I

(Resoluções, recomendações e pareceres)

RECOMENDAÇÕES

CONSELHO

RECOMENDAÇÃO DO CONSELHO

de 8 de dezembro de 2022

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

(Texto relevante para efeitos do EEE)

(2023/C 20/01)

O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º e o artigo 292.º, primeira e segunda frases,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

(1) A fim de assegurar o funcionamento do mercado interno, é do interesse de todos os Estados-Membros e da União no seu conjunto identificar de forma clara e proteger as infraestruturas críticas pertinentes que asseguram serviços essenciais nesse mercado, nomeadamente em setores-chave, como os da energia, das infraestruturas digitais, dos transportes e do espaço, bem como as com importante relevância transfronteiriça ([1]), cuja perturbação pode afetar de forma significativa outros Estados-Membros.

(2) A presente recomendação, que constitui um ato não vinculativo, demonstra a vontade política dos Estados-Membros de cooperarem, bem como o seu empenho nas medidas recomendadas, salientado num plano de cinco pontos emitido pela presidente da Comissão Europeia, no pleno respeito das competências dos Estados-Membros. A presente recomendação não afeta a proteção dos interesses essenciais dos Estados-Membros em matéria de segurança nacional, segurança pública ou defesa e nenhum Estado-Membro deverá ser obrigado a partilhar informações que possam prejudicar tais interesses.

(3) Se a responsabilidade pela segurança e a prestação de serviços essenciais assegurada por infraestruturas críticas recai primariamente sobre os Estados-Membros e os seus operadores de infraestruturas críticas, impõe-se, não obstante, reforçar a coordenação a nível da União, mormente à luz das ameaças em constante evolução que podem ter impacto em vários Estados-Membros ao mesmo tempo, como é o caso da guerra de agressão da Rússia contra a Ucrânia e das campanhas híbridas contra os Estados-Membros, ou que podem afetar a resiliência e o bom funcionamento da economia, do mercado interno e da sociedade da UE em geral. Deverá prestar-se especial atenção às infraestruturas críticas fora do território dos Estados-Membros, nomeadamente as infraestruturas críticas submarinas ou as infraestruturas energéticas ao largo.

([1]) Os Estados-Membros deverão avaliar essa relevância em consonância com as suas práticas nacionais, podendo fazê-lo com base, nomeadamente, numa avaliação de risco e no impacto e na natureza do evento.

(4) Nas suas conclusões de 20 e 21 de outubro de 2022, o Conselho Europeu condenou com firmeza os atos de sabotagem contra infraestruturas críticas, como os que visaram os gasodutos *Nord Stream*, indicando a vontade da União de dar a qualquer perturbação deliberada das infraestruturas críticas ou a outras ações híbridas uma resposta unida e determinada.

(5) Tendo em conta a rápida evolução do cenário das ameaças, importa tomar medidas de reforço da resiliência com caráter prioritário em setores-chave, como os da energia, das infraestruturas digitais, dos transportes e do espaço, bem como noutros setores pertinentes identificados pelos Estados-Membros. Essas medidas deverão incidir no reforço da resiliência das infraestruturas críticas, tendo em conta riscos pertinentes, em especial os efeitos em cascata, as perturbações na cadeia de abastecimento, a dependência, os impactos das alterações climáticas, fornecedores e parceiros pouco fiáveis e ameaças e campanhas híbridas, nomeadamente a manipulação da informação e a ingerência por parte de agentes estrangeiros. No que diz respeito às infraestruturas críticas nacionais, tendo em conta as possíveis consequências, importa dar prioridade às infraestruturas críticas com importante relevância transfronteiriça. Os Estados-Membros são incentivados a tomar as referidas medidas para reforçar a resiliência, se for caso disso, com caráter de urgência, mantendo simultaneamente a abordagem estabelecida no quadro jurídico em evolução.

(6) A proteção das infraestruturas críticas europeias nos setores da energia e dos transportes é atualmente regida pela Diretiva 2008/114/CE do Conselho ([2]) e a segurança das redes e da informação em toda a União, que incide sobre as ameaças relacionadas com o ciberespaço, é assegurada pela Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([3]). A fim de garantir um elevado nível comum de resiliência e a proteção das infraestruturas críticas, de cibersegurança e do mercado financeiro, o quadro jurídico em vigor está a ser alterado e complementado através da adoção de novas regras aplicáveis a entidades críticas (a «Diretiva REC»), regras reforçadas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (a «Diretiva SRI 2») e novas regras aplicáveis à resiliência operacional digital do setor financeiro («DORA»).

(7) Os Estados-Membros deverão, em conformidade com o direito nacional e da União, utilizar todas as ferramentas disponíveis para fazer avançar e ajudar a reforçar a resiliência física e cibernética. A este respeito, o conceito de infraestruturas críticas deverá incluir as infraestruturas críticas pertinentes identificadas por um Estado-Membro a nível nacional ou designadas como infraestruturas críticas europeias nos termos da Diretiva 2008/114/CE, bem como as entidades críticas a identificar nos termos da Diretiva REC ou, se for caso disso, as entidades abrangidas pela Diretiva SRI 2. O conceito de resiliência deverá ser entendido como a capacidade de uma infraestrutura crítica para prevenir, proteger, reagir, resistir, atenuar, absorver, adaptar ou recuperar em caso de eventos que perturbam ou têm potencial para perturbar significativamente a prestação de serviços essenciais no mercado interno, ou seja, serviços de importância crucial para a manutenção de funções societais e económicas vitais, a segurança pública, a saúde da população ou o ambiente.

