COMISSÃO
EUROPEIA

Estrasburgo, 18.10.2022
COM(2022) 551 final

2022/0338 (NLE)

Proposta de

RECOMENDAÇÃO DO CONSELHO

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

(Texto relevante para efeitos do EEE)

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DA PROPOSTA

• Razões e objetivos da proposta

A segurança é um objetivo essencial da União Europeia. Se a responsabilidade pela proteção dos cidadãos recai primariamente sobre os Estados-Membros, a ação coletiva a nível da União contribui de modo significativo para a segurança da União no seu conjunto. A coordenação contribui para reforçar a resiliência, melhorar a vigilância e fortalecer a nossa resposta coletiva. No contexto da União da Segurança da UE, tomaram-se medidas importantes para criar capacidades e competências de prevenção, deteção e resposta rápida a numerosas ameaças à segurança, bem como para unir os intervenientes dos setores público e privado num esforço comum.

Dotar a UE de meios para lidar com o panorama de ameaças em constante mutação exige uma vigilância e adaptação permanentes. A guerra de agressão da Rússia contra a Ucrânia trouxe novos riscos, amiúde combinados sob a forma de uma ameaça híbrida. Um deles é o risco de perturbação da prestação de serviços essenciais assegurados por entidades que exploram infraestruturas críticas na Europa. Tal tornou-se ainda mais evidente com a aparente sabotagem dos gasodutos Nord Stream e com outros incidentes recentes. A sociedade depende fortemente de infraestruturas físicas e digitais, pelo que a interrupção dos serviços essenciais, quer através de ataques físicos convencionais ou de ciberataques, quer mediante uma combinação de ambos, pode ter consequências graves para o bem-estar dos cidadãos, as nossas economias e a confiança nos nossos sistemas democráticos.

Além disso, assegurar o bom funcionamento do mercado interno é outro objetivo-chave da UE, nomeadamente no que diz respeito aos serviços essenciais prestados por entidades que exploram infraestruturas críticas. Por conseguinte, a UE já tomou uma série de medidas para reduzir as vulnerabilidades e aumentar a resiliência das entidades críticas, tanto no que diz respeito aos riscos cibernéticos como aos riscos não cibernéticos.

Urge atuar para fortalecer a capacidade da UE para enfrentar potenciais ataques contra infraestruturas críticas, sobretudo na própria UE, mas também, quando necessário, na sua vizinhança direta.

A proposta de recomendação do Conselho visa intensificar o apoio da UE ao aumento da resiliência das infraestruturas críticas e assegurar uma coordenação a nível da UE em termos de preparação e resposta. Pretende maximizar e acelerar os trabalhos para proteger os meios, as instalações e os sistemas necessários ao funcionamento da economia e à prestação de serviços essenciais de que os cidadãos dependem, bem como para atenuar o impacto de eventuais ataques, assegurando uma recuperação tão célere quanto possível. Embora seja necessário proteger todas essas infraestruturas, a primeira prioridade neste momento são os setores da energia, das infraestruturas digitais, dos transportes e do espaço, atendendo à sua particular transversalidade para a sociedade e a economia e tendo em conta as atuais avaliações de risco.

A UE tem um papel especial a desempenhar no que toca a garantir a resiliência das infraestruturas que atravessam fronteiras terrestres ou marítimas e afetam os interesses de vários Estados-Membros ou que são utilizadas para prestar serviços essenciais além-fronteiras. As infraestruturas críticas com impacto em vários Estados-Membros podem, no entanto, estar situadas num único Estado-Membro ou inclusive fora do território de um Estado-Membro, como é o caso, por exemplo, dos cabos ou condutas submarinos. É do interesse de todos os Estados-Membros e da UE no seu conjunto identificar de maneira clara

as infraestruturas críticas e as entidades que as exploram, a par dos riscos a elas associados, e assumir um compromisso coletivo de as proteger.

O Parlamento Europeu e o Conselho já chegaram a um acordo político para aprofundar o quadro legislativo da UE na ótica de contribuir para reforçar a resiliência das entidades que exploram infraestruturas críticas. No verão de 2022, alcançaram-se acordos sobre a Diretiva Resiliência das Entidades Críticas (Diretiva REC)[1] e a Diretiva Segurança das Redes e da Informação (Diretiva SRI 2)[2] revista. Estes instrumentos constituirão um reforço considerável das capacidades em comparação com o quadro legislativo em vigor, designadamente a Diretiva 2008/114/CE, 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 («Diretiva ICE»)[3] e a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União («Diretiva SRI»)[4]. Prevê-se que a nova legislação entre em vigor no final de 2022 ou no início de 2023, devendo os Estados-Membros dar prioridade à sua transposição e aplicação, em conformidade com o direito da União.

Assim sendo, e perante a potencial urgência de enfrentar as ameaças decorrentes da guerra de agressão da Rússia contra a Ucrânia, importaria antecipar desde já as medidas delineadas na nova legislação, na medida do possível e do apropriado. A intensificação da cooperação mútua com caráter imediato também ajudaria a criar uma dinâmica conducente a uma aplicação eficaz quando a nova legislação estivesse plenamente em vigor.

Tal traduzir-se-ia numa abordagem que já iria além dos enquadramentos atuais, tanto em termos do alcance da ação como da abrangência dos setores visados. A nova Diretiva REC define um novo quadro de cooperação e um conjunto de obrigações para os Estados-Membros e as entidades críticas com o fito de reforçar a resiliência física não cibernética contra as ameaças naturais e de origem humana que afetam as entidades que prestam serviços essenciais no mercado interno, especificando onze setores[5]. A Diretiva SRI 2 prevê uma ampla cobertura setorial das obrigações em matéria de cibersegurança, incluindo um novo requisito de os Estados-Membros integrarem, quando pertinente, os cabos submarinos nas suas estratégias de cibersegurança.

A legislação exige que a Comissão assuma um papel substancial de coordenação. Ao abrigo da Diretiva REC, a Comissão desempenha funções de apoio e de facilitação, coadjuvada pelo Grupo para a Resiliência das Entidades Críticas (CERG) criado pela referida diretiva, cabendo-lhe complementar as atividades dos Estados-Membros mediante o desenvolvimento de boas práticas, materiais de orientação e metodologias. No que diz respeito à cibersegurança, o Conselho, nas suas conclusões sobre a postura de cibersegurança da UE emitidas no verão de 2022, já tinha convidado a Comissão, o alto representante e o grupo de cooperação SRI a elaborarem avaliações e cenários de risco numa perspetiva de cibersegurança. Essa coordenação poderá inspirar uma abordagem aplicável a outras infraestruturas críticas essenciais.

Em 5 de outubro de 2022, a presidente Ursula von der Leyen apresentou um plano de cinco pontos em que definiu uma abordagem coordenada para as ações que é necessário realizar no

---

1 COM(2020) 829 final.
2 COM(2020) 823 final.
3 JO L 345 de 23.12.2008.
4 JO L 194 de 19.7.2016.
5 Energia, transportes, infraestruturas digitais, serviços bancários, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, administração pública, espaço e alimentação.

futuro. Os seus principais elementos eram os seguintes: reforçar a preparação; trabalhar com os Estados-Membros na realização de testes de esforço das suas infraestruturas críticas, começando pelo setor da energia e prosseguindo para outros setores de alto risco; aumentar a capacidade de resposta em particular, através do Mecanismo de Proteção Civil da União; tirar bom partido da capacidade dos satélites para detetar potenciais ameaças; e reforçar a cooperação com a OTAN e com os principais parceiros em matéria de resiliência das infraestruturas críticas. O plano de cinco pontos sublinhava a importância de antecipar a legislação que já é alvo de consenso político.

