COMISSÃO
EUROPEIA

Bruxelas, 29.1.2020
COM(2020) 50 final

COMUNICAÇÃO DA COMISSÃO AO PARLAMENTO EUROPEU, AO CONSELHO, AO COMITÉ ECONÓMICO E SOCIAL EUROPEU E AO COMITÉ DAS REGIÕES

Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da UE

1. Introdução

A quinta geração (5G) de redes de telecomunicações deverá desempenhar um papel fundamental no desenvolvimento da sociedade e da economia europeias. Espera-se que ofereça grandes oportunidades económicas e que constitua uma base importante para a transformação digital e ecológica em domínios como os transportes, a energia, a indústria transformadora, a saúde, a agricultura e os meios de comunicação social.

Por conseguinte, a tecnologia 5G terá potencial impacto em quase todos os aspetos da vida dos cidadãos da UE, sendo a cibersegurança das redes 5G essencial não só para proteger as nossas economias, sociedades e processos democráticos, mas também para assegurar uma transformação digital de confiança, em benefício de todos os cidadãos da UE.

Uma vez que muitos serviços críticos dependerão das redes 5G, as consequências de perturbações sistémicas e generalizadas seriam particularmente graves e, dada a natureza interligada dos ecossistemas digitais, poderiam ter impactos significativos para além das fronteiras nacionais. Consequentemente, garantir a cibersegurança das redes 5G é uma questão de importância estratégica para a União, numa altura em que os ciberataques estão a aumentar, estão mais sofisticados do que nunca e são levados a cabo por um vasto leque de perpetradores, nomeadamente países terceiros ou entidades apoiadas por Estados. No que respeita à segurança de infraestruturas críticas como as redes 5G, a estratégia escolhida consiste em definir, pela primeira vez, uma abordagem europeia comum. Esta abordagem respeita plenamente a abertura do mercado interno da UE, contanto que sejam cumpridos os requisitos de segurança da UE baseados no risco.

O Conselho Europeu de 22 de março de 2019 apelou à adoção de uma abordagem concertada da segurança das redes 5G. Em 26 de março de 2019, a Comissão adotou a Recomendação (UE) 2019/534 sobre a cibersegurança das redes 5G[1]. A recomendação instava os Estados-Membros a concluírem avaliações nacionais dos riscos, a reverem as medidas nacionais, a trabalharem em conjunto a nível da UE numa avaliação coordenada dos riscos e a prepararem um conjunto de possíveis medidas de atenuação. A presente comunicação é parte integrante da estratégia europeia global para o digital da Comissão, tal como solicitado pelo Conselho Europeu.

2. Implantação das redes 5G na UE

A implantação de infraestruturas de redes 5G na Europa é fundamental para a estratégia industrial e a competitividade europeias. A Comissão reconheceu a implantação das tecnologias das redes 5G como um importante elemento facilitador de futuros serviços digitais. Em 2016, a Comissão adotou o Plano de Ação 5G para garantir que a União disponha das infraestruturas de conectividade necessárias para a sua transformação digital a partir de 2020 e para uma implantação abrangente nas zonas urbanas e ao longo das principais vias de transporte até 2025[2]. A comunicação sobre a sociedade a gigabits estabelece a ambição de

[1] Recomendação (UE) 2019/534 sobre a cibersegurança das redes 5G (JO L 88 de 29.3.2019, p. 42).
[2] COM(2016) 588 de 14 de setembro de 2016, intitulada «5G para a Europa: um Plano de Ação».

assegurar o acesso à conectividade de dados móveis em toda a parte[3], incluindo nas zonas rurais e periféricas.

No que diz respeito à atribuição de frequências, os Estados-Membros atribuíram 16 % das faixas pioneiras 5G[4]. Tendo em conta a obrigação legal de permitir a utilização de todas as faixas pioneiras 5G até ao final do ano, deverão ser realizadas consultas relativas a uma série de procedimentos de atribuição nos próximos meses.

A Europa é uma das regiões mais avançadas do mundo no que respeita ao lançamento comercial de serviços 5G[5]. Atualmente, prevê-se que os primeiros serviços 5G estejam disponíveis em 138 cidades europeias até ao final de 2020. As primeiras redes 5G baseiam-se na atual quarta geração (4G) de tecnologias de rede e os serviços 5G são principalmente prestados ao público em geral, seja como uma melhoria da 4G em termos de capacidade e de velocidade, seja como uma alternativa, sem fios e eficaz em termos de custos, às redes fixas[6].

No que se refere às oportunidades oferecidas no domínio dos novos serviços entre empresas, nomeadamente nos setores energético, alimentar e agrícola, dos cuidados de saúde, da indústria transformadora ou dos transportes, a Europa está bastante avançada, contando com um investimento da ordem dos 1 000 milhões de EUR, incluindo 300 milhões de EUR de financiamento da UE afetados no âmbito da parceria público-privada 5G ao abrigo do programa Horizonte 2020. Este investimento inclui mais de 160 ensaios em grande escala de 5G identificados na Europa, incluindo dez corredores rodoviários transfronteiriços para a realização de ensaios em grande escala de serviços de mobilidade conectada e automatizada baseados na tecnologia 5G. Os ensaios incluem aplicações baseadas na tecnologia 5G em domínios que vão da prestação de cuidados de saúde sustentáveis à mobilidade automatizada, passando pela agricultura eficiente em termos de recursos, as redes elétricas inteligentes e a Indústria 4.0. Além disso, o BEI, com o apoio do Fundo Europeu para Investimentos Estratégicos, concedeu empréstimos para acelerar a investigação e o desenvolvimento da tecnologia 5G.