(8) É necessário reunir peritos nacionais para coordenar o trabalho a fim de alcançar um nível comum mais elevado de resiliência e proteção das infraestruturas críticas através das novas regras aplicáveis às entidades críticas. Esse trabalho coordenado permitirá a cooperação entre os Estados-Membros e a partilha de informações sobre atividades como a elaboração de metodologias para identificar os serviços essenciais assegurados por infraestruturas críticas. A Comissão já começou a reunir os peritos e a atuar como facilitadora do seu trabalho, propondo-se prosseguir esta linha de ação. Após a entrada em vigor da Diretiva REC e uma vez criado um Grupo para a Resiliência das Entidades Críticas ao abrigo da referida diretiva, cabe a este grupo dar continuidade ao trabalho antecipatório desenvolvido em conformidade com as funções que lhe forem atribuídas.

(9) Reconhecendo a mudança do cenário das ameaças, importa continuar a desenvolver o potencial da realização de testes de esforço em infraestruturas críticas a nível nacional, uma vez que esses testes poderão ser úteis para reforçar a resiliência das infraestruturas críticas. Dada a sua importância específica e as consequências em toda a União de possíveis perturbações a este nível, o setor da energia poderá ser o setor que mais beneficie da realização de testes de esforço com base em princípios definidos de comum acordo. Esses testes de esforço são da competência dos Estados-Membros, que deverão incentivar e apoiar os operadores de infraestruturas críticas a realizarem-nos, sempre que sejam considerados benéficos e em consonância com os seus quadros jurídicos nacionais.

([2]) Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75)

([3]) Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

(10) A fim de assegurar uma resposta coordenada e eficaz a ameaças atuais e antecipadas, incentiva-se a Comissão a prestar apoio adicional aos Estados-Membros, nomeadamente fornecendo informações pertinentes sob a forma de notas de informação, manuais e orientações não vinculativos. O Serviço Europeu para a Ação Externa (SEAE), em especial através do Centro de Situação e de Informações da UE e da sua célula de fusão contra as ameaças híbridas, e com o apoio da Direção de Informações do Estado-Maior da União Europeia (EMUE) no âmbito da Capacidade Única de Análise de Informações (SIAC), deverá fornecer avaliações de ameaças. Convida-se igualmente a Comissão a, em cooperação com os Estados-Membros, promover a adoção de projetos de investigação e inovação financiados pela União.

(11) Face à crescente interdependência das infraestruturas físicas e digitais, é possível que as ciberatividades mal-intencionadas que visam áreas críticas causem perturbações ou danos nas infraestruturas físicas, ou que a sabotagem das infraestruturas físicas comprometa o acesso aos serviços digitais. Os Estados-Membros são convidados a acelerar os trabalhos preparatórios para a transposição e a aplicação do novo quadro jurídico aplicável às entidades críticas e do quadro jurídico reforçado para a cibersegurança, com base na experiência adquirida no âmbito do grupo de cooperação criado pela Diretiva (UE) 2016/1148 («grupo de cooperação SRI»), o mais rapidamente possível, tendo em conta os prazos de transposição e que os referidos trabalhos deverão progredir em paralelo e de forma coerente.

(12) Para além de melhorar a preparação, é igualmente importante reforçar as capacidades de resposta rápida e eficaz a perturbações nos serviços essenciais assegurados por infraestruturas críticas. Por conseguinte, a presente recomendação prevê medidas a tomar tanto a nível da União como a nível nacional, nomeadamente destacando o papel de apoio e o valor acrescentado que pode ser obtido graças ao reforço da cooperação e do intercâmbio de informações no contexto do Mecanismo de Proteção Civil da União (MPCU) criado pela Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho ([4]) e utilizando os ativos pertinentes do Programa Espacial da União criado ao abrigo do Regulamento (UE) 2021/696 do Parlamento Europeu e do Conselho ([5]).

(13) A Comissão, o alto representante da União para os Negócios Estrangeiros e a Política de Segurança («alto representante») e o grupo de cooperação SRI, em coordenação com os organismos e agências civis e militares pertinentes e com as redes estabelecidas, incluindo a Rede Europeia de Organizações de Coordenação de Cibercrises (EU-CyCLONe), deverão realizar uma avaliação do risco e elaborar cenários de risco. Além disso, na sequência do apelo ministerial conjunto de Nevers, o grupo de cooperação SRI está atualmente a realizar uma avaliação do risco, com o apoio da Comissão e da Agência da União Europeia para a Cibersegurança (ENISA), e em cooperação com o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE). Ambos os exercícios serão coerentes e coordenados com o exercício de elaborar cenários ao abrigo do MPCU, incluindo eventos de cibersegurança e o seu impacto na vida real, atualmente em fase de desenvolvimento pela Comissão e pelos Estados-Membros. No interesse da eficiência, eficácia e coerência, e para assegurar a aplicação adequada da presente recomendação, os resultados desses exercícios deverão repercutir-se a nível nacional.

(14) A fim de reforçar a título imediato a preparação e a capacidade de resposta a incidentes de cibersegurança de grande escala, a Comissão criou um programa de curto prazo para apoiar os Estados-Membros, mediante o financiamento adicional afetado à ENISA. Os serviços propostos incluirão, nomeadamente, ações de preparação, como testes de penetração para identificar as vulnerabilidades das entidades. O programa poderá igualmente reforçar as possibilidades de assistência aos Estados-Membros em caso de incidentes de cibersegurança de grande escala que afetem entidades críticas. Trata-se de um primeiro passo em consonância com as conclusões do Conselho, de 23 de maio de 2022, sobre o desenvolvimento da postura de cibersegurança da União Europeia («conclusões do Conselho sobre a postura de cibersegurança da UE»), nas quais se solicita à Comissão que apresente uma proposta relativa a um fundo de ciberemergência. É importante que os Estados-Membros tirem pleno partido dessas oportunidades, em conformidade com os requisitos aplicáveis, sendo incentivados a prosseguir os trabalhos no domínio da gestão de crises de cibersegurança na União, em especial acompanhando e fazendo periodicamente o balanço dos progressos alcançados na execução do roteiro para a gestão de cibercrises recentemente desenvolvido no Conselho. O referido roteiro é um documento dinâmico e deverá ser revisto e atualizado sempre que necessário.