A presente proposta de recomendação do Conselho congratula-se com essa abordagem, visando estruturar o apoio aos Estados-Membros e coordenar os seus esforços de sensibilização para os riscos, de preparação e de resposta às ameaças atuais. Nesse contexto, pretende-se convocar reuniões de peritos para debater a resiliência das entidades que exploram infraestruturas críticas na perspetiva da entrada em vigor da Diretiva REC e do Grupo para a Resiliência das Entidades Críticas (GREC) por ela criado.

Será essencial reforçar a cooperação com os principais parceiros e com os países vizinhos e outros países terceiros pertinentes em matéria de resiliência das entidades que exploram infraestruturas críticas, em particular através do diálogo estruturado UE-OTAN sobre a resiliência.

A presente recomendação centra-se no reforço da capacidade da União para antecipar, prevenir e responder às novas ameaças emergentes da guerra de agressão da Rússia contra a Ucrânia. Por conseguinte, põe a tónica na abordagem dos riscos relacionados com a segurança e das ameaças às infraestruturas críticas. Note-se, porém, que os acontecimentos recentes também puseram em evidência a necessidade premente de prestar mais atenção aos impactos das alterações climáticas nas infraestruturas e serviços críticos no respeitante, por exemplo, ao abastecimento de água para o arrefecimento das centrais nucleares, sujeito a flutuações sazonais potencialmente problemáticas e imprevisíveis, à energia hidroelétrica e à navegação interior, ou ao risco de danos materiais nas infraestruturas de transporte, elementos esses que podem causar perturbações de vulto nos serviços essenciais. Estas preocupações continuarão a ser abordadas mediante a legislação e a coordenação correspondentes.

- **Coerência com as disposições existentes da mesma política setorial**

A presente proposta de recomendação do Conselho está em plena consonância com o quadro jurídico atual e futuro relativo à resiliência das entidades que exploram infraestruturas críticas, a Diretiva ICE e a Diretiva REC, respetivamente, uma vez que visa, entre outros aspetos, facilitar a cooperação entre os Estados-Membros neste domínio e apoiar medidas concretas para reforçar a resiliência face às atuais ameaças iminentes contra as entidades que exploram infraestruturas críticas na UE.

Também complementa e antecipa a Diretiva REC ao incentivar desde já os Estados-Membros a darem prioridade à transposição atempada da diretiva, ao promover a cooperação através das reuniões de peritos convocadas no âmbito do plano de cinco pontos anunciado pela Comissão e ao procurar coordenar o modo de adotar uma abordagem comum para a realização de testes de esforço em infraestruturas críticas da UE.

A proposta também está em consonância com a Diretiva SRI e a futura Diretiva SRI 2, que revogará a Diretiva SRI, apelando para um arranque precoce dos trabalhos de aplicação e transposição. Reflete igualmente o apelo conjunto proferido em Nevers em março de 2022, bem como as conclusões do Conselho sobre a postura de cibersegurança da UE, de maio de 2022, no que diz respeito ao pedido que os Estados-Membros dirigiram à Comissão no sentido de elaborar avaliações do risco e cenários de risco.

A proposta também está em consonância com a política da UE em matéria de proteção civil, com base na qual, no caso de uma perturbação avassaladora das operações das infraestruturas/entidades críticas, os Estados-Membros e os países terceiros podem solicitar assistência através do Centro de Coordenação de Resposta de Emergência (CCRE) ao abrigo do Mecanismo de Proteção Civil da União (MPCU). Em caso de ativação do MPCU, o CCRE pode coordenar e cofinanciar a mobilização para o país afetado de equipamento, materiais e conhecimentos especializados essenciais disponíveis nos Estados-Membros (em parte no contexto da Reserva Europeia de Proteção Civil) e no âmbito do rescEU. A assistência a prestar mediante pedido inclui, por exemplo, o fornecimento de combustíveis, geradores, infraestruturas de eletricidade, capacidade de abrigo, capacidade de purificação da água e capacidades médicas de emergência.

A proposta está igualmente em conformidade com o acervo da UE em matéria de segurança do aprovisionamento energético.

O setor da energia nuclear não está especificamente incluído na proposta de recomendação do Conselho, exceto eventuais infraestruturas conexas (como linhas de transporte para centrais nucleares) suscetíveis de comprometer a segurança do aprovisionamento. Os elementos nucleares específicos são abrangidos pela legislação pertinente nesse domínio ao abrigo do Tratado Euratom e/ou pela legislação nacional[6]. Com base nos ensinamentos retirados do acidente de Fucoxima, a legislação europeia em matéria de segurança nuclear foi reforçada, pelo que cabe às autoridades nacionais realizar regularmente análises de segurança periódicas para cada instalação, a fim de assegurar o cumprimento permanente dos mais elevados requisitos de segurança e identificar outras melhorias a introduzir em matéria de segurança, bem como seis análises temáticas anuais pelos pares a nível da UE.

A Estratégia de Segurança Marítima da UE[7] e o respetivo plano de ação[8] salientam a natureza dinâmica das ameaças no domínio marítimo e apelam para um empenho renovado na 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 da sensibilização marítima através da melhoria da interoperabilidade e da racionalização do intercâmbio de informações.

A proposta está igualmente em conformidade com outra legislação setorial pertinente. Por conseguinte, a aplicação da presente recomendação deve estar em consonância com as medidas específicas que regem ou poderão vir a reger determinados aspetos da resiliência das entidades que operam nos setores em causa, como o setor dos transportes. Tal inclui outras iniciativas relevantes neste contexto, como o plano de emergência para os transportes[9], o plano de contingência para garantir o abastecimento alimentar e a segurança alimentar em tempos de crise[10] e o Mecanismo Europeu de Preparação e Resposta a Crises de Segurança Alimentar. De um modo mais geral, a recomendação deve, naturalmente, ser aplicada no pleno respeito de todas as regras aplicáveis do direito da UE, incluindo as estabelecidas nas Diretivas ICE e SRI.

A proposta está ainda em consonância com a Bússola Estratégica para a Segurança e a Defesa, que salientou a necessidade de reforçar substancialmente a resiliência e a capacidade

6 Considerando 9 da Diretiva 2008/114/CE do Conselho (Diretiva ICE).
7 11205/14.
8 10494/18.
9 COM(2022) 211.
10 COM(2021) 689.

para combater as ameaças híbridas e os ciberataques, bem como a necessidade de reforçar a resiliência dos países parceiros e de cooperar com a OTAN. Está também em consonância com o enquadramento para uma resposta coordenada da UE às ameaças e campanhas híbridas que afetam a UE, os Estados-Membros e os parceiros[11].

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

• Base jurídica

A proposta baseia-se no artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), que prevê a aproximação das legislações para a melhoria do mercado interno, juntamente com o artigo 292.º do TFUE. Tal justifica-se pelo facto de a proposta de recomendação do Conselho visar sobretudo antecipar as medidas previstas nas novas diretivas REC e NIS 2, ambas igualmente baseadas no artigo 114.º do TFUE. Em consonância com a lógica que justifica a invocação desse artigo como base jurídica das diretivas em causa, impõe-se uma ação da UE para assegurar o bom funcionamento do mercado interno, em particular tendo em conta a natureza e o âmbito transfronteiriços dos serviços em causa e as potenciais consequências em caso de perturbações, bem como as medidas nacionais reais e emergentes destinadas a reforçar a resiliência das entidades que exploram infraestruturas críticas na União.