O Código Europeu das Comunicações Eletrónicas[7], aplicável a partir de 21 de dezembro de 2020, constitui uma base importante para criar um ambiente favorável ao investimento para as redes 5G e não só. Além disso, os programas de financiamento público, como o Mecanismo Interligar a Europa[8] ou os fundos europeus estruturais e de investimento, também serão essenciais para apoiar a futura implantação de redes 5G, nomeadamente através da ligação das comunidades a serviços baseados na tecnologia 5G, como escolas, hospitais, municípios e administrações locais.

[3] COM(2016) 587, intitulada «Conectividade para um Mercado Único Digital Concorrencial – Rumo a uma Sociedade Europeia a Gigabits».

[4] http://www.5GObservatory.eu.

[5] http://www.5GObservatory.eu

[6] Algumas das novas funcionalidades das redes 5G serão introduzidas segundo uma abordagem faseada. Numa primeira fase (a curto ou muito curto prazo), a implantação da tecnologia 5G consistirá principalmente em redes «não autónomas» – em que apenas a rede de acesso via rádio é atualizada para 5G, continuando, em tudo o mais, a depender de redes principais 4G existentes –, que proporcionarão desempenhos em banda larga móvel melhorados aos utilizadores finais. Com o tempo, durante as fases subsequentes (curto/médio a longo prazo), a implantação de redes 5G «autónomas», incluindo funções da rede principal 5G, exigirá e resultará numa alteração muito mais profunda da arquitetura da rede.

[7] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho que estabelece o Código Europeu das Comunicações Eletrónicas (reformulação).

[8] Proposta de regulamento do Parlamento Europeu e do Conselho, de 6 de junho de 2018, que cria o Mecanismo Interligar a Europa e revoga os Regulamentos (UE) n.º 1316/2013 e (UE) n.º 283/2014, (COM(2018) 438).

Tendo em conta as oportunidades estratégicas na Europa no domínio dos serviços 5G para vários setores, será extremamente importante que os operadores e prestadores de serviços invistam em soluções avançadas de redes e de serviços 5G. Estas necessitarão não só de novas redes de rádio 5G, mas também de novas redes principais «autónomas» 5G, a fim de oferecer funcionalidades 5G avançadas, como a divisão da rede[9] e a computação de proximidade[10].

A Comissão continuará a promover plenamente uma implantação bem-sucedida da tecnologia 5G na UE, nomeadamente através de uma colaboração com os Estados-Membros e as partes interessadas no sentido de aproveitar as oportunidades oferecidas pelas redes 5G. Os aspetos sanitários relevantes serão devidamente considerados, com base no princípio da precaução[11], em cooperação com as organizações internacionais pertinentes e a comunidade científica.

3. Avaliação coordenada dos riscos em matéria de cibersegurança das redes 5G na UE

Trabalhando coletivamente no âmbito do grupo de cooperação SRI[12], todos os Estados-Membros concluíram as respetivas avaliações nacionais dos riscos das suas próprias infraestruturas de redes 5G e transmitiram os resultados à Comissão e à ENISA, a Agência da União Europeia para a Cibersegurança, no início de julho de 2019.

Com base nestas avaliações nacionais dos riscos, em 9 de outubro de 2019, o grupo de cooperação SRI, composto por representantes dos Estados-Membros, da Comissão e da ENISA, publicou um relatório sobre a avaliação coordenada dos riscos em matéria de cibersegurança das redes 5G na UE[13]. Este relatório identifica as principais ameaças e perpetradores, os ativos mais sensíveis e as principais vulnerabilidades (técnicas e outras) que afetam as redes 5G. Nesta base, o relatório identificou também uma série de categorias de risco de importância estratégica na perspetiva da UE, ilustradas por cenários de risco concretos, que refletem combinações pertinentes dos diferentes parâmetros (vulnerabilidades, ameaças e perpetradores) para os diferentes ativos (ver apêndice).

A fim de complementar o referido relatório e como contributo suplementar para o conjunto de instrumentos, a ENISA realizou um levantamento do panorama de ameaças específicas[14], que consiste numa análise pormenorizada de determinados aspetos técnicos, nomeadamente na identificação dos ativos da rede e das ameaças que sobre eles pendem.

O relatório sobre a avaliação coordenada dos riscos na UE destaca uma série de aspetos importantes para as redes 5G. Mais especificamente:

---

[9] A divisão da rede 5G permite um elevado grau de separação entre as diferentes camadas de serviço (*service layers*) na mesma rede física, aumentando assim as possibilidades de oferta de serviços diferenciados em toda a rede.

[10] A computação de proximidade (*edge computing*) é um paradigma de computação distribuída que aproxima a computação e o armazenamento de dados do local onde são necessários, a fim de melhorar os tempos de resposta e de economizar largura de banda.

