Conselho da
União Europeia

Bruxelas, 20 de novembro de 2017
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	20 de novembro de 2017
para:	Delegações
n.º doc. ant.:	13943/17 + COR 1
n.° doc. Com.:	12210/17, 12211/17
Assunto:	Conclusões do Conselho sobre a comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE – Conclusões do Conselho (20 de novembro de 2017)

Juntam-se em anexo, à atenção das Delegações, as Conclusões do Conselho sobre a comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE, adotadas pelo Conselho dos Assuntos Gerais em 20 de novembro de 2017.

ANEXO

Conclusões do Conselho sobre a comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE

O Conselho da União Europeia,

1. RECONHECENDO a importância da cibersegurança para a prosperidade, o crescimento e a segurança da UE e a integridade das nossas sociedades livres e democráticas e dos processos que lhes estão subjacentes na era digital, ao proteger tanto o Estado de direito como os direitos humanos e as liberdades fundamentais de todas as pessoas;

2. SUBLINHANDO a necessidade de tratar a cibersegurança no quadro de uma abordagem coerente a nível nacional, da UE e mundial, uma vez que as ciberameaças podem ter repercussões na nossa democracia, prosperidade, estabilidade e segurança;

3. OBSERVA que a existência de um elevado nível de ciber-resiliência em toda a UE é também importante para conquistar a confiança no Mercado Único Digital e para a continuação do desenvolvimento de uma Europa digital;

4. REITERANDO que a UE promoverá continuamente um ciberespaço aberto, mundial, livre, pacífico e seguro, onde os direitos humanos e as liberdades fundamentais, em particular o direito à liberdade de expressão, o acesso à informação, a proteção de dados, a privacidade e a segurança, bem como os valores e os princípios fundamentais da UE, sejam plenamente observados e respeitados tanto na UE como a nível mundial, e SALIENTANDO a importância crucial de assegurar um equilíbrio adequado entre os direitos humanos e as liberdades fundamentais e o cumprimento dos requisitos da política de segurança interna da UE[1],

5. RECONHECENDO que o direito internacional, nomeadamente a Carta das Nações Unidas no seu todo, o direito internacional humanitário e a legislação sobre os direitos humanos são aplicáveis no ciberespaço e SUBLINHANDO, por conseguinte, a necessidade de prosseguir os esforços para assegurar que o direito internacional seja respeitado no ciberespaço;

[1] Doc. 12650/17.

6. RECORDANDO as suas conclusões sobre a Estratégia da União Europeia para a Cibersegurança[2], sobre a governação da Internet[3], sobre o reforço do sistema de ciberresiliência da Europa[4], sobre a ciberdiplomacia[5], sobre um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas[6], sobre a melhoria da justiça penal no ciberespaço[7]; sobre Segurança e Defesa no contexto da Estratégia Global da UE[8], o Quadro comum em matéria de luta contra as ameaças híbridas[9] e sobre a revisão intercalar da Estratégia Renovada de Segurança Interna da União Europeia para 2015-2020[10];

7. RECONHECENDO que o quadro previsto pela Convenção do Conselho da Europa sobre o Cibercrime (a Convenção de Budapeste), proporciona uma base sólida, entre um grupo diversificado de países, para a utilização de uma norma jurídica eficaz para as diferentes legislações nacionais e para a cooperação internacional que tratam da cibercriminalidade;

8. RECONHECENDO a necessidade de dar um novo destaque à execução do Quadro Estratégico da UE para a Ciberdefesa, de 2014, e de o atualizar de modo a integrar ainda mais a cibersegurança e a ciberdefesa na política comum de segurança e defesa (PCSD) e numa agenda de segurança e defesa mais ampla;

9. RECONHECENDO que uma indústria europeia competitiva a nível mundial é um elemento importante para atingir um elevado nível de cibersegurança a nível nacional e em toda a UE;

10. RECORDANDO que, de acordo com o artigo 4.º, n.º 2, do Tratado da União Europeia, a segurança nacional é da exclusiva responsabilidade de cada Estado-Membro.

---

2 Docs. 12109/13 e 6225/13 (Comunicação conjunta da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido (COM JOIN (2013) 1 final).

3 Doc. 16200/14 e doc. 6460/14 (Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – A política e a governação da Internet. O papel da Europa na configuração da governação da Internet no futuro (COM(2014) 72 final)).

4 Doc. 14540/16 e doc. 11013/16 (Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Reforçar o sistema de ciberresiliência da Europa e promover uma indústria de cibersegurança competitiva e inovadora (COM 2016(410) final).

5 Doc. 6122/15.

6 Doc. 9916/17.

7 Doc. 10007/16.

8 Doc. 9178/17.

9 7688/16 (Comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho: Quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia).

10 Doc. 12650/17.

PELAS PRESENTES CONCLUSÕES

11. CONGRATULA-SE com a comunicação conjunta ao Parlamento Europeu e ao Conselho intitulada: Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE, por apresentar o objetivo ambicioso de reforçar a cibersegurança na UE. A comunicação contribui também para a autonomia estratégica da UE, tal como é referido nas conclusões do Conselho sobre a estratégia global para a política externa e de segurança da União[11], ao ter como objetivo construir uma Europa digital que será mais segura, inspiradora de confiança, consciente dos seus pontos fortes, competitiva, aberta ao mundo, respeitadora dos valores comuns da União Europeia quanto a uma Internet aberta, livre, pacífica e segura a nível mundial – e, por conseguinte, atingir um nível mais elevado de resiliência para prevenir, dissuadir, detetar e dar resposta às ciberameaças e ser capaz de responder em conjunto às ciberameaças em toda a UE, e

12. CONVIDA os Estados-Membros, as instituições, as agências e os organismos da UE a colaborarem, na observância das respetivas esferas de competência e dos princípios da subsidiariedade e da proporcionalidade, com vista à consecução dos objetivos estratégicos estabelecidos nas presentes conclusões, e

13. SUBLINHA a necessidade de a UE, os seus Estados-Membros e o setor privado assegurarem um financiamento suficiente, respeitando os recursos disponíveis para apoiar o reforço da ciber-resiliência e os esforços em matéria de investigação e desenvolvimento da cibersegurança em toda a UE, bem como para reforçar a cooperação a fim de prevenir, dissuadir, detetar e dar resposta às ciberameaças e ser capaz de responder conjuntamente aos ciberincidentes em grande escala e às ciberatividades maliciosas em toda a UE;

[11] Doc. 13202/16.

Capítulo I

GARANTIR A EFETIVA RESILIÊNCIA DO CIBERESPAÇO NA UE E A CONFIANÇA NO MERCADO ÚNICO DIGITAL

14. SUBLINHA que cada Estado-Membro é o primeiro responsável pelo reforço da sua própria cibersegurança e por assegurar a sua capacidade de resposta a incidentes e crises de cibersegurança, podendo a UE, por seu lado, proporcionar um forte valor acrescentado apoiando a cooperação entre os Estados-Membros. Neste contexto, SALIENTA a necessidade de todos os Estados-Membros disponibilizarem os recursos necessários às autoridades nacionais responsáveis pela cibersegurança, a fim de garantir a prevenção, a deteção e a resposta a incidentes e crises de cibersegurança em toda a UE;

15. SUBLINHA a necessidade de, sempre que possível, recorrer aos mecanismos, estruturas e organizações existentes a nível da UE;

16. CONGRATULA-SE COM:

- os progressos realizados na transposição da Diretiva SRI pelos Estados-Membros e SALIENTA a necessidade de alcançar a sua aplicação plena e efetiva até maio de 2018, tal como estipula a própria diretiva[12];
- o trabalho realizado pelo grupo de cooperação SRI no reforço da cooperação estratégica e da troca de informações entre os Estados-Membros;
- o trabalho realizado no âmbito da rede CSIRT, especialmente no que toca ao reforço da cooperação operacional dos Estados-Membros, à criação de um clima de confiança para a partilha de informações no tratamento de incidentes de cibersegurança em grande escala e, com base nas conclusões retiradas pelos Estados-Membros a nível nacional, no que respeita ao fornecimento de elementos para uma perceção partilhada da situação a nível europeu;
- o trabalho realizado no âmbito da parceria público-privada contratual em matéria de cibersegurança (PPPc).