• Subsidiariedade (no caso de competência não exclusiva)

A adoção de soluções a nível europeu no domínio da resiliência das entidades que exploram infraestruturas críticas é justificada, dada a natureza interdependente e transfronteiriça das relações entre as operações das infraestruturas críticas e os serviços essenciais prestados, bem como face à necessidade de uma abordagem europeia mais comum e coordenada, a fim de assegurar que as entidades em causa são suficientemente resilientes no atual contexto geopolítico. Se muitos dos desafios comuns, como a aparente sabotagem dos gasodutos Nord Stream, são, antes de mais, abordados através de medidas nacionais ou pelas entidades que exploram infraestruturas críticas, o apoio da UE, incluindo das agências pertinentes, sempre que apropriado, é necessário para reforçar a resiliência, melhorar a vigilância e fortalecer a resposta coletiva da UE.

• Proporcionalidade

A presente proposta está em conformidade com o princípio da proporcionalidade, como previsto no artigo 5.º, n.º 4, do Tratado da União Europeia.

Nem o conteúdo nem a forma da presente proposta de recomendação do Conselho excedem o necessário para atingir os seus objetivos. As ações propostas são proporcionadas em relação aos objetivos visados, na medida em que respeitam as prerrogativas e as obrigações dos Estados-Membros ao abrigo do direito nacional.

Por último, a proposta integra uma abordagem potencialmente diferenciada que reflete a variedade das realidades internas dos Estados-Membros no que diz respeito à preparação e à resposta a ameaças físicas contra infraestruturas críticas.

• Escolha do instrumento

A fim de alcançar os objetivos acima referidos, o TFUE prevê a adoção pelo Conselho de recomendações, nomeadamente no seu artigo 292.º, com base numa proposta da Comissão.

[11] Conselho da União Europeia 10016/22 de 21 de junho de 2022.

Uma recomendação do Conselho é um instrumento adequado no caso presente, atendendo também ao atual contexto legislativo, como explicado acima. Enquanto ato jurídico, ainda que de natureza não vinculativa, uma recomendação do Conselho reflete o empenho dos Estados-Membros nas medidas incluídas e proporciona uma base política sólida para a cooperação nestes domínios, respeitando plenamente a autoridade dos Estados-Membros.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

• Consultas das partes interessadas

Na elaboração desta proposta, tiveram-se em conta os pontos de vista dos peritos dos Estados-Membros tal como expressos na reunião de 12 de outubro de 2022. Registou-se um amplo consenso quanto à utilidade de uma maior coordenação a nível da União em matéria de preparação e de resposta no atual contexto de ameaças e da possibilidade de antecipar determinados elementos da Diretiva REC antes da sua adoção formal. Os Estados-Membros mostraram-se abertos à partilha de experiências e boas práticas sobre as medidas e as metodologias destinadas a reforçar a resiliência das entidades que exploram infraestruturas críticas. Manifestaram-se igualmente disponíveis para adotar uma abordagem coordenada dos testes de esforço das entidades que exploram infraestruturas críticas numa base voluntária e assente em princípios comuns. Apontaram como prioritárias, para efeitos da presente recomendação, as entidades que exploram infraestruturas críticas nos setores da energia, das infraestruturas digitais e dos transportes, nomeadamente as que têm impacto em vários Estados-Membros. Congratularam-se ainda com a intenção da Comissão de convocar novas reuniões de peritos dos Estados-Membros nas próximas semanas.

• Explicação pormenorizada das disposições específicas da proposta

A proposta de recomendação do Conselho prevê o seguinte:

– O capítulo I estabelece o objetivo da proposta, o seu âmbito de aplicação e a definição de prioridades relativamente às medidas recomendadas.

– O capítulo II centra-se nas medidas que cumpre tomar para reforçar o grau de preparação, tanto a nível da União como dos Estados-Membros.

– O capítulo III propõe uma resposta reforçada, tanto a nível da UE como dos Estados-Membros.

– O capítulo IV trata da cooperação internacional e das medidas a tomar para reforçar a resiliência das entidades que exploram infraestruturas críticas.

2022/0338 (NLE)

Proposta de

RECOMENDAÇÃO DO CONSELHO

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

(Texto relevante para efeitos do EEE)

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,

Tendo em conta a proposta da Comissão Europeia,

Considerando o seguinte:

(1) A UE tem um papel particular a desempenhar no que diz respeito às infraestruturas transfronteiriças que afetam os interesses de vários Estados-Membros ou que são de alguma forma utilizadas por entidades que prestam serviços essenciais numa base transfronteiriça. Essa prestação de serviços e essas infraestruturas críticas com impacto em vários Estados-Membros podem, no entanto, estar situadas num único Estado-Membro ou fora do território dos Estados-Membros, como é o caso, por exemplo, dos cabos ou condutas submarinos. É do interesse de todos os Estados-Membros e da União no seu conjunto identificar de maneira clara tais infraestruturas e entidades, bem como as ameaças que elas enfrentam, e assumir um compromisso coletivo de as proteger.

(2) A proteção das infraestruturas críticas em dois setores é atualmente regida pela Diretiva 2008/114/CE do Conselho[12]. Esta diretiva estabelece um procedimento de identificação e designação das infraestruturas críticas europeias e uma abordagem comum relativa à avaliação da necessidade de melhorar a sua proteção, de modo a contribuir para a proteção das pessoas, abrangendo os setores da energia e dos transportes. A fim de melhorar a resiliência das entidades críticas, os serviços essenciais que elas prestam e as infraestruturas críticas de que dependem, está em curso de adoção, pelo legislador da União, uma nova Diretiva relativa à resiliência das entidades críticas[13] (Diretiva REC), que substituirá a Diretiva 2008/114/CE e abrangerá mais setores, incluindo as infraestruturas digitais.

(3) Além disso, a 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

[12] 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 23.12.2009, p. 75).

[13] COM(2020) 829.

segurança das redes e da informação em toda a União[14] incide sobre as ameaças relacionadas com o ciberespaço. Essa diretiva será substituída por uma nova diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União[15] (Diretiva SRI 2), que também está em curso de adoção pelo legislador da União.

(4) Tendo em conta a rápida evolução do panorama das ameaças, em particular no contexto da aparente sabotagem das infraestruturas de gás Nord Stream 1 e 2, as entidades que exploram infraestruturas críticas enfrentam desafios específicos no que diz respeito à sua resiliência contra atos hostis e outras ameaças de origem humana, ao mesmo tempo que os desafios decorrentes de fatores naturais e das alterações climáticas estão a aumentar e podem interagir com os atos hostis. Cabe, pois, a tais entidades, com o apoio dos Estados-Membros, adotar medidas adequadas de reforço da resiliência. O alcance dessas medidas e do apoio concomitante deve ir para além das ações previstas ao abrigo da Diretiva 2008/114/CE e da Diretiva (UE) 2016/1148, inclusivamente antes da adoção, entrada em vigor e transposição das novas diretivas REC e SRI 2.

(5) Na pendência da adoção, entrada em vigor e transposição dessas novas diretivas, a União e os Estados-Membros são incentivados, em conformidade com o direito da União, a utilizar todos os instrumentos disponíveis para fazer avançar e ajudar a reforçar a resiliência física e cibernética das entidades em causa e das infraestruturas críticas por elas operadas para prestarem serviços essenciais no mercado interno, ou seja, serviços de importância crucial para a manutenção de funções societais vitais, a atividade económica, a saúde e a segurança públicas e o ambiente. A este propósito, cabe entender o conceito de resiliência como dizendo respeito à capacidade de uma entidade para prevenir, proteger, reagir, resistir, atenuar, absorver, acomodar e recuperar de acontecimentos que perturbam ou têm potencial para perturbar significativamente a prestação dos serviços essenciais em questão.

