Conselho da
União Europeia

Bruxelas, 23 de março de 2021
(OR. en)

7290/21

CYBER 80
TELECOM 124
COPEN 144
CODEC 443
COPS 107
COSI 50
CSC 119
CSCI 45
IND 70
RECH 117
ESPACE 21

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	22 de março de 2021
para:	Delegações
Assunto:	Conclusões do Conselho sobre a Estratégia de Cibersegurança da UE para a década digital – Conclusões do Conselho aprovadas pelo Conselho na sua reunião de 22 de março de 2021

Junto se enviam, à atenção das delegações, as Conclusões do Conselho sobre a Estratégia de Cibersegurança da UE para a década digital, aprovadas pelo Conselho na sua reunião de 22 de março de 2021.

ANEXO

Conclusões do Conselho
sobre a Estratégia de Cibersegurança da UE para a década digital

O CONSELHO DA UNIÃO EUROPEIA,

Recordando as suas conclusões sobre:

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

– a governação da Internet[2],

– a comunicação conjunta ao Parlamento Europeu e ao Conselho intitulada: "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE"[3], de 20 de novembro de 2017,

– o desenvolvimento de capacidades e competências em matéria de cibersegurança na UE[4],

– a importância da tecnologia 5G para a economia europeia e a necessidade de atenuar os riscos de segurança a ela associados[5],

– o futuro de uma Europa altamente digitalizada para além de 2020: "Impulsionar a competitividade digital e económica na União e a coesão digital"[6],

– os esforços complementares para aumentar a resiliência e combater as ameaças híbridas[7],

– "Construir o futuro digital da Europa"[8],

---

1 12109/13
2 16200/14
3 14435/17 + COR 1
4 7737/19
5 14517/19
6 9596/19
7 14972/19
8 8711/20

– a diplomacia digital[9],

– o reforço da resiliência e a luta contra as ameaças híbridas, incluindo a desinformação no contexto da pandemia de COVID-19[10],

– a ciberdiplomacia[11],

– a resposta coordenada da UE a incidentes e crises de cibersegurança de grande escala[12],

– um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas ("instrumentos de ciberdiplomacia")[13],

– as diretrizes da UE para o reforço das cibercapacidades externas[14],

– uma recuperação que promova a transição para uma indústria europeia mais dinâmica, resiliente e competitiva[15],

– a cibersegurança dos dispositivos conectados[16],

– o reforço do sistema de ciberresiliência da Europa e a promoção der uma indústria de cibersegurança competitiva e inovadora[17],

– a sua resolução sobre encriptação – Segurança através da encriptação e segurança apesar da encriptação[18],

---

9 12804/20
10 14064/20
11 6122/15 + COR 1
12 10086/18
13 10474/17
14 10496/18
15 13004/20
16 13629/20
17 14540/16
18 13084/1/20 REV 1

– e a declaração dos Estados-Membros, de 15 de outubro de 2020, intitulada "Construir a computação em nuvem da próxima geração para as empresas e o setor público na UE",

RECORDANDO as conclusões do Conselho Europeu sobre a COVID-19, o mercado único, a política industrial e a digitalização e as relações externas, de 1 e 2 de outubro de 2020[19], e sobre desinformação e ameaças híbridas e uma nova agenda estratégica para 2019-2024, de 20 de junho de 2019[20],

TENDO EM CONTA a "Estratégia global para a política externa e de segurança da União Europeia – Visão partilhada, ação comum: uma Europa mais forte", de 28 de junho de 2016,

RECORDANDO as comunicações da Comissão Europeia intituladas "Construir o futuro digital da Europa", de 19 de dezembro de 2020[21], e "a Estratégia da UE para a União da Segurança", de 24 de julho de 2020[22],

RECORDANDO a comunicação conjunta da Comissão Europeia e do alto representante intitulada "Uma nova agenda UE-EUA para uma mudança a nível mundial", de 2 de dezembro de 2020[23],

1. SALIENTA que a cibersegurança é essencial para construir uma Europa resiliente, ecológica e digital e CONGRATULA-SE com a comunicação conjunta ao Parlamento Europeu e ao Conselho intitulada "Estratégia de cibersegurança da UE para a década digital", que define o novo quadro para a ação da UE no domínio da "resiliência, soberania tecnológica e liderança", de forma a proteger os seus cidadãos, empresas e instituições de incidentes e ameaças no domínio do ciberespaço, reforçando simultaneamente a confiança dos indivíduos e das organizações na capacidade da UE para promover a segurança e a fiabilidade das redes e sistemas de informação, das infraestruturas e da conectividade, e para promover e proteger um ciberespaço global, aberto, livre, estável e seguro, alicerçado nos direitos humanos, nas liberdades fundamentais, na democracia e no Estado de direito.