[12] Sem prejuízo da competência dos Estados-Membros para proceder à transposição da Diretiva SRI, especialmente no que respeita aos operadores de serviços essenciais.

17. CONGRATULA-SE com o facto de a Comunicação Conjunta confirmar, por um lado, que a cifragem forte e de confiança é extremamente importante para garantir devidamente os direitos humanos e as liberdades fundamentais na UE e para a confiança dos cidadãos no Mercado Único Digital, tendo simultaneamente em conta a necessidade de as autoridades de polícia terem acesso aos dados necessários às suas investigações, e, por outro lado, que a identificação e comunicação digitais em condições de segurança são fundamentais para garantir uma eficaz cibersegurança na UE;

18. CONGRATULA-SE com o plano previsto na Comunicação Conjunta no sentido de elevar o nível de ambição na realização regular de exercícios pan-europeus de cibersegurança, tomando por base a experiência adquirida com os exercícios Cyber Europe, que combina a resposta a diferentes níveis, já que este será um elemento importante no reforço da preparação dos Estados-Membros e das instituições da UE para dar resposta a ciberincidentes em grande escala;

19. EXORTA a UE e os seus Estados-Membros a realizarem regularmente exercícios estratégicos de cibersegurança nas diversas formações do Conselho, com base na experiência adquirida durante o EU CYBRID 2017 e

20. Sem prejuízo do resultado do processo legislativo:

- CONGRATULA-SE com a proposta de atribuir à ENISA um mandato forte e permanente, com o objetivo principal de apoiar e desenvolver uma cooperação mais estreita entre os Estados-Membros, a fim de aumentar as suas capacidades e reforçar a confiança na Europa digital;

- REAFIRMA que a futura ENISA deverá beneficiar da experiência e especialização dos Estados-Membros e da UE e apoiar o desenvolvimento e a aplicação coerentes das atuais e futuras políticas e regulamentações da UE em matéria de cibersegurança, sem deixar de garantir que todas as competências da ENISA sejam desenvolvidas em complemento das dos Estados-Membros;

- REITERA o objetivo de reforçar a confiança na Europa digital, aumentando a confiança nas soluções e inovações digitais, incluindo a Internet das Coisas, o comércio eletrónico e a administração em linha, especialmente em termos de um quadro europeu de certificação da cibersegurança de craveira mundial[13]. Trata-se de uma condição fundamental para reforçar a confiança nos produtos e serviços digitais e a segurança destes, proteger as infraestruturas críticas, os dados da administração do Estado, dos cidadãos e das empresas e para adotar uma abordagem de segurança desde a conceção para os produtos, serviços e processos do Mercado Único Digital;

- SALIENTA que a atividade legislativa que visa reforçar a certificação da cibersegurança a nível da UE terá de satisfazer as necessidades do mercado e dos utilizadores, tirando partido da experiência, das capacidades e dos processos de certificação existentes na UE (por exemplo, o quadro SOG-IS) e deverá criar um quadro rapidamente adaptável às mais modernas inovações digitais;

- SALIENTA que ao reforçar a certificação da cibersegurança na UE, deverá ser abrangida toda a gama dos requisitos de segurança, até aos mais exigentes, tendo que ficar demonstrada a resistência às capacidades dos atacantes. Os principais fatores de sucesso seriam assegurar um processo fiável, transparente e independente de certificação da segurança para promover a disponibilidade de dispositivos, software e serviços fiáveis e seguros dentro do Mercado Único e não só; reconhecer os conhecimentos especializados respetivos da indústria, do aparelho do Estado e dos especialistas da avaliação por meio de normas europeias e mundiais[14]; respeitar as funções dos Estados-Membros no processo de certificação, em especial no que diz respeito à avaliação aos mais elevados níveis de segurança e, sobretudo, em relação às necessidades essenciais em matéria de segurança e avaliação de competências. Este quadro de certificação deverá igualmente garantir que qualquer regime de certificação à escala da UE seja proporcional ao nível de garantia necessário para a utilização dos produtos, serviços e/ou sistemas TIC envolvidos, e permitir que as empresas de todas as dimensões realizem atividades de comércio transfronteiras, a fim de desenvolverem e comercializarem novos produtos, tanto no interior da UE como nos mercados fora da UE.

