Conselho da
União Europeia

Bruxelas, 20 de outubro de 2021
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	19 de outubro de 2021
para:	Delegações
n.º doc. ant.:	12534/21
Assunto:	Conclusões do Conselho - Explorar o potencial da iniciativa relativa a uma ciberunidade conjunta - complementar a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala – Conclusões do Conselho (19 de outubro de 2021)

Enviam-se em anexo, à atenção das delegações, as Conclusões do Conselho intituladas "Explorar o potencial da iniciativa relativa a uma ciberunidade conjunta – complementar a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala", adotadas pelo Conselho na sua reunião realizada a 19 de outubro de 2021.

ANEXO

Conclusões do Conselho – Explorar o potencial da iniciativa relativa a uma ciberunidade conjunta – complementar a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala

O CONSELHO DA UNIÃO EUROPEIA,

RECORDANDO as suas conclusões sobre

– a Estratégia de Cibersegurança da UE para a década digital[1],

– a resposta coordenada da UE a incidentes e crises de cibersegurança em grande escala[2],

– a ciberdiplomacia[3],

– um quadro para uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas ("instrumentos de ciberdiplomacia")[4],

– Segurança e Defesa[5],

– o Quadro Estratégico da UE em matéria de Ciberdefesa[6],

– Construir o futuro digital da Europa[7],

– Decisão de Execução (UE) 2018/1993 do Conselho, de 11 de dezembro de 2018, relativa ao Mecanismo Integrado da UE de Resposta Política a Situações de Crise,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– a Comunicação Conjunta ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE[8],

– o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE[9],

1. SALIENTA a importância da cibersegurança para a construção de uma Europa resiliente, digital e ecológica. REALÇA que a cibersegurança é indispensável para a prosperidade e segurança da UE e dos seus Estados-Membros, dos seus cidadãos, das suas empresas e instituições, bem como para defender a integridade das nossas sociedades livres e democráticas.

2. RECONHECE a natureza transfronteiriça e intersetorial de muitas ciberameaças, bem como os riscos e as implicações potenciais das constantes campanhas de ciberatividades mal-intencionadas com maiores repercussões e que são mais sofisticadas, dirigidas, complexas, persistentes e/ou insidiosas[10]. A pandemia de COVID-19 veio revelar ainda mais as vulnerabilidades das nossas sociedades e os potenciais danos que ciberincidentes em grande escala podem causar à economia, à democracia, aos serviços essenciais e às infraestruturas críticas, nomeadamente no setor da saúde. A pandemia veio aumentar igualmente a importância da conectividade e a dependência da sociedade de redes e sistemas de informação fiáveis, de confiança e seguros. Em última análise, veio sublinhar a necessidade de garantir uma Internet mundial, aberta, livre, estável e segura e de confiar nos produtos, processos e serviços das tecnologias da informação e comunicação (TIC), incluindo a necessidade de assegurar uma cadeia de abastecimento resiliente.

---

8 14435/17 + COR 1.
9 7737/19.
10 ENISA Threat Landscape 2020 (Panorama das ameaças em 2020 elaborado pela ENISA).

3. REITERA a importância da ciber-resiliência e do desenvolvimento do quadro da UE de gestão de crises de cibersegurança[11], tendo em vista uma resposta eficiente e atempada a nível da UE a incidentes e crises de cibersegurança em grande escala, e a importância de a integrar ainda mais nos mecanismos horizontais e setoriais de resposta a situações de crise que existem na UE. SALIENTA o papel do Conselho e do Mecanismo Integrado de Resposta Política a Situações de Crise (IPCR) em garantir uma coordenação e uma resposta atempadas a nível político da União a situações de crise, independentemente de terem origem dentro ou fora da União, e que têm grande alcance ou significado político. DESTACA a importância de testar esses quadros e mecanismos em exercícios periódicos.

4. RECORDA que as atividades desenvolvidas a nível da UE relativas a ciberincidentes e cibercrises em grande escala se pautam pelos princípios da subsidiariedade, proporcionalidade, complementaridade, não duplicação e confidencialidade. REITERA que os Estados-Membros são os principais responsáveis por dar resposta aos incidentes e crises de cibersegurança em grande escala que os afetem. RECORDA a importância de respeitar as competências dos Estados-Membros e a sua exclusiva responsabilidade pela segurança nacional, em conformidade com o artigo 4.º, n.º 2, do Tratado da União Europeia, nomeadamente no domínio da cibersegurança.

