRT. Além disso, as CSIRT trocam informações no contexto da rede de CSIRT, em conformidade com a Diretiva (UE) 2022/2555. Os SOC transfronteiriços devem constituir uma nova capacidade complementar à rede de CSIRT mediante a mutualização e partilha de dados sobre ameaças à cibersegurança provenientes de entidades públicas e privadas, a valorização desses dados através de análises de peritos e de ferramentas de ponta e infraestruturas adquiridas conjuntamente, e o contributo para o desenvolvimento das capacidades e da soberania tecnológica da União.	(15) A nível nacional, a monitorização, a deteção e a análise das ciberameaças são normalmente asseguradas pelos SOC de entidades públicas e privadas, em combinação com as CSIRT. Além disso, as CSIRT trocam informações no contexto da rede de CSIRT, em conformidade com a Diretiva (UE) 2022/2555. Os SOC transfronteiriços devem constituir uma nova capacidade complementar à rede de CSIRT mediante a mutualização e partilha de dados sobre ameaças à cibersegurança provenientes de entidades públicas e privadas, a valorização desses dados através de análises de peritos e de ferramentas de ponta e infraestruturas adquiridas conjuntamente, e o contributo para o desenvolvimento das capacidades e da soberania tecnológica da União. ***Neste contexto, a fim de reforçar a autonomia da União no domínio cibernético e no que se refere ao artigo 47.º, n.º 4, da proposta de Regulamento relativo às orientações da União para o desenvolvimento da rede transeuropeia de transportes (COM(2021)0812), é igualmente necessário impedir o acesso a dados que conduzam a ciberameaças mediante a aplicação de um quadro regulamentar sólido que reja a propriedade e os***

	investimentos estrangeiros em infraestruturas críticas, como os transportes.

Alteração 12

Proposta de regulamento
Considerando 21

Texto da Comissão	*Alteração*
(21) Embora o ciberescudo europeu seja um projeto de caráter civil, a comunidade de ciberdefesa poderá beneficiar do desenvolvimento de capacidades civis mais fortes de deteção e de conhecimento da situação para proteger as infraestruturas críticas da UE. Os SOC transfronteiriços, com o apoio da Comissão e do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança («ECCC»), e em cooperação com o alto representante da União para a Política Externa e a Política de Segurança («alto representante»), devem desenvolver progressivamente protocolos e normas específicos para permitir a cooperação com a comunidade de ciberdefesa, incluindo condições de investigação e de segurança. O desenvolvimento do ciberescudo europeu deve ser acompanhado de uma reflexão que permita uma futura colaboração com as redes e plataformas responsáveis pela partilha de informações na comunidade de ciberdefesa, em estreita cooperação com o alto representante.	(21) Embora o ciberescudo europeu seja um projeto de caráter civil, a comunidade de ciberdefesa poderá beneficiar do desenvolvimento de capacidades civis mais fortes de deteção e de conhecimento da situação para proteger as infraestruturas críticas da UE. Os SOC transfronteiriços, com o apoio da Comissão e do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança («ECCC»), e em cooperação com o alto representante da União para a Política Externa e a Política de Segurança («alto representante»), devem desenvolver progressivamente protocolos e normas específicos para permitir a cooperação com a comunidade de ciberdefesa, incluindo condições de investigação e de segurança. O desenvolvimento do ciberescudo europeu deve ser acompanhado de uma reflexão que permita uma futura colaboração com as redes e plataformas responsáveis pela partilha de informações na comunidade de ciberdefesa, em estreita cooperação com o alto representante. ***Deve igualmente possibilitar sinergias com o Plano de Ação para a Mobilidade Militar 2.0. Para funcionar corretamente, uma rede de mobilidade militar deve ser resiliente, designadamente no contexto de ciberameaças e de outras ameaças híbridas suscetíveis de afetar pontos críticos do sistema de transportes que sejam de dupla utilização. Por exemplo, um ciberataque a sistemas utilizados em aeroportos, portos ou ferrovias ou um***

	ciberataque a meios militares pode ter consequências graves. Consequentemente, a digitalização dos processos e dos procedimentos, nomeadamente para a cooperação civil e militar necessárias, exigirão o reforço dos sistemas informáticos contra ciberameaças.

