Conselho da
União Europeia

Bruxelas, 13 de setembro de 2018
(OR. en)

12104/18
ADD 5

Dossiê interinstitucional:
2018/0328 (COD)

CYBER 187
TELECOM 282
CODEC 1456
COPEN 290
COPS 313
COSI 190
CSC 252
CSCI 123
IND 239
JAI 874
RECH 374
ESPACE 39

NOTA DE ENVIO

de:	Secretário-Geral da Comissão Europeia, assinado por Jordi AYET PUIGARNAU, Diretor
data de receção:	12 de setembro de 2018
para:	Jeppe TRANHOLM-MIKKELSEN, Secretário-Geral do Conselho da União Europeia
n.° doc. Com.:	SWD(2018) 404 final
Assunto:	DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO – RESUMO DA AVALIAÇÃO DE IMPACTO que acompanha o documento PROPOSTA DE REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação

Envia-se em anexo, à atenção das delegações, o documento SWD(2018) 404 final.

Anexo: SWD(2018) 404 final

COMISSÃO
EUROPEIA

Bruxelas, 12.9.2018
SWD(2018) 404 final

DOCUMENTO DE TRABALHO DOS SERVIÇOS DA COMISSÃO

RESUMO DA AVALIAÇÃO DE IMPACTO

que acompanha o documento

PROPOSTA DE REGULAMENTO DO PARLAMENTO EUROPEU E DO CONSELHO

que estabelece o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação

{COM(2018) 630 final} - {SEC(2018) 396 final} - {SWD(2018) 403 final}

Ficha de síntese

Avaliação de impacto sobre a: Proposta de criação de uma Rede de Centros de Competências e de um Centro Europeu de Investigação e Competências em Cibersegurança

A. Necessidade de agir

Porquê? Qual é o problema em causa?

Atualmente, a UE carece de capacidades tecnológicas e industriais suficientes para proteger autonomamente a sua economia e as suas infraestruturas críticas e tornar-se um líder mundial no domínio da cibersegurança. A presente iniciativa visa contribuir para a resolução das seguintes problemáticas e impulsionadores conexos que contribuem para esta situação:

Problemática 1: nível insuficiente de coordenação e cooperação estratégica e sustentável entre indústrias, comunidades de investigação no domínio da cibersegurança e governos para proteger a economia, a sociedade e a democracia com soluções de cibersegurança europeias de vanguarda.

Problemática 2: investimento insuficiente e acesso limitado a conhecimentos, competências e instalações de cibersegurança na Europa.

Problemática 3: poucos resultados da investigação e inovação europeias no domínio da cibersegurança traduzidos em soluções comercializáveis e amplamente implantados na economia.

Estas problemáticas têm diversos fatores subjacentes, nomeadamente o nível insuficiente de confiança entre diferentes intervenientes do mercado da cibersegurança, as limitações inerentes da cooperação existente e dos mecanismos de agrupamento de fundos, a ausência de um quadro para contratos públicos conjuntos para infraestruturas e produtos/soluções de cibersegurança dispendiosos, bem como a não utilização do potencial de mecanismos de estimulação do mercado a montante e a jusante.

O que se espera alcançar com esta iniciativa?

Esta iniciativa destina-se a garantir que a UE conserva e desenvolve as capacidades essenciais (tecnológicas e industriais) para assegurar autonomamente a sua economia, sociedade e democracia digitais e que os Estados-Membros beneficiam das soluções de cibersegurança e das capacidades de ciberdefesa mais avançadas. A iniciativa visa igualmente aumentar a competitividade global das empresas de cibersegurança da UE e assegurar que as indústrias europeias em diferentes setores têm acesso às capacidades e recursos para transformar a cibersegurança na sua vantagem competitiva. Tal deve ser alcançado mediante o desenvolvimento de mecanismos eficazes para a cooperação estratégica a longo prazo de todos os intervenientes relevantes (autoridades públicas, indústrias, comunidade de investigação tanto no setor civil como no militar), para congregar conhecimentos e recursos para criar capacidades e infraestruturas de vanguarda, para promover uma vasta implantação de produtos e soluções de cibersegurança europeus na economia e no setor público, para apoiar as empresas em fase de arranque e as PME no domínio da cibersegurança, bem como ajudar a colmatar a lacuna de competências em cibersegurança.