([4]) 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).

([5]) Regulamento (UE) 2021/696 do Parlamento Europeu e do Conselho, de 28 de abril de 2021, que cria o Programa Espacial da União e a Agência da União Europeia para o Programa Espacial e que revoga os Regulamentos (UE) n.º 912/2010, (UE) n.º 1285/2013 e (UE) n.º 377/2014 e a Decisão n.º 541/2014/UE (JO L 170 de 12.5.2021, p. 69).

(15) Os cabos submarinos de comunicações mundiais são essenciais para a conectividade mundial e intra-UE. Devido ao comprimento significativo de tais cabos e à sua instalação no leito marítimo, é extremamente difícil assegurar a monitorização visual subaquática da maioria das secções de cabos. A competência partilhada e outras questões jurisdicionais relacionadas com tais cabos constituem um caso específico para a cooperação europeia e internacional em matéria de proteção e recuperação das infraestruturas. Por conseguinte, é necessário complementar as avaliações do risco em curso e previstas relativas às infraestruturas digitais e físicas subjacentes aos serviços digitais com avaliações do risco específicas e opções de medidas de atenuação relativas aos cabos submarinos de comunicações. Os Estados-Membros convidam a Comissão a realizar estudos para o efeito e a partilhar com eles os respetivos resultados.

(16) Os setores da energia e dos transportes também podem ser afetados por ameaças relacionadas com as infraestruturas digitais, como é o caso, por exemplo, das tecnologias energéticas que incorporam componentes digitais. A segurança das cadeias de abastecimento associadas é importante para a continuidade da prestação de serviços essenciais e para o controlo estratégico das infraestruturas críticas do setor da energia. Há que ter em conta essas circunstâncias ao tomar medidas para reforçar a resiliência das infraestruturas críticas em conformidade com a presente recomendação.

(17) Tendo em conta a importância crescente das infraestruturas espaciais, dos ativos terrestres relacionados com o espaço, incluindo as instalações de produção, e dos serviços espaciais para as atividades relacionadas com a segurança, é essencial assegurar a resiliência e a proteção do setor espacial da União e dos seus ativos e serviços terrestres na União. Pelos mesmos motivos, também é essencial, no âmbito da presente recomendação, utilizar de forma mais estruturada os dados e serviços espaciais fornecidos pelos sistemas e programas espaciais para a vigilância e o rastreio de objetos no espaço e a proteção de infraestruturas críticas noutros setores. A futura estratégia espacial da UE para a segurança e a defesa proporá ações adequadas a este respeito, que deverão ser tidos em conta ao aplicar a presente recomendação.

(18) A cooperação a nível internacional também é necessária para enfrentar com eficácia os riscos para as infraestruturas críticas situadas, nomeadamente, nas águas internacionais. Por conseguinte, incentivam-se os Estados-Membros a cooperarem com a Comissão e o alto representante e a tomarem medidas no sentido de alcançar tal cooperação, tendo em conta que as medidas só podem ser tomadas em conformidade com as respetivas atribuições e responsabilidades ao abrigo do direito da União, nomeadamente as disposições dos Tratados em matéria de relações externas.

(19) Como estabelecido na sua comunicação de 15 de fevereiro de 2022, intitulada «Contributo da Comissão para a defesa europeia», em apoio à Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais, a Comissão avaliará os requisitos de base da resiliência a nível setorial em cooperação com o alto representante e os Estados-Membros, identificando lacunas e necessidades, bem como as medidas para as colmatar até 2023. Essa iniciativa deverá contribuir para o trabalho realizado no âmbito da presente recomendação, ajudando a aumentar a partilha de informações e a coordenação das ações, por forma a reforçar a resiliência, incluindo a das infraestruturas críticas.

(20) A Estratégia de Segurança Marítima da UE de 2014 e o respetivo plano de ação revisto apelavam a uma maior proteção das infraestruturas marítimas críticas, incluindo as infraestruturas subaquáticas e, em especial, das infraestruturas do transporte marítimo, da energia e das comunicações, nomeadamente mediante o reforço do conhecimento situacional marítimo graças à melhoria da interoperabilidade e da racionalização do intercâmbio de informações (tanto obrigatório como voluntário). Essa estratégia e esse plano de ação estão atualmente em curso de atualização e incluirão ações reforçadas destinadas a proteger as infraestruturas marítimas críticas. Essas ações deverão complementar a presente recomendação.

(21) O reforço da resiliência das infraestruturas críticas contribui para os esforços mais gerais de luta contra as ameaças e campanhas híbridas que visam a União e os seus Estados-Membros. A presente recomendação baseia-se na comunicação conjunta ao Parlamento Europeu e ao Conselho, intitulada «Quadro comum em matéria de luta contra as ameaças híbridas – uma resposta da União Europeia». A ação 1 do quadro comum, a saber, o estudo sobre os riscos híbridos, desempenha um papel essencial para identificar as vulnerabilidades suscetíveis de afetar as estruturas e as redes nacionais e pan-europeias. Além disso, a execução das conclusões do Conselho, de 21 de junho de 2022, sobre um enquadramento para uma resposta coordenada da UE às campanhas híbridas, permitirá ações mais coordenadas através da aplicação do conjunto de instrumentos da UE contra as ameaças híbridas em todos os domínios afetados.

