Parlamento Europeu
2019-2024

Comissão dos Assuntos Externos

2023/0109(COD)

27.10.2023

PARECER

da Comissão dos Assuntos Externos

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: Dragoş Tudorache

PA_Legam

Alteração 1

Proposta de regulamento
Considerando 1

Texto da Comissão	*Alteração*
(1) A utilização e a dependência de tecnologias da informação e comunicação tornaram-se características fundamentais de todos os setores de atividade económica, uma vez que as nossas administrações públicas, as nossas empresas e os nossos cidadãos nunca estiveram tão interligados e dependentes de outros setores e países.	(1) A utilização e a dependência de tecnologias da informação e comunicação tornaram-se características fundamentais de todos os setores de atividade económica ***e militar***, uma vez que as nossas administrações públicas, as nossas empresas e os nossos cidadãos***, assim como os intervenientes no domínio militar e da defesa,*** nunca estiveram tão interligados e dependentes de outros setores e países.

Alteração 2

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	(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. ***O regresso da guerra ao nosso continente fez com que a gravidade destas ameaças se tornasse ainda mais pertinente. Estas ameaças vão*** além da agressão militar da Rússia contra a Ucrânia e é provável que ***persistam***, dada a multiplicidade de intervenientes associados

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 países.	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 ***e à segurança*** da União e até ter consequências para a saúde ou ser potencialmente fatais***, por serem suscetíveis de comprometer as instalações locais ou nacionais relacionadas com a segurança***. 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 países. ***A cibersegurança é importante para a proteção dos nossos valores europeus e garante o funcionamento das nossas democracias ao proteger os nossos processos democráticos e infraestruturas eleitorais de qualquer ingerência estrangeira.***

Alteração 3

Proposta de regulamento
Considerando 2-A (novo)

Texto da Comissão	*Alteração*
	(2-A) A cibersegurança é fundamental para salvaguardar a segurança da União e impedir que intervenientes maliciosos, sejam eles estatais ou não estatais, enfraqueçam a nossa democracia, economia e segurança. Importa evitar um cenário fragmentado, uma vez que tal situação não seria uma abordagem adequada, sobretudo perante o desafio de um futuro ciberataque em grande escala contra vários Estados-Membros simultaneamente ou contra as infraestruturas críticas transnacionais.

	Como tal, é necessário um organismo da União que funcione como uma plataforma de coordenação de todos os instrumentos, fundos e mecanismos existentes e futuros em matéria de cibersegurança.

Alteração 4

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 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***, assim como a sua capacidade para agir pró-ativamente e reagir de forma determinada a ameaças e incidentes de cibersegurança***.
[16] https://futureu.europa.eu/en/	[16] https://futureu.europa.eu/en/

Alteração 5

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]. 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***,*** eficiente ***e pró-ativamente***, 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. ***Ademais, a União aprovou e lançou a sua Bússola Estratégica para a Segurança e a Defesa em março de 2022, que se centra, nomeadamente, no reforço da cibersegurança e no aumento da cooperação internacional com aliados e parceiros democráticos que partilham das mesmas ideias, em particular nesta matéria. De resto, a cibersegurança foi um ponto focal da recente terceira Declaração Conjunta UE-OTAN, de janeiro de 2023. Em especial, o relatório de avaliação final do grupo de missão UE-OTAN recomendou que se tirasse pleno partido das sinergias entre a UE e a OTAN[1], incluindo através do***

intercâmbio, entre intervenientes civis e militares, de boas práticas relativas à aplicação de políticas e legislação pertinentes relacionadas com o ciberespaço.

[1] https://commission.europa.eu/document/34209534-3c59-4b01-b4f0-b2c6ee2df736_en

---

[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 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).

[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 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 6

Proposta de regulamento
Considerando 6

Texto da Comissão	*Alteração*
(6) A Comunicação Conjunta sobre a política de ciberdefesa da UE[22], adotada em 10 de novembro de 2022, anunciava uma iniciativa da UE em matéria de cibersolidariedade com os seguintes objetivos: o reforço das capacidades comuns de deteção, conhecimento da situação e resposta da UE mediante a promoção da implantação de uma infraestrutura de centros de operações de segurança («SOC») na UE, o apoio à criação progressiva de uma reserva de cibersegurança a nível da UE com serviços de fornecedores privados de confiança e a avaliação das potenciais vulnerabilidades das entidades críticas com base em avaliações dos riscos da UE.	(6) A Comunicação Conjunta sobre a política de ciberdefesa da UE[22], adotada em 10 de novembro de 2022, anunciava uma iniciativa da UE em matéria de cibersolidariedade com os seguintes objetivos: o reforço das capacidades comuns de deteção, conhecimento da situação e resposta da UE mediante a promoção da implantação de uma infraestrutura de centros de operações de segurança («SOC») na UE, o apoio à criação progressiva de uma reserva de cibersegurança a nível da UE com serviços de fornecedores privados de confiança e a avaliação das potenciais vulnerabilidades das entidades críticas com base em avaliações dos riscos da UE. ***Por outro lado, conforme salientado pelo Conselho nas suas conclusões sobre a política de ciberdefesa da UE[1], a rápida evolução do panorama das ciberameaças e o ritmo acelerado dos desenvolvimentos tecnológicos demonstram também a necessidade de reforçar a coordenação e a cooperação entre os setores civil e militar.*** ***[1] Conclusões do Conselho sobre a política de ciberdefesa da UE, aprovadas pelo Conselho na sua reunião de 22 de maio de 2023 (9618/23).***
[22] Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Política de ciberdefesa da UE» [JOIN(2022) 49 final].	[22] Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Política de ciberdefesa da UE» [JOIN(2022) 49 final].

Alteração 7

Proposta de regulamento
Considerando 6-A (novo)

Texto da Comissão	*Alteração*
	(6-A) Tendo em conta o esbatimento da

linha entre os domínios civil e militar e a dupla utilização inerente às ciberferramentas e tecnologias, é necessária uma abordagem abrangente e holística do domínio digital. Importa criar mecanismos adequados de gestão de crises e governação, para lidar com eventuais incidentes e crises de cibersegurança em grande escala que envolvam dois ou mais Estados-Membros. Essas estruturas devem organizar o intercâmbio de informações, a coordenação e a cooperação com as estruturas de segurança externa e de gestão de crises militares da União e com os organismos dos Estados-Membros responsáveis pela segurança e defesa (a comunidade de ciberdefesa). O mesmo deve aplicar-se às operações e missões da política comum de segurança e defesa conduzidas pela União para garantir a paz e a estabilidade na sua vizinhança e para além dela.

Alteração 8

Proposta de regulamento
Considerando 7

Texto da Comissão	*Alteração*
(7) É necessário reforçar a deteção e o conhecimento da situação relativamente a ciberameaças e ciberincidentes na União e intensificar a solidariedade, aumentando a preparação e as capacidades dos Estados-Membros e da União para dar resposta a incidentes de cibersegurança significativos e em grande escala. Por conseguinte, importa implantar uma infraestrutura pan-europeia de SOC (ciberescudo europeu) para criar e reforçar capacidades comuns de deteção e conhecimento da situação; criar um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande	(7) É necessário reforçar a deteção e o conhecimento da situação relativamente a ciberameaças e ciberincidentes na União e intensificar a solidariedade, aumentando a preparação e as capacidades dos Estados-Membros e da União para dar resposta a incidentes de cibersegurança significativos e em grande escala. Por conseguinte, importa implantar uma infraestrutura pan-europeia de SOC (ciberescudo europeu) para criar e reforçar capacidades comuns de deteção e conhecimento da situação; criar um mecanismo de emergência em matéria de cibersegurança para apoiar os Estados-Membros na preparação, resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande

escala; e criar um mecanismo de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala específicos. As referidas ações não prejudicam os artigos 107.º e 108.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

escala***, incluindo os incidentes que envolvam vários Estados-Membros. Sempre que viável e necessário, um mecanismo de emergência em matéria de cibersegurança deve organizar a partilha de informações e a cooperação com as autoridades de defesa dos Estados-Membros, com o apoio das instituições, órgãos e organismos da União (comunidade de ciberdefesa da UE)***; e criar um mecanismo de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala específicos. ***Estas novas estruturas devem igualmente apoiar as operações e missões da PCSD da UE.*** As referidas ações não prejudicam os artigos 107.º e 108.º do Tratado sobre o Funcionamento da União Europeia (TFUE).