(6) A fim de assegurar uma abordagem eficaz e tão coerente quanto possível com a nova Diretiva REC, as medidas contidas na presente recomendação devem dizer respeito às infraestruturas designadas por um Estado-Membro como infraestruturas críticas, abrangendo tanto as infraestruturas críticas nacionais como as infraestruturas críticas europeias designadas em conformidade com a Diretiva 2008/114/CE, independentemente de a entidade operadora da infraestrutura já ter sido designada como entidade crítica nos termos da nova diretiva. Para efeitos da presente recomendação, o termo «infraestruturas críticas» deve ser entendido em conformidade.

(7) Tendo em conta as ameaças existentes, as medidas de reforço da resiliência devem ser tomadas com caráter prioritário nos setores-chave da energia, das infraestruturas digitais, dos transportes e do espaço, pondo a tónica no reforço da resiliência das entidades que exploram infraestruturas críticas face aos riscos de origem humana. No que diz respeito às infraestruturas críticas nacionais, tendo em conta as possíveis consequências num cenário em que os riscos se concretizem, importa dar prioridade às infraestruturas com impacto transfronteiriço.

---

[14] 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).

[15] COM(2020) 823.

(8) Nesse sentido, as medidas previstas na presente recomendação visam sobretudo complementar as novas Diretivas REC e SRI 2, que têm por base o artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), antecipando e complementando as medidas previstas nessas novas diretivas. Por conseguinte, e tendo em conta a natureza e o impacto transfronteiriços dos serviços essenciais e das infraestruturas críticas em causa, bem como as disparidades atuais e emergentes das legislações nacionais que distorcem o mercado interno, é apropriado basear a presente recomendação também no artigo 114.º do TFUE, juntamente com o artigo 292.º do TFUE.

(9) A aplicação da presente recomendação não deverá ser entendida como afetando os requisitos atuais e futuros do direito da União no atinente a determinados aspetos da resiliência das entidades em causa, devendo ser coerente com eles. Esses requisitos estão estabelecidos em instrumentos gerais, como a Diretiva 2008/114/CE e a Diretiva (UE) 2016/1148 e as novas diretivas REC e SRI 2 que as substituem, mas também em determinados instrumentos setoriais específicos, como no domínio dos transportes, em que a Comissão adotou uma iniciativa relativa ao plano de emergência para os transportes[16]. Em conformidade com o princípio da cooperação leal, a presente recomendação deve ser aplicada no pleno cumprimento dos deveres recíprocos de respeito e de assistência.

(10) Em 5 de outubro de 2022, a Comissão anunciou um plano de cinco pontos que estabelece uma abordagem coordenada para enfrentar os desafios futuros, incluindo um esforço de preparação antecipativo e assente na adoção e na entrada em vigor da nova Diretiva REC, bem como um trabalho de colaboração com os Estados-Membros com vista à realização de testes de esforço das entidades que exploram infraestruturas críticas com base em princípios comuns, começando pelo setor da energia. A presente recomendação, que contribuirá para esse plano, acolhe favoravelmente a abordagem proposta e delineia formas possíveis de a pôr em prática.

(11) Face a um cenário de ameaças em rápida evolução e ao atual ambiente de risco caracterizado por riscos de origem humana, em particular no atinente às infraestruturas críticas com impacto transfronteiriço, é essencial dispor de uma imagem exata, atualizada e completa dos riscos mais importantes enfrentados pelas entidades que exploram infraestruturas críticas. Por conseguinte, os Estados-Membros devem tomar as medidas necessárias para realizar ou atualizar as suas avaliações desses riscos. Embora a presente recomendação se centre nos riscos relacionados com a segurança, cumpre continuar a envidar esforços para fazer face às alterações climáticas e aos riscos ambientais, em particular quando os fenómenos naturais têm potencial para exacerbar ainda mais os riscos de origem humana.

(12) Tendo em conta esse panorama de ameaças, importa incentivar os Estados-Membros a tomar, com a maior brevidade, medidas adequadas para reforçar a resiliência das infraestruturas críticas, inclusive para além do que consta das referidas avaliações de risco, medidas essas que serão subsequentemente exigidas ao abrigo da nova Diretiva REC.

(13) No âmbito da execução do plano de cinco pontos anunciado pela Comissão, é necessário coordenar o trabalho reunindo peritos nacionais em antecipação da criação do Grupo para a Resiliência das Entidades Críticas pela nova Diretiva REC, a fim de permitir a cooperação entre os Estados-Membros e o intercâmbio de informações no

[16] COM(2022) 211.

que diz respeito à resiliência das entidades que exploram infraestruturas críticas. Tal deve incluir a cooperação e o intercâmbio de informações sobre atividades como a identificação das entidades e infraestruturas críticas, a preparação do desenvolvimento e da promoção de um conjunto comum de princípios para a realização de testes de esforço, a recolha de ensinamentos comuns dos testes de esforço e a identificação das vulnerabilidades e das possíveis capacidades. Estes processos também devem beneficiar a resiliência das entidades que exploram infraestruturas críticas face aos riscos climáticos e ambientais. Esta ação permitirá igualmente estabelecer prioridades comuns para os trabalhos relativos aos testes de esforço, com destaque para os setores da energia, das infraestruturas digitais, dos transportes e do espaço. A Comissão já começou a reunir os peritos e a atuar como facilitadora do seu trabalho, fazendo tenções de prosseguir esta linha de ação. Após a entrada em vigor da Diretiva REC e uma vez criado o Grupo para a Resiliência das Entidades Críticas, cabe a este grupo dar continuidade ao trabalho antecipatório desenvolvido em conformidade com as funções que lhe foram atribuídas ao abrigo da referida diretiva.

(14) Importa complementar o exercício dos testes de esforço com a elaboração de um plano de resposta a incidentes e crises em infraestruturas críticas que descreva e defina os objetivos e as modalidades de cooperação entre os Estados-Membros e as instituições, órgãos, organismos e agências da UE na resposta a incidentes contra infraestruturas críticas, em particular quando estes implicarem perturbações significativas na prestação de serviços essenciais para o mercado interno. Este plano deverá utilizar as disposições atuais do Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) para a coordenação da resposta, funcionar de forma coerente e complementar com o plano de resposta a ciberincidentes de grande escala e prever um acordo sobre as principais mensagens a comunicar ao público, uma vez que a comunicação em caso de crise desempenha um papel importante na atenuação dos efeitos negativos dos incidentes e crises nas infraestruturas críticas.

(15) A fim de assegurar uma resposta coordenada e eficaz às ameaças atuais e previstas, a Comissão prestará apoio adicional aos Estados-Membros tendo em vista o reforço da resiliência à luz dessas ameaças, nomeadamente fornecendo informações pertinentes sob a forma de notas de informação, manuais e orientações, promovendo a adoção de projetos de investigação e inovação financiados pela União, tomando as medidas de antecipação necessárias e otimizando a utilização dos meios de vigilância da União. O SEAE, em especial através do Centro de Situação e de Informações da UE, deve fornecer avaliações das ameaças.

(16) As agências setoriais da União e outros organismos pertinentes também deverão prestar apoio em questões relacionadas com a resiliência, na medida em que os respetivos mandatos, estabelecidos em conformidade com os devidos instrumentos do direito da União, o permitam. Em particular, a Agência Europeia para a Cibersegurança (ENISA) poderá prestar assistência em matéria de cibersegurança; a Agência Europeia da Segurança Marítima (EMSA) poderá contribuir com os seus conhecimentos especializados para apoiar os Estados-Membros, através do seu serviço de vigilância marítima, em questões relacionadas com a segurança e a proteção marítimas; a Agência da União Europeia para a Cooperação Policial (Europol) poderá prestar apoio em matéria de recolha de informações e de realização de investigações no âmbito de ações coercivas de cariz transfronteiriço; e 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.