ADOTOU A PRESENTE RECOMENDAÇÃO:

CAPÍTULO I: OBJETIVO, ÂMBITO DE APLICAÇÃO E DEFINIÇÃO DE PRIORIDADES

(1) A presente recomendação estabelece uma série de medidas específicas a nível da União e a nível nacional destinadas a apoiar e reforçar a resiliência das infraestruturas críticas, a título voluntário, com destaque para as infraestruturas críticas com importante relevância transfronteiriça e em setores-chave identificados, como os da energia, das infraestruturas digitais, dos transportes e do espaço. Essas ações específicas visam o reforço do grau de preparação, a melhoria da resposta e a cooperação internacional.

(2) As informações partilhadas para assegurar o cumprimento dos objetivos da presente recomendação que sejam classificadas como confidenciais nos termos de regras da União e de regras nacionais, bem como de regras em matéria de sigilo comercial, só poderão ser trocadas com a Comissão e com outras autoridades competentes nos casos em que esse intercâmbio seja necessário para efeitos de aplicação adequada da presente recomendação. A presente recomendação não afeta a proteção dos interesses essenciais dos Estados-Membros em matéria de segurança nacional, segurança pública ou defesa e os Estados-Membros não deverão ser obrigados a partilhar informações que possam prejudicar tais interesses.

CAPÍTULO II: PREPARAÇÃO REFORÇADA

Ações a nível dos Estados-Membros

(3) Os Estados-Membros deverão prever uma abordagem multirrisco aquando da atualização das respetivas avaliações do risco ou análises equivalentes existentes, em conformidade com a natureza evolutiva das ameaças atuais às suas infraestruturas críticas, em especial nos setores-chave identificados e, se possível, em todos os setores abrangidos pelo futuro quadro jurídico aplicável às entidades críticas.

(4) Os Estados-Membros são convidados a acelerar os trabalhos preparatórios e a adotar medidas de reforço da resiliência, quando possível, em conformidade com o futuro quadro jurídico aplicável às entidades críticas, com especial destaque para a cooperação e a partilha de informações pertinentes entre os Estados-Membros e com a Comissão, para identificar as entidades críticas com importante relevância transfronteiriça e para reforçar o apoio prestado às entidades críticas identificadas a fim de aumentar a sua resiliência.

(5) Os Estados-Membros deverão apoiar a formação e os exercícios de peritos, bem como a partilha mútua de boas práticas e de ensinamentos retirados. Os Estados-Membros deverão incentivar os peritos a participar nas plataformas de formação existentes, tanto nacionais como internacionais, por exemplo no âmbito do MPCU.

(6) Os Estados-Membros deverão incentivar e apoiar os operadores de infraestruturas críticas, pelo menos no setor da energia, na realização de testes de esforço em conformidade com os princípios definidos de comum acordo a nível da União, sempre que adequado. Os testes de esforço deverão avaliar a resiliência das infraestruturas críticas contra ameaças antagonistas de origem humana. Por conseguinte, os Estados-Membros deverão procurar identificar infraestruturas críticas pertinentes para testar e consultar os operadores das infraestruturas críticas pertinentes com a maior brevidade possível e, o mais tardar, até ao final do primeiro trimestre de 2023. Além disso, os Estados--Membros deverão apoiar os operadores das infraestruturas críticas para que estes realizem os testes com a maior brevidade possível e procurem concluí-los até ao final de 2023, em conformidade com o direito nacional. O Conselho tenciona fazer o ponto da situação dos testes de esforço até ao final de abril de 2023.

(7) Devido à rápida evolução das ameaças às infraestruturas críticas, é essencial manter um elevado nível e proteção dessas infraestruturas Os Estados-Membros são incentivados a afetar recursos financeiros suficientes para reforçar as capacidades das autoridades nacionais competentes, e a apoiá-las, a fim de poderem aumentar a resiliência das infraestruturas críticas. Os Estados-Membros são igualmente incentivados a dotar as autoridades responsáveis pela gestão de incidentes de cibersegurança de grande escala de recursos financeiros suficientes, a apoiá-las e a assegurar que as suas equipas de resposta a incidentes de segurança informática (CSIRT) e autoridades competentes se encontrem plenamente mobilizadas no quadro da rede de equipas de resposta a incidentes de segurança informática e da EU-CyCLONe, respetivamente.

(8) Os Estados-Membros são convidados a tirar, eles próprios, partido, em conformidade com os requisitos aplicáveis, das potenciais oportunidades de financiamento a nível da União e a nível nacional a fim de reforçar a resiliência das infraestruturas críticas da União, e também a incentivar os operadores das infraestruturas críticas a aproveitarem tais oportunidades de financiamento, incluindo, por exemplo, as redes transeuropeias, contra todo o leque de ameaças significativas, nomeadamente ao abrigo dos programas financiados pelo Fundo para a Segurança Interna, criado pelo Regulamento (UE) 2021/1149 do Parlamento Europeu e do Conselho ([6]), pelo Fundo Europeu de Desenvolvimento Regional, criado pelo Regulamento (UE) n.º 1301/2013 do Parlamento Europeu e do Conselho ([7]), pelo MPCU e pelo plano REPowerEU da Comissão. Os Estados-Membros são também incentivados a utilizar da melhor forma os resultados dos projetos pertinentes desenvolvidos no âmbito de programas de investigação, como o Horizonte Europa, criado pelo Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho ([8]).