Qual é o valor acrescentado de uma ação a nível da UE?

A iniciativa poderia acrescentar valor aos esforços atuais a nível nacional, ajudando a criar um ecossistema industrial e de investigação no domínio da cibersegurança interligado e que abranja toda a Europa. Deverá fomentar uma melhor cooperação entre as partes interessadas relevantes (incluindo os setores da cibersegurança civil e militar), a fim de utilizar da melhor forma os recursos e os conhecimentos especializados no domínio da cibersegurança que se encontram atualmente espalhados pela Europa. Deverá ajudar a UE e os Estados-Membros a adotarem uma perspetiva estratégica, proativa e de mais longo prazo da política industrial em matéria de cibersegurança que vá além da mera investigação e desenvolvimento. Esta abordagem deverá ajudar não só a encontrar soluções inovadoras para os desafios enfrentados pelos setores público e privado em matéria de cibersegurança, mas também apoiar a implementação efetiva dessas soluções. Deverá ainda proporcionar às comunidades industriais e de investigação pertinentes, bem como às autoridades públicas, o acesso a capacidades essenciais, tais como instalações de testes e experimentação, que estão muitas vezes fora do alcance dos Estados-Membros a título individual, devido à insuficiência de recursos financeiros e humanos. Contribuirá ainda para colmatar as lacunas de competências e para evitar a fuga de cérebros, assegurando que os melhores talentos podem aceder a projetos europeus de grande escala, proporcionando-lhes, assim, desafios profissionais interessantes. Tudo o exposto anteriormente é igualmente considerado necessário para a Europa ser reconhecida mundialmente como líder em cibersegurança.

B. Soluções

Quais foram as opções legislativas e não legislativas ponderadas? Há uma opção preferida? Porquê?

Foram tidas em consideração várias opções políticas, tanto legislativas como não legislativas. As opções que se seguem foram selecionadas para uma avaliação aprofundada:

1. **Cenário de base** — Opção colaborativa — assume a continuação da abordagem atual de criar capacidades industriais e tecnológicas de cibersegurança na UE através do apoio à investigação e inovação e de mecanismos de colaboração conexos ao abrigo do programa Horizonte Europa;
2. **Opção 1:** Rede de Competências em Cibersegurança com um Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança habilitado para pôr em prática medidas de apoio a tecnologias industriais, bem como no domínio da investigação e inovação;
3. **Opção 2:** Rede de Competências em Cibersegurança com um Centro Europeu de Investigação e Competências em Cibersegurança limitado exclusivamente a atividades de investigação e inovação.

As opções descartadas numa fase inicial incluíram: 1) não prever qualquer ação; 2) criar apenas uma rede de centros de competências existentes; 3) utilizar uma agência existente (ENISA, REA ou INEA).

Atendendo ao compromisso geral já assumido pela Comissão para a presente iniciativa e ao papel importante a desempenhar pelos Estados-Membros, a principal distinção entre as duas opções políticas analisadas pormenorizadamente reside no seu âmbito, conforme patente na respetiva base jurídica: uma entidade apenas baseada no artigo 187.º do TFUE (opção 2) limitaria a iniciativa à esfera da investigação e inovação e pressuporia, normalmente, uma contribuição financeira de intervenientes privados. Por outro lado, uma entidade assente numa dupla base jurídica — artigos 187.º e 173.º do TFUE (opção 1) — beneficiaria de um mandato mais alargado, abrangendo também, entre outras, a implantação e o apoio à indústria e criando sinergias mais fortes com a ciberdefesa. Conferiria igualmente um papel mais proeminente aos Estados-Membros, tanto em termos do seu papel na governação quanto no de potenciais adquirentes de tecnologia de cibersegurança.