Alteração 9

Proposta de regulamento
Considerando 11

Texto da Comissão	*Alteração*
(11) Para efeitos de boa gestão financeira, devem ser estabelecidas regras específicas para a transição de dotações de autorização e de pagamento não utilizadas. Respeitando o princípio de que o orçamento da União é fixado anualmente, o presente regulamento deve, devido à natureza imprevisível, excecional e específica do panorama da cibersegurança, prever possibilidades de transição de fundos não utilizados para além dos previstos no Regulamento Financeiro, maximizando assim a capacidade do mecanismo de emergência em matéria de cibersegurança para ajudar os Estados-Membros a lutar eficazmente contra as ciberameaças.	(11) Para efeitos de boa gestão financeira, devem ser estabelecidas regras específicas para a transição de dotações de autorização e de pagamento não utilizadas. Respeitando o princípio de que o orçamento da União é fixado anualmente, o presente regulamento deve, devido à natureza imprevisível, excecional e específica do panorama da cibersegurança, prever possibilidades de transição de fundos não utilizados para além dos previstos no Regulamento Financeiro, maximizando assim a capacidade do mecanismo de emergência em matéria de cibersegurança para ajudar os Estados-Membros a lutar eficazmente contra as ciberameaças. ***Essas regras específicas permitirão igualmente um apoio financeiro a mais longo prazo com vista à aquisição conjunta de ferramentas e***

	infraestruturas ultrasseguras de próxima geração, de modo a melhorar as capacidades de deteção coletivas através da utilização das mais recentes tecnologias de inteligência artificial (IA) e análise de dados.

Alteração 10

Proposta de regulamento
Considerando 13

Texto da Comissão	*Alteração*
(13) Cada Estado-Membro deve designar um organismo público a nível nacional encarregado de coordenar as atividades de deteção de ciberameaças nesse Estado-Membro. Estes SOC nacionais devem funcionar como ponto de referência e acesso a nível nacional para a participação no ciberescudo europeu e assegurar que as informações sobre ciberameaças provenientes de entidades públicas e privadas são partilhadas e recolhidas a nível nacional de forma eficaz e simplificada.	(13) Cada Estado-Membro deve designar um organismo público a nível nacional encarregado de coordenar as atividades de deteção de ciberameaças nesse Estado-Membro. Estes SOC nacionais devem funcionar como ponto de referência e acesso a nível nacional para a participação no ciberescudo europeu e assegurar que as informações sobre ciberameaças provenientes de entidades públicas e privadas são partilhadas e recolhidas a nível nacional de forma eficaz e simplificada. ***Sempre que viável e necessário, os SOC devem também permitir a participação de entidades de defesa, estabelecendo um «pilar de defesa» em termos de governação e do tipo de informações partilhadas, conforme estipulado na Comunicação Conjunta sobre a política de ciberdefesa da UE[1] e defendido pelo alto representante.***
	[1] Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Política de ciberdefesa da UE» [JOIN(2022) 49 final].

Alteração 11

Proposta de regulamento
Considerando 14

Texto da Comissão	*Alteração*
(14) No âmbito do ciberescudo europeu, devem ser criados vários centros de operações de cibersegurança transfronteiriços («SOC transfronteiriços»), que devem reunir os SOC nacionais de, pelo menos, três Estados-Membros para que os benefícios da deteção de ameaças transfronteiras e da partilha e gestão de informações possam ser plenamente alcançados. O objetivo geral dos SOC transfronteiriços deve ser o reforço das capacidades de análise, prevenção e deteção de ameaças à cibersegurança e o apoio à produção de informações de alta qualidade sobre ameaças à cibersegurança, nomeadamente através da partilha de dados de várias fontes, públicas ou privadas, bem como da partilha e utilização conjunta de ferramentas de ponta, e do desenvolvimento conjunto de capacidades de deteção, análise e prevenção num ambiente de confiança. Os SOC transfronteiriços devem proporcionar novas capacidades adicionais, tendo por base e complementando os SOC existentes, as equipas de resposta a incidentes informáticos («CSIRT») e outros intervenientes relevantes.	(14) No âmbito do ciberescudo europeu, devem ser criados vários centros de operações de cibersegurança transfronteiriços («SOC transfronteiriços»), que devem reunir os SOC nacionais de, pelo menos, três Estados-Membros***, incluindo um «pilar de defesa»,*** para que os benefícios da deteção de ameaças transfronteiras e da partilha e gestão de informações possam ser plenamente alcançados. O objetivo geral dos SOC transfronteiriços deve ser o reforço das capacidades de análise, prevenção e deteção de ameaças à cibersegurança e o apoio à produção de informações de alta qualidade sobre ameaças à cibersegurança, nomeadamente através da partilha de dados de várias fontes, públicas ou privadas, ***e, quando viável e necessário, de fontes militares, com orientações suficientes sobre a partilha de informações,*** bem como da partilha e utilização conjunta de ferramentas de ponta, e do desenvolvimento conjunto de capacidades de deteção, análise e prevenção num ambiente de confiança. Os SOC transfronteiriços devem proporcionar novas capacidades adicionais, tendo por base e complementando os SOC existentes, as equipas de resposta a incidentes informáticos («CSIRT») e outros intervenientes relevantes.

Alteração 12

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	(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.

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 ***resiliência*** da União.

Alteração 13

Proposta de regulamento
Considerando 16

Texto da Comissão	*Alteração*
(16) Os SOC transfronteiriços devem funcionar como um ponto central que permita uma ampla mutualização de dados pertinentes e informações sobre ciberameaças, possibilitar a divulgação de informações sobre ameaças entre um conjunto vasto e diversificado de intervenientes [por exemplo, equipas de resposta a emergências informáticas («CERT»), CSIRT, centros de partilha e análise de informações («ISAC») e operadores de infraestruturas críticas]. As informações trocadas entre os participantes num SOC transfronteiriço podem incluir dados de redes e sensores, fluxos de informações sobre ameaças, indicadores de exposição a riscos e informações contextualizadas sobre incidentes, ameaças e vulnerabilidades. Além disso, os SOC transfronteiriços devem também celebrar acordos de cooperação com outros SOC transfronteiriços.	(16) Os SOC transfronteiriços devem funcionar como um ponto central que permita uma ampla mutualização de dados pertinentes e informações sobre ciberameaças, possibilitar a divulgação de informações sobre ameaças entre um conjunto vasto e diversificado de intervenientes [por exemplo, equipas de resposta a emergências informáticas («CERT»), CSIRT, centros de partilha e análise de informações («ISAC») e operadores de infraestruturas críticas***, bem como a comunidade de ciberdefesa***]. As informações trocadas entre os participantes num SOC transfronteiriço podem incluir dados de redes e sensores, fluxos de informações sobre ameaças, indicadores de exposição a riscos e informações contextualizadas sobre incidentes, ameaças e vulnerabilidades. Além disso, os SOC transfronteiriços devem também celebrar acordos de cooperação com outros SOC transfronteiriços ***e, quando criada, com a rede operacional de equipas militares de resposta a emergências informáticas***

(MICNET).

Alteração 14

Proposta de regulamento
Considerando 17

Texto da Comissão	*Alteração*
(17) A partilha do conhecimento da situação entre as autoridades competentes é uma condição prévia indispensável para a preparação e coordenação a nível da União no que diz respeito a incidentes de cibersegurança significativos e em grande escala. A Diretiva (UE) 2022/2555 cria a UE-CyCLONe para apoiar a gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível operacional e para assegurar o intercâmbio regular de informações pertinentes entre os Estados-Membros e as instituições, órgãos e organismos da União. A Recomendação (UE) 2017/1584 sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala aborda o papel de todos os intervenientes relevantes. A Diretiva (UE) 2022/2555 recorda igualmente as responsabilidades da Comissão no âmbito do Mecanismo de Proteção Civil da União (MPCU), criado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, bem como no que se refere à apresentação de relatórios analíticos para o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR) ao abrigo da Decisão de Execução (UE) 2018/1993. Por conseguinte, nas situações em que os SOC transfronteiriços obtenham informações relacionadas com um incidente de cibersegurança em grande escala, potencial ou em curso, devem fornecer informações pertinentes à UE-CyCLONe, à rede de CSIRT e à Comissão. Concretamente, dependendo da situação, as informações a partilhar podem incluir informações técnicas, informações sobre a natureza e os	(17) A partilha do conhecimento da situação entre as autoridades competentes é uma condição prévia indispensável para a preparação e coordenação a nível da União no que diz respeito a incidentes de cibersegurança significativos e em grande escala. A Diretiva (UE) 2022/2555 cria a UE-CyCLONe para apoiar a gestão coordenada de crises e incidentes de cibersegurança em grande escala a nível operacional e para assegurar o intercâmbio regular de informações pertinentes entre os Estados-Membros e as instituições, órgãos e organismos da União. A Recomendação (UE) 2017/1584 sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala aborda o papel de todos os intervenientes relevantes. A Diretiva (UE) 2022/2555 recorda igualmente as responsabilidades da Comissão no âmbito do Mecanismo de Proteção Civil da União (MPCU), criado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, bem como no que se refere à apresentação de relatórios analíticos para o Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR) ao abrigo da Decisão de Execução (UE) 2018/1993. Por conseguinte, nas situações em que os SOC transfronteiriços obtenham informações relacionadas com um incidente de cibersegurança em grande escala, potencial ou em curso, devem fornecer informações pertinentes à UE-CyCLONe, à rede de CSIRT***, à comunidade de ciberdefesa*** e à Comissão. Concretamente, dependendo da situação, as informações a partilhar podem incluir informações técnicas, informações

motivos do agressor ou potencial agressor, bem como informações não técnicas de nível mais elevado sobre um incidente de cibersegurança em grande escala, potencial ou em curso. Neste contexto, deve ser dada a devida atenção ao princípio da necessidade de conhecer e à natureza potencialmente sensível das informações partilhadas.	sobre a natureza e os motivos do agressor ou potencial agressor, bem como informações não técnicas de nível mais elevado sobre um incidente de cibersegurança em grande escala, potencial ou em curso. Neste contexto, deve ser dada a devida atenção ao princípio da necessidade de conhecer e à natureza potencialmente sensível das informações partilhadas.