Alteração 13

Proposta de regulamento
Considerando 21-A (novo)

Texto da Comissão	*Alteração*
	(21-A) Caso ocorra uma crise de cibersegurança, é fundamental que haja um intercâmbio eficaz de informações para garantir o conhecimento da situação nos setores dos transportes civis e militares. Este intercâmbio de informações deve também promover a cooperação entre as autoridades setoriais pertinentes responsáveis pelos transportes, as autoridades competentes em matéria de cibersegurança, os SOC e as CSIRT.

Alteração 14

Proposta de regulamento
Considerando 29

Texto da Comissão	*Alteração*
(29) No âmbito das ações de preparação, a fim de promover uma abordagem coerente e de reforçar a segurança em toda a União e o seu mercado interno, deve ser prestado apoio para testar e avaliar de forma coordenada a cibersegurança das entidades que operam nos setores altamente críticos identificados nos termos da Diretiva (UE) 2022/2555. Para o efeito, a Comissão, com o apoio da ENISA e em colaboração com o grupo de cooperação	(29) No âmbito das ações de preparação, a fim de promover uma abordagem coerente e de reforçar a segurança em toda a União e o seu mercado interno, deve ser prestado apoio para testar e avaliar de forma coordenada a cibersegurança das entidades que operam nos setores altamente críticos identificados nos termos da Diretiva (UE) 2022/2555. Para o efeito, a Comissão, com o apoio da ENISA e em colaboração com o grupo de cooperação

SRI criado pela Diretiva (UE) 2022/2555, deve identificar regularmente os setores ou subsetores pertinentes que devem ser elegíveis para receber apoio financeiro para a realização de testes coordenados a nível da União. Os setores ou subsetores devem ser selecionados do anexo I da Diretiva (UE) 2022/2555 («setores de importância crítica»). Os exercícios de teste coordenados devem basear-se em cenários e metodologias de risco comuns. A seleção dos setores e o desenvolvimento de cenários de risco devem ter em conta as avaliações dos riscos e os cenários de risco pertinentes à escala da União, incluindo a necessidade de evitar duplicações, como a avaliação dos riscos e os cenários de risco exigidos nas Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, a realizar pela Comissão, pelo alto representante e pelo grupo de cooperação SRI, em coordenação com os organismos e agências civis e militares competentes e com as redes estabelecidas, incluindo a UE-CyCLONe, bem como a avaliação do risco das redes e infraestruturas de comunicação solicitada pelo apelo ministerial conjunto de Nevers e realizada pelo grupo de cooperação SRI, com o apoio da Comissão e da ENISA, e em cooperação com o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE), as avaliações coordenadas dos riscos a realizar nos termos do artigo 22.º da Diretiva (UE) 2022/2555 e os testes de resiliência operacional digital previstos no Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho[29]. A seleção dos setores deve também ter em conta a Recomendação do Conselho relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas.