[11] Recomendação 1999/519/CE do Conselho, de 12 de julho de 1999, relativa à limitação da exposição da população aos campos eletromagnéticos (0 Hz – 300 GHz).

[12] 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 (Diretiva SRI). O grupo de cooperação SRI foi criado pela Diretiva SRI para assegurar a cooperação estratégica e o intercâmbio de informações sobre cibersegurança entre os Estados-Membros da UE.

[13] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[14] *ENISA Threat landscape for 5G networks*: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks.

a) As mudanças tecnológicas introduzidas pela tecnologia 5G aumentarão a superfície de ataque global e o número de potenciais pontos de entrada para atacantes:

– devido a uma melhor funcionalidade na margem da rede e a uma arquitetura menos centralizada do que nas anteriores gerações de redes móveis, algumas funções das redes principais podem ser integradas noutras partes das redes, o que torna os equipamentos correspondentes mais sensíveis (por exemplo, estações de base ou funções MANO),

– a maior parte do software *dos equipamentos 5G acarreta um aumento dos riscos relacionados com o desenvolvimento de* software *e com os processos de atualização, cria novos riscos de erros de configuração e confere um papel mais importante na análise da segurança às escolhas feitas por cada operador de rede móvel no decorrer da fase de implantação da rede.*

b) Estas novas características tecnológicas aumentarão a importância da dependência dos operadores de redes móveis em relação a fornecedores terceiros, bem como a importância do papel por estes desempenhado na cadeia de abastecimento 5G.

Por sua vez, tal aumentará o número de vias de ataque que podem ser exploradas pelos perpetradores, nomeadamente países terceiros ou entidades apoiadas por Estados, devido às suas capacidades (intenção e recursos) para a execução de ataques contra redes de telecomunicações dos Estados-Membros da UE, bem como a potencial gravidade do impacto desses ataques.

Neste contexto de exposição crescente a ataques facilitados por fornecedores terceiros, o perfil de risco individual dos fornecedores tornar-se-á particularmente importante, em especial quando um fornecedor tem uma presença significativa em determinadas redes ou zonas.

c) Uma forte dependência de um único fornecedor aumenta a exposição a uma potencial falha do mesmo, bem como as suas consequências. Além disso, agrava as potenciais consequências das deficiências ou vulnerabilidades e da sua possível exploração pelos perpetradores, em especial quando a dependência diz respeito a um fornecedor que apresenta um elevado grau de risco.

d) Se alguns dos novos casos de utilização previstos para as comunicações 5G se concretizarem, as redes 5G acabarão por representar uma parte importante da cadeia de abastecimento de muitas aplicações informáticas críticas. Nesse caso, não só os requisitos de confidencialidade e de privacidade serão afetados, como a integridade e a disponibilidade dessas redes se tornarão também questões prementes de segurança nacional e um importante desafio de segurança do ponto de vista da UE.

Fonte: Avaliação coordenada dos riscos na UE

O relatório sobre a avaliação coordenada dos riscos na UE conclui ainda que estes desafios criam um novo paradigma de segurança, exigindo uma reavaliação do atual quadro político e de segurança aplicável ao setor 5G e ao seu ecossistema e tornando imperativa a tomada das necessárias medidas de atenuação pelos Estados-Membros.

Para dar resposta aos riscos identificados de forma eficaz e reforçar a segurança e a resiliência das redes 5G, é necessária uma abordagem global, o que implica a adoção de um conjunto de medidas fundamentais, bem como ações de apoio conexas que cumpram simultaneamente o mesmo propósito. A avaliação coordenada dos riscos na UE serviu de base para identificar medidas de atenuação aplicáveis a nível nacional e europeu.

Nas suas conclusões de 3 de dezembro de 2019, o Conselho apoiou as conclusões da avaliação coordenada dos riscos e salientou que «importa seguir uma abordagem coordenada e aplicar efetivamente a recomendação, a fim de evitar fragmentações no mercado único»[15]. Para o efeito, o Conselho exortou os Estados-Membros, a Comissão e a ENISA a «no âmbito das suas competências […] tomarem todas as medidas necessárias para garantir a segurança e a integridade das redes de comunicações eletrónicas, em especial as redes 5G, e continuarem a seguir uma abordagem coordenada para fazer face aos desafios de segurança relacionados com as tecnologias 5G».

4. Conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G

Em 29 de janeiro de 2020, o grupo de cooperação SRI publicou o conjunto de medidas de atenuação dos riscos da UE[16], que aborda todos os riscos identificados no relatório sobre a avaliação coordenada dos riscos.