(17) Se a responsabilidade pela proteção dos cidadãos recai primariamente sobre os Estados-Membros, impõe-se, não obstante, um reforço da coordenação a nível da União, mormente à luz das ameaças que podem ter impacto em vários Estados-Membros ao mesmo tempo, como é o caso da guerra de agressão da Rússia contra a Ucrânia, ou que podem afetar a resiliência e o bom funcionamento da economia, do mercado único e das sociedades da União.

(18) A presente recomendação não implica o fornecimento de informações cuja divulgação seria contrária aos interesses essenciais dos Estados-Membros em matéria de segurança nacional, segurança pública ou defesa.

(19) Com a crescente interdependência das infraestruturas físicas e digitais, as ciberatividades maliciosas que visam áreas críticas podem causar perturbações ou danos nas infraestruturas físicas, ao mesmo tempo que a sabotagem das infraestruturas físicas pode tornar os serviços digitais inacessíveis. Atendendo à ameaça crescente constituída pelos ataques híbridos sofisticados, os Estados-Membros também deveriam integrar essa questão no seu trabalho de aplicação da presente recomendação. Tendo em conta as interligações entre a cibersegurança e a segurança física dos operadores, é importante que os trabalhos de preparação para a transposição e a aplicação da nova Diretiva SRI 2 tenham início o mais rapidamente possível e que o trabalho correspondente ao abrigo da nova Diretiva REC também progrida em paralelo.

(20) Para além de melhorar a preparação, é igualmente importante reforçar as capacidades de resposta rápida e eficaz no caso de se concretizarem os riscos de perturbações da prestação de serviços essenciais assegurados por entidades que exploram infraestruturas críticas. Por conseguinte, a presente recomendação deverá prever as medidas a tomar tanto a nível dos Estados-Membros como a nível da União, incluindo o reforço da cooperação e do intercâmbio de informações no contexto do Mecanismo de Proteção Civil da União e a utilização dos meios pertinentes do Programa Espacial da União.

(21) Na sequência do convite do Conselho, nas suas Conclusões sobre a postura de cibersegurança da UE[17], a Comissão, o alto representante da União para os Negócios Estrangeiros e a Política de Segurança («alto representante») e o grupo de cooperação criado pela Diretiva (UE) 2016/1148 («grupo de cooperação SRI»), em coordenação com os organismos e agências civis e militares competentes e com as redes estabelecidas, incluindo a EU CyCLONe, estão a realizar uma avaliação do risco e a criar cenários de risco numa perspetiva de cibersegurança em caso de ameaça ou de potencial ataque contra Estados-Membros ou países parceiros. Este exercício centrar-se-á em setores críticos como a energia, as infraestruturas digitais, os transportes e o espaço.

(22) No apelo ministerial conjunto proferido em Nevers[18] e nas conclusões do Conselho sobre a postura de cibersegurança da UE também se exortou ao reforço da resiliência das infraestruturas e redes de comunicações da União, formulando recomendações aos Estados-Membros e à Comissão, com base numa avaliação do risco. Esta avaliação do risco está atualmente a ser realizada pelo grupo de cooperação SRI, com o apoio da Comissão e da ENISA, e em cooperação com o Organismo dos Reguladores Europeus

[17] Postura de cibersegurança:Conselho aprova conclusões [em inglês] — Consilium (europa.eu)

[18] https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

das Comunicações Eletrónicas (ORECE). A avaliação do risco e a análise das lacunas debruçam-se sobre os riscos de ciberataques para os vários subsetores das infraestruturas de comunicações, incluindo as infraestruturas fixas e móveis, os satélites, os cabos submarinos, os serviços de encaminhamento da Internet, etc., proporcionando assim uma base para o trabalho no âmbito da presente recomendação. Esta avaliação do risco contribuirá para a avaliação transetorial dos riscos cibernéticos, atualmente em curso, e para os cenários solicitados pelo Conselho nas conclusões do Conselho de 23 de maio de 2022.

(23) Ambos os exercícios serão coerentes e coordenados com o exercício relativo a cenários centrados na proteção civil no contexto de uma vasta gama de catástrofes naturais e de origem humana, incluindo eventos de cibersegurança e o seu impacto na vida real, atualmente em curso de elaboração pela Comissão e pelos Estados-Membros ao abrigo da Decisão n.º 1313/2013/UE do Parlamento Europeu e do Conselho[19]. Por razões de eficiência, eficácia e coerência, há que aplicar a presente recomendação tendo em conta os resultados desses exercícios.

(24) O conjunto de instrumentos da UE para a cibersegurança das redes 5G[20] estabelece medidas e planos de atenuação para reforçar a segurança das redes 5G. Tendo em conta a dependência de muitos serviços essenciais das redes 5G e a natureza interligada dos ecossistemas digitais, é essencial que todos os Estados-Membros concretizem urgentemente a aplicação das medidas recomendadas no conjunto de instrumentos e, em particular, que apliquem as restrições pertinentes aos fornecedores de alto risco no que respeita a ativos essenciais definidos como críticos e sensíveis na avaliação coordenada do risco a nível da UE.

(25) A fim de reforçar a título imediato a preparação e as capacidades de resposta a ciberincidentes graves, a Comissão criou um programa de curto prazo para apoiar os Estados-Membros, mediante o financiamento adicional afetado à ENISA. Os serviços abrangidos incluirão ações de preparação, como testes de penetração de entidades críticas para identificar vulnerabilidades. Reforçará igualmente as possibilidades de assistência aos Estados-Membros em caso de incidentes graves que afetem entidades críticas. Trata-se de um primeiro passo em consonância com as conclusões do Conselho sobre a postura de cibersegurança, 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.

(26) A rede mundial de dados submarinos e de comunicações eletrónicas por cabo é essencial para a conectividade mundial e intra-UE. Devido ao comprimento significativo dos cabos e à sua instalação no solo oceânico, é extremamente difícil efetuar a monitorização visual subaquática da maioria das secções de cabos. A competência partilhada e outras questões jurisdicionais relacionadas com estes cabos constituem um caso particular 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. A Comissão

---

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

realizará, pois, estudos para o efeito e partilhará os respetivos resultados com os Estados-Membros.

(27) Os setores prioritários identificados na presente recomendação no domínio da energia e dos transportes também podem ser afetados pelos riscos relacionados com as infraestruturas digitais — considere-se, por exemplo, o caso 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 operadas por entidades do setor da energia. Há que ter em conta essas circunstâncias ao tomar medidas para reforçar a resiliência das entidades que exploram infraestruturas críticas na União em conformidade com a presente recomendação.

(28) A importância crescente das infraestruturas espaciais e dos serviços espaciais para as atividades relacionadas com a segurança faz com que seja essencial assegurar a resiliência e a proteção dos recursos e dos serviços espaciais da União no território da UE, bem como, 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 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 serão de ter em conta ao aplicar a presente recomendação.

(29) A cooperação a nível internacional também é necessária para enfrentar com eficácia os riscos para a resiliência das entidades que exploram infraestruturas críticas tanto na União como nos países terceiros pertinentes e nas águas internacionais. Por conseguinte, importa incentivar a Comissão, o alto representante e os Estados-Membros a tomarem medidas nesse sentido, sendo implícito que estas têm de estar em conformidade com as respetivas atribuições e responsabilidades ao abrigo do direito da União, nomeadamente as disposições dos Tratados da UE em matéria de relações externas.