5. RECORDA, ao mesmo tempo, a importância de respeitar as competências e os mandatos das instituições, organismos e agências da UE. O alto representante, a Comissão e demais instituições, organismos e agências da UE têm também um papel essencial a desempenhar, decorrente do direito da União, nomeadamente devido às eventuais repercussões de incidentes e crises de cibersegurança em grande escala sobre o mercado único, bem como sobre o funcionamento das próprias instituições, organismos e agências da UE.

---

[11] 10086/18.

6. SUBLINHA a necessidade de evitar duplicações desnecessárias e de procurar complementaridade e valor acrescentado no futuro desenvolvimento do quadro da UE de gestão de crises de cibersegurança, bem como de assegurar o alinhamento com os mecanismos, iniciativas, processos e procedimentos existentes a nível nacional e europeu. REALÇA a importância de racionalizar os processos e estruturas existentes, a fim de reduzir a complexidade, e, no interesse da coesão na União, de melhorar a acessibilidade e a capacidade de dar resposta aos que solicitam assistência e solidariedade.

7. RECONHECE a aplicabilidade do direito internacional, inclusive da Carta das Nações Unidas na sua íntegra, do direito internacional humanitário e do direito em matéria de direitos humanos no ciberespaço, e PROMOVE a adesão às normas, regras e princípios voluntários e não vinculativos de comportamento responsável dos Estados no ciberespaço, aprovados por todos os Estados membros das Nações Unidas.

8. CONGRATULA-SE com os progressos alcançados nos últimos anos no Conselho, em especial no Grupo Horizontal das Questões do Ciberespaço (HWPCI) e noutros grupos pertinentes do Conselho, bem como na criação de outras iniciativas, redes e mecanismos de cooperação e partilha de informações entre os Estados-Membros, nomeadamente o grupo de cooperação SRI e a rede de CSIRT, instituída pela Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, a Rede de Organizações de Coordenação de Cibercrises (CyCLONe), bem como os projetos pertinentes relacionados com a ciberdefesa lançados no âmbito da cooperação estruturada permanente (CEP)[12], o grupo de missão "Ação Conjunta contra o Cibercrime" (J-CAT), a Rede Judiciária Europeia em matéria de Cibercriminalidade (RJEC), as contribuições voluntárias dos Estados-Membros para o INTCEN e a coordenação e cooperação no contexto dos Instrumentos de Ciberdiplomacia.

---

[12] Em especial, as "Equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança", coordenadas pela Lituânia, o "Centro de Coordenação no Domínio da Cibernética e da Informação", coordenado pela Alemanha, e a "Plataforma de partilha de informações relativas às ciberameaças e à resposta a incidentes informáticos", coordenada pela Grécia.

9. RECORDA os quadros de cooperação existentes entre as instituições, organismos e agências da UE, como a cooperação estruturada entre a ENISA e a CERT-UE e o Memorando de Entendimento entre a ENISA, a Agência Europeia de Defesa, Centro Europeu da Cibercriminalidade (EC3) da Europol e a CERT-UE. SALIENTA a importância de continuar a partilhar periodicamente informações com o Conselho sobre a evolução futura destes quadros de cooperação.

10. REALÇA a importância de reforçar a cooperação e a partilha de informações entre as várias cibercomunidades na UE e nos seus Estados-Membros a todos os níveis necessários — técnicos, operacionais e estratégicos/políticos — e de ligar os mecanismos, redes, estruturas, processos e procedimentos de gestão de crises sempre que tal seja de molde a apoiar e aperfeiçoar o tratamento de ciberincidentes e cibercrises em grande escala.

11. RECONHECE os progressos alcançados por um grupo de Estados-Membros com a criação de uma cibercapacidade operacional conjunta designada por "Equipas de resposta rápida a ciberataques" no âmbito do quadro da CEP, com o objetivo de aprofundar a cooperação voluntária no domínio do ciberespaço através da assistência mútua, inclusive em resposta a ciberincidentes e cibercrises em grande escala.

12. RECONHECE a experiência e a capacidade de resposta demonstradas, 24 horas, sete dias por semana, pelos serviços responsáveis pela aplicação da lei no domínio da cooperação operacional e do intercâmbio seguro de informações contra importantes ciberataques transfronteiriços, no quadro do Protocolo da UE de Resposta de Emergência dos Serviços Repressivos.

13. RECONHECE a continuação da aplicação do quadro para uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas ("instrumentos de ciberdiplomacia"). RECORDA que cada Estado-Membro é livre de tomar as sua própria decisão soberana, caso a caso, no que diz respeito à atribuição de uma ciberatividade mal-intencionada. RECORDA que as medidas tomadas no quadro de uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas deverão basear-se numa apreciação comum da situação acordada entre os Estados-Membros. O INTCEN da UE desempenha um papel central enquanto plataforma que disponibiliza conhecimento situacional e uma avaliação das ameaças em matéria de cibersegurança para a UE, com base em contributos voluntários dos Estados-Membros e sem prejuízo das suas competências.