O conjunto de instrumentos da UE identifica e descreve um conjunto de medidas estratégicas e técnicas, bem como ações de apoio conexas destinadas a reforçar a sua eficácia, que podem ser aplicadas para atenuar os riscos identificados. As **medidas estratégicas** abrangem medidas relativas ao reforço dos poderes regulamentares das autoridades para examinar a adjudicação de contratos públicos e a implantação de redes, medidas específicas para fazer face aos riscos associados a vulnerabilidades não técnicas, bem como possíveis iniciativas para promover uma cadeia de abastecimento e de valor 5G sustentável e diversificada, a fim de evitar riscos de dependência sistémicos e a longo prazo. As **medidas técnicas** incluem medidas destinadas a reforçar a segurança das redes e dos equipamentos 5G, dando resposta aos riscos decorrentes de tecnologias, processos e fatores humanos e físicos. Além disso, o conjunto de instrumentos prevê, para cada uma das áreas de risco identificadas na avaliação coordenada dos riscos na UE, **planos de atenuação dos riscos** baseados nas medidas de maior eficácia.

Entre estas, as conclusões do conjunto de instrumentos da UE, aprovadas pelo grupo de cooperação SRI, recomendam um conjunto de **medidas fundamentais** a aplicar por todos os Estados-Membros e pela Comissão, do seguinte modo:

Conclusões do conjunto de instrumentos da UE

O conjunto de instrumentos da UE define uma série de medidas e ações que – se adequadamente combinadas e eficazmente aplicadas – constituem a base para uma abordagem coordenada neste domínio. Com efeito, atendendo ao vasto leque e à natureza diversificada das áreas de risco identificadas na avaliação coordenada dos riscos na UE, nenhum tipo de medida será suficiente se

[15] Conclusões do Conselho sobre a importância da tecnologia 5G para a economia europeia e a necessidade de atenuar os riscos de segurança a ela associados, 3 de dezembro de 2019, 14517/19. https://data.consilium.europa.eu/doc/document/ST-14517-2019-INIT/pt/pdf.

[16] *Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures*, 29 de janeiro de 2020. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group.

utilizado isoladamente. Em vez disso, será necessário utilizar uma combinação adequada de uma série de medidas, a fim de abordar todas as principais áreas de risco.

Com base na avaliação de possíveis planos de atenuação e na identificação das medidas de maior eficácia, este conjunto de instrumentos recomenda o seguinte:

1. Todos os Estados-Membros devem certificar-se de que dispõem de medidas (incluindo poderes conferidos às autoridades nacionais) para responder de forma adequada e proporcionada aos riscos atualmente identificados e aos riscos futuros, e, em especial, certificar-se de que são capazes de restringir, proibir e/ou impor condições ou requisitos específicos, segundo uma abordagem assente no risco, ao fornecimento, implantação e exploração de equipamento de rede 5G com base numa série de razões relacionadas com a segurança.

Devem, nomeadamente:

- *reforçar os **requisitos de segurança** para os operadores de redes móveis (por exemplo, controlos rigorosos de acesso, regras em matéria de segurança do funcionamento e da monitorização, limitação da externalização de funções específicas, etc.),*

- *avaliar o perfil de risco dos fornecedores e, consequentemente, **aplicar restrições adequadas aos fornecedores considerados de alto risco – incluindo exclusões necessárias para atenuar eficazmente os riscos – no que respeita a ativos essenciais** definidos como críticos e sensíveis na avaliação coordenada dos riscos na UE (por exemplo, funções de rede principal, funções de gestão e orquestração da rede e funções da rede de acesso),*

- *garantir que cada operador disponha de uma estratégia adequada de diversificação de fornecedores para **evitar ou limitar qualquer dependência significativa** de um único fornecedor (ou de fornecedores com um perfil de risco semelhante), assegurar um equilíbrio adequado entre fornecedores a nível nacional e **evitar a dependência de fornecedores considerados de alto risco**; para tal, é também necessário evitar situações de dependência absoluta de um único fornecedor, incluindo mediante a promoção de uma maior interoperabilidade dos equipamentos.*

2. A Comissão Europeia, juntamente com os Estados-Membros, deverá contribuir para:

- *manter uma **cadeia de abastecimento 5G diversificada e sustentável**, a fim de evitar a dependência a longo prazo, devendo para tal:*

  - *utilizar plenamente os instrumentos e as ferramentas da UE existentes, em especial para analisar potenciais **investimentos diretos estrangeiros** (IDE) que afetem os principais ativos 5G e evitar **distorções** no mercado de abastecimento de 5G decorrentes de potenciais práticas de* dumping *ou de concessão de subvenções, e*

  - *continuar a reforçar as **capacidades da UE nas tecnologias 5G e pós-5G**, recorrendo a programas e financiamentos pertinentes da UE,*

- *facilitar a coordenação entre os Estados-Membros no que diz respeito à **normalização**, a fim de alcançar objetivos de segurança específicos, e desenvolver **sistema(s) de certificação pertinentes a nível da UE**, de modo a promover produtos e processos mais seguros.*

3. Para garantir que esta abordagem coordenada resiste à passagem do tempo, importa alargar o mandato do grupo de cooperação SRI nesta vertente de trabalho, assim como a cooperação com outros organismos e entidades pertinentes, a fim de, nomeadamente:

- *rever periodicamente – com o apoio da Comissão e da ENISA – as **avaliações dos riscos nacionais e a nível da UE** sobre a segurança das redes 5G e pós-5G, aprofundar e alinhar a metodologia de avaliação seguida e adaptar-se à evolução da tecnologia 5G,*

- *realizar **monitorizações e avaliações** exaustivas e regulares **da aplicação** do conjunto de instrumentos, com base em relatórios estruturados dos Estados-Membros,*

- *coordenar e apoiar a execução de **ações de apoio** que exijam cooperação a nível da UE, em especial no que se refere à elaboração de orientações e ao intercâmbio de boas práticas sobre as várias medidas,*

- *apoiar o prosseguimento de uma eventual coordenação a nível da UE, se for caso disso, nomeadamente para promover uma maior convergência **no que diz respeito aos requisitos técnicos e organizativos de segurança aplicáveis aos operadores de rede**.*

Fonte: Conjunto de instrumentos da UE.