(9) No que diz respeito às infraestruturas de comunicações e redes da União, convida-se o grupo de cooperação SRI, agindo em conformidade com o artigo 11.º da Diretiva (UE) 2016/1148, a acelerar os trabalhos em curso, com base no apelo ministerial conjunto de Nevers, para uma avaliação específica dos riscos e apresentar as primeiras recomendações logo que possível. Essa avaliação do risco contribuirá para a avaliação transetorial dos riscos cibernéticos, atualmente em curso, e para os cenários solicitados pelo Conselho nas suas conclusões sobre a postura de cibersegurança da UE. Além disso, esse trabalho deverá ser realizado assegurando a coerência e a complementaridade com o trabalho realizado pelo grupo de cooperação SRI sobre a segurança da cadeia de abastecimento das tecnologias da informação e da comunicação, bem como por outros grupos pertinentes.

(10) O grupo de cooperação SRI é igualmente convidado a prosseguir, com o apoio da Comissão e da ENISA, os seus trabalhos sobre a segurança das infraestruturas digitais, inclusive no que diz respeito às infraestruturas submarinas, nomeadamente os cabos submarinos de comunicações. É também convidado a encetar os seus trabalhos no setor espacial, inclusive através da elaboração, se necessário, de orientações políticas e de metodologias de gestão dos riscos de cibersegurança, de acordo com uma abordagem multirrisco e uma abordagem baseada no risco, destinadas aos operadores do setor espacial, com vista a aumentar a resiliência das infraestruturas terrestres que apoiam a prestação de serviços espaciais.

(11) Os Estados-Membros deverão tirar pleno partido dos serviços de preparação para a cibersegurança oferecidos no âmbito do programa de apoio a curto prazo da Comissão aplicado com a ENISA, por exemplo no que diz respeito aos testes de penetração para identificar vulnerabilidades, sendo incentivados, neste contexto, a dar prioridade às entidades que exploram infraestruturas críticas nos setores da energia, das infraestruturas digitais e dos transportes.

(12) Os Estados-Membros deverão utilizar plenamente o Centro Europeu de Competências em Cibersegurança (ECCC). Os Estados-Membros deverão incentivar os seus Centros Nacionais de Coordenação a colaborarem proativamente com os membros da comunidade de cibersegurança para reforçar as capacidades a nível da União e a nível nacional com vista a prestar maior apoio aos operadores de serviços essenciais.

(13) É importante que os Estados-Membros concretizem a aplicação das medidas recomendadas no conjunto de instrumentos da UE para a cibersegurança das redes 5G e, em especial, que adotem restrições em relação aos fornecedores de alto risco, uma vez que perdas de tempo podem aumentar a vulnerabilidade das redes da União, e que reforcem também a proteção física e não física das partes críticas e sensíveis das redes 5G, inclusive através de controlos de acesso rigorosos. Além disso, cabe aos Estados-Membros, em cooperação com a Comissão, avaliar a necessidade de adotar medidas complementares, a fim de assegurar um nível coerente de segurança e resiliência das redes 5G.

(14) Os Estados-Membros, juntamente com a Comissão e a ENISA, deverão concentrar-se na aplicação das conclusões do Conselho, de 17 de outubro de 2022, sobre a segurança da cadeia de abastecimento das TIC.

([6]) Regulamento (UE) 2021/1149 do Parlamento Europeu e do Conselho, de 7 de julho de 2021, que cria o Fundo para a Segurança Interna (JO L 251 de 15.7.2021, p. 94).

([7]) Regulamento (UE) n.º 1301/2013 do Parlamento Europeu e do Conselho, de 17 de dezembro de 2013, relativo ao Fundo Europeu de Desenvolvimento Regional e que estabelece disposições específicas relativas ao objetivo de investimento no crescimento e no emprego, e que revoga o Regulamento (CE) n.º 1080/2006 (JO L 347 de 20.12.2013, p. 289).

([8]) Regulamento (UE) 2021/695 do Parlamento Europeu e do Conselho, de 28 de abril de 2021, que estabelece o Horizonte Europa — Programa-Quadro de Investigação e Inovação, que define as suas regras de participação e difusão, e que revoga os Regulamentos (UE) n.º 1290/2013 e (UE) n.º 1291/2013 (JO L 170 de 12.5.2021, p. 1).

(15) Os Estados-Membros deverão ter em conta o futuro código de rede para os aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade[...], baseando-se na experiência adquirida com a aplicação da Diretiva (UE) 2016/1148 e nas orientações pertinentes elaboradas pelo grupo de cooperação SRI, com destaque para o seu documento de referência sobre medidas de segurança para os operadores de serviços essenciais.

(16) Os Estados-Membros deverão desenvolver a utilização do Copernicus, do Galileo e do Serviço Europeu Complementar Geoestacionário de Navegação (EGNOS) para fins de vigilância, com vista a partilhar informações pertinentes com o grupo de peritos reunidos em conformidade com o ponto 15. Importa tirar o devido partido das capacidades oferecidas pela comunicação governamental por satélite (GOVSATCOM) do Programa Espacial da União para o acompanhamento das infraestruturas críticas e o apoio à previsão e à resposta a crises.