Alteração 15

Proposta de regulamento
Considerando 19

Texto da Comissão	*Alteração*
(19) A fim de permitir o intercâmbio de dados sobre ameaças à cibersegurança provenientes de várias fontes, em grande escala e num ambiente de confiança, as entidades que participam no ciberescudo europeu devem estar equipadas com ferramentas, equipamentos e infraestruturas de ponta e altamente seguros. Tal deverá permitir a melhoria das capacidades de deteção coletivas e alertas atempados às autoridades e entidades pertinentes, nomeadamente através da utilização das mais recentes tecnologias de inteligência artificial e de análise de dados.	(19) A fim de permitir o intercâmbio de dados sobre ameaças à cibersegurança provenientes de várias fontes, em grande escala e num ambiente de confiança, as entidades que participam no ciberescudo europeu***, excetuando os fornecedores de alto risco de produtos críticos com elementos digitais,*** devem estar equipadas com ferramentas, equipamentos e infraestruturas de ponta e altamente seguros. Tal deverá permitir a melhoria das capacidades de deteção coletivas e alertas atempados às autoridades e entidades pertinentes, nomeadamente através da utilização das mais recentes tecnologias de inteligência artificial e de análise de dados. ***É fundamental garantir uma supervisão humana durante a utilização da inteligência artificial e assegurar que quem exerce tal função disponha de um nível suficiente de literacia em inteligência artificial e do apoio e autoridade necessários para o efeito.***

Alteração 16

Proposta de regulamento
Considerando 19-A (novo)

Texto da Comissão	*Alteração*
	(19-A) Em conformidade com o Regulamento [XX/XXXX] (Regulamento Ciber-resiliência)], as entidades que participam no ciberescudo europeu também devem observar os requisitos previstos no presente regulamento no que se refere a todos os produtos com elementos digitais. Tendo em conta os riscos acrescidos decorrentes das dependências económicas, cumpre minimizar a exposição a fornecedores de alto risco de produtos críticos, o que deve ser feito através de um quadro estratégico comum para a segurança económica da UE. As dependências de fornecedores de alto risco de produtos críticos com elementos digitais acarretam um risco estratégico que deve ser atenuado a nível da União, em particular sempre que um país se envolva em espionagem económica ou coerção económica e a sua legislação permita um acesso arbitrário a quaisquer tipos de operações ou dados empresariais, e principalmente quando esteja prevista a utilização de produtos críticos pelas entidades essenciais a que se refere a Diretiva (UE) 2022/2555.

Alteração 17

Proposta de regulamento
Considerando 20

Texto da Comissão	*Alteração*
(20) Ao recolher, partilhar e trocar dados, o ciberescudo europeu deverá reforçar a soberania tecnológica da União. A mutualização de dados selecionados de alta qualidade deverá também contribuir para o desenvolvimento de tecnologias avançadas de inteligência artificial e de análise de dados. A referida mutualização de dados deve ser facilitada através da ligação do ciberescudo europeu à	(20) Ao recolher, partilhar e trocar dados, o ciberescudo europeu deverá reforçar a soberania tecnológica***, a autonomia estratégica, a competitividade e a resiliência*** da União. A mutualização de dados selecionados de alta qualidade deverá também contribuir para o desenvolvimento de tecnologias avançadas de inteligência artificial e de análise de dados. A referida mutualização de dados

infraestrutura pan-europeia de computação de alto desempenho criada pelo Regulamento (UE) 2021/1173 do Conselho[25].

deve ser facilitada através da ligação do ciberescudo europeu à infraestrutura pan-europeia de computação de alto desempenho criada pelo Regulamento (UE) 2021/1173 do Conselho[25].

---

[25] Regulamento (UE) 2021/1173 do Conselho, de 13 de julho de 2021, que cria a Empresa Comum para a Computação Europeia de Alto Desempenho e revoga o Regulamento (UE) 2018/1488 (JO L 256 de 19.7.2021, p. 3).

[25] Regulamento (UE) 2021/1173 do Conselho, de 13 de julho de 2021, que cria a Empresa Comum para a Computação Europeia de Alto Desempenho e revoga o Regulamento (UE) 2018/1488 (JO L 256 de 19.7.2021, p. 3).

Alteração 18

Proposta de regulamento
Considerando 25

Texto da Comissão	*Alteração*
(25) O mecanismo de ciberemergência deve prestar apoio aos Estados-Membros em complemento das suas próprias medidas e recursos, assim como de outras opções de apoio existentes para a resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala, tais como os serviços prestados pela Agência da União Europeia para a Cibersegurança (ENISA) em conformidade com o seu mandato, a resposta coordenada e a assistência da rede de CSIRT, o apoio à atenuação por parte da UE-CyCLONe, bem como a assistência mútua entre os Estados-Membros, nomeadamente no contexto do artigo 42.º, n.º 7, do TUE, das equipas de resposta rápida a ciberataques no âmbito da CEP e das equipas de resposta rápida às ameaças híbridas***[2]***. Deve atender à necessidade de assegurar a disponibilidade de meios especializados para apoiar a preparação e a resposta a incidentes de cibersegurança em toda a União e em países terceiros.	(25) O mecanismo de ciberemergência deve prestar apoio aos Estados-Membros em complemento das suas próprias medidas e recursos, assim como de outras opções de apoio existentes para a resposta e recuperação imediata de incidentes de cibersegurança significativos e em grande escala, tais como os serviços prestados pela Agência da União Europeia para a Cibersegurança (ENISA) em conformidade com o seu mandato, a resposta coordenada e a assistência da rede de CSIRT, o apoio à atenuação por parte da UE-CyCLONe, bem como a assistência mútua entre os Estados-Membros, nomeadamente no contexto do artigo 42.º, n.º 7, do TUE, das equipas de resposta rápida a ciberataques no âmbito da CEP***[1], do novo projeto da CEP, o Centro de coordenação do domínio da cibernética e da informação, e do seu sucessor proposto, o Centro de Coordenação da Ciberdefesa da UE (EUCDCC),*** e das equipas de resposta rápida às ameaças híbridas. Deve atender à necessidade de assegurar a disponibilidade de meios especializados para apoiar a preparação e a resposta a incidentes de

cibersegurança em toda a União e em países terceiros***, em especial os países candidatos à adesão à UE alinhados com a política externa e de segurança comum e com a política comum de segurança e defesa da UE, apoiando-os no desenvolvimento das suas cibercapacidades e no reforço da cooperação regional e transfronteiriça entre si no domínio cibernético***.

[1] DECISÃO (PESC) 2017/2315 DO CONSELHO, de 11 de dezembro de 2017, que estabelece uma cooperação estruturada permanente (CEP) e determina a lista de Estados-Membros participantes.

---

[26] DECISÃO (PESC) 2017/2315 DO CONSELHO, de 11 de dezembro de 2017, que estabelece uma cooperação estruturada permanente (CEP) e determina a lista de Estados-Membros participantes.

---

[26] DECISÃO (PESC) 2017/2315 DO CONSELHO, de 11 de dezembro de 2017, que estabelece uma cooperação estruturada permanente (CEP) e determina a lista de Estados-Membros participantes.

Alteração 19

Proposta de regulamento
Considerando 26

Texto da Comissão	*Alteração*
(26) O presente instrumento não prejudica os procedimentos e quadros de coordenação da resposta a situações de crise a nível da União, em especial o MPCU[27], o IPCR[28], e a Diretiva (UE) 2022/2555. Pode contribuir para, ou complementar, ações executadas no contexto do artigo 42.º, n.º 7, do TUE ou nas situações definidas no artigo 222.º do TFUE. A utilização deste instrumento deve também ser coordenada com a aplicação das medidas do conjunto de instrumentos de ciberdiplomacia, ***se for caso disso***.	(26) O presente instrumento não prejudica os procedimentos e quadros de coordenação da resposta a situações de crise a nível da União, em especial o MPCU[27], o IPCR[28], e a Diretiva (UE) 2022/2555. Pode contribuir para, ou complementar, ações executadas no contexto do artigo 42.º, n.º 7, do TUE ou nas situações definidas no artigo 222.º do TFUE. A utilização deste instrumento deve também ser coordenada com a aplicação das medidas do conjunto de instrumentos de ciberdiplomacia, ***melhorando, a nível estratégico, operacional e técnico, a cooperação entre as comunidades de ciberdefesa e outras cibercomunidades,***

	em particular com vista a reforçar as capacidades de luta contra as ameaças à cibersegurança provenientes de fora da UE, incluindo medidas restritivas, que podem ser usadas para prevenir e responder a ciberatividades mal intencionadas.
[27] Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 347 de 20.12.2013, p. 924).	[27] Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativa a um Mecanismo de Proteção Civil da União Europeia (JO L 347 de 20.12.2013, p. 924).
[28] Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR) e em conformidade com a 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.	[28] Mecanismo Integrado da UE de Resposta Política a Situações de Crise (IPCR) e em conformidade com a 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.