14. REITERA a importância da assistência mútua e da solidariedade, em conformidade com o artigo 42.º, n.º 7, do Tratado da União Europeia e o artigo 222.º do Tratado sobre o Funcionamento da União Europeia, e APELA à realização de novos exercícios com uma ciberdimensão. RECORDA a necessidade de refletir sobre a articulação entre o quadro da UE de gestão de crises de cibersegurança, os instrumentos de ciberdiplomacia e as disposições dos artigos acima referidos em caso de ciberincidentes ou cibercrises em grande escala. RECORDA ainda que as obrigações que incumbem aos Estados-Membros por força do artigo 42.º, n.º 7, do Tratado da União Europeia não afetam o caráter específico da política de segurança e defesa de determinados Estados-Membros. RECORDA também que a OTAN continua a ser o fundamento da defesa coletiva para os Estados que são membros desta organização.

15. RECONHECE a cooperação UE-OTAN em matéria de cibersegurança e ciberdefesa, inclusive no respeitante à partilha de informações entre a CERT-UE e a Capacidade de Resposta a Incidentes Informáticos da OTAN (NCIRC), no pleno respeito dos princípios da transparência, reciprocidade e inclusividade, bem como da autonomia de decisão de ambas as organizações.

16. RECONHECE a importância da cooperação, sempre que necessário, com o setor privado em termos de exercícios de partilha de informações e de disponibilização de conhecimentos especializados pertinentes, bem como de soluções e serviços de confiança, incluindo, por exemplo, o apoio à resposta a incidentes e o reforço do conhecimento situacional entre as várias cibercomunidades.

17. SALIENTA a importância de canais de comunicação seguros para o intercâmbio de informações classificadas e sensíveis. REALÇA a necessidade de novos progressos.

A este respeito, e tendo em conta o que precede,

18. REGISTA a recomendação da Comissão relativa à criação de uma ciberunidade conjunta enquanto iniciativa a ter em conta para efeitos do desenvolvimento futuro do quadro da UE de gestão de crises de cibersegurança[13].

19. INSTA a UE e os seus Estados-Membros a prosseguirem os seus esforços no sentido de desenvolverem um quadro da UE de gestão de crises de cibersegurança mais abrangente e eficaz, com base nos mecanismos existentes e nos progressos já alcançados, e a terem em conta o potencial da iniciativa relativa a uma ciberunidade conjunta, a fim de complementar estes mecanismos adotando uma abordagem faseada. SALIENTA que um processo gradual, transparente e inclusivo é essencial para reforçar a confiança, sendo, por conseguinte, fundamental para o futuro desenvolvimento de um quadro da UE de gestão de crises de cibersegurança. Este processo deverá respeitar as funções, competências e mandatos existentes dos Estados-Membros e das instituições, organismos e agências da UE, bem como os princípios enunciados nas presentes conclusões, nomeadamente a proporcionalidade, a subsidiariedade, a inclusividade, a complementaridade, a não duplicação e a confidencialidade das informações. SALIENTA, ao mesmo tempo, que a eventual participação ou contributo dos Estados-Membros para uma potencial ciberunidade conjunta é de natureza voluntária.

[13] C(2021) 4520 final (11155/21 e 11155/21 ADD1).

20. SALIENTA a necessidade de estabelecer métodos de trabalho e governação adequados, com o objetivo de permitir o envolvimento e a participação de todos os Estados-Membros nas deliberações, no desenvolvimento e em processos eficazes de tomada de decisões sobre o quadro da UE de gestão de crises de cibersegurança, nomeadamente no que se refere à potencial iniciativa relativa a uma ciberunidade conjunta. APELA ao respeito das prerrogativas do Conselho ao abrigo dos Tratados e do princípio da cooperação leal.