Ações a nível da União

(17) O diálogo e a cooperação entre os peritos designados pelos Estados-Membros e com a Comissão deverão ser intensificados com vista a reforçar a resiliência física das infraestruturas críticas, nomeadamente:

a) Contribuindo para a elaboração, o desenvolvimento e a promoção de instrumentos voluntários comuns para apoiar os Estados-Membros no reforço dessa resiliência, incluindo metodologias e cenários de risco;

b) Apoiando os Estados-Membros na implementação do novo quadro jurídico aplicável às entidades críticas, inclusive incentivando a Comissão a adotar o ato delegado em tempo útil;

c) Apoiando a realização dos testes de esforço a que se refere o ponto 6, com base em princípios comuns, começando pelos testes centrados nas ameaças antagonistas de origem humana no setor da energia e, subsequentemente, noutros setores-chave, bem como, a pedido de um Estado-Membro, prestando apoio e aconselhamento no tocante à realização desses testes de esforço;

d) Utilizando qualquer plataforma segura, uma vez criada pela Comissão, para recolher, fazer o balanço e partilhar, a título voluntário, as boas práticas, os ensinamentos retirados das experiências nacionais e outras informações relacionadas com essa resiliência.

Os trabalhos desses peritos designados deverão incidir em especial sobre as dependências transetoriais e as infraestruturas críticas com importante relevância transfronteiriça e deverão ser continuados no Conselho e na Comissão, se for caso disso.

(18) Os Estados-Membros são incentivados a tirar partido do apoio oferecido pela Comissão, por exemplo através da elaboração de manuais e orientações, como um manual sobre a proteção das infraestruturas críticas e dos espaços públicos contra os sistemas de aeronaves não tripuladas, bem como ferramentas para a avaliação do risco. O SEAE, em especial através do Centro de Situação e de Informações da UE e da sua célula de fusão contra as ameaças híbridas, e com o apoio da Direção de Informações do EMUE no âmbito do quadro da Capacidade Única de Análise de Informações, é convidado a realizar sessões de informação sobre as ameaças às infraestruturas críticas na União, a fim de melhorar o conhecimento da situação.

(19) Os Estados-Membros deverão apoiar as ações levadas a cabo pela Comissão para promover a integração dos resultados dos projetos sobre a resiliência das infraestruturas críticas financiadas ao abrigo dos programas de investigação e inovação da União. O Conselho regista a intenção da Comissão de aumentar o financiamento para essa resiliência no âmbito do orçamento afetado ao Horizonte Europa ao abrigo do quadro financeiro plurianual 2021-2027, sem prejuízo do financiamento proveniente de outros projetos de investigação e inovação relacionados com a segurança civil ao abrigo do Horizonte Europa.

(20) De acordo com o mandato atribuído nas conclusões do Conselho sobre a postura de cibersegurança da UE, a Comissão, o alto representante e o grupo de cooperação SRI são convidados a intensificar, em conformidade com as respetivas funções e responsabilidades ao abrigo do direito da União, o seu trabalho com as redes e os organismos e agências civis e militares pertinentes para a avaliação do risco e a elaboração de cenários de risco cibernético, tendo em conta, em especial, a importância das infraestruturas da energia, digitais, dos transportes e do espaço, bem como as interdependências intersetoriais e entre os Estados-Membros. Esse exercício deverá ter em conta os riscos conexos para as infraestruturas de que esses setores dependem. Se considerado útil, deverão ser efetuadas e elaboradas avaliações e cenários de risco com regularidade, assegurando que complementam e se baseiam nas avaliações de risco existentes ou previstas nesses setores, evitando ao mesmo tempo duplicações, a fim de contribuir para os debates sobre o modo de reforçar a resiliência global das entidades que exploram infraestruturas críticas e de colmatar as vulnerabilidades.

(21) A Comissão é convidada e acelerar as suas atividades, em conformidade com as respetivas atribuições no âmbito da gestão de crises de cibersegurança, com vista a apoiar a preparação dos Estados-Membros e a sua resposta aos incidentes de cibersegurança de grande escala, e, em especial:

a) A fim de complementar as avaliações de risco pertinentes no contexto da segurança das redes e da informação, realizar um estudo exaustivo ([9]) que elenque as infraestruturas submarinas, nomeadamente os cabos submarinos de comunicações, que ligam os Estados-Membros e a Europa ao resto do mundo, devendo os resultados ser partilhados com os Estados-Membros;

b) Apoiar a preparação e a resposta dos Estados-Membros e das instituições, organismos e agências da União a incidentes de cibersegurança de grande escala ou incidentes graves, em conformidade com o quadro jurídico reforçado para a cibersegurança e com outras regras pertinentes aplicáveis ([10]);

c) Acelerar a definição do conceito principal do fundo de ciberemergência através de debates adequados com os Estados-Membros.

(22) A Comissão é incentivada a intensificar os trabalhos sobre as medidas antecipativas prospetivas, nomeadamente a colaboração com os Estados-Membros, nos termos dos artigos 6.º e 10.º da Decisão 1313/2013/UE, e sob a forma de planos de contingência para apoiar a preparação operacional do Centro de Coordenação de Resposta de Emergência (CCRE) e a resposta a perturbações nas infraestruturas críticas, a aumentar o investimento em abordagens preventivas e na preparação da população e a intensificar o apoio no que diz respeito ao reforço de capacidades no âmbito da Rede Europeia de Conhecimentos sobre Proteção Civil.

(23) A Comissão deverá fomentar a utilização dos meios de vigilância da União (Copernicus, Galileo e EGNOS) para apoiar os Estados-Membros na monitorização das infraestruturas críticas e da sua vizinhança imediata, quando necessário, bem como para apoiar outras opções de vigilância previstas no Programa Espacial da União, como os quadros em matéria de conhecimento da situação no espaço e de vigilância e rastreio de objetos no espaço da UE.