A análise revelou que a opção 1 é mais adequada para alcançar os objetivos da iniciativa ao mesmo tempo que oferece maior impacto económico, social e ambiental e salvaguarda os interesses da União. Os principais argumentos a favor desta opção incluíram a flexibilidade para permitir diferentes modelos de cooperação com a comunidade e a rede de centros de competências para otimizar a utilização dos conhecimentos e recursos existentes; a capacidade de estruturar a cooperação das partes interessadas públicas e privadas provenientes de todos os setores relevantes, nomeadamente a defesa; a capacidade de criar uma verdadeira política industrial de cibersegurança mediante o apoio a atividades relacionadas não apenas com a investigação e o desenvolvimento, mas também com a implantação no mercado. Por último, a opção 1 permite igualmente aumentar a coerência, atuando como um mecanismo de execução para financiamento relacionado com cibersegurança do programa Europa Digital e do Horizonte Europa, e reforçar as sinergias entre as dimensões civil e militar da cibersegurança em relação ao Fundo Europeu de Defesa.

Quem apoia cada uma das opções?

De acordo com o resultado da consulta e dos processos de recolha de dados existe uma procura clara, da parte das comunidades industriais e de investigação, de um mecanismo que permita à UE ter uma política industrial coerente no domínio da cibersegurança que vá além de meras atividades de investigação e desenvolvimento, para que a Europa se torne, de facto, um líder mundial em cibersegurança. Ao mesmo tempo, as partes interessadas sublinharam que a chave para o sucesso será a atribuição de um papel bem definido ao Centro no apoio e facilitação dos esforços da Rede e das comunidades relevantes, bem como uma abordagem inclusiva e colaborativa à rede para evitar a criação de novos silos. Esta estrutura deve também ser flexível de modo a poder ser facilmente adaptada, uma vez que a cibersegurança constitui um ambiente com ritmo acelerado. Ao longo do processo, os Estados-Membros destacaram a necessidade da inclusão de todos os Estados-Membros e dos seus centros de excelência e competências existentes e de prestar especial atenção à complementaridade das ações. Concretamente, no atinente ao Centro, os Estados-Membros salientaram a importância do seu papel de coordenação no apoio à rede. Por conseguinte, qualquer iniciativa da Comissão terá de encontrar o equilíbrio certo nas estruturas de governação e de execução e refletir este equilíbrio nessas mesmas estruturas, de modo a assegurar uma efetiva coordenação europeia, tendo simultaneamente em conta os desenvolvimentos a nível nacional.

C. Impactos da opção preferida

Quais são os benefícios da opção preferida (se existir; caso contrário, das opções principais)?

A opção preferida permitirá às autoridades públicas e indústrias nos Estados-Membros prevenir e responder mais eficazmente a ciberameaças mediante a oferta de produtos e soluções mais seguros com os quais aquelas se poderão munir. Este aspeto é particularmente relevante para a proteção do acesso a serviços essenciais (por exemplo, transportes, saúde, serviços bancários e financeiros). Terá também um impacto positivo na competitividade da UE e das PME, porquanto assume constituir um mecanismo capaz de criar capacidades industriais em cibersegurança nos Estados-Membros e na União e traduzir eficazmente a excelência científica europeia em soluções comercializáveis que poderão ser implantadas na economia. Esta opção permite reunir recursos para investir nas capacidades necessárias a nível dos Estados-Membros e desenvolver ativos europeus partilhados, obtendo, ao mesmo tempo, economias de escala. Tal é suscetível de conduzir a um maior acesso por parte das PME, das indústrias e dos investigadores a essas instalações, o que estimulará a inovação e agilizará os processos de desenvolvimento. Também reduzirá os custos para algumas empresas do lado da procura e ajudá-las-á a transformar a cibersegurança na sua vantagem competitiva. A opção permite tirar partido das oportunidades de mercado de dupla utilização, permitindo às comunidades civis e militares trabalharem conjuntamente em desafios partilhados. É também suscetível de acrescentar valor aos esforços nacionais relacionados com a resolução da lacuna de competências em cibersegurança. A nível da UE, esta opção também permite melhorar a coerência e as sinergias entre diferentes mecanismos de financiamento.