21. SUBLINHA a importância de identificar e envolver todas as cibercomunidades pertinentes na UE e nos seus Estados-Membros, tendo simultaneamente em conta as respetivas funções e responsabilidades em diferentes tipos de ciberincidentes e cibercrises em grande escala. SUBLINHA o papel fundamental do Conselho, em especial através do HWPCI, na definição de políticas e na coordenação respeitantes ao desenvolvimento do quadro da UE de gestão de crises de cibersegurança. CONVIDA, por conseguinte, os Estados-Membros, a Comissão, o Serviço Europeu para a Ação Externa (SEAE), o INTCEN da UE, a CERT-UE, a ENISA, a Europol (EC3), a Eurojust (EJCN), o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC), bem como representantes da rede de CSIRT, a CyCLONe, o grupo de cooperação SRI, a AED e os projetos pertinentes da CEP, e outras eventuais partes interessadas, a participarem neste processo. Poderá continuar a ser estudada a eventual criação de um grupo de trabalho, tal como proposto na recomendação da Comissão, que assegure uma representação adequada de todos os Estados-Membros e que aja sob a orientação política do Conselho, para servir de fórum temporário que reúna representantes de todas as cibercomunidades relevantes nos Estados-Membros e na UE. Esse grupo de trabalho deverá apresentar regularmente relatórios sobre as suas atividades e enviar eventuais sugestões ao Conselho para debate e aprovação e orientações adicionais. Além disso, poderão ser estabelecidas outras formas de diálogo dentro e entre comunidades, nomeadamente através de ateliês, seminários, formação conjunta e exercícios.

22. SUBLINHA o papel do Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança (ECCC) e da Rede de Centros Nacionais de Coordenação no contexto da potencial ciberunidade conjunta, especialmente tendo em conta o seu papel de aumentar substancialmente as capacidades tecnológicas e as soluções, capacidades e competências tecnológicas no domínio da cibersegurança da União.

23. CONVIDA a UE e os seus Estados-Membros a empenharem-se em continuar a desenvolver o quadro da UE de gestão de crises de cibersegurança, nomeadamente explorando o potencial de uma iniciativa relativa a uma ciberunidade conjunta, criando e definindo o processo, com as respetivas metas e um calendário, e clarificando os objetivos e as possíveis funções e responsabilidades. REALÇA a necessidade de consolidar, com caráter prioritário, as redes e interações existentes em cada comunidade, bem como proceder ao levantamento exaustivo das eventuais lacunas e necessidades em matéria de partilha de informações dentro e entre as cibercomunidades, bem como dentro e entre as instituições, organismos e agências europeus e, subsequentemente, chegar a acordo sobre possíveis objetivos e prioridades principais de uma potencial ciberunidade conjunta. Sem prejuízo dos resultados, SALIENTA a necessidade de concentrar as atenções na identificação das necessidades de partilha de informações, a fim de estabelecer um conhecimento comum da situação entre todos os serviços competentes. Ao identificar as lacunas e necessidades em matéria de partilha de informações, incluindo a eventual utilização de plataformas virtuais, importa continuar a prestar a devida atenção aos canais de comunicação seguros para o intercâmbio de informações classificadas e sensíveis, SALIENTANDO simultaneamente a importância de utilizar as infraestruturas já existentes. A introdução de uma abordagem gradual visa criar confiança e constituir uma base para eventuais novas medidas relacionadas com o reforço da preparação e da cooperação operacional. RECONHECE que em função dos objetivos poderão ser necessárias soluções diferentes e a participação de um conjunto diferente de representantes das cibercomunidades pertinentes na UE e nos seus Estados-Membros.

24. APELA a uma análise mais aprofundada da base jurídica para a potencial ciberunidade conjunta ao longo de todo o processo, incluindo uma avaliação das tarefas e funções em relação às atribuídas à ENISA na recomendação, à luz do artigo 7.º do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019. APELA a uma maior reflexão sobre os elementos individuais da recomendação relativa à criação de uma ciberunidade conjunta, nomeadamente no que diz respeito às equipas de reação rápida da UE em matéria de cibersegurança e ao Plano de Resposta da UE a Incidentes e Crises de Cibersegurança. REALÇA que uma potencial ciberunidade conjunta terá de respeitar as competências, os mandatos e os poderes legais dos seus eventuais futuros participantes.

25. APELA à UE e aos seus Estados-Membros a estudarem o potencial de uma iniciativa relativa a uma ciberunidade conjunta, também do ponto de vista das instituições, organismos e agências da UE, a fim de complementar os esforços em curso a nível dos Estados-Membros. CONGRATULA-SE com a intenção da Comissão de reforçar a resiliência das instituições, organismos e agências pertinentes da UE através da sua futura proposta de regulamento relativo a regras comuns vinculativas em matéria de cibersegurança para as instituições, organismos e agências da UE.

26. Em conclusão, REITERA o seu compromisso de reforçar a ciber-resiliência e de continuar a desenvolver o quadro da UE de gestão de crises de cibersegurança e ACOMPANHARÁ PERIODICAMENTE os progressos e fornecerá orientações adicionais para complementar o quadro da UE de gestão de crises de cibersegurança.