As conclusões do conjunto de instrumentos demonstram que existe uma forte determinação dos Estados-Membros em responder coletivamente aos desafios de segurança das redes 5G. Trata-se de um aspeto crucial para a segurança nos Estados-Membros e em toda a UE, para as economias nacionais, bem como para o mercado interno da UE e para a soberania tecnológica da Europa. Tanto a avaliação coordenada dos riscos na UE como o conjunto de instrumentos da UE mostram o elevado valor do trabalho coletivo realizado no âmbito do grupo de cooperação SRI, que contou com a forte colaboração entre representantes de todos os Estados-Membros, da Comissão e da ENISA.

O conjunto de instrumentos permite uma abordagem comum da UE em matéria de cibersegurança das redes 5G, promovendo, através das políticas e da coordenação a nível da UE, a coerência em todo o mercado interno, bem como o exercício das competências dos Estados-Membros, nomeadamente no que respeita à segurança nacional. As medidas e os planos de atenuação nele incluídos permitem uma resposta adequada, eficaz e proporcionada por parte da UE a desafios comuns no domínio da cibersegurança das redes 5G.

A Comissão congratula-se com a publicação do conjunto de instrumentos da UE em matéria de cibersegurança das redes 5G e apoia plenamente todas as suas conclusões acima referidas.

A Comissão insta os Estados-Membros e as instituições, agências e outros organismos competentes da União a:

i) assegurar a rápida aplicação de estratégias eficazes e adequadas de atenuação dos riscos em toda a UE, em conformidade com o conjunto de instrumentos da UE,

ii) tomar todas as medidas adicionais necessárias para garantir a coordenação a nível da União, nomeadamente através da prossecução do trabalho no âmbito do grupo de cooperação SRI e da criação de um mecanismo sólido para acompanhar a aplicação do conjunto de instrumentos da UE, de modo a assegurar a eficácia das medidas e o bom funcionamento do mercado interno.

5. Aplicação do conjunto de instrumentos

A determinação dos Estados-Membros em utilizar plenamente o conjunto de instrumentos é essencial para uma abordagem europeia da segurança das redes 5G credível e bem-sucedida. Embora caiba aos Estados-Membros decidir sobre a adequação de uma determinada medida em função das circunstâncias nacionais, é absolutamente essencial**, tal como recomendado pelo grupo de cooperação SRI (ver acima as conclusões do conjunto de instrumentos),**

estabelecer um conjunto de medidas fundamentais em todos os Estados-Membros e, no que respeita a algumas das medidas, a nível da UE, a fim de dar resposta aos riscos identificados.

A Comissão está disposta a continuar a prestar todo o seu apoio durante as próximas fases e insta os Estados-Membros:

– a tomarem, **até 30 de abril de 2020**, medidas concretas e mensuráveis para aplicar o conjunto de medidas fundamentais recomendadas nas conclusões do conjunto de instrumentos da UE,

– a elaborarem, **até 30 de junho de 2020**, um relatório do grupo de cooperação SRI sobre o estado de execução destas medidas fundamentais em cada Estado-Membro, com base na apresentação de relatórios e na monitorização efetuadas, nomeadamente, no âmbito do grupo de cooperação SRI, com o apoio da Comissão e da ENISA.

5.1. Uma abordagem concertada e baseada nos riscos no que respeita aos fornecedores de 5G

Tendo em conta que o objetivo final consiste em garantir a segurança e a resiliência das redes 5G e a sua sustentabilidade, os Estados-Membros chegaram a acordo sobre a necessidade de avaliar o perfil de risco de cada fornecedor e, por conseguinte, de aplicar restrições adequadas aos fornecedores considerados de alto risco, incluindo exclusões necessárias para atenuar eficazmente os riscos, no que respeita a ativos essenciais, tal como indicado no conjunto de instrumentos. A Comissão está disposta a prestar o seu apoio aos Estados-Membros na aplicação destas medidas.

Tendo em vista a sua aplicação em toda a UE, a avaliação coordenada dos riscos na UE e o conjunto de instrumentos da UE fornecem orientações sobre: 1) a avaliação do perfil de risco dos fornecedores[17]; 2) a sensibilidade dos elementos e funções da rede[18], bem como de outros ativos. Tanto a avaliação coordenada dos riscos na UE como as medidas do conjunto de instrumentos abrangem os riscos relacionados com os fornecedores de equipamentos de rede e de serviços de rede 5G. Não abrangem os outros produtos ou serviços que estes ou outros fornecedores possam disponibilizar.