Alteração 20

Proposta de regulamento
Considerando 28

Texto da Comissão	*Alteração*
(28) A Diretiva (UE) 2022/2555 exige que os Estados-Membros designem ou criem uma ou mais autoridades de gestão de cibercrises e se certifiquem de que dispõem dos recursos adequados para desempenhar as suas funções de forma eficaz e eficiente. Exige igualmente que os Estados-Membros identifiquem as capacidades, os ativos e os procedimentos que podem ser utilizados em caso de crise, bem como que adotem um plano nacional de resposta a crises e incidentes de cibersegurança em grande escala que estabeleça os objetivos e as modalidades de gestão de crises e de incidentes de cibersegurança em grande escala. Os Estados-Membros são igualmente obrigados a criar uma ou várias CSIRT	(28) A Diretiva (UE) 2022/2555 exige que os Estados-Membros designem ou criem uma ou mais autoridades de gestão de cibercrises e se certifiquem de que dispõem dos recursos adequados para desempenhar as suas funções de forma eficaz e eficiente. Exige igualmente que os Estados-Membros identifiquem as capacidades, os ativos e os procedimentos que podem ser utilizados em caso de crise, bem como que adotem um plano nacional de resposta a crises e incidentes de cibersegurança em grande escala que estabeleça os objetivos e as modalidades de gestão de crises e de incidentes de cibersegurança em grande escala. Os Estados-Membros são igualmente obrigados a criar uma ou várias CSIRT

responsáveis pelo tratamento de incidentes de acordo com um processo bem definido e que abranja, pelo menos, os setores, subsetores e tipos de entidades incluídos no âmbito de aplicação da referida diretiva, bem como a assegurar que as mesmas dispõem dos recursos adequados para desempenharem eficazmente as suas funções. O presente regulamento não prejudica o papel da Comissão na garantia do cumprimento, pelos Estados-Membros, das obrigações decorrentes da Diretiva (UE) 2022/2555. O mecanismo de ciberemergência deve prestar assistência para ações destinadas a reforçar a preparação, bem como para ações de resposta a incidentes que visem atenuar o impacto dos incidentes de cibersegurança significativos e em grande escala, apoiar a recuperação imediata e/ou restabelecer o funcionamento dos serviços essenciais.

responsáveis pelo tratamento de incidentes de acordo com um processo bem definido e que abranja, pelo menos, os setores, subsetores e tipos de entidades incluídos no âmbito de aplicação da referida diretiva, bem como a assegurar que as mesmas dispõem dos recursos adequados para desempenharem eficazmente as suas funções. O presente regulamento não prejudica o papel da Comissão na garantia do cumprimento, pelos Estados-Membros, das obrigações decorrentes da Diretiva (UE) 2022/2555. O mecanismo de ciberemergência deve prestar assistência para ações destinadas a reforçar a preparação, bem como para ações de resposta a incidentes que visem atenuar o impacto dos incidentes de cibersegurança significativos e em grande escala, apoiar a recuperação imediata e/ou restabelecer o funcionamento dos serviços essenciais***, utilizando de forma adequada todo o leque de opções defensivas à disposição das comunidades civil e militar***.

Alteração 21

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 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	(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.

da União. ***Se for caso disso, deve também ser associado o Serviço Europeu para a Ação Externa (SEAE), em especial através do Centro de Análise de Informações da UE (INTCEN) e da sua Célula de Fusão contra as Ameaças Híbridas, com o apoio da Direção de Informações do Estado-Maior da União Europeia (EMUE), ao abrigo da Capacidade Única de Análise de Informações (SIAC), de modo a fornecer avaliações atualizadas, contribuindo assim para a identificação dos*** setores ou subsetores ***que*** 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. ***Esses exercícios deverão também desempenhar um papel importante no que se refere a melhorar a cooperação entre entidades civis e militares. Quando organizam exercícios, a Comissão, o SEAE e a ENISA devem, por conseguinte, ponderar sistematicamente a inclusão de participantes de outras cibercomunidades, como a Agência Europeia de Defesa (AED) e outras entidades pertinentes.*** 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***[1]***. 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.
	[1] 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.	[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 22

Proposta de regulamento
Considerando 32

Texto da Comissão	*Alteração*
(32) O mecanismo de ciberemergência deve apoiar a assistência prestada pelos Estados-Membros a um Estado-Membro afetado por um incidente de cibersegurança significativo ou em grande escala, incluindo pela rede de CSIRT estabelecida no artigo 15.º da Diretiva (UE) 2022/2555. Os Estados-Membros que prestam	(32) O mecanismo de ciberemergência deve apoiar a assistência prestada pelos Estados-Membros a um Estado-Membro afetado por um incidente de cibersegurança significativo ou em grande escala, incluindo pela rede de CSIRT estabelecida no artigo 15.º da Diretiva (UE) 2022/2555. Os Estados-Membros que prestam

assistência devem ser autorizados a apresentar pedidos para cobrir os custos relacionados com o envio de equipas de peritos no quadro da assistência mútua. Os custos elegíveis podem incluir as despesas de viagem, alojamento e as ajudas de custo diárias dos peritos em cibersegurança.	assistência devem ser autorizados a apresentar pedidos para cobrir os custos relacionados com o envio de equipas de peritos no quadro da assistência mútua***, assegurando uma coordenação eficiente entre os programas e instrumentos pertinentes da UE, incluindo o Mecanismo Europeu de Apoio à Paz (MEAP), a PESC e o IVCDCI, ao prestar assistência a países terceiros, em especial a Ucrânia e a Moldávia***. Os custos elegíveis podem incluir as despesas de viagem, alojamento e as ajudas de custo diárias dos peritos em cibersegurança.

Alteração 23

Proposta de regulamento
Considerando 33

Texto da Comissão	*Alteração*
(33) Deve ser criada progressivamente uma reserva de cibersegurança a nível da União, composta por prestadores privados de serviços de segurança geridos para apoiar ações de resposta e recuperação imediata em caso de incidentes de cibersegurança significativos ou em grande escala. A Reserva de Cibersegurança da UE deve assegurar a disponibilidade e prontidão dos serviços. Os serviços da Reserva de Cibersegurança da UE devem servir para apoiar as autoridades nacionais na prestação de assistência às entidades afetadas que operam em setores críticos ou altamente críticos em complemento das suas próprias ações a nível nacional. Ao solicitarem o apoio da Reserva de Cibersegurança da UE, os Estados-Membros devem especificar o apoio prestado à entidade afetada a nível nacional, que deve ser tido em conta na avaliação do pedido do Estado-Membro. Os serviços da Reserva de Cibersegurança da UE podem também servir para apoiar as instituições, órgãos e organismos da União	(33) Deve ser criada progressivamente uma reserva de cibersegurança a nível da União, composta por prestadores privados de serviços de segurança geridos para apoiar ações de resposta e recuperação imediata em caso de incidentes de cibersegurança significativos ou em grande escala. A Reserva de Cibersegurança da UE deve assegurar a disponibilidade e prontidão dos serviços. Os serviços da Reserva de Cibersegurança da UE devem servir para apoiar as autoridades nacionais na prestação de assistência às entidades afetadas que operam em setores críticos ou altamente críticos em complemento das suas próprias ações a nível nacional. Ao solicitarem o apoio da Reserva de Cibersegurança da UE, os Estados-Membros devem especificar o apoio prestado à entidade afetada a nível nacional, que deve ser tido em conta na avaliação do pedido do Estado-Membro. Os serviços da Reserva de Cibersegurança da UE podem também servir para apoiar as instituições, órgãos e organismos da União***, incluindo as missões da PCSD,*** em

em condições semelhantes.

condições semelhantes.