SRI criado pela Diretiva (UE) 2022/2555, deve identificar regularmente os setores ou subsetores pertinentes que devem ser elegíveis para receber apoio financeiro para a realização de testes coordenados a nível da União. Os setores ou subsetores devem ser selecionados do anexo I da Diretiva (UE) 2022/2555 («setores de importância crítica»). ***Deve ser prestada especial atenção ao setor dos transportes e aos seus subsetores (aéreo, ferroviário, marítimo e rodoviário), uma vez que integram infraestruturas críticas que, se afetadas por incidentes e ataques cibernéticos, poderiam prejudicar gravemente a segurança dos passageiros e dos operadores.*** Os exercícios de teste coordenados devem basear-se em cenários e metodologias de risco comuns. A seleção dos setores e o desenvolvimento de cenários de risco devem ter em conta as avaliações dos riscos e os cenários de risco pertinentes à escala da União, incluindo a necessidade de evitar duplicações, como a avaliação dos riscos e os cenários de risco exigidos nas Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, a realizar pela Comissão, pelo alto representante e pelo grupo de cooperação SRI, em coordenação com os organismos e agências civis e militares competentes e com as redes estabelecidas, incluindo a UE-CyCLONe, bem como a avaliação do risco das redes e infraestruturas de comunicação solicitada pelo apelo ministerial conjunto de Nevers e realizada pelo grupo de cooperação SRI, com o apoio da Comissão e da ENISA, e em cooperação com o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE), as avaliações coordenadas dos riscos a realizar nos termos do artigo 22.º da Diretiva (UE) 2022/2555 e os testes de resiliência operacional digital previstos no Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho[29]. A seleção dos setores deve também ter em conta a Recomendação do Conselho

relativa a uma abordagem coordenada à escala da União para reforçar a resiliência das infraestruturas críticas.

[29] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011.

[29] Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011.

Alteração 15

Proposta de regulamento
Considerando 30-A (novo)

Texto da Comissão	*Alteração*
	(30-A) Tendo em conta a importância crítica do setor e as consequências das ciberameaças na mobilidade e, consequentemente, na vida dos passageiros e dos peões, deve ser dada prioridade ao setor dos transportes no que diz respeito aos testes coordenados de preparação de entidades.

Alteração 16

Proposta de regulamento
Considerando 35-A (novo)

Texto da Comissão	*Alteração*
	(35-A) Tendo em conta o aumento das competências e das responsabilidades atribuídas à ENISA pela presente proposta e pela proposta de ato legislativo sobre a ciber-resiliência, é necessária a adoção do orçamento retificativo n.º 1/2022 da ENISA para a implementação-piloto de uma ação de apoio à cibersegurança. Para além disso, tendo em conta os interesses da União em

causa, devem ser atribuídos recursos financeiros e humanos suplementares à ENISA.

Alteração 17

Proposta de regulamento
Considerando 38-A (novo)

Texto da Comissão	*Alteração*
	(38-A) O desenvolvimento de competências e de aptidões deve, por conseguinte, ocupar um lugar central em todos os setores, sobretudo nos que são vulneráveis às ameaças de cibersegurança, designadamente pessoal que trabalha em transportes públicos ou em infraestruturas críticas, nomeadamente sistemas de controlo de comboios e ferramentas digitais de planeamento de transportes para todos os modos de transporte. A introdução e posterior desenvolvimento de uma cultura de cibersegurança são, portanto, fundamentais para o êxito da aplicação do presente regulamento, tanto para a sensibilização dos cidadãos como para os conhecimentos dos especialistas em todos os setores das infraestruturas críticas.

Alteração 18

Proposta de regulamento
Artigo 1 – parágrafo 2 – alínea a)

Texto da Comissão	*Alteração*
a) Reforçar a deteção e o conhecimento da situação comuns a nível da União relativamente a ciberameaças e ciberincidentes, permitindo assim reforçar a posição competitiva dos setores da indústria e dos serviços da União na economia digital e contribuir para a soberania tecnológica da União no domínio	a) Reforçar a deteção e o conhecimento da situação comuns a nível da União relativamente a ciberameaças e ciberincidentes, permitindo assim reforçar a posição competitiva dos setores da indústria***, das infraestruturas de transporte*** e dos serviços da União na economia digital e contribuir para a soberania tecnológica da União no domínio

da cibersegurança;	da cibersegurança;

Alteração 19

Proposta de regulamento
Artigo 1 – n.º 2 – alínea b)