Tal como definido no ponto 2.37 da avaliação coordenada dos riscos na UE, os perfis de risco de cada fornecedor podem ser avaliados com base em vários indicadores.

A avaliação dos perfis de risco dos fornecedores só deve ser efetuada por razões de segurança e com base em critérios objetivos. A fim de facilitar uma abordagem coordenada da aplicação destas medidas, o conjunto de instrumentos recomenda que os Estados-Membros troquem informações sobre as estratégias e as melhores práticas nacionais. Além disso, a Comissão considera que esta ação deve ser uma das principais prioridades da próxima fase dos trabalhos realizados no âmbito do grupo de cooperação SRI em colaboração com a Comissão e a ENISA.

[17] Ponto 2.37 da avaliação coordenada dos riscos na UE.

[18] O ponto 2.21 da avaliação coordenada dos riscos na UE apresenta as principais categorias de elementos e funções e o seu nível global de sensibilidade, e enumera uma série de elementos-chave identificados pelos Estados-Membros para cada categoria. Por sua vez, os pontos 2.28 e 2.29 identificam uma série de outros tipos de ativos ou áreas sensíveis (por exemplo, entidades ou áreas geográficas específicas).

É importante que as restrições relativas aos fornecedores considerados de alto risco, incluindo as exclusões necessárias para reduzir eficazmente os riscos, bem como as medidas destinadas a evitar a dependência dos mesmos, sejam tomadas em tempo útil. A intervenção numa fase precoce, incluindo, sempre que possível, no âmbito dos processos de licenciamento de frequências 5G, aumentará também a previsibilidade para os operadores de mercado, contribuindo assim para uma rápida implantação das redes 5G, e assegurará a segurança a longo prazo das redes 5G e a resiliência da cadeia de abastecimento 5G.

Simultaneamente, os calendários de aplicação destas medidas podem diferir a nível nacional, sempre que necessário e justificado, em particular em caso de elevado grau de dependência em relação a equipamentos ou serviços de fornecedores avaliados como de alto risco (por exemplo, tendo em conta os ciclos de atualização dos equipamentos, em especial a migração de redes 5G «não autónomas» para redes 5G «autónomas»). Os Estados-Membros poderão considerar a possibilidade de definir planos de execução que incluam períodos de transição adequados para os operadores de rede afetados. Neste contexto, os períodos de transição devem ser definidos de modo a preservar ou mesmo reforçar os incentivos ao investimento em equipamentos de rede modernos, nomeadamente a aceleração da implantação de verdadeiras redes principais 5G («autónomas») e a substituição dos equipamentos 4G existentes noutras partes das redes (por exemplo, na rede de acesso via rádio), em conformidade com os objetivos do Plano de Ação 5G[19].

Além disso, devido à complexidade das redes 5G baseadas em *software*, os operadores de telecomunicações poderão ter de recorrer cada vez mais a entidades terceiras para executar determinadas tarefas, como a manutenção e atualização das redes e do *software* 5G, bem como outros serviços externalizados, para além do fornecimento de equipamento de rede. Tal como descrito na avaliação coordenada dos riscos na UE, tal constitui uma fonte de graves riscos para a segurança. Por conseguinte, deve prestar-se especial atenção a este aspeto. É essencial que seja também efetuada uma avaliação de segurança exaustiva do perfil de risco dos fornecedores encarregados destes serviços, em particular quando as tarefas não sejam executadas na UE. Devem ser tomadas medidas adequadas, incluindo no atinente à aplicação de restrições, em especial nas partes sensíveis das redes 5G, ou à necessária exclusão de entidades de alto risco, em conformidade com as medidas de atenuação do conjunto de instrumentos, a fim de preservar a integridade a longo prazo das infraestruturas 5G.

5.2. O papel da Comissão no apoio à aplicação do conjunto de instrumentos

A Comissão continuará a apoiar a aplicação da estratégia da UE em matéria de cibersegurança das redes 5G em geral, bem como a tomar iniciativas específicas em relação às medidas e aos objetivos do conjunto de instrumentos em que pode acrescentar valor. A Comissão utilizará plenamente as suas competências e os instrumentos pertinentes, na medida do necessário, para dar resposta às questões de segurança identificadas. Ao fazê-lo, e ao atuar conjuntamente com os Estados-Membros e o setor privado, a Comissão procura apoiar medidas estratégicas que contribuam para assegurar a soberania e liderança tecnológicas da UE no âmbito do futuro desenvolvimento de tecnologias de rede, das tecnologias de cibersegurança e de todos os elementos constitutivos pertinentes de que dependam, no seu todo, a nossa economia e a nossa segurança.

[19] COM(2016) 588, de 14 de setembro de 2016, intitulada «5G para a Europa: um Plano de Ação».

Mais especificamente, para garantir a aplicação das medidas de atenuação correspondentes previstas no conjunto de instrumentos nos domínios da sua competência, a Comissão levará a cabo as seguintes ações:

Preservação da cibersegurança das redes 5G e da diversidade da cadeia de valor 5G:

– **Cooperação no domínio da cibersegurança**: continuar a prestar apoio aos Estados-Membros, com vista à aplicação eficaz, coordenada e atempada das medidas nacionais, através do grupo de cooperação SRI.