---

19 EUCO 13/20
20 EUCO 9/19
21 COM(2020) 67 final, de 19.2.2020
22 COM(2020) 605 final, de 24.7.2020
23 JOIN(2020) 22 final, de 2.12.2020

2. RECONHECE que a pandemia de COVID-19 fez com que a necessidade crescente de confiança nas ferramentas e sistemas das tecnologias da informação e comunicação (TIC) e a sua segurança se tornassem essenciais na nossa vida quotidiana. SALIENTA que a cibersegurança e a Internet global e aberta são vitais para o funcionamento da administração pública e das instituições, tanto a nível nacional como da UE, bem como para a nossa sociedade e a economia no seu todo.

3. REALÇA a necessidade de aumentar a sensibilização para as questões do ciberespaço a nível da decisão política e estratégica, facultando conhecimentos e informações pertinentes aos decisores, e SUBLINHA que é imperativo sensibilizar mais o público em geral e promover a ciber-higiene.

4. APELA à promoção e proteção dos valores fundamentais da UE como a democracia, o Estado de direito, os direitos humanos e as liberdades fundamentais, incluindo o direito à liberdade de expressão e de informação, o direito à liberdade de reunião e de associação e o direito à privacidade no ciberespaço. CONGRATULA-SE, a este respeito, com os esforços sustentados para proteger os defensores dos direitos humanos, a sociedade civil e o mundo académico, focando-se em questões como a cibersegurança, a privacidade dos dados, a vigilância e a censura em linha, traçando novas orientações práticas, promovendo boas práticas e intensificando os esforços da UE para prevenir violações e atropelos dos direitos humanos e a utilização indevida de tecnologias emergentes, recorrendo inclusive, sempre que necessário, a medidas diplomáticas e controlando as exportações dessas tecnologias. DESTACA, neste contexto, a importância do Plano de Ação da UE para os Direitos Humanos e a Democracia 2020-2024 e das suas diretrizes em matéria de direitos humanos relativas à liberdade de expressão em linha e fora de linha.

5. SALIENTA que um dos objetivos fundamentais da União é alcançar a autonomia estratégica, preservando ao mesmo tempo uma economia aberta que lhe permita autodeterminar a sua trajetória e os seus interesses económicos. Passa isso por reforçar a capacidade de fazer escolhas autónomas no domínio da cibersegurança, com o objetivo de consolidar a liderança digital da UE e as suas capacidades estratégicas. RECORDA que tal implica também identificar e reduzir as dependências estratégicas e aumentar a resiliência nos ecossistemas industriais e domínios específicos mais sensíveis. SUBLINHA que esse processo pode consistir em diversificar as cadeias de produção e abastecimento, promover e atrair investimentos e a produção na Europa, estudar soluções alternativas e modelos circulares e fomentar uma ampla cooperação industrial entre os Estados-Membros.

6. Tendo em conta a escassez de competências digitais e de cibersegurança entre a população ativa, SALIENTA a importância de satisfazer a procura de mão de obra formada no domínio digital e da cibersegurança, em particular desenvolvendo, conservando e atraindo os melhores talentos, por exemplo através do ensino e da formação, a fim de poder digitalizar a nossa sociedade de forma cibersegura. INCENTIVA o aumento da participação das mulheres e das raparigas no ensino da ciência, tecnologia, engenharia e matemática ("CTEM") e na melhoria e requalificação das competências digitais do emprego no setor das TIC como um dos meios para colmatar o fosso digital entre homens e mulheres.