(24) Se for caso disso e em conformidade com os respetivos mandatos, as agências da União e outros organismos competentes são convidados a prestar apoio em áreas relacionadas com a resiliência das infraestruturas críticas, nomeadamente:

a) A Agência da União Europeia para a Cooperação Policial (EUROPOL), no que diz respeito à recolha de informações, à análise da criminalidade e ao apoio à investigação em ações de aplicação da lei transfronteiriças e, se for pertinente e adequado, à partilha dos resultados com os Estados-Membros;

b) A Agência Europeia da Segurança Marítima (EMSA), no que diz respeito a questões relacionadas com a segurança e a proteção do setor marítimo na União, incluindo os serviços de vigilância marítima ativos nesse domínio;

c) A Agência da União Europeia para o Programa Espacial (EUSPA) e o Centro de Satélites da UE (SatCen) poderão prestar assistência através de operações no âmbito do Programa Espacial da União;

d) O ECCC, no que diz respeito às atividades relacionadas com a cibersegurança, também em cooperação com a ENISA, poderá apoiar a inovação e à política industrial em matéria de cibersegurança.

([9]) Este estudo deverá incluir um levantamento das suas capacidades e redundâncias, vulnerabilidades, ameaças e riscos para a disponibilidade de serviços, o impacto do tempo de inatividade dos cabos submarinos (transatlânticos) para os Estados-Membros e a União no seu conjunto e medidas de atenuação dos riscos, tendo simultaneamente em conta a sensibilidade de tais informações e a necessidade de as proteger.

([10]) Importa igualmente prestar especial atenção a todas as atividades de preparação para uma resposta coordenada eficaz a nível da União em caso de incidentes de cibersegurança transfronteiriços graves ou de ameaças conexas que possam ter um impacto sistémico no setor financeiro da União, em conformidade com o novo quadro jurídico em matéria de resiliência operacional digital.

CAPÍTULO III: RESPOSTA REFORÇADA

Ações a nível dos Estados-Membros

(25) Os Estados-Membros são convidados a:

a) Continuar a coordenar a sua resposta, se for caso disso, e manter a visão de conjunto da resposta transetorial a perturbações agudas dos serviços essenciais assegurados pelas infraestruturas críticas. Tal poderia ser feito no quadro de um futuro plano de resposta coordenada a perturbações das infraestruturas críticas com importante relevância transfronteiriça, no quadro das disposições atuais do Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) para a coordenação da resposta política no que diz respeito a infraestruturas críticas com impacto transfronteiriço, no âmbito do plano de resposta a incidentes e crises de cibersegurança de grande escala ao abrigo da Recomendação da Comissão (UE) 2017/1584 ([11]); no âmbito da EU-CyCLONe, no contexto do enquadramento para uma resposta coordenada da UE às campanhas híbridas e do conjunto de instrumentos da UE contra as ameaças híbridas, no caso de ameaças e campanhas híbridas, e no quadro do Sistema de Alerta Rápido em caso de desinformação;

b) Aumentar o intercâmbio de informações a nível operacional com o CCRE no contexto do MPCU, a fim de reforçar o alerta rápido e coordenar a sua resposta no âmbito do mecanismo em caso de perturbações das infraestruturas críticas com importante relevância transfronteiriça, assegurando assim uma reação mais rápida facilitada pela União, quando necessário;

c) Aumentar a prontidão da sua resposta a tais perturbações importantes referidas na alínea a), se for caso disso, por meio de ferramentas existentes ou a desenvolver;

d) Colaborar no desenvolvimento das capacidades de resposta pertinentes no âmbito da Reserva Europeia de Proteção Civil e do rescEU;

e) Incentivar os operadores de infraestruturas críticas e as autoridades nacionais competentes a reforçarem as suas capacidades para restabelecer rapidamente o funcionamento básico dos serviços essenciais prestados por esses operadores de infraestruturas críticas;

f) Incentivar os operadores de infraestruturas críticas a que, quando procedem à reconstrução das suas infraestruturas, as tornem tão resilientes quanto possível, tendo em conta a proporcionalidade das medidas no que diz respeito aos custos e às avaliações de risco, ao leque completo de riscos significativos a que possam estar sujeitas, incluindo cenários climáticos adversos.

(26) Os Estados-Membros são convidados a acelerar os trabalhos preparatórios, quando possível, em conformidade com o quadro jurídico reforçado para a cibersegurança, visando reforçar as capacidades das respetivas Equipas de Resposta a Incidentes de Segurança Informática (CSIRT), tendo em conta as suas novas funções, bem como o maior número de entidades de novos setores, revendo e atualizando as suas estratégias de cibersegurança em tempo útil e adotando com a maior brevidade planos nacionais de resposta a incidentes e crises de cibersegurança, caso ainda não existam.

(27) Os Estados-Membros são convidados a examinar, a nível nacional, os meios mais pertinentes para assegurar que as partes interessadas estão conscientes da necessidade de desenvolver a resiliência das infraestruturas críticas mediante a cooperação com fornecedores e parceiros fiáveis. É importante investir em capacidades adicionais, em especial nos setores em que as infraestruturas atuais estejam no fim da respetiva vida útil, por exemplo, as infraestruturas de cabos submarinos de comunicações, a fim de poder assegurar a continuidade da prestação de serviços essenciais em caso de perturbações, e de reduzir as dependências indesejadas.

(28) Os Estados-Membros são incentivados a prestar atenção à comunicação estratégica proativa a nível nacional no contexto da luta contra as ameaças e campanhas híbridas e atendendo ao potencial risco de os adversários optarem pela manipulação da informação e pela ingerência a partir do estrangeiro, manipulando a narrativa em torno de incidentes que visam infraestruturas críticas.