Texto da Comissão	*Alteração*
b) Aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos na União e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, nomeadamente mediante a disponibilização de apoio da União para resposta a incidentes de cibersegurança a países terceiros associados ao Programa Europa Digital;	b) Aumentar o grau de preparação das entidades que operam em setores críticos e altamente críticos na União e reforçar a solidariedade através do desenvolvimento de capacidades comuns de resposta a incidentes de cibersegurança significativos ou em grande escala, ***prestando especial atenção às infraestruturas informáticas e físicas críticas,*** nomeadamente mediante a disponibilização de apoio da União para resposta a incidentes de cibersegurança a países terceiros associados ao Programa Europa Digital;

Alteração 20

Proposta de regulamento
Artigo 1 – n.º 2 – alínea c-A) (nova)

Texto da Comissão	*Alteração*
	c-A) Reforçar a preparação, a cooperação e a eficácia da União em matéria de proteção das infraestruturas e dos serviços de transporte nos Estados-Membros face a incidentes de cibersegurança, a fim de assegurar a continuidade do funcionamento do setor dos transportes, a integridade das cadeias de abastecimento e a mobilidade a nível da União.

Alteração 21

Proposta de regulamento
Artigo 3 – n.º 2 – parágrafo 1 – alínea c)

Texto da Comissão	*Alteração*
c) Contribuir para uma melhor proteção e para uma melhor resposta às ciberameaças;	c) Contribuir para uma melhor proteção e para uma melhor resposta às ciberameaças***, nomeadamente para as infraestruturas de transporte de natureza transfronteiriça, como a RTE-T, ou para o intercâmbio de dados através de tecnologias sem fios, como os sistemas de transporte inteligentes***;

Alteração 22

Proposta de regulamento
Artigo 3 – n.º 2 – parágrafo 2

Texto da Comissão	*Alteração*
O ciberescudo europeu deve ser desenvolvido em cooperação com a infraestrutura pan-europeia de computação de alto desempenho estabelecida nos termos do Regulamento (UE) 2021/1173.	O ciberescudo europeu deve ser desenvolvido em cooperação com a infraestrutura pan-europeia de computação de alto desempenho estabelecida nos termos do Regulamento (UE) 2021/1173. ***Deve permitir a colaboração, mediante normas e protocolos específicos, com a comunidade de ciberdefesa, de modo a garantir o desenvolvimento de capacidades civis mais fortes de deteção e de conhecimento da situação para proteger as infraestruturas críticas. Neste contexto, devem igualmente ser desenvolvidas sinergias com o Plano de Ação para a Mobilidade Militar 2.0 e deve ser assegurado um intercâmbio eficaz de informações, a fim de permitir o conhecimento da situação nos setores de transportes civis e militares.***

Alteração 23

Proposta de regulamento
Artigo 8 – n.º 2-A (novo)

Texto da Comissão	*Alteração*
	2-A. No seu parecer dirigido aos Estados-Membros no quadro da proposta

	de Regulamento relativo à rede transeuropeia de transportes (COM(2021)0812), a Comissão deve envolver o ciberescudo europeu, em especial os SOC transfronteiriços, sempre que qualquer tipo de participação ou de contribuição de uma pessoa singular de um país terceiro ou de uma empresa de um país terceiro seja suscetível de afetar a cibersegurança de infraestruturas críticas transfronteiriças, como a RTE-T.

Alteração 24

Proposta de regulamento
Artigo 10 – parágrafo 1 – alínea a)

Texto da Comissão	*Alteração*
a) Ações de preparação, nomeadamente testes coordenados de preparação de entidades que operam em setores altamente críticos na União;	a) Ações de preparação, nomeadamente testes coordenados de preparação de entidades que operam em setores altamente críticos na União***, prestando especial atenção às infraestruturas de transporte e aos seus subsetores, enumerados no anexo I da Diretiva (UE) 2022/2555***;