Alteração 24

Proposta de regulamento
Considerando 34

Texto da Comissão	*Alteração*
(34) Para efeitos da seleção de prestadores de serviços privados para a prestação de serviços no contexto da Reserva de Cibersegurança da UE, importa estabelecer um conjunto de critérios mínimos que devem ser incluídos no convite à apresentação de propostas correspondente, a fim de assegurar que as necessidades das autoridades e entidades dos Estados-Membros que operam em setores críticos ou altamente críticos são satisfeitas.	(34) Para efeitos da seleção de prestadores de serviços privados para a prestação de serviços no contexto da Reserva de Cibersegurança da UE, importa estabelecer um conjunto de critérios mínimos que devem ser incluídos no convite à apresentação de propostas correspondente, a fim de assegurar que as necessidades das autoridades e entidades dos Estados-Membros que operam em setores críticos ou altamente críticos são satisfeitas***, tendo igualmente em conta os riscos inerentes à participação de fornecedores de países concorrentes estratégicos, que pode ocasionar riscos para a segurança económica, bem como as implicações daí decorrentes para a segurança estratégica da União***.

Alteração 25

Proposta de regulamento
Considerando 36

Texto da Comissão	*Alteração*
(36) A fim de apoiar os objetivos do presente regulamento de promover o conhecimento comum da situação, reforçar a resiliência da União e permitir uma resposta eficaz a incidentes de cibersegurança significativos e em grande escala, a UE-CyCLONe, a rede de CSIRT ou a Comissão devem poder solicitar à ENISA a análise e avaliação de ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande	(36) A fim de apoiar os objetivos do presente regulamento de promover o conhecimento comum da situação, reforçar a resiliência da União e permitir uma resposta eficaz a incidentes de cibersegurança significativos e em grande escala, a UE-CyCLONe, a rede de CSIRT ou a Comissão devem poder solicitar à ENISA a análise e avaliação de ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande

escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA deve elaborar um relatório de análise de incidentes em colaboração com as partes interessadas pertinentes, incluindo representantes do setor privado, dos Estados-Membros, da Comissão e de outras instituições, órgãos e organismos competentes da UE. No que diz respeito ao setor privado, a ENISA está a desenvolver canais para o intercâmbio de informações com prestadores especializados, incluindo prestadores de soluções de segurança geridas e fornecedores, a fim de contribuir para a missão da ENISA de alcançar um elevado nível comum de cibersegurança na União. Com base na colaboração com as partes interessadas, incluindo o setor privado, o relatório de análise de incidentes específicos deve ter por objetivo avaliar as causas, os impactos e as medidas de atenuação de um incidente após a sua ocorrência. Deve ser prestada especial atenção aos contributos e ensinamentos partilhados pelos prestadores de serviços de segurança geridos que satisfaçam as condições de maior integridade profissional, imparcialidade e conhecimentos técnicos necessários, conforme exigido pelo presente regulamento. O relatório deve ser apresentado e contribuir para o trabalho da UE-CyCLONe, da rede de CSIRT e da Comissão. Se o incidente disser respeito a um país terceiro, será igualmente partilhado pela Comissão com o alto representante.

escala específico. ***Tendo em vista o desenvolvimento de um sistema de conetividade seguro, com base na Infraestrutura Europeia de Comunicação Quântica (EuroQCI) e na Comunicação Governamental por Satélite da União Europeia (GOVSATCOM), em especial a implementação do GNSS Galileo para os utilizadores no domínio da defesa, qualquer eventual desenvolvimento futuro deve ter em conta o advento da «hiperguerra», que conjuga a velocidade e a sofisticação da computação quântica com sistemas militares altamente autónomos.*** Após a conclusão da análise e avaliação de um incidente, a ENISA deve elaborar um relatório de análise de incidentes em colaboração com as partes interessadas pertinentes, incluindo representantes do setor privado, dos Estados-Membros, da Comissão e de outras instituições, órgãos e organismos competentes da UE. No que diz respeito ao setor privado, a ENISA está a desenvolver canais para o intercâmbio de informações com prestadores especializados, incluindo prestadores de soluções de segurança geridas e fornecedores, a fim de contribuir para a missão da ENISA de alcançar um elevado nível comum de cibersegurança na União. Com base na colaboração com as partes interessadas, incluindo o setor privado, o relatório de análise de incidentes específicos deve ter por objetivo avaliar as causas, os impactos e as medidas de atenuação de um incidente após a sua ocorrência. Deve ser prestada especial atenção aos contributos e ensinamentos partilhados pelos prestadores de serviços de segurança geridos que satisfaçam as condições de maior integridade profissional, imparcialidade e conhecimentos técnicos necessários, conforme exigido pelo presente regulamento. O relatório deve ser apresentado e contribuir para o trabalho da UE-CyCLONe, da rede de CSIRT e da Comissão. Se o incidente disser respeito a

um país terceiro, será igualmente partilhado pela Comissão com o alto representante***, com o SEAE e, através do respetivo quartel-general, com qualquer missão da PCSD no país afetado pelo incidente***.

Alteração 26

Proposta de regulamento
Considerando 37

Texto da Comissão	*Alteração*
(37) Tendo em conta a natureza imprevisível dos ataques à cibersegurança e o facto de frequentemente não se confinarem a uma área geográfica específica e representarem um elevado risco de disseminação, o reforço da resiliência dos países vizinhos e da sua capacidade para responder eficazmente a incidentes de cibersegurança significativos em grande escala contribuem para a proteção da União no seu conjunto. Por conseguinte, os países terceiros associados ao Programa Europa Digital ***podem*** receber apoio da Reserva de Cibersegurança da UE ***sempre que tal esteja previsto no respetivo acordo de associação ao Programa Europa Digital***. O financiamento dos países terceiros associados deve ser apoiado pela União no quadro de parcerias e instrumentos de financiamento pertinentes para esses países. O apoio deve abranger serviços no domínio da resposta a incidentes de cibersegurança significativos ou em grande escala e da recuperação imediata dos mesmos. Aquando da prestação de apoio aos países terceiros associados ao Programa Europa Digital, devem aplicar-se as condições estabelecidas no presente regulamento relativamente à Reserva de Cibersegurança da UE aos prestadores de confiança.	(37) Tendo em conta a natureza imprevisível dos ataques à cibersegurança e o facto de frequentemente não se confinarem a uma área geográfica específica e representarem um elevado risco de disseminação, o reforço da resiliência dos países vizinhos***, em particular a Ucrânia e a Moldávia,*** e da sua capacidade para responder eficazmente a incidentes de cibersegurança significativos em grande escala contribuem para a proteção da União no seu conjunto. Por conseguinte, os países terceiros associados ao Programa Europa Digital ***devem*** receber apoio da Reserva de Cibersegurança da UE. ***O apoio também deve abranger os países terceiros nos quais tenha sido destacada uma missão da PCSD com um mandato específico no sentido de reforçar a resiliência a ameaças híbridas, incluindo ciberameaças, ou nos quais tenha sido adotada uma medida de assistência do MEAP com vista a reforçar a ciber-resiliência do país.*** O financiamento dos países terceiros associados deve ser apoiado pela União no quadro de parcerias e instrumentos de financiamento pertinentes para esses países. O apoio deve abranger serviços no domínio da resposta a incidentes de cibersegurança significativos ou em grande escala e da recuperação imediata dos mesmos. Aquando da prestação de apoio aos países terceiros

	associados ao Programa Europa Digital, devem aplicar-se as condições estabelecidas no presente regulamento relativamente à Reserva de Cibersegurança da UE aos prestadores de confiança.

Alteração 27

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

Texto da Comissão	*Alteração*
c) Criação de um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes significativos ou em grande escala.	c) Criação de um mecanismo europeu de análise de incidentes de cibersegurança para analisar e avaliar incidentes ***ou ameaças*** significativos ou em grande escala.

Alteração 28

Proposta de regulamento
Artigo 1 – n.º 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 da cibersegurança;	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 ***resiliência*** tecnológica da União no domínio da cibersegurança;

Alteração 29

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	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;	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 ***ou aos países terceiros candidatos à adesão que não sejam contrários aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC, nos termos do título V do TUE; Os Estados-Membros devem prever um programa ativo de ciberdefesa como parte integrante da sua estratégia nacional de cibersegurança, que incorpore a realização regular de exercícios de formação entre Estados-Membros e organizações internacionais. Esse programa deve proporcionar uma capacidade sincronizada e em tempo real para descobrir, detetar, analisar e atenuar ameaças***;

Alteração 30

Proposta de regulamento
Artigo 1 – n.º 2-A (novo)

Texto da Comissão	*Alteração*
	2-A. Reduzir os riscos sistémicos de cibersegurança decorrentes das dependências de equipamentos críticos de países que sejam contrários aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC, nos termos do título V do TUE;

Alteração 31

Proposta de regulamento
Artigo 2 – ponto 2-A (novo)

Texto da Comissão	*Alteração*
	«Comunidade de ciberdefesa», as autoridades de defesa dos Estados-Membros, apoiadas pelas instituições, órgãos e organismos da UE, conforme estabelecido na Comunicação Conjunta sobre a política de ciberdefesa da UE[1];
	[1] Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada «Política de ciberdefesa da UE» [JOIN(2022) 49 final].