– **Regras relativas às telecomunicações e à cibersegurança**: apoiar a aplicação das medidas previstas no conjunto de instrumentos relativas aos requisitos de segurança, nomeadamente no que respeita às disposições aplicáveis da regulamentação europeia em matéria de comunicações eletrónicas, e ponderar o valor acrescentado de eventuais atos de execução que especifiquem medidas técnicas e organizativas de segurança, a fim de complementar as regras nacionais e de aumentar a eficácia e a coerência das medidas de segurança impostas aos operadores.

– **Normalização**: tomar medidas para ajudar a manter e, se necessário, aumentar a participação europeia nos vários organismos de normalização, de modo a alcançar os objetivos da Europa em termos de segurança e de interoperabilidade. Em particular, a Comissão avaliará e promoverá, juntamente com os Estados-Membros, as especificações e normas técnicas que permitam a interoperabilidade entre fornecedores de equipamentos 5G em diferentes partes da rede, incluindo em redes antigas, a fim de possibilitar um verdadeiro enquadramento de oferta múltipla, por exemplo, através de interfaces abertas e interoperáveis.

– **Certificação**: apoiar o desenvolvimento de sistemas de certificação 5G que deem resposta às necessidades das redes 5G, ao abrigo do quadro europeu de certificação da cibersegurança.

– **Análise do investimento direto estrangeiro (IDE)**: apoiar a aplicação do regime de análise da UE, efetuando um levantamento da cadeia de valor 5G, incluindo dos ativos de rede sensíveis, e assegurando a monitorização regular do IDE ao longo da cadeia de valor. Em conformidade com o calendário de análise do IDE (a partir de outubro de 2020), a Comissão examinará os investimentos estrangeiros no domínio da tecnologia 5G, em conformidade com as orientações previstas no Regulamento (UE) 2019/452, tendo em conta a avaliação coordenada dos riscos na UE e o conjunto de instrumentos da UE.

– **Instrumentos de defesa comercial**: acompanhar todas as evoluções pertinentes do mercado na UE e em países terceiros e proteger os intervenientes da UE no mercado europeu das redes 5G com medidas de defesa comercial contra eventuais práticas de distorção do comércio (*dumping* ou subvenções), incluindo, se for caso disso, através do lançamento de inquéritos preliminares.

– Regras de concorrência: acompanhar o funcionamento dos mercados de fornecimento de *hardware* e *software* 5G, a fim de garantir resultados concorrenciais, nomeadamente para evitar possíveis situações de bloqueio contratual ou técnico.

– **Programas de financiamento da UE**: assegurar que a participação em programas de financiamento da UE em domínios tecnológicos relevantes esteja sujeita ao cumprimento de requisitos de segurança, utilizando plenamente e continuando a impor condições de segurança no âmbito dos programas de I&I, nomeadamente do Horizonte Europa, do Programa Europa

Digital e do Mecanismo Interligar a Europa 2, bem como no âmbito dos fundos europeus estruturais e de investimento e de outros programas pertinentes. Deverá ser seguida uma abordagem semelhante nos programas de financiamento externo e nos instrumentos financeiros da UE, incluindo no que respeita ao financiamento concedido através de instituições financeiras internacionais.

– Contratação pública: servir-se dos contratos públicos no domínio das redes 5G para promover objetivos identificados em matéria de segurança, diversidade dos fornecedores e sustentabilidade a longo prazo das redes 5G; em particular, procurar garantir que os aspetos de segurança sejam devidamente tidos em consideração durante a adjudicação de contratos públicos relacionados com o domínio das redes 5G, em conformidade com as regras de contratação pública da UE.

– **Resposta a incidentes e gestão de crises (plano de ação) e exercícios de cibersegurança**: tirar pleno partido do desenvolvimento do plano de ação da UE[20] sobre a resposta coordenada a incidentes de cibersegurança em grande escala. Além disso, juntamente com a ENISA, ponderar a possibilidade de realizar um exercício de cibersegurança das redes 5G assim que a maturidade do mercado o permita.

Por fim, sob a responsabilidade do alto representante da União para os Negócios Estrangeiros e a Política de Segurança e vice-presidente da Comissão, e do Conselho:

– **Quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas («instrumentos de ciberdiplomacia»)[21]**: em caso de ciberatividades maliciosas que ameacem a integridade e a segurança da UE, os Estados-Membros são incentivados a utilizar as medidas pertinentes do âmbito da política externa e de segurança comum incluídas nos instrumentos de ciberdiplomacia da UE (incluindo, se necessário, medidas restritivas), a fim de incentivar a cooperação, facilitar a atenuação das ameaças e influenciar o comportamento dos potenciais agressores.

Além disso, vários programas contribuirão para os objetivos de evitar ou limitar o risco de dependência a longo prazo, promovendo um mercado diversificado e sustentável para as redes 5G, nomeadamente mantendo as capacidades da UE na cadeia de valor 5G e investindo na inovação, em conformidade com as obrigações internacionais da UE.