Alteração 25

Proposta de regulamento
Artigo 18 – n.º 2

Texto da Comissão	*Alteração*
2. Para elaborar o relatório de análise do incidente referido no n.º 1, a ENISA colabora com todas as partes interessadas pertinentes, incluindo representantes dos Estados-Membros, a Comissão, outras instituições, órgãos e organismos competentes da UE, prestadores de serviços de segurança geridos e utilizadores de serviços de cibersegurança. Se for caso disso, a ENISA colabora igualmente com as entidades afetadas por incidentes de cibersegurança significativos	2. Para elaborar o relatório de análise do incidente referido no n.º 1, a ENISA colabora com todas as partes interessadas pertinentes, incluindo representantes dos Estados-Membros, a Comissão, outras instituições, órgãos e organismos competentes da UE, prestadores de serviços de segurança geridos e utilizadores de serviços de cibersegurança. Se for caso disso, a ENISA colabora igualmente com as entidades afetadas por incidentes de cibersegurança significativos

ou em grande escala. Para apoiar a análise, a ENISA pode também consultar outros tipos de partes interessadas. Os representantes consultados devem divulgar qualquer potencial conflito de interesses.	ou em grande escala***, designadamente os operadores de transporte***. Para apoiar a análise, a ENISA pode também consultar outros tipos de partes interessadas. Os representantes consultados devem divulgar qualquer potencial conflito de interesses.

Alteração 26

Proposta de regulamento
Artigo 19 – parágrafo 1 – ponto 1 – alínea b)
Regulamento (UE) 2021/694
Artigo 6 – n.º 2-A (novo)

Texto da Comissão	*Alteração*
	2-A. Tendo em conta os interesses da União em causa, relacionados com as suas responsabilidades pela preparação de futuros sistemas de certificação nos termos do Regulamento (UE) 2019/881, as suas responsabilidades pela análise e avaliação de ciberameaças, de vulnerabilidades e de atenuação de ciberameaças, pela realização de um relatório de análise de incidentes para o mecanismo de análise de incidentes de cibersegurança e pela prestação de formação contra incidentes e ataques cibernéticos a operadores de infraestruturas críticas e à luz das novas responsabilidades que lhe incumbem no quadro da proposta de ato legislativo sobre a ciber-resiliência, a ENISA deve ser dotada dos recursos necessários no âmbito do orçamento da União, em conformidade com a legislação aplicável.

Alteração 27

Proposta de regulamento
Artigo 19 – parágrafo 1 – ponto 1-A (novo)
Regulamento (UE) 2021/694
Artigo 7 – n.º 1 – alínea c-A) (nova)

Texto da Comissão	*Alteração*

(1-A) O artigo 7.º é alterado do seguinte modo:

a) O n.º 1 é alterado do seguinte modo:

(1) É inserida a seguinte alínea c-A):

c-A) Apoiar uma formação de elevada qualidade para os operadores de transporte e os gestores e o pessoal de infraestruturas críticas de transporte, designadamente para partilhar e aplicar eficazmente práticas de atenuação face a incidentes ou ataques cibernéticos a infraestruturas críticas, nomeadamente as práticas incluídas no conjunto de ferramentas para a cibersegurança dos transportes.

PROCESSO DA COMISSÃO ENCARREGADA DE EMITIR PARECER

Título	Estabelecer medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ameaças e incidentes de cibersegurança
Referências	COM(2023)0209 – C9-0136/2023 – 2023/0109(COD)
Comissão competente quanto ao fundo Data de comunicação em sessão	ITRE 1.6.2023
Parecer emitido por Data de comunicação em sessão	TRAN 1.6.2023
Relator de parecer: Data de designação	Gheorghe Falcă 7.7.2023
Data de aprovação	25.10.2023
Resultado da votação final	+: 38 –: 0 0: 0
Deputados presentes no momento da votação final	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
Suplentes presentes no momento da votação final	Sara Cerdas, Josianne Cutajar, Roman Haider, Pär Holmgren, Pierre Karleskind, Colm Markey, Ljudmila Novak, Dorien Rookmaker

VOTAÇÃO NOMINAL FINAL NA COMISSÃO ENCARREGADA DE EMITIR PARECER

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

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções