Conselho da
União Europeia

Bruxelas, 23 de maio de 2022
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	23 de maio de 2022
para:	Delegações
Assunto:	Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço – Conclusões do Conselho aprovadas pelo Conselho na sua reunião de 23 de maio de 2022

Junto se enviam, à atenção das delegações, as Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, aprovadas pelo Conselho na sua reunião de 23 de maio de 2022.

ANEXO

Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço

O CONSELHO DA UNIÃO EUROPEIA,

RECORDANDO:

– as suas conclusões sobre a comunicação conjunta ao Parlamento Europeu e ao Conselho, de 25 de junho de 2013, intitulada "Estratégia da União Europeia para a Cibersegurança: um ciberespaço aberto, seguro e protegido"[1]

– o Quadro Estratégico da UE em matéria de Ciberdefesa[2],

– as Conclusões do Conselho sobre a governação da Internet[3],

– as Conclusões do Conselho sobre a ciberdiplomacia[4],

– as Conclusões do Conselho sobre o reforço do sistema de ciberresiliência da Europa e a promoção de uma indústria de cibersegurança competitiva e inovadora[5],

– as Conclusões do Conselho sobre a comunicação conjunta ao Parlamento Europeu e ao Conselho intitulada: "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE[6],

– as Conclusões do Conselho sobre um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas ("instrumentos de ciberdiplomacia")[7],

– as Conclusões do Conselho sobre a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala[8],

– as Conclusões do Conselho sobre as diretrizes da UE para o reforço das cibercapacidades externas[9],

– a 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[10],

---

1 12109/13
2 15585/14
3 16200/14
4 6122/15 + COR 1
5 14540/16
6 14435/17 + COR 1
7 10474/17
8 10086/18
9 10496/18
10 JO L 320 de 17.12.2018, p. 28.

– as Conclusões do Conselho sobre o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE[11],

– as 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[12],

– as Conclusões do Conselho sobre o futuro de uma Europa altamente digitalizada para além de 2020: "Impulsionar a competitividade digital e económica na União e a coesão digital"[13],

– as Conclusões do Conselho sobre os esforços complementares para aumentar a resiliência e combater as ameaças híbridas[14],

– as Conclusões do Conselho intituladas "Construir o futuro digital da Europa"[15],

– as Conclusões do Conselho sobre a cibersegurança dos dispositivos conectados[16],

– as Conclusões do Conselho sobre a Estratégia de Cibersegurança da UE para a década digital[17],

– as Conclusões do Conselho sobre segurança e defesa[18],

– 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"[19],

– A 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[20],

---

11 7737/19
12 14517/19
13 9596/19
14 14972/19
15 8711/20
16 13629/20
17 7290/21
18 8396/21
19 13048/21
20 7371/22

1. SALIENTA que os comportamentos maliciosos no ciberespaço da autoria de intervenientes tanto estatais como não estatais se intensificaram nos últimos anos, incluindo um aumento acentuado e constante de atividades maliciosas que visam as infraestruturas críticas, as cadeias de abastecimento e a propriedade intelectual da UE e dos seus Estados-Membros, um aumento do risco de efeitos indiretos, bem como um aumento dos ataques com programas sequestradores contra as nossas empresas, organizações e cidadãos. OBSERVA que, com o regresso da política das relações de poder, alguns países estão a tentar cada vez mais contestar e comprometer a ordem internacional assente em regras no ciberespaço, transformando a ciberesfera, juntamente com o alto mar, o ar e o espaço exterior, num domínio cada vez mais disputado. RECONHECE que os ciberataques em grande escala ou as tentativas de intrusão, perturbação ou destruição de redes e sistemas de informação com efeitos sistémicos se tornaram mais comuns, podem comprometer a nossa segurança económica e afetar as nossas instituições e processos democráticos, e evidenciam que alguns intervenientes estão dispostos a pôr em risco a segurança e a estabilidade internacionais. SUBLINHA que a agressão militar da Rússia contra a Ucrânia demonstrou que as ciberatividades ofensivas podem ser conduzidas como parte integrante de estratégias híbridas que combinam intimidação, desestabilização e perturbações económicas.

2. REITERA que, perante as atuais mudanças geopolíticas, a força da nossa União reside na unidade, na solidariedade e na determinação, e que a execução da Bússola Estratégica reforçará a autonomia estratégica da UE e a sua capacidade de trabalhar com os parceiros para salvaguardar os seus valores e interesses, nomeadamente no domínio do ciberespaço. SUBLINHA que uma UE mais forte e com mais capacidade no plano da segurança e da defesa contribuirá positivamente para a segurança mundial e transatlântica e complementa a OTAN, que continua a ser a base da defesa coletiva dos membros que a compõem. REAFIRMA que é intenção da UE intensificar o apoio à ordem internacional assente em regras, centrada nas Nações Unidas.

3. Em consonância com as Conclusões do Conselho sobre a Estratégia da UE para a Cibersegurança e a Bússola Estratégica, REITERA a necessidade de desenvolver a postura da União no ciberespaço, aumentando a nossa capacidade para prevenir ciberataques mediante o reforço e desenvolvimento das capacidades, a formação, os exercícios, o reforço da resiliência e utilizando todas as ferramentas disponíveis na UE para dar uma resposta firme aos ciberataques contra a UE e os seus Estados-Membros. Implica isto que se demonstre ainda mais a determinação da UE em dar respostas imediatas e a longo prazo aos autores das ameaças que procuram impedir o nosso acesso seguro e aberto ao ciberespaço e afetar os nossos interesses estratégicos, inclusive a segurança dos nossos parceiros. Neste contexto, SALIENTA que a postura no ciberespaço visa combinar as várias iniciativas que concorrem nas ações da UE no sentido de consolidar a paz e a estabilidade no ciberespaço e a favor de um ciberespaço aberto, livre, mundial, estável e seguro, coordenando melhor ao mesmo tempo as ações a curto, médio e longo prazo destinadas a prevenir, desencorajar, dissuadir e responder a ciberameaças e ciberataques e mobilizar as cibercapacidades. SALIENTA que estes elementos deverão ser incorporados na postura da União no ciberespaço, de acordo com cinco funções que a UE desempenha no domínio do ciberespaço: reforçar a gestão solidária e abrangente de crises; promover a nossa visão do ciberespaço; reforçar a cooperação com países parceiros e organizações internacionais; prevenir os ciberataques defender-se e dar-lhes resposta.

I. REFORÇAR A NOSSA CIBERRESILIÊNCIA E AS CAPACIDADES DE PROTEÇÃO

4. REITERA a necessidade de aumentar o nível global de cibersegurança da UE, AGUARDA COM EXPECTATIVA a rápida adoção do projeto de diretiva relativa a medidas destinadas a alcançar um elevado nível comum de cibersegurança na União (SRI), do projeto de regulamento relativo à resiliência operacional digital do setor financeiro (Regulamento DORA), do projeto de diretiva relativa à resiliência das entidades críticas (REC) e TOMA NOTA da proposta de regulamento que estabelece medidas relativas a um elevado nível de cibersegurança nas instituições, órgãos e organismos da União, a fim de promover uma União Europeia que proteja os seus cidadãos, os serviços públicos e as empresas no ciberespaço. INCENTIVA a Comissão a concluir a adoção de propostas fundamentais para garantir a segurança das infraestruturas, das tecnologias, dos produtos e dos serviços digitais, a fim de emitir um sinal claro quanto às ambições da UE relativamente a estes temas e permitir a prestação de apoio às empresas para que estas estejam à altura do desafio. EXORTA a Comissão a propor requisitos comuns da UE para dispositivos conectados e processos e serviços associados em matéria de cibersegurança, através da legislação relativa à ciberresiliência que deverá ser proposta pela Comissão antes do final de 2022, tendo em conta a necessidade de uma abordagem horizontal e holística que abranja todo o ciclo de vida dos produtos digitais, bem como a regulamentação em vigor, especialmente no domínio da cibersegurança.

5. CONVIDA as autoridades competentes, como o Organismo dos Reguladores Europeus das Comunicações Eletrónicas (ORECE), a Agência da União Europeia para a Cibersegurança (ENISA) e o Grupo de Cooperação para a Segurança das Redes e da Informação (SRI) a, juntamente com a Comissão Europeia, formularem, com base numa avaliação dos riscos, recomendações destinadas aos Estados-Membros e à Comissão Europeia, a fim de reforçar a resiliência das redes e das infraestruturas de comunicações na União Europeia, incluindo a continuação da aplicação do instrumentário da UE para a segurança das redes 5G.

6. EXORTA a UE e os seus Estados-Membros a redobrarem de esforços para aumentar o nível global de cibersegurança, por exemplo facilitando a emergência de prestadores fiáveis de serviços de cibersegurança, e FRISA que o incentivo ao desenvolvimento desses prestadores deverá constituir uma prioridade da política industrial da UE no domínio da cibersegurança. A fim de resistir e combater melhor os ciberataques com potenciais efeitos sistémicos, e retirados os ensinamentos da gestão das vulnerabilidades do Solarwinds, Microsoft Exchange e Apache Log4J, CONVIDA a Comissão a propor opções para incentivar a emergência de um setor de serviços fiáveis de cibersegurança, reforçar a cibersegurança da cadeia de abastecimento das TIC, obviar aos potenciais efeitos das vulnerabilidades do software para a UE e os seus Estados-Membros, nomeadamente tendo em vista a futura legislação relativa à ciberresiliência, bem como melhorar as capacidades de deteção e partilha de ciberameaças nos Estados-Membros e entre eles.

7. REITERANDO que investir na inovação e utilizar melhor a tecnologia civil é fundamental para reforçar a nossa soberania tecnológica, nomeadamente no domínio do ciberespaço, APELA à Comissão para que operacionalize rapidamente o Centro Europeu de Competências em Cibersegurança para desenvolver um ecossistema europeu sólido nos setores da investigação, da indústria e da tecnologia em matéria de ciberespaço, SUBLINHA a necessidade de impulsionar a investigação e a inovação, investir mais em domínios civis e de defesa para reforçar a base industrial e tecnológica da UE no domínio da defesa (BITDE) e desenvolver as cibercapacidades da UE e dos seus Estados-Membros, nomeadamente capacidades de apoio estratégico. DESTACA a importância da utilização intensiva de novas tecnologias, nomeadamente nos domínios da computação quântica, da inteligência artificial e dos megadados, a fim de obter vantagens comparativas, inclusive em termos de operações de resposta aos ciberincidentes.

8. RECONHECENDO que o reforço da nossa cibersegurança é uma forma de aumentar a eficácia e a segurança dos nossos esforços em terra, no ar, no mar e no espaço exterior, SALIENTA a importância de integrar as considerações de cibersegurança em todas as políticas públicas da UE, incluindo a legislação setorial que complemente a Diretiva SRI 2, e CONVIDA a Comissão a explorar opções para aumentar a cibersegurança em toda a cadeia de abastecimento da base industrial e tecnológica da UE no domínio da defesa (BITDE).

9. RECONHECE que assegurar a atribuição de recursos financeiros e humanos adequados à cibersegurança e tomar medidas destinadas a criar um ambiente propício à competitividade do setor privado são essenciais para desenvolver a postura da UE no ciberespaço e que a questão do financiamento estável e a longo prazo da cibersegurança também deverá ser abordada a nível da UE através da conceção e aplicação de um mecanismo horizontal que combine múltiplas fontes de financiamento, incluindo o custo de recursos humanos altamente qualificados. Por conseguinte, APELA a que Comissão explore opções quanto a um mecanismo desse tipo antes do final de 2022, para análise nas instâncias competentes do Conselho.

10. SALIENTA a necessidade de intensificarmos os nossos esforços e de reforçarmos a cooperação na luta contra a cibercriminalidade internacional, em especial a que recorre a programas sequestradores, através do mecanismo da EMPACT (Plataforma Multidisciplinar Europeia contra as Ameaças Criminosas), através de intercâmbios entre os setores da cibersegurança, da aplicação da lei e da diplomacia, e ainda através do reforço das capacidades de aplicação da lei na investigação e ação penal contra a cibercriminalidade. REITERA o seu compromisso de informar o público sobre as ciberameaças e as medidas tomadas a nível nacional e da UE contra tais ameaças, envolvendo a sociedade civil, o setor privado e o meio académico, a fim de aumentar a sensibilização e incentivar um nível adequado de ciberproteção e ciber-higiene. SALIENTA a necessidade de concentrar a atenção nas competências e capacidades dos cidadãos em matéria de cibersegurança a nível da UE e dos Estados-Membros, bem como a necessidade de envolver ativamente os utilizadores na sua própria proteção.

II. REFORÇAR A GESTÃO SOLIDÁRIA E ABRANGENTE DE CRISES

11. Com base nos exercícios anuais de cibersegurança, noutros exercícios que envolvam uma ciberdimensão e no exercício de gestão de cibercrises de 2022 (EU CyCLES), SALIENTA a importância de estabelecer um programa de exercícios regulares de cibersegurança intercomunitários e a vários níveis, a fim de testar e desenvolver a resposta interna e externa da UE a ciberincidentes em grande escala, com a participação do Conselho, do SEAE, da Comissão e de partes interessadas como a ENISA e o setor privado, programa esse que será articulado e contribuirá para a política global da UE em matéria de exercícios. SALIENTA a importância de continuar a desenvolver os exercícios Cyber Europe e BlueOLEx, combinando respostas a diferentes níveis. RECONHECE a necessidade de avaliar e consolidar os exercícios existentes e de explorar a possibilidade de haver novos exercícios em segmentos específicos no domínio do ciberespaço, nomeadamente um exercício militar das CERT e um exercício centrado na cooperação em situações de crise entre as EUIBA. RECONHECE que a postura da UE no ciberespaço reforçará a nossa capacidade para prevenir ciberataques através de várias ações, incluindo no domínio da formação, e, por conseguinte, CONVIDA os Estados-Membros a reforçarem a cooperação civil-militar na formação em cibersegurança e exercícios conjuntos.

12. SUBLINHA a necessidade de continuar a testar e reforçar a cooperação operacional e o conhecimento situacional comum entre os Estados-Membros, nomeadamente através de redes estabelecidas, como a rede de CSIRT e a Rede de Organizações de Coordenação de Cibercrises (EU CyCLONe), a fim de fazer avançar o grau de preparação da UE para enfrentar ciberincidentes em grande escala. SUBLINHA a importância de trabalhar no desenvolvimento de uma linguagem comum entre os Estados-Membros e com as EUIBA, que seja especificamente adaptada ao debate a nível político, a fim de apoiar a elaboração de uma avaliação consolidada da gravidade e do impacto dos ciberincidentes relevantes, bem como de eventuais cenários de evolução e das necessidades deles decorrentes, conforme adequado. SUBLINHA, a este respeito, a necessidade de melhorar a complementaridade dos relatórios partilhados de avaliação da situação, incluindo os relatórios da EU CyCLONe sobre o impacto e a gravidade dos ciberincidentes em grande escala nos Estados-Membros e as avaliações de ameaças fornecidas pelo INTCEN no âmbito do conjunto de instrumentos de ciberdiplomacia da UE. CONVIDA a Comissão, o alto representante e o grupo de cooperação SRI a, em coordenação com os organismos e agências civis e militares competentes, bem como as redes já estabelecidas, nomeadamente o EU CyCLONe, procederem, até ao final de 2022, a uma avaliação dos riscos e a criarem cenários de risco de uma perspetiva de cibersegurança numa situação de ameaça ou possível ataque contra Estados-Membros ou países parceiros e a apresentá-los às instâncias competentes do Conselho. SALIENTA a necessidade de uma comunicação pública adequada e coordenada sobre a resposta da UE a ciberincidentes em grande escala.

13. Em caso de ciberincidente em grande escala, SALIENTA a necessidade de reforçar a coordenação e, se for caso disso, com base nos progressos alcançados e no trabalho realizado pelas Equipas de resposta rápida a ciberataques no âmbito da CEP e a partir do trabalho da rede CSIRT e da EU CyCLONe, a mutualização voluntária das nossas capacidades de resposta a incidentes entre os Estados-Membros. RECONHECE que o desenvolvimento de laços com o setor privado poderá ser um amplificador das capacidades públicas, em especial num contexto de escassez de competências em toda a UE, e que a identificação e coordenação destes parceiros privados poderá ser determinante em caso de incidentes em grande escala. A fim de assegurar a plena preparação para enfrentar ciberincidentes em grande escala, CONVIDA a Comissão a apresentar uma proposta relativa a um novo Fundo de Resposta de Emergência para a Cibersegurança até ao final do terceiro trimestre de 2022.

14. Em conformidade com a Bússola Estratégica, REITERA a necessidade de investirmos na nossa assistência mútua, em conformidade com o artigo 42.º, n.º 7, do Tratado da União Europeia, bem como na solidariedade, em conformidade com o artigo 222.º do Tratado sobre o Funcionamento da União Europeia, em especial através de exercícios frequentes. Neste contexto, SALIENTA a necessidade de continuar a trabalhar na prestação e coordenação do apoio bilateral civil e/ou militar, nomeadamente explorando o eventual apoio prestado pela UE a pedido expresso dos Estados-Membros, e na identificação de medidas de resposta adequadas, nomeadamente através do desenvolvimento de uma estratégia de comunicação coordenada, no contexto da aplicação do artigo 42.º, n.º 7. OBSERVA que tal deve passar também pela exploração das ligações com os atuais mecanismos de gestão de crises da UE e o Mecanismo de Proteção Civil da UE.

15. SUBLINHA que o reforço da postura da UE no ciberespaço exigirá um reforço da segurança das comunicações. Para o efeito, REITERA as orientações dadas pela Bússola Estratégica a este respeito e CONVIDA a Comissão e outras instituições, órgãos e organismos competentes a levarem a cabo, até ao final de 2022, um levantamento dos instrumentos existentes para uma comunicação segura no domínio do ciberespaço, a ser analisado nas instâncias competentes do Conselho e com os grupos de cooperação pertinentes, nomeadamente a rede CSIRT e a EU CyCLONe.

III. PROMOVER A NOSSA VISÃO DO CIBERESPAÇO

16. RECORDA que a abordagem comum e abrangente da UE em matéria de ciberdiplomacia visa contribuir para a prevenção de conflitos, a atenuação das ameaças à cibersegurança e uma maior estabilidade nas relações internacionais. Neste contexto, REAFIRMA o empenho da UE na resolução de litígios internacionais no ciberespaço por meios pacíficos e na aplicação do direito internacional às ações dos Estados no ciberespaço, nomeadamente do direito internacional em matéria direitos humanos e do direito internacional humanitário. SUBLINHA o compromisso da UE e dos seus Estados-Membros de agirem em conformidade com as normas voluntárias e não vinculativas do comportamento responsável dos Estados no ciberespaço acordadas por todos os Estados membros das Nações Unidas. SALIENTA a importância de um ciberespaço aberto, livre, mundial, estável e seguro, em que os direitos humanos, as liberdades fundamentais e o Estado de direito sejam inteiramente aplicados a favor do bem-estar social, do crescimento económico, da prosperidade e da integridade das nossas sociedades livres e democráticas, e REAFIRMA o compromisso da UE e dos seus Estados-Membros de continuarem a promover esses valores e princípios. A fim de criar canais para um diálogo construtivo, franco e aberto com as principais partes interessadas no domínio do ciberespaço, SALIENTA a importância de tornar as questões do ciberespaço, incluindo o conjunto de instrumentos de ciberdiplomacia da UE, parte integrante das negociações de adesão à UE e dos diálogos estratégicos e políticos da UE tanto com parceiros internacionais como com concorrentes, e, ao mesmo tempo, APELA ao alto representante para que reveja os diálogos bilaterais existentes em matéria de ciberdiplomacia e, se necessário, proponha iniciar uma cooperação semelhante com outros países ou organizações internacionais pertinentes.

17. RECORDA a importância de que se reveste a cooperação multilateral, uma vez que há outras partes interessadas que são igualmente responsáveis pela cibersegurança, nomeadamente no que diz respeito à aplicação das recomendações e decisões tomadas nas instâncias internacionais e regionais. INSTA a UE e os seus Estados-Membros a continuarem a promover o nosso modelo de ciberespaço e Internet com base na abordagem multilateral e através de iniciativas como o Apelo de Paris à Confiança e à Segurança no Ciberespaço e a Declaração sobre o Futuro da Internet, salientando os benefícios comuns da estabilidade no ciberespaço e aumentando a sensibilização a nível mundial para os perigos de uma visão da Internet centrada no Estado e autoritária, e APELA à UE e aos seus Estados-Membros para que continuem a reforçar a cooperação com a comunidade multilateral, nomeadamente através do recurso a projetos pertinentes, como a Iniciativa da UE para a Ciberdiplomacia no quadro do Instrumento de Política Externa da UE.

18. ASSUME O COMPROMISSO de se empenhar continuamente nas organizações internacionais competentes, sobretudo nos processos relacionados com a Primeira e Terceira Comissão das Nações Unidas, salientando ao mesmo tempo que o direito internacional em vigor é aplicável, sem reservas, no ciberespaço e relativamente a este. SALIENTA a importância de prosseguir os esforços para defender e promover o quadro das Nações Unidas para um comportamento responsável dos Estados e SUBLINHA que a UE e os seus Estados-Membros trabalharão ativamente no sentido de reforçar a sua aplicação, nomeadamente através da criação do Programa de Ação para promover o comportamento responsável dos Estados no ciberespaço. SALIENTA que a UE e os seus Estados-Membros participarão ativamente nas negociações para uma futura Convenção das Nações Unidas que constitua um instrumento eficaz para as autoridades policiais e judiciais na luta mundial contra a cibercriminalidade, tendo plenamente em conta o quadro existente de instrumentos internacionais e regionais neste domínio, em particular a Convenção de Budapeste sobre o Cibercrime. DESTACA a importância de continuar a apoiar a elaboração e a operacionalização de medidas geradoras de confiança (MGC) a nível regional e internacional e de continuar a incentivar o recurso às MGC vigentes no domínio do ciberespaço na OSCE, nomeadamente em tempos de tensões internacionais.

19. RECORDA que adotar uma abordagem proativa baseada nos direitos humanos que assegure a existência de normas internacionais nos domínios das tecnologias emergentes e da arquitetura fundamental da Internet, em consonância com os valores e princípios democráticos, é essencial para que a Internet continue a ser mundial, não fragmentada e aberta, e APOIA o princípio de que a utilização e o desenvolvimento de tecnologias respeitam os direitos humanos e se centram na privacidade, e de que o seu uso é lícito, seguro e ético. INCENTIVA o alto representante e a Comissão a desenvolverem uma visão estratégica sobre questões técnicas no domínio digital que tenham implicações em matéria de política externa e possam ter impacto na estabilidade do ciberespaço e da Internet em particular, nomeadamente nas organizações internacionais especializadas competentes (União Internacional das Telecomunicações, etc.).

IV. REFORÇAR A COOPERAÇÃO COM PAÍSES TERCEIROS E ORGANIZAÇÕES INTERNACIONAIS

20. SALIENTA a necessidade de estabelecer uma melhor ligação entre a estratégia de reforço das cibercapacidades da UE e as normas das Nações Unidas em matéria de comportamento responsável dos Estados no ciberespaço, nomeadamente através do desenvolvimento de programas de cooperação e reforço de capacidades específicos para apoiar os países terceiros nos seus esforços de execução e, ao fazê-lo, prosseguir e expandir os nossos esforços para impulsionar o Programa de Ação das Nações Unidas para promover o comportamento responsável dos Estados no ciberespaço. DESTACA a importância de integrar plenamente o reforço das cibercapacidades como parte da oferta da UE enquanto garante da segurança, com uma coordenação adequada dos esforços entre os Estados-Membros e as instituições, órgãos e organismos da UE, e, em especial, CONGRATULA-SE com a cooperação entre os Estados-Membros, bem como com os parceiros dos setores público e privado, nomeadamente através da EU CyberNet (rede da UE de reforço das cibercapacidade) e do Fórum Global de Cibercompetências (GFCE), a fim de assegurar a coordenação e evitar duplicações de esforços.

EXORTA o alto representante e a Comissão a criarem um *comité de reforço das cibercapacidades da UE* até ao terceiro trimestre de 2022 e a procederem a intercâmbios regulares no âmbito do Grupo Horizontal das Questões do Ciberespaço. EXORTA a Comissão e o alto representante a mobilizarem ainda mais o Instrumento de Vizinhança, de Cooperação para o Desenvolvimento e de Cooperação Internacional (IVCDCI), o Instrumento de Assistência de Pré-adesão (IPA III) e outros instrumentos financeiros, como o Mecanismo Europeu de Apoio à Paz (MEAP) e a Iniciativa Gateway Global, a fim de apoiar o reforço da resiliência dos nossos parceiros, a sua capacidade para identificarem e fazerem face às ciberameaças e para investigarem e moverem ações penais por cibercrimes, bem como o

desenvolvimento de projetos de cooperação, incluindo no contexto de crises, INCENTIVA a cooperação com os parceiros dos Balcãs Ocidentais e da Vizinhança Oriental e Meridional da UE, bem como o destacamento de peritos da UE e dos Estados-Membros para prestar apoio em cibercrises, tendo em conta os mandatos jurídicos existentes.

21. SALIENTA a necessidade de intensificar esforços para desenvolver uma abordagem estruturada e aberta de sensibilização da UE quanto à forma de promover um entendimento comum a nível mundial da aplicação do direito internacional no ciberespaço, o quadro das Nações Unidas para um comportamento responsável dos Estados no ciberespaço, incluindo a iniciativa relativa a um Programa de Ação das Nações Unidas para promover o comportamento responsável dos Estados no ciberespaço, bem como quanto à posição da UE e dos seus Estados-Membros nas negociações em curso para a celebração de uma Convenção das Nações Unidas sobre o Cibercrime, e, no âmbito destes esforços, SOLICITA ao alto representante que apresente ao Conselho um plano de sensibilização até ao final de 2022. INCENTIVA o alto representante e os serviços da Comissão a recorrerem plena e sistematicamente às 145 delegações e a desenvolverem uma colaboração regular e frutuosa entre estas e as embaixadas dos Estados-Membros nos países terceiros, sob os auspícios da prevista rede da UE em matéria de ciberdiplomacia. INSTA o alto representante a criar, até ao terceiro trimestre de 2022, a rede da UE em matéria de ciberdiplomacia, que contribua para o intercâmbio de informações, atividades de formação conjuntas para o pessoal da UE e dos Estados-Membros, esforços coerentes em matéria de reforço das capacidades e a consolidação da aplicação do quadro das Nações Unidas para um comportamento responsável dos Estados, bem como para medidas geradoras de confiança entre os Estados.