7. 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 seu empenho na resolução de litígios internacionais no ciberespaço por meios pacíficos e a necessidade de todos os esforços diplomáticos da UE terem como prioridade a promoção da segurança e da estabilidade no ciberespaço através de uma maior cooperação internacional, bem como a redução do risco de mal-entendidos, de escalada e de conflito que possam resultar de incidentes no domínio das TIC, e APOIA o desenvolvimento e a operacionalização de medidas geradoras de confiança a nível regional e internacional. REITERA o apelo lançado pela Assembleia Geral das Nações Unidas, acordado por consenso, a que os Estados membros das Nações Unidas se inspirem nas recomendações dos relatórios do GPG ao utilizarem as TIC e REAFIRMA que o direito internacional, em particular a Carta das Nações Unidas na sua integralidade, se aplicam também ao ciberespaço.

8. INSISTE em que, através de uma abordagem multilateral, é essencial continuar a desenvolver normas e padrões na União, a fim de adaptar consideravelmente as normas e padrões internacionais nos domínios das tecnologias emergentes e das infraestruturas técnicas e lógicas essenciais para a disponibilidade geral e a integridade do núcleo público da Internet, de modo a que estas sejam consentâneas com os valores universais e da UE. Tal assegurará que a Internet continua a ser global, aberta, livre, estável e segura e que a utilização e o desenvolvimento das tecnologias digitais respeitam os direitos humanos, sendo o seu uso lícito, seguro e ético. TOMA NOTA da futura estratégia de normalização e COMPROMETE-SE a adotar uma abordagem proativa e coordenada para promover a liderança da UE e os seus objetivos a nível internacional, nomeadamente em vários organismos internacionais de normalização e graças à cooperação estabelecida com parceiros que partilham as mesmas ideias, com a sociedade civil, o mundo académico e o setor privado.

9. APOIA FIRMEMENTE o modelo multilateral para a governação da Internet e a cibersegurança e compromete-se a intensificar em fóruns internacionais os intercâmbios regulares e estruturados com as partes interessadas, incluindo o setor privado, o meio académico e a sociedade civil, nomeadamente no contexto do Apelo de Paris à Confiança e à Segurança no Ciberespaço. PROMOVE o acesso universal, equitativo e a preços comportáveis à Internet com o objetivo de colmatar as clivagens digitais, fomentando, em particular, a emancipação das mulheres e raparigas e das pessoas em situações vulneráveis ou marginalizadas, tanto a nível do desenvolvimento de políticas como da utilização da Internet.

10. SALIENTA a necessidade de incluir a cibersegurança nos investimentos e iniciativas digitais nos próximos anos e de contribuir progressivamente para a criação de condições de concorrência equitativas neste domínio, REGISTANDO que a Comissão tenciona aumentar as despesas públicas e potenciar o investimento privado no domínio da cibersegurança. REALÇA a importância das pequenas e médias empresas (PME) no ecossistema de cibersegurança e RECONHECE a importância dos instrumentos financeiros disponíveis para apoiar uma forte ênfase na cibersegurança no âmbito da transformação digital operada durante o período abrangido pelo Quadro Financeiro Plurianual (QFP) 2021-2027 e, bem assim, do Mecanismo de Recuperação e Resiliência (MRR).

11. AGUARDA COM EXPECTATIVA a rápida aplicação do regulamento que institui o Centro Europeu de Competências Industriais, Tecnológicas e de Investigação em Cibersegurança e a Rede de Centros Nacionais de Coordenação, nomeadamente a rápida criação e operacionalização do Centro Europeu de Competências em Cibersegurança, em Bucareste. A rápida adoção da agenda contribuirá para tirar o máximo partido dos efeitos dos investimentos destinados a reforçar a liderança e a autonomia estratégica da União no domínio da cibersegurança, apoiar as capacidades e competências tecnológicas e aumentar a competitividade global da União, com o contributo da indústria e das comunidades académicas no domínio da cibersegurança, incluindo as PME e os centros de investigação, que beneficiarão de uma colaboração mais sistemática, inclusiva e estratégica que tenha em conta a coesão da União e de todos os seus Estados-Membros.

12. CONGRATULA-SE com os trabalhos que estão a ser conduzidos pela ENISA, juntamente com os Estados-Membros e as partes interessadas, para fornecer à UE sistemas de certificação de produtos, serviços e processos de TIC que contribuam para elevar o nível global de cibersegurança no mercado único digital. Neste contexto, AGUARDA COM EXPECTATIVA o programa de trabalho evolutivo da União com vista ao desenvolvimento de sistemas de certificação da cibersegurança da UE no âmbito do Regulamento Cibersegurança. RECONHECE, neste contexto, o papel central da UE no desenvolvimento de normas capazes de moldar o panorama de cibersegurança e contribuir para assegurar uma concorrência leal na UE e na cena mundial, promovendo o acesso ao mercado e procurando enfrentar os riscos em matéria de segurança, garantindo simultaneamente a aplicabilidade do quadro legislativo da UE.

13. REITERA a importância de avaliar a necessidade de dispor, a longo prazo, de legislação horizontal que especifique também as condições necessárias para a colocação no mercado, a fim de abordar todos os aspetos relevantes da cibersegurança dos dispositivos conectados, como a disponibilidade, a integridade e a confidencialidade. CONGRATULA-SE, a este respeito, com a realização de um debate destinado a explorar o âmbito de aplicação dessa legislação e as suas ligações ao quadro de certificação da cibersegurança, tal como definido no Regulamento Cibersegurança, com o objetivo de aumentar o nível de segurança no mercado único digital. SALIENTA que os requisitos em matéria de cibersegurança deverão ser definidos em conformidade com a legislação pertinente da União, nomeadamente o Regulamento Cibersegurança, o novo quadro legislativo, o regulamento relativo à normalização europeia e a eventual legislação horizontal futura, de modo a evitar ambiguidades e a fragmentação da legislação.

14. RECONHECE a importância de se seguir uma abordagem abrangente e horizontal no domínio da cibersegurança na União, respeitando plenamente as competências e necessidades dos Estados-Membros, e de se apoiar continuamente a assistência técnica e a cooperação em matéria de reforço das capacidades dos Estados-Membros. Tendo em conta a evolução do panorama das ciberameaças, TOMA NOTA da nova proposta de diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que tem por base a Diretiva SRI, e reitera o seu apoio ao reforço e harmonização dos quadros nacionais de cibersegurança e à cooperação sustentada entre Estados-Membros. Além disso, SALIENTA a necessidade de alinhar e articular a legislação setorial neste domínio.

15. TOMA NOTA da proposta apresentada pela Comissão no sentido de apoiar os Estados-Membros na criação e no reforço de centros de operações de segurança, a fim de implantar em toda a UE uma rede de centros destinada a continuar a acompanhar e a antecipar os sinais de ataques às redes. Neste contexto, AGUARDA que a Comissão apresente planos pormenorizados relativos à criação da rede de centros de operações de segurança respeitando simultaneamente as competências dos Estados-Membros. RECORDA os esforços envidados pelos Estados-Membros, com o apoio da UE, para criar equipas setoriais, nacionais e regionais de resposta a incidentes de segurança informática (CSIRT) e centros de partilha e análise de informações a nível nacional ou europeu, no âmbito de uma rede eficaz de parcerias em matéria de cibersegurança na União. AGUARDA COM EXPECTATIVA que se explore o potencial desta rede para reforçar os centros de operações de segurança, bem como a sua complementaridade e capacidade de coordenação com as redes e os intervenientes existentes (sobretudo a rede de CSIRT), a fim de promover uma cultura de partilha de informações eficiente, segura e fiável. SALIENTA que este processo terá por base o trabalho realizado, por um lado, no contexto das iniciativas respeitantes à inteligência artificial e à computação de alto desempenho e, por outro, pelos polos europeus de inovação digital.

16. TOMA NOTA do possível desenvolvimento de um sistema de conectividade seguro, com base na infraestrutura europeia de comunicação quântica (EuroQCI) e na comunicação governamental por satélite da União Europeia (GOVSATCOM), e RECONHECE que qualquer possível desenvolvimento futuro se deverá basear num quadro de cibersegurança sólido e ter em conta toda a infraestrutura de comunicações eletrónicas, como os sistemas de redes espaciais, terrestres e submarinas.

17. AGUARDA COM EXPECTATIVA os debates com a Comissão, a ENISA, os dois operadores de servidores de raiz DNS da UE e a comunidade multipartidária a fim de avaliar o papel destes operadores quando se trata de assegurar que a Internet continua a ser mundialmente acessível e não fragmentada. CONGRATULA-SE com a continuação do debate sobre a intenção da Comissão de desenvolver um serviço europeu alternativo de acesso à Internet mundial (iniciativa "DNS4EU") com base num modelo transparente conforme com as mais recentes normas e regras em matéria de segurança, proteção de dados e privacidade desde a conceção e por defeito, a fim de contribuir para uma maior resiliência, mantendo e reforçando simultaneamente a conectividade internacional para todos os Estados-Membros.

18. RECONHECE a necessidade de um esforço conjunto da Comissão e dos Estados-Membros para acelerar a adoção das normas fundamentais da Internet, incluindo o IPv6, e de reconhecidas normas de segurança, fundamentais para aumentar o nível global de segurança, resiliência, abertura e interoperabilidade da Internet mundial, reforçando simultaneamente a competitividade da indústria da UE e, em particular, a dos operadores de infraestruturas da Internet.

19. SALIENTA a importância de uma abordagem coordenada, bem como do desenvolvimento e da aplicação a nível nacional de medidas eficazes para reforçar a cibersegurança das redes 5G. APOIA as próximas medidas a tomar em matéria de cibersegurança das redes 5G, apresentadas no apêndice da Estratégia de Cibersegurança da UE com base nos resultados do relatório sobre os impactos da recomendação da Comissão na segurança das redes 5G, designadamente no que diz respeito à definição de uma abordagem abrangente de longo prazo que tenha em conta toda a cadeia de valor e o ecossistema 5G. Tendo em vista continuar a reforçar a abordagem coordenada em matéria de segurança das redes 5G, INSTA os Estados-Membros, as instituições da UE e outros intervenientes relevantes a continuarem a efetuar balanços periódicos e intercâmbios de informações e boas práticas no âmbito do grupo de cooperação SRI que se dedica à cibersegurança 5G, informando regularmente o Conselho dos progressos realizados. Sublinhando embora a responsabilidade dos Estados-Membros pela proteção da segurança nacional, SALIENTA o seu forte empenho em aplicar e concluir rapidamente a implementação do conjunto de instrumentos da UE para as redes 5G e em prosseguir os esforços envidados para garantir a segurança das redes 5G e o desenvolvimento das futuras gerações de redes. A estreita cooperação estabelecida entre os Estados-Membros, a Comissão e a ENISA em matéria de segurança das redes 5G poderá servir de exemplo para outras questões do domínio da cibersegurança, sem deixar de respeitar as competências dos Estados-Membros e os princípios da subsidiariedade e da proporcionalidade.

20. RECONHECE a importância de uma maior integração da cibersegurança nos mecanismos da UE de resposta a crises e de testar esses mecanismos praticando exercícios pertinentes e SALIENTA que importa reforçar a cooperação e a partilha de informações entre as várias cibercomunidades na UE e ligar as iniciativas, estruturas e procedimentos existentes (como o IPCR, a rede CSIRT, o grupo de cooperação SRI, a rede CyCLONe, o Centro Europeu da Cibercriminalidade, o INTCEN e outros organismos relevantes da UE) em caso de ciberincidentes e ameaças transfronteiras e de grande escala. TENDO EM CONTA os progressos já alcançados neste domínio, AGUARDA a proposta da Comissão sobre o processo, as principais etapas e o calendário para a definição da ciberunidade conjunta, a fim de proporcionar valor acrescentado traçar uma linha de rumo clara e racionalizar o quadro da UE em matéria de gestão de crises de cibersegurança, nomeadamente através da preparação e do conhecimento comum da situação, intensificando a coordenação da resposta e a prática de exercícios de forma transparente e gradual, evitando duplicações e sobreposições e respeitando as competências dos Estados-Membros.

21. SALIENTA, por um lado, a importância de promover a cooperação e o intercâmbio de informações entre os intervenientes relevantes no setor da cibersegurança e as autoridades competentes no domínio da segurança e da justiça penal, nomeadamente as autoridades policiais e judiciais, e, por outro, a necessidade de alargar e melhorar a capacidade destas autoridades para investigar e julgar cibercrimes, bem como de promover as negociações internacionais e as regras da UE em matéria de acesso transnacional a provas eletrónicas. Independentemente do ambiente tecnológico do momento, é essencial preservar os poderes das autoridades competentes no domínio da segurança e da justiça penal conferindo-lhes acesso legal e permitindo-lhes, assim, desempenhar as suas funções como previsto e autorizado por lei. Qualquer legislação que estabeleça poderes de execução tem sempre de respeitar plenamente as garantias processuais e outras salvaguardas, bem como os direitos fundamentais, em particular o respeito pela vida privada e pela privacidade das comunicações e o direito à proteção dos dados pessoais.

22. REAFIRMA o seu apoio ao desenvolvimento, aplicação e utilização de um sistema de cifragem sólido como meio necessário para proteger os direitos fundamentais e a segurança digital das pessoas, dos governos, da indústria e da sociedade e, ao mesmo tempo, RECONHECE a necessidade de assegurar a capacidade das autoridades competentes no domínio da segurança e da justiça penal, designadamente das autoridades policiais e judiciais, para exercerem os seus poderes legais, tanto em linha como fora de linha, a fim de proteger as nossas sociedades e os nossos cidadãos. As autoridades competentes devem ter a possibilidade de aceder aos dados de forma lícita e com um propósito determinado, respeitando plenamente os direitos fundamentais e a legislação pertinente em matéria de proteção de dados e salvaguardando ao mesmo tempo a cibersegurança. SALIENTA que todas as medidas tomadas têm de ser fruto de um cuidadoso equilíbrio entre esses interesses e os princípios da necessidade, da proporcionalidade e da subsidiariedade.

23. APOIA e PROMOVE a Convenção de Budapeste sobre o Cibercrime e os trabalhos em curso no que respeita ao Segundo Protocolo Adicional à referida Convenção. Além disso, continua a participar em intercâmbios multilaterais sobre cibercriminalidade, nomeadamente em processos ligados ao Conselho da Europa, ao Gabinete das Nações Unidas contra a Droga e a Criminalidade (UNODC) e à Comissão para a Prevenção do Crime e a Justiça Penal (CPCJP), a fim de assegurar uma cooperação internacional reforçada no combate à cibercriminalidade que passe pelo intercâmbio de boas práticas e conhecimentos técnicos e pelo apoio ao reforço de capacidades, respeitando, promovendo e protegendo simultaneamente os direitos humanos e as liberdades fundamentais.

24. Embora a segurança nacional continue a ser da exclusiva responsabilidade de cada Estado-Membro, RECONHECE a importância da cooperação estratégica em matéria de informações sobre ciberameaças e ciberatividades e CONVIDA os Estados-Membros, através das suas autoridades competentes, a continuarem a contribuir para o trabalho do INTCEN enquanto plataforma de conhecimento situacional e avaliação de ameaças à cibersegurança da UE e a estudarem a proposta sobre a eventual criação de um grupo de trabalho dedicado à ciberinformação, a fim de reforçar a capacidade específica do INTCEN neste domínio com base nos contributos voluntariamente prestados pelos Estados-Membros em matéria de informações, sem prejuízo das respetivas competências.

25. SALIENTA a importância de instituir um quadro de segurança sólido e coerente para proteger todo o pessoal, dados, redes de comunicação e sistemas de informação da UE, bem como processos de tomada de decisão baseados em regras abrangentes, coerentes e homogéneas. Tal deve ser feito, em especial, através do fortalecimento da resiliência e da cultura de segurança da UE contra ciberameaças e de uma maior segurança das redes da UE, classificadas e não classificadas, assegurando simultaneamente uma governação adequada e recursos e capacidades suficientes, nomeadamente no contexto do reforço do mandato da CERT-UE. Neste contexto, CONGRATULA-SE com os debates em curso sobre o estabelecimento de regras comuns em matéria de segurança da informação, tendo devidamente em conta as regras de segurança do Conselho para a proteção das informações classificadas da UE, bem como com a definição de regras vinculativas comuns em matéria de cibersegurança para todas as instituições, órgãos e agências da UE.