---

[13] Por meio de normas mundiais desenvolvidas no espírito da OMC – Código de Boas Práticas OTC.

[14] Por meio de normas europeias e mundiais desenvolvidas no espírito da OMC – Código de Boas Práticas OTC.

21. CONGRATULA-SE com a intenção de criar uma rede de centros de competência em matéria de cibersegurança, a fim de estimular o desenvolvimento e a implantação de tecnologias de cibersegurança e de dar um novo ímpeto à inovação da indústria da UE no plano mundial para desenvolver a próxima geração de tecnologias inovadoras, como a inteligência artificial, a computação quântica, a tecnologia de cifragem progressiva (blockchain) e a identificação digital segura;

22. FRISA a necessidade de a rede de centros de competência em matéria de cibersegurança não excluir nenhum dos Estados-Membros nem os centros de excelência e a competência de que já dispõem, prestando ao mesmo tempo especial atenção à complementaridade e, tendo em mente estes aspetos, TOMA NOTA dos planos de criação do Centro Europeu de Investigação em matéria de Cibersegurança, que deve ter por principal função garantir a complementaridade e evitar a duplicação dentro da rede de centros de competência em matéria de cibersegurança e com outras agências da UE;

23. SALIENTA que a rede de centros de competência em matéria de cibersegurança deverá concentrar a sua atenção numa série de questões, da investigação à indústria e, por conseguinte, contribuir, entre outras coisas, para a consecução do objetivo de alcançar a autonomia estratégica europeia;

24. Tendo em vista a proposta de criação da rede de centros de competência em matéria de cibersegurança, REAFIRMA a necessidade de a UE, através dos seus Estados-Membros, desenvolver uma capacidade europeia de avaliação da resistência da criptografia utilizada em produtos e serviços ao dispor dos cidadãos, das empresas e das administrações públicas dentro do Mercado Único Digital, reconhecendo que as políticas de criptografia são um elemento essencial da segurança nacional e por isso se inserem na esfera de competência dos Estados-Membros;

25. CONVIDA todas as partes interessadas a aumentarem o investimento nas aplicações das novas tecnologias para a cibersegurança, a fim de contribuir para que a cibersegurança fique garantida em todos os setores da economia europeia;

26. Salienta a importância de que se reveste a credibilidade, fiabilidade e coordenação da prestação de serviços de cibersegurança às instituições da UE e SOLICITA à COMISSÃO e outras instituições da UE que continuem a desenvolver a CERT-UE de acordo com estes objetivos e que assegurem para isso a existência dos recursos adequados;

27. CONGRATULA-SE com o apelo no sentido de se reconhecer o importante papel desempenhado pelos investigadores de outras partes em matéria de segurança para revelar as vulnerabilidades dos atuais produtos e serviços e EXORTA os Estados-Membros a partilharem as boas práticas de divulgação coordenada de tais vulnerabilidades;

28. DESTACA a responsabilidade de todos no domínio da cibersegurança e CONVIDA a UE e os seus Estados-Membros a promoverem as competências digitais e a literacia mediática para ajudar os utilizadores a protegerem as suas informações digitais em linha e aumentarem o seu conhecimento dos riscos que correm quando introduzem dados pessoais na Internet;

29. CONGRATULA-SE com o destaque dado na Comunicação Conjunta à educação, à ciber-higiene e à sensibilização para a cibersegurança nos Estados-Membros e na UE;