Promoção da inovação e do investimento em cibersegurança e em tecnologias de infraestruturas de rede:

– **Programas** de financiamento da UE: aumentar o investimento em investigação, inovação e implantação de tecnologias de rede e dos elementos constitutivos conexos pertinentes. A Comissão propôs cerca de 3 000 milhões de EUR de investimentos em tecnologias de cibersegurança ao abrigo do próximo orçamento da UE (2021-2027). Este montante inclui a investigação e a inovação no âmbito do Horizonte Europa e o apoio às capacidades de cibersegurança previsto no Programa Europa Digital. O programa InvestEU também pode prestar apoio financeiro à investigação e ao desenvolvimento no domínio da tecnologia 5G, bem como apoiar a sua implantação.

[20] Recomendação (UE) 2017/1584 da Comissão sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala.
[21] Conclusões do Conselho de 20 de novembro de 2017, 9916/17.

Além disso, no âmbito do próximo Horizonte Europa[22], a Comissão propôs a criação de uma parceria institucionalizada da UE para a Internet de nova geração e a tecnologia 6G («redes e serviços inteligentes»), em parceria com a indústria e em coordenação com os Estados-Membros, para concluir a implantação da tecnologia 5G e, sobretudo, **preparar caminho para a tecnologia 6G**, a próxima geração de tecnologia móvel. Foram propostos mais de 2 500 milhões de EUR de investimentos da UE provenientes do orçamento da UE (2021-27), que deverão ser complementados com, pelo menos, 7 500 milhões de EUR de investimento privado nesta iniciativa.

– **Desenvolvimento e implantação industrial**: avaliar eventuais lacunas ou deficiências do mercado ao longo da cadeia de valor 5G, que justifiquem intervenções específicas no âmbito do próximo orçamento de longo prazo ou um possível projeto importante de interesse europeu comum (IPCEI) em matéria de cibersegurança, em conformidade com as sugestões do Fórum de Alto Nível sobre IPCEI. A decisão de conceber e criar IPCEI cabe aos Estados-Membros e às empresas. As regras da UE proporcionam um quadro propício e a Comissão está disposta a facilitar os contactos necessários e a fornecer orientações.

6. Conclusão

As redes 5G deverão criar uma série de oportunidades para os cidadãos, a sociedade e a economia europeus. Por conseguinte, é essencial garantir a segurança e a resiliência das redes 5G. Ao mesmo tempo, as ameaças à cibersegurança (incluindo o risco de interferência de países terceiros ou de entidades apoiadas por Estados) constituem um desafio em constante evolução, cuja relevância aumenta à medida que aumenta a dependência em relação à tecnologia e aos dados. Negligenciar a cibersegurança prejudicaria a confiança no desenvolvimento da economia e da sociedade digitais e impediria a UE de usufruir de todos os seus benefícios. Este desafio exige uma resposta igualmente evolutiva e reforçada.

É essencial definir uma abordagem coordenada e coerente da cibersegurança na UE para as tecnologias e redes críticas, para que a UE garanta a sua soberania tecnológica, mantendo e desenvolvendo capacidades industriais. A Comissão dará todo o seu apoio à aplicação da abordagem da UE em matéria de cibersegurança das redes 5G, assegurando simultaneamente que os mercados da UE permaneçam abertos a produtos e serviços que respeitem os requisitos de cibersegurança e de confiança em evolução.

Para tal, é importante que todas as partes interessadas continuem fortemente empenhadas na segurança 5G. É também necessária uma colaboração contínua entre os Estados-Membros, a Comissão e a ENISA.

Como próxima etapa imediata, conforme referido anteriormente, a Comissão insta os Estados-Membros a adotarem rapidamente os procedimentos necessários para aplicar de forma eficaz e objetiva as medidas acordadas no âmbito do conjunto de instrumentos e a continuarem a colaborar, com o apoio da Comissão e da ENISA, para assegurar a coordenação a nível da UE. Paralelamente, a Comissão lançará todas as ações pertinentes no âmbito das suas competências para apoiar a aplicação do conjunto de instrumentos pelos Estados-Membros e para reforçar o seu impacto.

[22] Pode também ser assegurado financiamento através do MIE 2.0 e do Programa Europa Digital.

Apêndice: Categorias de risco (fonte: Avaliação coordenada dos riscos na UE).

	Categorias de risco
Cenários de risco relacionados com medidas de segurança insuficientes	*R1: Má configuração das redes*
	R2: Falta de controlos de acesso
Cenários de risco relacionados com a cadeia de abastecimento 5G	*R3: Fraca qualidade dos produtos*
	R4: Dependência de um único fornecedor em determinadas redes ou falta de diversidade a nível nacional
Cenários de risco relacionados com o* modus operandi *dos principais perpetradores	*R5: Interferência de Estados através da cadeia de abastecimento 5G*
	R6: Exploração de redes 5G pela criminalidade organizada ou organizações criminosas que visem os utilizadores finais
Cenários de risco relacionados com interdependências entre redes 5G e outros sistemas críticos	*R7: Perturbação significativa de infraestruturas ou serviços críticos*
	R8: Falha generalizada das redes devido à interrupção do fornecimento de eletricidade ou de outros sistemas de apoio
Cenários de risco relacionados com dispositivos dos utilizadores finais	*R9: Exploração da IdC (Internet das coisas)*