26. Com base nos esforços envidados pela UE no domínio da ciberdiplomacia, COMPROMETE-SE a aumentar a eficácia e eficiência do conjunto de instrumentos de ciberdiplomacia e AGUARDA COM EXPECTATIVA o aprofundamento dos debates sobre o seu alcance e utilização com base nos ensinamentos até agora retirados da aplicação deste instrumento. Esses debates deverão contribuir para promover a segurança a nível internacional, fomentando o diálogo e uma visão partilhada das questões de cibersegurança, reforçando a prevenção, a estabilidade e a cooperação, instigando a confiança e o reforço de capacidades e, se necessário, aplicando medidas restritivas, a fim de prevenir, desencorajar, dissuadir e dar resposta a ciberatividades maliciosas que visem a integridade e a segurança da UE e dos seus Estados-Membros, contribuindo assim para a segurança e estabilidade internacionais e consolidando a ciberpostura da UE, no pleno respeito das competências e prerrogativas nacionais. Haverá sobretudo que atender especialmente à prevenção e luta contra os ciberataques com efeitos sistémicos que possam afetar as nossas cadeias de abastecimento, infraestruturas críticas e serviços essenciais, instituições e processos democráticos e comprometer a nossa segurança económica, incluindo o roubo de propriedade intelectual propiciado pelo ciberespaço. Os Estados-Membros e as instituições da UE devem também refletir mais aprofundadamente sobre a articulação entre o quadro da UE em matéria de gestão de crises de cibersegurança, o conjunto de instrumentos de ciberdiplomacia e as disposições do artigo 42.º, n.º 7, do TUE e do artigo 222.º do TFUE, nomeadamente graças a um trabalho baseado em cenários concretos que permita gerar um entendimento comum das modalidades práticas com vista à aplicação do artigo 42.º, n.º 7, do TUE.

27. RECONHECE a importância de reforçar a cooperação com organizações internacionais e países parceiros a fim não só de propiciar uma compreensão partilhada do cenário de ameaças, desenvolver diálogos e mecanismos de cooperação e identificar, se necessário, respostas diplomáticas em colaboração, mas também de melhorar a partilha de informações, nomeadamente através da educação, da formação e da prática de exercícios. Em particular, SALIENTA que uma parceria transatlântica forte no domínio da cibersegurança contribui para a nossa segurança, estabilidade e prosperidade comuns e REGISTA as disposições em matéria de cooperação na área da cibersegurança estabelecidas no Acordo de Comércio e Cooperação entre a UE e o Reino Unido. 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, reitera a importância de uma cooperação melhorada, mutuamente reforçada e benéfica através da educação, da formação, da prática de exercícios e da resposta coordenada a ciberatividades maliciosas, 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.

28. A fim de contribuir para um ciberespaço global, aberto, livre, estável e seguro, de importância crescente para que a prosperidade, o crescimento, a segurança, o bem-estar, a conectividade e a integridade das nossas sociedades continuem a progredir, ASSUME O COMPROMISSO de se empenhar constantemente nos processos de definição de normas nas organizações internacionais, sobretudo nos processos relacionados com a Primeira Comissão das Nações Unidas, promovendo e contribuindo para o reconhecimento da aplicação do direito internacional no ciberespaço e para a adesão às normas, regras e princípios que norteiam o comportamento responsável dos Estados no ciberespaço, nomeadamente propiciando a rápida elaboração de um programa de ação destinado a encorajar esse comportamento responsável e dando assim seguimento, de forma construtiva, inclusiva e consensual, aos processos atualmente adotados pelo Grupo de Peritos Governamentais (GPG) e pelo grupo de trabalho aberto.