30. SOLICITA À COMISSÃO que forneça rapidamente uma avaliação de impacto e apresente, até meados de 2018, propostas de instrumentos jurídicos relevantes para a execução da iniciativa de criação de uma rede de centros de competência em matéria de cibersegurança e de um Centro Europeu de Investigação e de Competências em matéria de Cibersegurança;

31. CONVIDA os Estados-Membros a:

- darem prioridade à sensibilização para o ciberespaço em campanhas de informação e estimularem a cibersegurança nos programas curriculares académicos, do ensino geral e da formação profissional. Deverá ser dada uma ênfase especial à educação dos jovens e à promoção das competências digitais, para formar profissionais aptos a enfrentar o futuro e os desafios no domínio da segurança, da economia e dos serviços;

- intensificarem os seus esforços para abrir programas especializados de alto nível no domínio da cibersegurança, a fim de preencher o atual défice de profissionais de cibersegurança na UE;

- criarem uma rede de cooperação eficaz dos pontos de contacto da área da educação, sob a égide da ENISA. A rede de pontos de contacto deverá ter por objetivo aperfeiçoar a coordenação e o intercâmbio de boas práticas entre os Estados-Membros em matéria de educação e sensibilização para a cibersegurança, bem como de formação, exercício e reforço de capacidades;

- ponderarem a aplicação das regras da Diretiva SRI também às administrações públicas que participem em atividades societais ou económicas determinantes, se não forem já abrangidas pela legislação nacional e se se julgar adequado, e a darem formação relacionada com a cibersegurança também às administrações públicas, dado o papel que estas desempenham na nossa sociedade e economia.

Capítulo II

REFORÇO DA CAPACIDADE DA UE PARA PREVENIR, DISSUADIR, DETETAR E DAR RESPOSTA A CIBERATIVIDADES MALICIOSAS

32. SALIENTA que um ciberincidente ou uma cibercrise particularmente grave pode constituir razão suficiente para um Estado-Membro invocar a cláusula de solidariedade[15] e/ou a cláusula de assistência mútua da UE[16].

33. CONGRATULA-SE com a adoção do "Quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas", que contribui para a prevenção de conflitos, a cooperação e a estabilidade no ciberespaço, ao definir medidas no âmbito da PESC, inclusive medidas restritivas, que podem ser usadas para prevenir e dar resposta a ciberatividades maliciosas, e EXORTA o SEAE e os Estados-Membros, a fazerem regularmente exercícios no âmbito desse quadro;

[15] Artigo 222.º do TFUE
[16] Artigo 42.º, n.º 7, do TUE

34. SALIENTA a necessidade de uma resposta eficiente a nível da UE a ciberincidentes e a cibercrises de grande escala, respeitando simultaneamente as competências dos Estados-Membros e a necessidade de a cibersegurança ser integrada nos atuais mecanismos de gestão de crises a nível da UE[17]. Para alcançar esse objetivo, APELA a que a resposta a nível da UE a ciberincidentes de grande escala seja exercitada regularmente – desde as respostas estratégico-diplomáticas a respostas técnicas – com base nos quadros e procedimentos pertinentes, e melhorando-os sempre que necessário[18];

35. SALIENTA a importância de uma resposta e de mecanismos de intercâmbio de informações bem integrados entre as diferentes comunidades que são determinantes para garantir a cibersegurança na Europa, nomeadamente entre os organismos pertinentes da UE e as autoridades dos Estados-Membros. Esses mecanismos terão de ser testados e verificados no âmbito de exercícios de cibersegurança a nível da UE, e formalizados por acordos neste domínio, se necessário;

36. REGISTA a possibilidade de examinar, no caso de a Comissão apresentar uma proposta para a criação de um Fundo de Resposta de Emergência para a Cibersegurança, a par dos atuais esforços dos Estados-Membros e no respeito dos recursos disponíveis (especialmente no âmbito do Quadro Financeiro Plurianual da UE) a concessão de ajuda aos Estados-Membros para darem resposta aos ciberincidentes em grande escala e atenuarem esses incidentes, desde que o Estado-Membro em causa tenha criado, a nível nacional, um sistema prudente de cibersegurança antes do incidente, incluindo a plena aplicação da Diretiva SRI e de quadros devidamente desenvolvidos em matéria de gestão de riscos e de supervisão;