(30) Como estabelecido na comunicação intitulada «Contributo da Comissão para a defesa europeia»[21], 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[22], 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. Esta iniciativa deverá informar o trabalho realizado no âmbito da presente recomendação, ajudando a fortalecer a partilha de informações e a coordenação das ações, por forma a reforçar ulteriormente a resiliência, incluindo a das infraestruturas críticas.

(31) A Estratégia de Segurança Marítima da UE de 2014 e o respetivo plano de ação apelavam para 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 da sensibilização marítima através da melhoria da interoperabilidade e da racionalização do intercâmbio de informações (tanto obrigatório como voluntário). A estratégia e o plano de ação estão atualmente em curso de atualização e incluirão ações reforçadas destinadas a

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

22 Conselho da União Europeia, doc. n.º 7371/22 de 21 de março de 2022:

proteger as infraestruturas marítimas críticas. Essas ações deverão informar e complementar a presente recomendação.

(32) Os Estados-Membros deverão ter em conta o pleno potencial do programa de investigação da União em matéria de segurança, designadamente tirando partido da sua prioridade específica em matéria de infraestruturas críticas, em particular ao abrigo dos programas financiados pelo Fundo para a Segurança Interna, bem como de outras oportunidades potenciais de financiamento a nível da União, como o Fundo Europeu de Desenvolvimento Regional, na medida em que as medidas específicas cumpram os seus requisitos de elegibilidade. O plano REPowerEU também poderá oferecer possibilidades de financiamento da resiliência. O aproveitamento das oportunidades oferecidas pelo financiamento da União deve sempre realizar-se em conformidade com os requisitos legais aplicáveis,

ADOTOU A PRESENTE RECOMENDAÇÃO:

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

(1) A presente recomendação 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.

(2) As medidas estabelecidas na presente recomendação dizem respeito às infraestruturas que um dado Estado-Membro designou como infraestruturas críticas, incluindo como infraestruturas críticas europeias.

(3) Na aplicação da presente recomendação, importa dar prioridade ao reforço da resiliência das entidades que operam nos setores da energia, das infraestruturas digitais, dos transportes e do espaço, bem como das infraestruturas críticas exploradas por essas entidades com impacto transfronteiriço, no que diz respeito aos riscos de origem humana.

CAPÍTULO II: PREPARAÇÃO REFORÇADA

Ações a nível dos Estados-Membros

(4) Os Estados-Membros são incentivados a efetuar ou a atualizar as avaliações do risco relativas à resiliência das entidades que exploram as infraestruturas críticas europeias designadas nos setores dos transportes e da energia ao abrigo da Diretiva 2008/114/CE e a prosseguir a cooperação entre si no que respeita a essas avaliações de risco e às medidas de reforço da resiliência daí resultantes, conforme adequado e em conformidade com a referida diretiva.

(5) A fim de alcançar um elevado nível de resiliência das entidades que exploram infraestruturas críticas, os Estados-Membros devem acelerar os trabalhos preparatórios para transpor e aplicar, logo que possível, a nova Diretiva REC, adotando para tal as seguintes medidas:

(a) Acelerar a adoção ou a atualização das estratégias nacionais para reforçar a resiliência das entidades que exploram infraestruturas críticas com vista a dar resposta às ameaças atuais, comunicando os elementos relevantes dessas estratégias à Comissão;

(b) Realizar ou atualizar avaliações do risco em consonância com a natureza evolutiva das ameaças atuais, no que diz respeito à resiliência das entidades que exploram infraestruturas críticas em setores pertinentes para além da energia, das infraestruturas digitais, dos transportes e do espaço e, sempre que possível, nos setores abrangidos pela nova Diretiva REC, a saber, os serviços bancários, as infraestruturas do mercado financeiro, as infraestruturas digitais, a saúde, a água potável, as águas residuais, a administração pública, o espaço e a produção, transformação e distribuição de produtos alimentares, tendo presente a potencial natureza híbrida das ameaças relevantes, incluindo os efeitos em cascata e os efeitos das alterações climáticas;

(c) Informar a Comissão dos tipos de riscos identificados por setor e subsetor e dos resultados das avaliações do risco, o que é exequível com recurso a um modelo comum de comunicação de informações elaborado pela Comissão em cooperação com os Estados-Membros;

(d) Acelerar o processo de identificação e designação das entidades críticas, conferindo prioridade às entidades críticas que:

(a) Utilizam infraestruturas críticas fisicamente ligadas entre dois ou mais Estados-Membros;

(b) Pertencem a estruturas empresariais que estão ligadas ou conectadas a entidades críticas de outros Estados-Membros;

(c) Foram identificadas como tal num Estado-Membro e prestam serviços essenciais em seis ou mais Estados-Membros, revestindo, por isso, particular importância europeia, cabendo informar a Comissão em conformidade;

(d) Cooperar entre si, em particular no que diz respeito às entidades críticas, aos serviços essenciais e às infraestruturas críticas com impacto transfronteiriço, nomeadamente efetuando consultas entre si para efeitos do ponto 5, alínea d), e informando-se mutuamente em caso de incidentes com um efeito perturbador de caráter transfronteiriço significativo ou potencialmente significativo, mantendo a Comissão informada na medida do necessário;

(e) Reforçar o apoio às entidades críticas designadas a fim de melhorar a sua resiliência, o que pode passar pela disponibilização de materiais de orientação e metodologias, pela organização de exercícios para testar a sua resiliência e pela prestação de aconselhamento e formação ao pessoal, bem como pela realização de verificações dos antecedentes das pessoas que desempenham funções sensíveis, em conformidade com a legislação nacional e da União, no quadro das medidas de gestão da segurança dos trabalhadores adotadas pelas entidades críticas;

(f) Acelerar a designação ou a criação de um ponto de contacto único na autoridade competente com funções de ligação a fim de assegurar a cooperação transfronteiriça relacionada com a resiliência das entidades que exploram infraestruturas críticas entre os pontos de contacto único de outros Estados-Membros;

(6) Os Estados-Membros são incentivados a realizar testes de esforço às entidades que exploram infraestruturas críticas, pondo uma tónica especial em fazer avançar o grau de preparação dos Estados-Membros e das entidades em causa no setor da energia, e levar a cabo testes de esforço neste setor, sempre que possível de acordo com os princípios acordados de comum acordo a nível da União e numa base voluntária, assegurando simultaneamente uma comunicação eficaz com as entidades em causa. Quando necessário, poder-se-á considerar a possibilidade de realizar, numa fase

posterior, testes de esforço noutros setores prioritários, nomeadamente nas infraestruturas digitais, nos transportes e no espaço, tomando em devida conta as inspeções nos subsetores aéreo e marítimo nos termos do direito da União, bem como as disposições pertinentes da legislação setorial.

(7) Os Estados-Membros são incentivados a cooperar, quando apropriado e em conformidade com o direito da União, com os países terceiros pertinentes no que diz respeito à resiliência das entidades que exploram infraestruturas críticas com impacto transfronteiriço.