29. RECORDA o seu firme empenho num multilateralismo efetivo e numa ordem mundial assente em regras, centrada nas Nações Unidas, e a sua determinação em reforçar a cooperação e a coordenação com organizações internacionais e regionais, nomeadamente com o sistema das Nações Unidas, a OTAN, o Conselho da Europa, a OSCE, a OCDE, a União Africana, a Organização dos Estados Americanos, a ASEAN, o Fórum Regional da ASEAN, o Conselho de Cooperação do Golfo e a Liga dos Estados Árabes, no que diz respeito aos debates sobre questões relacionadas com o ciberespaço, bem como à continuação e expansão dos diálogos e consultas estruturados da UE com países terceiros. SALIENTA o seu apoio ativo às Nações Unidas, em particular no que respeita à Agenda 2030 e aos Objetivos de Desenvolvimento Sustentável, e CONGRATULA-SE com o Roteiro para a Cooperação Digital e a Agenda para o Desarmamento, ambos definidos pelo secretário-geral das Nações Unidas, que promovem a responsabilização e a adesão às normas no ciberespaço e contribuem para a prevenção e a resolução pacífica de conflitos decorrentes da prática de atividades maliciosas no ciberespaço. LOUVA a proposta de criação de uma rede informal da UE em matéria de ciberdiplomacia, apresentada pelo alto representante para os Negócios Estrangeiros e a Política de Segurança com vista a envolver mais a UE e os Estados-Membros e desenvolver os seus conhecimentos especializados relativamente a questões internacionais do domínio do ciberespaço e a reforçar a coordenação das ações de sensibilização.

30. AGUARDA COM EXPECTATIVA a futura proposta de revisão do Quadro Estratégico da UE para a Ciberdefesa e COMPROMETE-SE a continuar a defender o reforço das dimensões da cibersegurança e da ciberdefesa, com vista a assegurar a sua plena integração no domínio mais vasto da segurança e da defesa, em particular no contexto dos trabalhos sobre as orientações estratégicas. CONSIDERA que a futura "Visão e Estratégia Militar para o Ciberespaço como Domínio da Atividade Militar" contribuirá para aprofundar os debates nessa matéria. CONGRATULA-SE com a iniciativa lançada pela Agência Europeia de Defesa (AED) para promover a cooperação entre as CERT militares e APOIA os esforços envidados para aumentar as sinergias civilo-militares e a coordenação em matéria de ciberdefesa e cibersegurança, inclusive no que toca aos aspetos relacionados com o espaço, nomeadamente através dos projetos específicos elaborados no âmbito da CEP.

31. CONGRATULA-SE com a proposta de elaboração de uma agenda da UE para o reforço das cibercapacidades externas, com a proposta de criação de um comité de reforço das cibercapacidades da UE e com a criação e implantação da EU CyberNet (rede da UE de reforço das cibercapacidades), que visam aumentar a ciber-resiliência e as capacidades em todo o mundo. Neste contexto, REGOZIJA-SE com a cooperação estabelecida com os Estados-Membros e com parceiros dos setores público e privado, entre os quais o Fórum Global de Cibercompetências (GFCE) e outros organismos internacionais relevantes, a fim de assegurar a coordenação e evitar duplicações. Em especial, INCENTIVA a cooperação com os parceiros dos Balcãs Ocidentais e da vizinhança oriental e meridional da UE.

32. A fim de garantir que todos os países possam colher os benefícios sociais, económicos e políticos da Internet e da utilização das tecnologias, COMPROMETE-SE a ajudar os países parceiros a enfrentarem o desafio crescente das ciberatividades maliciosas, nomeadamente das que prejudicam o desenvolvimento das suas economias e sociedades e a integridade e segurança dos sistemas democráticos, em consonância com os esforços desenvolvidos, entre outros, no âmbito do Plano de Ação para a Democracia Europeia.

33. A fim de assegurar o desenvolvimento, a aplicação e o acompanhamento das propostas apresentadas na Estratégia de Cibersegurança da UE, e tendo em conta o caráter plurianual de algumas das iniciativas, INCENTIVA a Comissão e o alto representante para os Negócios Estrangeiros e a Política de Segurança a estabelecerem um plano de execução pormenorizado que defina as prioridades e o calendário das ações previstas. ACOMPANHARÁ o evoluir da aplicação das presentes conclusões através de um plano de ação que será periodicamente revisto e atualizado pelo Conselho, em estreita cooperação com a Comissão Europeia e o alto representante.