Alteração 32

Proposta de regulamento
Artigo 3 – n.º 2 – parágrafo 1 – alínea b-A) (nova)

Texto da Comissão	*Alteração*
	b-A) Contribuir para a modernização de todos os sistemas de ciberdefesa, melhorando a qualidade das capacidades de ciberdefesa através da implantação de sistemas de IA e acelerar o intercâmbio de informações entre os SOC nacionais e transfronteiriços;

Alteração 33

Proposta de regulamento
Artigo 3 – n.º 2 – parágrafo 1 – alínea d-A) (nova)

Texto da Comissão	*Alteração*
	d-A) Analisar e avaliar tecnologias e equipamentos críticos de cibersegurança utilizados pelos SOC na resposta a incidentes de cibersegurança, para identificar riscos sistémicos decorrentes do controlo de fornecedores de alto risco por parte de países que sejam contrários aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC,

	nos termos do título V do TUE;

Alteração 34

Proposta de regulamento
Artigo 4 – n.° 1 – parágrafo 2

Texto da Comissão	*Alteração*
Tem capacidade para atuar como ponto de referência e de acesso a outras organizações públicas e privadas a nível nacional para recolher e analisar informações sobre ameaças e incidentes de cibersegurança e contribuir para um SOC transfronteiriço. Deve estar equipado com tecnologias de ponta capazes de detetar, agregar e analisar dados relevantes para as ameaças e incidentes de cibersegurança.	Tem capacidade para atuar como ponto de referência e de acesso a outras organizações públicas e privadas***, e, quando necessário, militares,*** a nível nacional para recolher e analisar informações sobre ameaças e incidentes de cibersegurança e contribuir para um SOC transfronteiriço. Deve estar equipado com tecnologias de ponta capazes de detetar, agregar e analisar dados relevantes para as ameaças e incidentes de cibersegurança.

Alteração 35

Proposta de regulamento
Artigo 4 – n.º 2

Texto da Comissão	*Alteração*
2. Na sequência de um convite à manifestação de interesse, os SOC nacionais são selecionados pelo Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança («ECCC») para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder subvenções aos SOC nacionais selecionados para financiar o funcionamento dessas ferramentas e infraestruturas. A contribuição financeira da União cobre até 50 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo Estado-Membro. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o SOC	2. Na sequência de um convite à manifestação de interesse, os SOC nacionais são selecionados pelo Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança («ECCC») para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder subvenções aos SOC nacionais selecionados para financiar o funcionamento dessas ferramentas e infraestruturas***, sob a estrita condição de que tais ferramentas e infraestruturas sejam fornecidas por prestadores de confiança, em conformidade com o artigo 16.º.*** A contribuição financeira da União cobre até 50 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os

nacional devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.	restantes custos ser cobertos pelo Estado-Membro. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o SOC nacional devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.

Alteração 36

Proposta de regulamento
Artigo 5 – n.º 2

Texto da Comissão	*Alteração*
2. Na sequência de um convite à manifestação de interesse, o ECCC seleciona um consórcio de acolhimento para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder ao consórcio de acolhimento uma subvenção para financiar o funcionamento das ferramentas e infraestruturas. A contribuição financeira da União cobre até 75 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo consórcio de acolhimento. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o consórcio de acolhimento devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.	2. Na sequência de um convite à manifestação de interesse, o ECCC seleciona um consórcio de acolhimento para participar numa aquisição conjunta de ferramentas e infraestruturas com o ECCC. O ECCC pode conceder ao consórcio de acolhimento uma subvenção para financiar o funcionamento das ferramentas e infraestruturas***, sob a estrita condição de que tais ferramentas e infraestruturas sejam fornecidas por prestadores de confiança, em conformidade com o artigo 16.º.*** A contribuição financeira da União cobre até 75 % dos custos de aquisição das ferramentas e infraestruturas e até 50 % dos custos operacionais, devendo os restantes custos ser cobertos pelo consórcio de acolhimento. Antes de lançar o procedimento de aquisição das ferramentas e infraestruturas, o ECCC e o consórcio de acolhimento devem celebrar uma convenção de acolhimento e utilização que regule a utilização das mesmas.

Alteração 37

Proposta de regulamento
Artigo 5 – n.º 2-A (novo)

Texto da Comissão	*Alteração*

2-A. Qualquer infraestrutura ou fornecedor originários de um país terceiro de risco elevado são automaticamente excluídos.

Alteração 38

Proposta de regulamento
Artigo 6 – n.º 1 – alínea b-A) (nova)

Texto da Comissão	*Alteração*
	b-A) Apoie diretamente o reforço das capacidades militares e de defesa dos membros participantes ou previna uma ameaça direta e iminente à sua segurança. Embora a exploração de vulnerabilidades no setor da defesa possa causar perturbações e danos significativos, a cibersegurança no domínio da indústria da defesa exige medidas especiais para garantir a segurança das cadeias de abastecimento, em especial das entidades que se encontram no final das cadeias de abastecimento, que não necessitam de acesso a informações classificadas, mas que podem acarretar sérios riscos para todo o setor. Deve ser dada especial atenção ao impacto que uma eventual violação pode ter e à ameaça de potenciais manipulações de informações da rede que possam tornar inutilizáveis ativos críticos de defesa, ou até mesmo assumir o controlo dos seus sistemas operativos, tornando-os vulneráveis à pirataria informática.

Alteração 39

Proposta de regulamento
Artigo 6 – n.º 1 – alínea b-A) (nova)

Texto da Comissão	*Alteração*
	b-B) Apoie o reforço das capacidades de defesa dos membros participantes ou

	previna uma ameaça direta e iminente à sua segurança, garantindo a segurança das cadeias de abastecimento, em especial as entidades nos níveis inferiores das cadeias de abastecimento, que não requerem acesso a informações classificadas, mas que podem acarretar sérios riscos para todo o setor.

Alteração 40

Proposta de regulamento
Artigo 7 – n.º 1

Texto da Comissão	*Alteração*
1. Caso obtenham informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, os SOC transfronteiriços devem fornecer, sem demora injustificada, informações pertinentes à UE-CyCLONe, à rede de CSIRT e à Comissão, tendo em conta as respetivas funções de gestão de crises, em conformidade com a Diretiva (UE) 2022/2555.	1. Caso obtenham informações relativas a um incidente de cibersegurança em grande escala, potencial ou em curso, os SOC transfronteiriços devem fornecer, sem demora injustificada, informações pertinentes à UE-CyCLONe, à rede de CSIRT e à Comissão***, incluindo ao alto representante e ao SEAE, caso o incidente diga respeito a um país terceiro***, tendo em conta as respetivas funções de gestão de crises, em conformidade com a Diretiva (UE) 2022/2555.

Alteração 41

Proposta de regulamento
Artigo 8 – n.º 1

Texto da Comissão	*Alteração*
1. Os Estados-Membros que participam no ciberescudo europeu devem garantir um elevado nível de segurança dos dados e de segurança física da infraestrutura do ciberescudo europeu e assegurar que a infraestrutura seja adequadamente gerida e controlada de forma a protegê-la de ameaças e a garantir a sua segurança e a segurança dos sistemas, incluindo a dos dados trocados através da	1. Os Estados-Membros que participam no ciberescudo europeu devem garantir um elevado nível de segurança dos dados e de segurança física da infraestrutura do ciberescudo europeu e assegurar que a infraestrutura seja adequadamente gerida e controlada de forma a protegê-la de ameaças e a garantir a sua segurança e a segurança dos sistemas, ***a diminuir os riscos e a promover a vantagem tecnológica da UE em setores***

infraestrutura.	***críticos,*** incluindo ***medidas para limitar ou excluir fornecedores de alto risco, bem como para proteger*** a ***segurança*** dos dados trocados através da infraestrutura.

Alteração 42

Proposta de regulamento
Artigo 8 – n.º 2

Texto da Comissão	*Alteração*
2. Os Estados-Membros que participam no ciberescudo europeu devem assegurar que a partilha de informações no âmbito do ciberescudo europeu com entidades que não sejam organismos públicos dos Estados-Membros não afeta negativamente os interesses de segurança da União.	2. Os Estados-Membros que participam no ciberescudo europeu devem assegurar que a partilha de informações no âmbito do ciberescudo europeu com entidades que não sejam organismos públicos dos Estados-Membros não afeta negativamente os interesses de segurança da União ***e que qualquer partilha de informações com fornecedores de alto risco tem um âmbito limitado e não prejudica a segurança nem os interesses estratégicos da União***.