(8) Os Estados-Membros são incentivados a tirar partido, em conformidade com os requisitos aplicáveis, das potenciais oportunidades de financiamento a nível da União e a nível nacional para reforçar a resiliência das entidades que exploram infraestruturas críticas na União, incluindo, por exemplo, ao longo das redes transeuropeias, por exemplo, contra a gama completa de ameaças significativas, nomeadamente ao abrigo dos programas financiados pelo Fundo para a Segurança Interna e pelo Fundo Europeu de Desenvolvimento Regional, sob reserva do cumprimento dos respetivos critérios de elegibilidade, bem como pelo Mecanismo Interligar a Europa, incluindo disposições em matéria de resistência às alterações climáticas. O financiamento do Mecanismo de Proteção Civil da União também pode ser utilizado para esse efeito, em conformidade com os requisitos aplicáveis, em particular para projetos relacionados com avaliações do risco, planos ou estudos de investimento, o reforço de capacidades ou a melhoria da base de conhecimentos. O plano REPowerEU também poderá oferecer possibilidades de financiamento da resiliência.

(9) No que diz respeito às infraestruturas de comunicações e redes da União, o grupo de cooperação SRI deverá, agindo em conformidade com o artigo 11.º da Diretiva (UE) 2016/1148 e com o artigo 14.º da Diretiva SRI 2, acelerar os trabalhos em curso para uma avaliação específica dos riscos e apresentar as primeiras recomendações no início de 2023. Esse trabalho deve 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, como o Grupo para a Resiliência das Entidades Críticas, a criar ao abrigo da nova Diretiva REC, e o Fórum de Fiscalização, a criar ao abrigo do novo Regulamento Resiliência Operacional Digital (DORA)[23].

(10) O grupo de cooperação SRI, que deve desempenhar as suas funções em conformidade com o artigo 11.º da Diretiva (UE) 2016/1148 e o artigo 14.º da Diretiva SRI 2, é convidado, com o apoio da Comissão e da ENISA, a dar prioridade ao seu trabalho sobre a segurança das infraestruturas digitais e dos setores espaciais, nomeadamente através da elaboração de orientações políticas e de metodologias e medidas de gestão dos riscos de cibersegurança com base numa abordagem que abrange todos os perigos em relação aos cabos de comunicações submarinos, em antecipação da entrada em vigor da Diretiva SRI 2, bem como a privilegiar o desenvolvimento de orientações para medidas de gestão dos riscos de cibersegurança destinadas aos operadores do setor espacial, com vista a aumentar a resiliência das infraestruturas terrestres que apoiam a prestação de serviços espaciais.

[23] COM(2020) 595 final.

(11) Os Estados-Membros devem utilizar plenamente os serviços de preparação para a cibersegurança oferecidos no âmbito do programa de apoio a curto prazo da Comissão aplicado com a ENISA, designadamente 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) É urgente que os Estados-Membros concretizem a aplicação das medidas recomendadas no conjunto de instrumentos da UE para a cibersegurança das redes 5G[24]. Os Estados-Membros que ainda não adotaram restrições em relação aos fornecedores de alto risco devem fazê-lo sem demora, uma vez que o tempo perdido pode agravar a vulnerabilidade das redes na União. Devem igualmente reforçar 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, incluindo requisitos juridicamente vinculativos a nível da União, a fim de assegurar um nível coerente de segurança e resiliência das redes 5G.

(13) Os Estados-Membros devem aplicar o mais rapidamente possível o futuro código de rede para os aspetos de cibersegurança dos fluxos transfronteiriços de eletricidade, com base na experiência adquirida com a aplicação da Diretiva SRI 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.

(14) Os Estados-Membros deverão desenvolver a utilização do Galileo e/ou do Copernicus para fins de vigilância e partilhar informações no âmbito do 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 resposta a situações de crise.

Ações a nível da União

(15) A Comissão pretende reforçar a cooperação entre os peritos dos Estados-Membros com vista a ajudar a reforçar a resiliência física não cibernética das entidades que exploram infraestruturas críticas na União, para tal tencionando:

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

(b) Apoiar a elaboração, pelos Estados-Membros, de princípios comuns sobre a realização dos testes de esforço a que se refere o ponto 6, começando pelos testes centrados nos riscos de origem humana no setor da energia e, subsequentemente, noutros setores-chave, como as infraestruturas digitais, os transportes e o espaço; dar resposta a outros riscos e perigos significativos, bem como, quando pertinente, prestar apoio e aconselhamento no tocante à realização desses testes de esforço;

(c) Proporcionar uma plataforma segura para recolher, fazer o balanço e partilhar as boas práticas, os ensinamentos retirados das experiências nacionais e outras informações relacionadas com essa resiliência, inclusive no tocante à realização desses testes de

[24] 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

esforço e à tradução dos respetivos resultados em protocolos e planos de contingência.

O trabalho desses peritos deve ter em particular atenção as dependências transetoriais e as entidades que exploram infraestruturas críticas com impacto transfronteiriço; o Grupo para a Resiliência das Entidades Críticas, uma vez criado, deverá dar-lhe continuidade.

(16) Os Estados-Membros deverão participar plenamente na cooperação reforçada a que se refere o ponto 15, inclusive mediante a designação de pontos de contacto com os conhecimentos especializados pertinentes e a partilha de experiências sobre as metodologias utilizadas para os testes de esforço e os protocolos e os planos de contingência elaborados com base nos mesmos. O intercâmbio de informações deve preservar a confidencialidade dessas informações e salvaguardar a segurança e os interesses comerciais das entidades críticas, respeitando em simultâneo a segurança dos Estados-Membros. Tal não implica o fornecimento de informações cuja divulgação seja contrária aos interesses essenciais dos Estados-Membros em matéria de segurança nacional, segurança pública ou defesa.

(17) A Comissão apoiará os Estados-Membros fornecendo manuais e orientações, incluindo a elaboração de 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, é convidado a realizar sessões de informação sobre as ameaças às infraestruturas críticas na UE, a fim de melhorar o conhecimento da situação.

(18) A Comissão apoiará a aceitação dos resultados dos projetos sobre a resiliência das entidades que exploram infraestruturas críticas financiadas ao abrigo dos programas de investigação e inovação da União. É sua intenção aumentar o financiamento dessa resiliência no âmbito do orçamento afetado ao Horizonte Europa ao abrigo do quadro financeiro plurianual 2021-2027. Tal deverá permitir dar resposta aos desafios atuais e futuros neste domínio, como a resistência das infraestruturas críticas às alterações climáticas, sem prejuízo do financiamento de outros fundos de investigação e inovação relacionados com a segurança civil ao abrigo do Horizonte Europa. A Comissão também redobrará esforços para divulgar os resultados dos projetos de investigação pertinentes financiados pela União.

(19) O grupo de cooperação SRI, em cooperação com a Comissão e o alto representante, é convidado 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 civis e militares pertinentes na realização da avaliação do risco e na construção de cenários de risco cibernético, com uma incidência inicial nas infraestruturas da energia, das comunicações, dos transportes e do espaço, bem como nas interdependências intersetoriais e entre os Estados-Membros. Este exercício deverá ter em conta os riscos conexos para as infraestruturas físicas de que estes setores dependem. Importa realizar as avaliações e os cenários de risco com regularidade, assegurando que complementam e se baseiam nas avaliações de risco existentes ou previstas nestes setores sem incorrer em duplicações, e que contribuem para os debates sobre o modo de reforçar a resiliência global das entidades que exploram infraestruturas críticas na União e de colmatar as vulnerabilidades.

(20) A Comissão acelerará as suas atividades de apoio à preparação dos Estados-Membros e à resposta aos incidentes de cibersegurança de grande escala, tencionando nomeadamente:

(a) Realizar, em complemento das avaliações de risco pertinentes no contexto da segurança das redes e da informação, um estudo exaustivo que faça um balanço da infraestrutura de cabos elétricos submarinos que liga os Estados-Membros e que liga a Europa a nível mundial, incluindo um levantamento das suas capacidades e redundâncias, vulnerabilidades, riscos para a disponibilidade de serviços e medidas de atenuação dos riscos. Os resultados do estudo deverão ser partilhados com os Estados-Membros;

(b) Apoiar a preparação dos Estados-Membros e das instituições, organismos e agências da UE para responder a incidentes graves de cibersegurança.