22. SUBLINHA o seu empenho em continuar a cooperar com as organizações internacionais e os países parceiros a fim de propiciar uma compreensão partilhada do cenário de ameaças, desenvolver mecanismos de cooperação e identificar, de forma proativa, respostas diplomáticas em colaboração. RECORDANDO as principais conquistas alcançadas graças à cooperação UE-OTAN no domínio da cibersegurança com a aplicação das Declarações Conjuntas de Varsóvia, em 2016, e de Bruxelas, em 2018, no pleno respeito da autonomia e dos procedimentos decisórios de ambas as organizações e com base nos princípios da transparência, da reciprocidade e da inclusividade, SALIENTA a necessidade de continuar a reforçar a cooperação cibernética com a OTAN através de exercícios, partilha de informações e intercâmbios entre peritos, nomeadamente no que toca ao desenvolvimento de capacidades, ao reforço das capacidades dos parceiros e às missões e operações, bem como à aplicabilidade do direito internacional e das normas das Nações Unidas em matéria de comportamento responsável dos Estados no ciberespaço e eventuais respostas coordenadas a ciberatividades maliciosas.

V. PREVENIR OS CIBERATAQUES, DEFENDER-SE E DAR-LHES RESPOSTA

23. RECONHECE que o ciberespaço se transformou num palco de concorrência geopolítica e, por isso, REITERA que a UE tem de ser capaz de reagir com rapidez e determinação aos ciberataques, tais como as ciberatividades mal intencionadas patrocinadas por Estados, dirigidos contra a UE e os seus Estados-Membros, pelo que deve reforçar o instrumentário de ciberdiplomacia da UE e tirar pleno partido de todos os meios ao seu dispor, incluindo os instrumentos políticos, económicos, diplomáticos, jurídicos e de comunicação estratégica disponíveis para prevenir, desencorajar, dissuadir e responder a ciberatividades mal intencionadas. SUBLINHA que os intervenientes hostis devem estar cientes de que os ciberataques contra os Estados-Membros e as instituições da UE serão detetados logo de início, rapidamente identificados e tratados com todos os instrumentos e políticas necessárias para lhes dar resposta. Com base, nomeadamente, nos elementos da postura no ciberespaço deles constantes e nos ensinamentos retirados da aplicação do instrumentário de ciberdiplomacia desde a sua criação, assim como do exercício de gestão de cibercrises (EU CyCLES), CONVIDA os Estados-Membros e o alto representante a, com o apoio da Comissão, envidarem esforços para apresentar até ao final do primeiro trimestre de 2023 uma versão revista das orientações de execução do instrumentário de ciberdiplomacia da UE, para a elaboração da qual deverão ser estudadas, nomeadamente, medidas suplementares de resposta.

24. SUBLINHA a necessidade de realizar intercâmbios regulares sobre o panorama das ciberameaças nos órgãos e comités competentes do Conselho, colaborando também regularmente com o setor privado e tendo em conta as conclusões da avaliação do impacto e da gravidade dos incidentes recentes, a fim de aumentar de uma forma global a sensibilização e o grau de preparação para novas aplicações do instrumentário de ciberdiplomacia da UE, e de desenvolver novas ferramentas para apoiar a sua execução. Embora a segurança nacional continue a ser da exclusiva responsabilidade de cada Estado-Membro, OBSERVA que é necessário reforçar a partilha de dados e de informações e a cooperação entre os Estados-Membros, bem como com o Centro de Situação e de Informações da UE (INTCEN), a fim de poder trocar informações no início do processo de decisão, nomeadamente sobre a questão da atribuição da responsabilidade, permitindo assim uma resposta rápida, eficaz e fundamentada às ciberatividades mal intencionadas dirigidas contra a UE e os seus parceiros. REITERA a importância de reforçar a capacidade do INTCEN no domínio do ciberespaço, com base em contributos voluntários dos Estados-Membros em matéria de informações e sem prejuízo das suas competências, e de estudar a proposta sobre a eventual criação de um grupo de trabalho dos Estados-Membros dedicado às ciberinformações.

25. RECONHECENDO que as declarações da UE e as medidas restritivas tomadas no quadro do instrumentário de ciberdiplomacia da UE emitiram uma firme mensagem de que são inaceitáveis as ciberatividades mal intencionadas que ameacem do exterior a UE, os seus Estados-Membros e os seus parceiros, o que contribui para prevenir, desencorajar, dissuadir e responder a ciberatividades mal intencionadas, REITERA o seu compromisso de recorrer a estas medidas para recordar as obrigações aplicáveis ao ciberespaço nos termos do direito internacional, incluindo da Carta das Nações Unidas na sua integralidade, e de promover o quadro das Nações Unidas para um comportamento responsável dos Estados no ciberespaço, nomeadamente a obrigação da devida diligência que todos os Estados devem fazer para não permitirem conscientemente que o seu território seja utilizado para a prática de atividades mal intencionadas com recurso às TIC, tendo em vista desenvolver e promover a visão partilhada na UE sobre a aplicação do direito internacional no ciberespaço. REGISTANDO que as mensagens rápidas e adequadas reduzem os riscos de escalada e podem desencorajar os agressores que visem interesses europeus, CONVIDA o alto representante a elaborar e apresentar aos Estados-Membros uma estratégia de comunicação coerente sobre a utilização do instrumentário de ciberdiplomacia da UE.