Ações a nível da União

(29) Convida-se a Comissão a trabalhar em estreita colaboração com os Estados-Membros, para continuar a desenvolver organismos, instrumentos, e capacidades de resposta pertinentes, com vista a melhorar a preparação operacional para fazer face aos efeitos imediatos e indiretos de perturbações significativas dos serviços essenciais pertinentes assegurados pelas infraestruturas críticas, em especial os peritos e os recursos disponíveis através da Reserva Europeia de Proteção Civil e do rescEU no quadro do MPCU ou das futuras equipas de resposta rápida às ameaças híbridas.

([11]) 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).

(30) Tendo em conta a evolução do cenário das ameaças e em cooperação com os Estados-Membros, convida-se a Comissão, no contexto do MPCU, a:

a) Analisar e testar continuamente a adequação e a prontidão operacional das capacidades de resposta existentes;

b) Acompanhar e identificar regularmente potenciais lacunas significativas em matéria de capacidades da Reserva Europeia de Proteção Civil e do RescEU;

c) Intensificar a colaboração transetorial para assegurar uma resposta adequada a nível da União e organizar formações ou exercícios regulares para testar tal colaboração, em cooperação com um ou mais Estados-Membros;

d) Continuar a desenvolver o CCRE para servir de plataforma transetorial de emergência a nível da União com vista à coordenação do apoio aos Estados-Membros afetados.

(31) O Conselho está empenhado em iniciar os trabalhos a fim de aprovar um plano de resposta coordenada a perturbações das infraestruturas críticas com importante relevância transfronteiriça, que descreva e defina os objetivos e as modalidades de cooperação entre os Estados-Membros e as instituições, órgãos e organismos da UE na resposta a incidentes contra tais infraestruturas críticas. O Conselho aguarda com expectativa o projeto da Comissão relativo ao referido plano, com base no apoio e nos contributos das agências competentes da União. O plano deverá ser plenamente coerente e interoperável com o protocolo operacional revisto da União para a luta contra as ameaças híbridas («manual tático da UE») e ter em conta o plano existente para uma resposta coordenada a incidentes e crises de cibersegurança transfronteiriços de grande escala ([12]) e o mandato da EU CyCLONe estipulado na Diretiva SRI 2, evitando a duplicação de estruturas e atividades. Esse plano deverá respeitar plenamente as disposições atuais do Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) para a coordenação da resposta.

(32) Convida-se a Comissão a consultar as partes interessadas e os peritos pertinentes sobre as medidas a tomar face a possíveis incidentes significativos relacionados com as infraestruturas submarinas, a apresentar em conjugação com o inventário referido no ponto 20, alínea a), e a aprofundar os planos de contingência, cenários de risco e objetivos de resiliência da União a catástrofes estabelecidos na Decisão n.º 1313/2013/UE.

CAPÍTULO IV: COOPERAÇÃO INTERNACIONAL

Ações a nível dos Estados-Membros

(33) Os Estados-Membros deverão cooperar, quando apropriado e em conformidade com o direito da União, com os países terceiros pertinentes no que diz respeito à resiliência das infraestruturas críticas com importante relevância transfronteiriça.

(34) Os Estados-Membros são incentivados a cooperar com a Comissão e o alto representante a fim de dar uma resposta eficaz aos riscos para as infraestruturas críticas nas águas internacionais.

(35) Os Estados-Membros são convidados a contribuir, em cooperação com a Comissão e o alto representante, para o desenvolvimento e a aplicação acelerados do conjunto de instrumentos da UE contra as ameaças híbridas e das orientações de execução referidas nas conclusões do Conselho, de 21 de junho de 2022, sobre um enquadramento para uma resposta coordenada da UE às campanhas híbridas, bem como a utilizá-los subsequentemente, a fim de dar pleno efeito ao enquadramento para uma resposta coordenada da UE às campanhas híbridas, em particular quando são estudadas e preparadas respostas abrangentes e coordenadas da União às campanhas híbridas e às ameaças híbridas, incluindo as que visam os operadores de infraestruturas críticas.

([12]) 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.

Ações a nível da União

(36) A Comissão e o alto representante são convidados a apoiar, quando apropriado e em conformidade com as respetivas funções e responsabilidades ao abrigo do direito da União, os países terceiros pertinentes no reforço da resiliência de infraestruturas críticas no seu território e, em especial, de infraestruturas críticas fisicamente ligadas ao seu território e ao de um Estado-Membro.

(37) A Comissão e o alto representante, em conformidade com as respetivas funções e responsabilidades ao abrigo do direito da União, reforçarão a coordenação com a OTAN em matéria de resiliência das infraestruturas críticas de interesse comum através do diálogo estruturado UE-OTAN sobre a resiliência, no pleno respeito das competências da União e dos Estados-Membros, em consonância com os Tratados e os princípios fundamentais que orientam a cooperação UE-OTAN, conforme acordados pelo Conselho Europeu, em especial os princípios da reciprocidade, da inclusividade e da autonomia de decisão. Neste contexto, essa cooperação será desenvolvida no âmbito do diálogo estruturado UE-OTAN sobre a resiliência, integrado no mecanismo existente entre os diferentes níveis do pessoal das duas organizações para a aplicação das declarações conjuntas, garantindo simultaneamente a total transparência e o envolvimento de todos os Estados-Membros.

(38) Convida-se a Comissão a considerar a participação de representantes de países terceiros pertinentes, sempre que necessário e adequado, no quadro da cooperação e do intercâmbio de informações entre os Estados-Membros no domínio da resiliência das infraestruturas críticas fisicamente ligadas ao território de um Estado-Membro e ao de um país terceiro.

Feito em Bruxelas, em 8 de dezembro de 2022.

Pelo Conselho
O Presidente
V. RAKUŠAN