(21) A Comissão intensificará o trabalho sobre as medidas antecipativas prospetivas, nomeadamente no âmbito do MPCU, em 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.

Em particular, fará o seguinte:

(a) Prosseguirá os trabalhos no Centro de Coordenação de Resposta de Emergência em matéria de antecipação e planeamento transetorial da prevenção, preparação e resposta, a fim de antecipar e preparar para eventuais perturbações da prestação de serviços essenciais assegurados por entidades que exploram infraestruturas críticas;

(b) Aumentará o investimento em abordagens preventivas e na preparação da população para a ocorrência de tais perturbações, com especial destaque para os agentes e explosivos químicos, biológicos, radiológicos e nucleares ou outras ameaças de origem humana emergentes;

(c) Reforçará o intercâmbio de conhecimentos e boas práticas pertinentes, bem como a conceção e a realização de atividades de desenvolvimento de capacidades, como cursos de formação e exercícios com as entidades que exploram as infraestruturas críticas, através das estruturas e dos conhecimentos especializados existentes, como a Rede Europeia de Conhecimentos sobre Proteção Civil;

(22) Fomentará a utilização dos meios de vigilância da UE (Copernicus e Galileo) 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.

(23) 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 entidades que exploram infraestruturas críticas, nomeadamente:

(a) A Europol, no que diz respeito à recolha de informações, à análise da criminalidade e ao apoio à investigação em ações coercivas de cariz transfronteiriço;

(b) A 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 EUSPA, no que diz respeito às atividades no âmbito do programa espacial da União;

(d) a ENISA, no que diz respeito às atividades relacionadas com a cibersegurança.

CAPÍTULO III: RESPOSTA REFORÇADA

Ações a nível dos Estados-Membros

(24) Os Estados-Membros deverão:

(a) Coordenar a resposta e manter a sua visão de conjunto da resposta transetorial a perturbações significativas da prestação de serviços essenciais assegurados pelas entidades que exploram infraestruturas críticas no quadro do mecanismo de crise do Conselho (Mecanismo Integrado da UE de Resposta Política a Situações de Crise — IPCR) 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 ou no enquadramento para uma resposta coordenada da UE às campanhas híbridas, no caso de uma campanha híbrida;

(b) Aumentar o intercâmbio de informações no âmbito do Mecanismo de Proteção Civil da União, a fim de reforçar o alerta rápido e coordenar a sua resposta no âmbito do mecanismo em caso de perturbações significativas, assegurando assim uma reação mais rápida viabilizada pela União, quando necessário;

(c) Aumentar a sua disponibilidade para responder, por meio do Mecanismo de Proteção Civil da União, a tais perturbações significativas, em particular nos casos em que estas sejam suscetíveis de ter implicações transfronteiriças ou mesmo pan-europeias significativas, bem como transetoriais;

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

(e) Incentivar as entidades que exploram infraestruturas críticas e as autoridades nacionais competentes a reforçarem a capacidade dessas entidades para restabelecer rapidamente um desempenho básico dos serviços essenciais prestados;

(f) Assegurar que, quando for necessário reconstruir infraestruturas críticas, estas sejam resilientes à gama completa de riscos significativos a que possam estar sujeitas, incluindo em cenários climáticos adversos.

(25) Os Estados-Membros são convidados a acelerar os trabalhos preparatórios para a transposição e a aplicação da Diretiva SRI 2, procedendo de imediato ao reforço das capacidades das respetivas Equipas de Resposta a Incidentes de Segurança Informática (CSIRT), tendo em conta as suas novas funções, bem como o número alargado de entidades de novos setores, atualizando rapidamente as suas estratégias de cibersegurança e adotando com a maior brevidade planos nacionais de resposta a incidentes e crises de cibersegurança.

Ações a nível da União

(26) A resposta a perturbações significativas na prestação de serviços essenciais assegurados por entidades que exploram infraestruturas críticas deve ser coordenada entre os peritos dos Estados-Membros no que diz respeito à resiliência dessas entidades e às respostas correspondentes, podendo o seu contributo especializado informar os trabalhos do mecanismo de crise do Conselho (IPCR).

(27) A Comissão trabalhará em estreita colaboração com os Estados-Membros para continuar a desenvolver capacidades mobilizáveis de resposta a emergências, incluindo peritos e reservas rescEU no âmbito do MPCU, com vista a melhorar a preparação operacional para fazer face aos efeitos imediatos e indiretos de perturbações significativas na prestação de serviços essenciais assegurados por entidades que exploram infraestruturas críticas.

(28) Tendo em conta a evolução do panorama do risco e em cooperação com os Estados-Membros, a Comissão irá, no contexto do MPCU:

(a) Analisar e testar continuamente a adequação e a prontidão operacional da capacidade de resposta existente;

(b) Analisar regularmente a necessidade eventual de desenvolver novas capacidades de resposta a nível da UE através do rescEU;

(c) Intensificar ulteriormente a colaboração transetorial para assegurar uma resposta adequada a nível da UE e organizar exercícios regulares para testar essa colaboração;

(d) Continuar a desenvolver o CCRE como a plataforma transetorial de crise a nível da UE para a coordenação do apoio aos Estados-Membros afetados.

(29) A Comissão, em estreita cooperação com o alto representante, em estreita consulta com os Estados-Membros e contando com o apoio das agências competentes da União, elaborará um plano de resposta a incidentes e crises em infraestruturas críticas que descreva e defina os objetivos e as modalidades de cooperação entre os Estados-Membros e as instituições, órgãos, organismos e agências da UE na resposta a incidentes contra infraestruturas críticas, em particular quando estes implicarem perturbações significativas na prestação de serviços essenciais para o mercado interno. Este plano deverá utilizar as disposições atuais do Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) para a coordenação da resposta.

(30) A Comissão trabalhará com as partes interessadas e os peritos sobre eventuais medidas de recuperação de incidentes que afetem as infraestruturas de cabos submarinos, a apresentar em conjunto com o balanço referido no ponto 20, alínea a), e na ótica de elaborar planos de contingência, cenários de risco e trabalhos sobre a resiliência da União a catástrofes no âmbito do Mecanismo de Proteção Civil da União.

CAPÍTULO IV: COOPERAÇÃO INTERNACIONAL

(31) A Comissão e o alto representante apoiarão, quando apropriado e em conformidade com as respetivas funções e responsabilidades ao abrigo do direito da União, os países parceiros no reforço da resiliência das entidades que exploram infraestruturas críticas no seu território.

(32) 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 através do diálogo estruturado UE-OTAN sobre a resiliência e criarão um grupo de trabalho para o efeito.

(33) 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 sobre um enquadramento para uma resposta coordenada da UE às campanhas híbridas[25], 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 ao considerar e ao elaborar respostas abrangentes e coordenadas da UE às campanhas híbridas e às ameaças híbridas, incluindo as que visam entidades que exploram infraestruturas críticas.

(34) A Comissão considerará a participação de representantes de países terceiros, sempre que pertinente e apropriado, no quadro da cooperação e do intercâmbio de informações entre os peritos dos Estados-Membros no domínio da resiliência das entidades que exploram infraestruturas críticas.

[…]

Feito em Estrasburgo, em

Pelo Conselho
O Presidente

25 Conclusões do Conselho sobre um enquadramento para uma resposta coordenada da UE às campanhas híbridas — Consilium (europa.eu)