Alteração 43

Proposta de regulamento
Artigo 8 – n.º 3

Texto da Comissão	*Alteração*
3. A Comissão pode adotar atos de execução que estabeleçam requisitos técnicos que os Estados-Membros devem respeitar para cumprir a obrigação que lhes incumbe por força dos n.os 1 e 2. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2, do presente regulamento. Ao fazê-lo, a Comissão, apoiada pelo alto representante, tem em conta as normas de segurança pertinentes a nível da defesa, a fim de facilitar a cooperação com intervenientes militares.	3. A Comissão pode adotar atos de execução que estabeleçam requisitos técnicos que os Estados-Membros devem respeitar para cumprir a obrigação que lhes incumbe por força dos n.os 1 e 2. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 21.º, n.º 2, do presente regulamento. Ao fazê-lo, a Comissão, apoiada pelo alto representante, ***informa o Parlamento Europeu e*** tem em conta as normas de segurança pertinentes a nível da defesa, a fim de facilitar a cooperação com intervenientes militares***, utilizando de forma adequada todo o leque de opções***

	defensivas à disposição das comunidades civil e militar para assegurar a segurança e a defesa mais amplas da UE.

Alteração 44

Proposta de regulamento
Artigo 9 – n.º 2

Texto da Comissão	*Alteração*
2. As ações de execução do mecanismo de ciberemergência são apoiadas por financiamento do Programa Europa Digital e executadas em conformidade com o Regulamento (UE) 2021/694 e, em especial, com o objetivo específico n.º 3 do mesmo regulamento.	2. As ações de execução do mecanismo de ciberemergência são apoiadas por financiamento do Programa Europa Digital e executadas em conformidade com o Regulamento (UE) 2021/694 e, em especial, com o objetivo específico n.º 3 do mesmo regulamento***, bem como pelo Mecanismo Europeu de Apoio à Paz (MEAP) aquando da disponibilização de medidas de assistência a países terceiros, em particular à Ucrânia e à Moldávia***.

Alteração 45

Proposta de regulamento
Artigo 10 – n.º 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***, como as infraestruturas públicas, as infraestruturas eleitorais, os transportes, os cuidados de saúde, os serviços financeiros, as telecomunicações, o abastecimento alimentar e a segurança*** na União;

Alteração 46

Proposta de regulamento
Artigo 10 – n.º 1 – alínea c)

Texto da Comissão	*Alteração*
c) Ações de assistência mútua que consistam na prestação de assistência por parte das autoridades nacionais de um Estado-Membro a outro Estado-Membro, em especial nos termos do artigo 11.º, n.º 3, alínea f), da Diretiva (UE) 2022/2555**.**	c) Ações de assistência mútua que consistam na prestação de assistência por parte das autoridades nacionais de um Estado-Membro a outro Estado-Membro, em especial nos termos do artigo 11.º, n.º 3, alínea f), da Diretiva (UE) 2022/2555 ***e no contexto do artigo 42.º, n.º 7, do TUE e do artigo 222.º do TFUE;***

Alteração 47

Proposta de regulamento
Artigo 10 – n.º 1 – alínea c-A) (nova)

Texto da Comissão	*Alteração*
	c-A) Substituição e eliminação progressiva de equipamentos críticos de fornecedores de alto risco que sejam contrários aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC, nos termos do título V do TUE.

Alteração 48

Proposta de regulamento
Artigo 11 – n.º 2

Texto da Comissão	*Alteração*
2. O grupo de cooperação SRI, em colaboração com a Comissão, a ENISA ***e*** o alto representante, deve desenvolver cenários e metodologias de risco comuns para os exercícios de teste coordenados.	2. O grupo de cooperação SRI, em colaboração com a Comissão, a ENISA***,*** o alto representante, ***o SEAE e, se for caso disso, a AED,*** deve desenvolver cenários e metodologias de risco comuns para os exercícios de teste coordenados.

Alteração 49

Proposta de regulamento
Artigo 12 – n.º 2

Texto da Comissão	*Alteração*
2. A Reserva de Cibersegurança da UE é constituída por serviços de resposta a incidentes de prestadores de confiança selecionados de acordo com os critérios estabelecidos no artigo 16.º. A reserva inclui serviços previamente afetados. Os serviços devem poder ser disponibilizados em todos os Estados-Membros.	2. A Reserva de Cibersegurança da UE é constituída por serviços de resposta a incidentes de prestadores de confiança selecionados de acordo com os critérios estabelecidos no artigo 16.º. A reserva inclui serviços previamente afetados. Os serviços devem poder ser disponibilizados em todos os Estados-Membros ***e em países terceiros que cumpram os requisitos aplicáveis do presente regulamento***.

Alteração 50

Proposta de regulamento
Artigo 12 – n.º 3 – alínea b)

Texto da Comissão	*Alteração*
b) Instituições, órgãos e organismos da União.	b) Instituições, órgãos e organismos da União***, incluindo missões da PCSD***.

Alteração 51

Proposta de regulamento
Artigo 12 – n.º 4

Texto da Comissão	*Alteração*
4. Os utilizadores a que se refere o n.º 3, alínea a), devem utilizar os serviços da Reserva de Cibersegurança da UE a fim de responder ou prestar apoio para a resposta e a recuperação imediata de incidentes significativos ou em grande escala que afetem entidades que operam em setores críticos ou altamente críticos.	4. Os utilizadores a que se refere o n.º 3, alínea a), devem utilizar os serviços da Reserva de Cibersegurança da UE a fim de responder ou prestar apoio para a resposta e a recuperação imediata de incidentes significativos ou em grande escala que afetem entidades que operam em setores críticos ou altamente críticos***, como as infraestruturas públicas, as infraestruturas eleitorais, os transportes, os cuidados de saúde, os serviços financeiros, as telecomunicações, o***

abastecimento alimentar e a segurança.

Alteração 52

Proposta de regulamento
Artigo 12 – n.º 5

Texto da Comissão	*Alteração*
5. Incumbe à Comissão a responsabilidade global pela execução da Reserva de Cibersegurança da UE. A Comissão determina as prioridades e a evolução da Reserva de Cibersegurança da UE em consonância com os requisitos dos utilizadores referidos no n.º 3, supervisiona a sua execução e assegura a complementaridade, a coerência, as sinergias e as ligações com outras ações de apoio ao abrigo do presente regulamento, bem como com outras ações ***e*** programas da União.	5. Incumbe à Comissão a responsabilidade global pela execução da Reserva de Cibersegurança da UE. A Comissão determina as prioridades e a evolução da Reserva de Cibersegurança da UE em consonância com os requisitos dos utilizadores referidos no n.º 3, supervisiona a sua execução e assegura a complementaridade, a coerência, as sinergias e as ligações com outras ações, programas ***e objetivos*** da União***, em especial o objetivo estratégico de reduzir as dependências de fornecedores de alto risco que sejam contrários aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC, nos termos do título V do TUE***.

Alteração 53

Proposta de regulamento
Artigo 12 – n.º 7

Texto da Comissão	*Alteração*
7. A fim de apoiar a Comissão na criação da Reserva de Cibersegurança da UE, a ENISA prepara um levantamento dos serviços necessários, após consulta dos Estados-Membros e da Comissão. A ENISA prepara um levantamento semelhante, após consulta da Comissão, para identificar as necessidades dos países terceiros elegíveis para apoio da Reserva de Cibersegurança da UE, nos termos do	7. A fim de apoiar a Comissão na criação da Reserva de Cibersegurança da UE, a ENISA prepara um levantamento dos serviços necessários, após consulta dos Estados-Membros e da Comissão. A ENISA prepara um levantamento semelhante, após consulta da Comissão, para identificar as necessidades dos países terceiros elegíveis para apoio da Reserva de Cibersegurança da UE, nos termos do

artigo 17.º. Se for caso disso, a Comissão consulta o alto representante.	artigo 17.º ***e com o apoio do SEAE***. Se for caso disso, a Comissão consulta o alto representante.

Alteração 54

Proposta de regulamento
Artigo 14 – n.º 2 – alínea a-A) (nova)

Texto da Comissão	*Alteração*
	a-A) O impacto do incidente na segurança e na defesa da União;

Alteração 55

Proposta de regulamento
Artigo 15 – n.º 3

Texto da Comissão	*Alteração*
3. Em consulta com o alto representante, o apoio prestado no âmbito do mecanismo de ciberemergência pode complementar a assistência prestada no contexto da política externa e de segurança comum e da política comum de segurança e defesa, nomeadamente através das equipas de resposta rápida a ciberataques. Pode igualmente complementar ou contribuir para a assistência prestada por um Estado-Membro a outro Estado-Membro no contexto do artigo 42.º, n.º 7, do Tratado da União Europeia.	3. Em consulta com o alto representante, o apoio prestado no âmbito do mecanismo de ciberemergência pode complementar a assistência prestada no contexto da política externa e de segurança comum e da política comum de segurança e defesa, nomeadamente através das equipas de resposta rápida a ciberataques***, para melhor apoiar os Estados-Membros da UE, as missões e operações da PCSD e os países terceiros que estejam alinhados, nos seus esforços de reforço da capacidade de ciberdefesa, com a política externa e de segurança comum e com a política comum de segurança e defesa da UE, em particular a Ucrânia e a Moldávia***. Pode igualmente complementar ou contribuir para a assistência prestada por um Estado-Membro a outro Estado-Membro no contexto do artigo 42.º, n.º 7, do Tratado da União Europeia.