Pode ser alcançado um impacto positivo indireto no ambiente mediante o desenvolvimento de soluções de cibersegurança para setores que têm potencialmente um enorme impacto ambiental (por exemplo, centrais nucleares), ajudando-os a evitar as consequências potencialmente devastadoras dos ciberataques a este tipo de infraestruturas.

Quais são os custos da opção preferida (se existir; caso contrário, das opções principais)?

Os custos decorrentes da opção preferida estão sobretudo relacionados com os custos de funcionamento do Centro e dos centros nacionais de coordenação. Os custos relacionados com a execução de diferentes programas de financiamento (Programa Europa Digital e Programa Horizonte Europa) estão sujeitos a avaliações de impacto separadas.

Como serão afetadas as empresas, as PME e as microempresas?

As empresas europeias, tanto a nível da procura como da oferta de cibersegurança, incluindo as PME e microempresas que operam no domínio da cibersegurança, estarão entre os grupos de partes interessadas mais afetadas. Embora a criação do Centro de Competências e da Rede não lhes imponha obrigações regulamentares, abrirá oportunidades em termos de redução de custos para a conceção de novos produtos e ajudá-las-á a obter acesso mais fácil à comunidade de investidores e a atrair o financiamento necessário para implantar soluções comercializáveis. No caso das PME e microempresas, o acesso a instalações de teste e experimentação financiadas com fundos públicos é ainda mais importante, dado que aquelas carecem de recursos para aquisições ou deslocações para fora do seu mercado (e muitas vezes fora da UE) com vista a encontrar as infraestruturas necessárias. Espera-se também que esta iniciativa abra novos mercados para as PME e microempresas europeias ativas no domínio da cibersegurança. Além disso, o mecanismo escolhido assegurará a coordenação entre a investigação e a indústria e, por conseguinte, direcionará os esforços de investigação para necessidades industriais concretas. A disponibilização de conhecimentos especializados e ferramentas de vanguarda no domínio da cibersegurança apoiará indiretamente os operadores económicos no cumprimento da Diretiva SRI.

Haverá impactos significativos nos orçamentos e administrações públicas nacionais?

A iniciativa permitirá aos Estados-Membros coordenarem investimentos em infraestruturas de cibersegurança necessárias a nível nacional e europeu. O mecanismo permitirá reunir recursos para ferramentas e infraestruturas que, de outra forma, seriam mais onerosas ou incomportáveis para os Estados-Membros a título individual. Uma abordagem deste tipo permitirá economias de escala e a racionalização de recursos. A contribuição financeira dos Estados-Membros para o Centro de Competências e as ações relevantes deve ser proporcional à contribuição da União.

Haverá outros impactos significativos?

Sim, a iniciativa tem um impacto positivo inequívoco uma vez que é suscetível de aumentar substancialmente as capacidades dos Estados-Membros para protegerem autonomamente as suas economias, incluindo os seus setores críticos, e aumentarem a competitividade das empresas de cibersegurança europeias, bem como as indústrias de diferentes setores, que serão capazes de proteger adequadamente os seus ativos existentes e conceber produtos inovadores seguros ao mesmo tempo que reduzem os custos de I&D relacionados com a segurança. Em última instância, tal deverá permitir à UE tornar-se líder na próxima geração de tecnologias digitais e de cibersegurança.

D. Acompanhamento
Quando será reexaminada a medida proposta?
Será incluída no instrumento jurídico uma cláusula explícita de acompanhamento dos indicadores-chave de desempenho (ICD), bem como uma cláusula de avaliação e revisão, por força da qual a Comissão Europeia realizará uma avaliação intercalar para medir o impacto do instrumento e o seu valor acrescentado. Posteriormente, a Comissão Europeia apresentará um relatório ao Parlamento Europeu e ao Conselho. Após esta avaliação, a Comissão poderá propor uma revisão e prorrogação dos mandatos do Centro de Competências e da Rede.