26. INCENTIVA o desenvolvimento de abordagens e respostas graduais, específicas e sustentadas às ciberatividades mal intencionadas, tirando partido da vasta gama de instrumentos proporcionados pelo instrumentário de ciberdiplomacia da UE, incluindo o regimes de cibersanções da UE, e prevendo medidas adicionais. SALIENTA a necessidade de aumentar a possibilidade de mobilizar, caso a caso, todos os instrumentos disponíveis, internos e externos, para prevenir, desencorajar, dissuadir e responder a ciberataques, implementando-os de forma rápida, eficaz, gradual, específica e sustentada, tendo por base um compromisso estratégico a longo prazo. INSTA o alto representante a, em colaboração com a Comissão, identificar possíveis respostas conjuntas da UE aos ciberataques, em todos os setores, inclusive a nível de sanções, a fim de que a UE esteja preparada para, sempre que necessário, tomar rapidamente medidas eficazes e a apresentar essas respostas ao Conselho até ao final do primeiro trimestre de 2023.

27. REGISTANDO que a ciberdefesa se insere principalmente na esfera da responsabilidade nacional, INCENTIVA os Estados-Membros a que continuem a desenvolver as suas próprias capacidades para levar a cabo operações de ciberdefesa, incluindo medidas pró-ativas para proteger, detetar, defender e dissuadir os ciberataques e, eventualmente, apoiar outros Estados-Membros e a UE. Todos os Estados-Membros são encorajados a reforçar, na medida do necessário, as suas próprias capacidades para prestar e receber assistência. SALIENTA que o desenvolvimento destas capacidades deverá ser um dos principais objetivos da futura política de ciberdefesa da UE. OBSERVA que a política de ciberdefesa da UE deverá prestar mais atenção ao papel que as instituições e organismos competentes da UE podem desempenhar para que haja uma maior cooperação entre os intervenientes da UE e dos Estados-Membros relevantes no domínio da ciberdefesa e um fortalecimento das suas próprias capacidades, de acordo com os respetivos mandatos. CONVIDA o alto representante a, juntamente com a Comissão, complementar o desenvolvimento da postura da UE no ciberespaço, apresentando para o efeito, em 2022, uma proposta ambiciosa de política de ciberdefesa da UE, abrindo assim caminho para que o Conselho continue a desenvolver a referida postura.

28. SALIENTA que é necessário aumentar a interoperabilidade e a partilha de informações através da cooperação entre equipas militares de resposta a emergências informáticas (milCERT). CONVIDA os Estados-Membros a, dando continuidade ao trabalho da AED, criarem uma rede milCERT para fomentar a cooperação e facilitar o intercâmbio de informações, o que também contribuiria para promover a coordenação com outras cibercomunidades, bem como uma rede de cibercomandantes militares, a fim de reforçar a cooperação estratégica entre os cibercomandantes dos Estados-Membros da UE ou outras autoridades congéneres. A criação destas redes, juntamente com os ciberprojetos da CEP, contribuiria para reforçar a ciberdefesa a nível da UE. Salienta a importância da cooperação entre a rede milCERT proposta e a rede de equipas de resposta a incidentes de segurança informática (CSIRT) já existente, a fim de reforçar a partilha de informações e melhorar o conhecimento da situação.

29. Com base na Visão e Estratégia Militar da UE para o Ciberespaço como Domínio da Atividade, e tomando nota da atual evolução do conceito para a ciberdefesa nas operações e missões militares lideradas pela UE, REITERA a necessidade de integrar a dimensão cibernética no planeamento e condução das missões e operações da PCSD, nomeadamente através do reforço das suas cibercapacidades, e SALIENTA que tal contribuirá para um melhor conhecimento da situação nessa matéria a nível da UE.

30. Para concluir, REGISTA que a postura no ciberespaço representará um passo no sentido da definição de uma doutrina da UE para a ação no ciberespaço, baseada no reforço da resiliência, das capacidades e das opções de resposta, bem como numa posição comum sobre a aplicação do direito internacional no ciberespaço. Em 2023, o Conselho FARÁ UM BALANÇO dos progressos realizados na aplicação das presentes conclusões, a fim de assegurar a continuação do desenvolvimento da postura da UE no ciberespaço.