Alteração 56

Proposta de regulamento
Artigo 16 – n.º 2 – alínea b-A) (nova)

Texto da Comissão	*Alteração*
	a-A) O prestador deve demonstrar que as suas estruturas de decisão e de gestão estão isentas de qualquer influência indevida por parte de governos de Estados que seja contrária aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC, nos termos do título V do TUE;

Alteração 57

Proposta de regulamento
Artigo 16 – n.º 2 – alínea f)

Texto da Comissão	*Alteração*
f) O prestador deve estar equipado com o equipamento técnico de hardware e software necessário para apoiar o serviço solicitado;	f) O prestador deve estar equipado com o equipamento técnico de hardware e software necessário para apoiar o serviço solicitado ***e cumpre os requisitos previstos no artigo X do Regulamento XX/XXXX (Regulamento Ciber-resiliência)***;

Alteração 58

Proposta de regulamento
Artigo 16 – n.º 2 – alínea j-A) (nova)

Texto da Comissão	*Alteração*
	j-A) Nenhum prestador originário de um país terceiro de risco elevado é admissível.

Alteração 59

Proposta de regulamento
Artigo 16 – n.º 2 – alínea j-B) (nova)

Texto da Comissão	*Alteração*
	j-B) O prestador deve, sempre que possível, cooperar estreitamente com as PME pertinentes;

Alteração 60

Proposta de regulamento
Artigo 17 – n.º 1

Texto da Comissão	*Alteração*
1. Os países terceiros podem solicitar apoio da Reserva de Cibersegurança da UE sempre que os acordos de associação celebrados relativamente à sua participação no Programa Europa Digital o prevejam.	1. Os países terceiros podem solicitar apoio da Reserva de Cibersegurança da UE sempre que***:***
	a) Os acordos de associação celebrados relativamente à sua participação no Programa Europa Digital o prevejam***;***
	b) Se trate de países terceiros nos quais tenha sido destacada uma missão da PCSD com um mandato específico no sentido de reforçar a resiliência contra ameaças híbridas, incluindo ciberameaças, ou nos quais tenha sido adotada uma medida de assistência do MEAP com vista a reforçar a sua ciber-resiliência.

Alteração 61

Proposta de regulamento
Artigo 17 – n.º 2

Texto da Comissão	*Alteração*
2. O apoio da Reserva de Cibersegurança da UE deve estar em conformidade com o presente regulamento e cumprir quaisquer condições específicas estabelecidas nos acordos de associação a que se refere o n.º 1.	2. O apoio da Reserva de Cibersegurança da UE deve estar em conformidade com o presente regulamento e cumprir quaisquer condições específicas estabelecidas nos acordos de associação a que se refere o n.º 1***, exceto no que se refere aos países terceiros abrangidos pelo***

disposto na alínea b) do n.º 1.

Alteração 62

Proposta de regulamento
Artigo 18 – n.º 1

Texto da Comissão	*Alteração*
1. A pedido da Comissão, da UE-CyCLONe ou da rede de CSIRT, a ENISA analisa e avalia as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA apresenta um relatório de análise do incidente à rede de CSIRT, à UE-CyCLONe e à Comissão, a fim de as apoiar no desempenho das suas funções, em especial tendo em conta as enunciadas nos artigos 15.º e 16.º da Diretiva (UE) 2022/2555. Se for caso disso, a Comissão partilha o relatório com o alto representante.	1. A pedido da Comissão, da UE-CyCLONe ou da rede de CSIRT, a ENISA analisa e avalia as ameaças, vulnerabilidades e medidas de atenuação no que diz respeito a um incidente de cibersegurança significativo ou em grande escala específico. Após a conclusão da análise e avaliação de um incidente, a ENISA apresenta um relatório de análise do incidente à rede de CSIRT, à UE-CyCLONe e à Comissão, a fim de as apoiar no desempenho das suas funções, em especial tendo em conta as enunciadas nos artigos 15.º e 16.º da Diretiva (UE) 2022/2555. Se for caso disso, ***e sobretudo nos casos em que o incidente diga respeito a um país terceiro,*** a Comissão partilha o relatório com o alto representante ***e com o SEAE***.

Alteração 63

Proposta de regulamento
Artigo 18 – n.º 3-A (novo)

Texto da Comissão	*Alteração*
	3-A. O relatório é partilhado com o Parlamento Europeu, em conformidade com o direito da União ou a legislação nacional sobre a proteção de informações classificadas sensíveis.

Alteração 64

Proposta de regulamento
Artigo 19 – parágrafo 1 – ponto 1 – alínea a) – ponto 1
Regulamento (UE) 2021/694
Artigo 6 – n.º 1

Texto da Comissão	*Alteração*
a-A) Apoiar o desenvolvimento de um ciberescudo da UE, incluindo o desenvolvimento, a implantação e o funcionamento de plataformas de centros de operações de segurança (SOC, do inglês Security Operations Centres) nacionais e transfronteiriços que contribuam para o conhecimento da situação na União e para o reforço das capacidades da União em matéria de informações sobre ciberameaças;»;	a-A) Apoiar o desenvolvimento de um ciberescudo da UE, incluindo o desenvolvimento, a implantação e o funcionamento de plataformas de centros de operações de segurança (SOC, do inglês Security Operations Centres) nacionais e transfronteiriços que contribuam para o conhecimento da situação na União, para o reforço das capacidades da União em matéria de informações sobre ciberameaças ***e para a redução da dependência da União em relação a fornecedores de alto risco de equipamentos ou componentes críticos de cibersegurança que sejam contrários aos interesses de segurança e defesa da União e dos seus Estados-Membros, tal como estabelecido no quadro da PESC, nos termos do título V do TUE***;

Alteração 65

Proposta de regulamento
Artigo 20 – n.º 1

Texto da Comissão	*Alteração*
Até [***quatro*** anos após a data de aplicação do presente regulamento], a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão do presente regulamento.	Até [***três*** anos após a data de aplicação do presente regulamento ***e a cada dois anos após essa data***], a Comissão apresenta ao Parlamento Europeu e ao Conselho um relatório sobre a avaliação e a revisão do presente regulamento.

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	AFET 1.6.2023
Relator de parecer Data de designação	Dragoş Tudorache 16.6.2023
Exame em comissão	18.9.2023
Data de aprovação	24.10.2023
Resultado da votação final	+: 39 –: 4 0: 0
Deputados presentes no momento da votação final	Alexander Alexandrov Yordanov, Petras Auštrevičius, Traian Băsescu, Anna Bonfrisco, Włodzimierz Cimoszewicz, Katalin Cseh, Michael Gahler, Giorgos Georgiou, Sunčana Glavak, Bernard Guetta, Sandra Kalniete, Dietmar Köster, Andrius Kubilius, David Lega, Leopoldo López Gil, Jaak Madison, Pedro Marques, David McAllister, Vangelis Meimarakis, Sven Mikser, Francisco José Millán Mon, Matjaž Nemec, Demetris Papadakis, Kostas Papadakis, Tonino Picula, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Jordi Solé, Sergei Stanishev, Tineke Strik, Dominik Tarczyński, Dragoş Tudorache, Thomas Waitz, Bernhard Zimniok, Željana Zovko
Suplentes presentes no momento da votação final	Attila Ara-Kovács, Lars Patrick Berg, Andrey Kovatchev, Georgios Kyrtsos, Sergey Lagodinsky, Giuliano Pisapia, Mick Wallace

VOTAÇÃO NOMINAL FINAL NA COMISSÃO ENCARREGADA DE EMITIR PARECER

39	+
ECR	Lars Patrick Berg, Dominik Tarczyński
ID	Anna Bonfrisco, Jaak Madison
PPE	Alexander Alexandrov Yordanov, Traian Băsescu, Michael Gahler, Sunčana Glavak, Sandra Kalniete, Andrey Kovatchev, Andrius Kubilius, David Lega, Leopoldo López Gil, David McAllister, Vangelis Meimarakis, Francisco José Millán Mon, Željana Zovko
Renew	Petras Auštrevičius, Katalin Cseh, Bernard Guetta, Georgios Kyrtsos, Dragoş Tudorache
S&D	Attila Ara-Kovács, Włodzimierz Cimoszewicz, Dietmar Köster, Pedro Marques, Sven Mikser, Matjaž Nemec, Demetris Papadakis, Tonino Picula, Giuliano Pisapia, Thijs Reuten, Nacho Sánchez Amor, Andreas Schieder, Sergei Stanishev
Verts/ALE	Sergey Lagodinsky, Jordi Solé, Tineke Strik, Thomas Waitz

4	-
ID	Bernhard Zimniok
NI	Kostas Papadakis
The Left	Giorgos Georgiou, Mick Wallace

0	0

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