37. RECONHECE as crescentes interligações entre cibersegurança e defesa e APELA à intensificação da cooperação em matéria de ciberdefesa, incentivando, nomeadamente, a cooperação entre as comunidades civis e militares de resposta a incidentes, e à continuação do reforço da cibersegurança nas missões e operações da PCSD;

---

17 C/2017/6100 final

18 9916/17 e C/2017/6100 final.

38. Salienta a necessidade de eventualmente tirar pleno partido das iniciativas de defesa propostas para acelerar o desenvolvimento de cibercapacidades adequadas na Europa, e RECONHECE as oportunidades de desenvolver eventualmente projetos de ciberdefesa através da CEP, se tal for considerado necessário pelos Estados-Membros que participam na CEP, e RECONHECE o papel desempenhado pela base tecnológica e industrial de defesa europeia (BITDE) e pela base industrial mais ampla da cibersegurança civil no fornecimento de meios para que os Estados-Membros salvaguardem os seus interesses em matéria de segurança e de defesa relacionados com o ciberespaço;

39. TOMA NOTA da proposta da Comissão de criar uma plataforma de formação e educação em matéria de ciberdefesa até ao final de 2018, e SALIENTA que a plataforma deveria aumentar as oportunidades de formação e de educação nos Estados-Membros e assegurar a complementaridade com outros esforços e iniciativas da UE, nomeadamente com a AESD e a AED;

40. EXORTA a UE e os seus Estados-Membros a serem sensíveis à ameaça de roubo de propriedade intelectual apoiada nas TIC, nomeadamente de segredos comerciais ou outras informações comerciais confidenciais, com o objetivo de assegurar vantagens competitivas a empresas ou setores comerciais;

41. RECONHECE a necessidade de combater os crimes no ciberespaço, incluindo na web invisível, a exploração sexual de crianças em linha, bem como a fraude e a contrafação de meios de pagamento que não em numerário, nomeadamente com o objetivo de criar um melhor quadro de informações, realizar investigações conjuntas e mutualizar o apoio operacional;

42. SAÚDA o trabalho desenvolvido pela UE e pelos seus Estados-Membros na resposta aos desafios colocados por sistemas que permitem que os criminosos e terroristas comuniquem através de canais a que as autoridades competentes não podem ter acesso, SALIENTA que esse trabalho tem de ter em conta que uma cifragem forte e de confiança é de grande importância para a cibersegurança e a confiança no Mercado Único Digital e para assegurar o respeito dos direitos humanos e das liberdades fundamentais;

43. SUBLINHA a importância de dotar as autoridades policiais de ferramentas que lhes permitam detetar, investigar e intentar ações penais contra os cibercrimes, de modo a que os crimes cometidos no ciberespaço não passem despercebidas ou impunes e CONGRATULA-SE com o contributo da Rede Judiciária europeia em matéria de cibercriminalidade na luta contra a criminalidade através da cooperação entre as autoridades judiciais;

44. SALIENTA a importância de garantir uma posição coordenada da UE a fim de moldar de forma eficaz a nível europeu e mundial as decisões de governação da Internet no seio da comunidade de múltiplas partes interessadas, como por exemplo assegurar a existência de bases de dados WHOIS de endereços IP e de nomes de domínios precisas e rapidamente acessíveis, por forma a que as capacidades de aplicação da lei e os interesses públicos sejam salvaguardados;

45. SALIENTA a importância da implantação do protocolo Internet IPv6, que é vital para o desenvolvimento em grande escala da Internet das coisas, bem como para melhorar a atribuição de crimes no ciberespaço;

46. INCENTIVA os trabalhos em curso sobre o acesso transfronteiras a meios de prova eletrónicos, resolvendo a questão da conservação dos dados, e sobre os desafios para o processo penal resultantes de sistemas que permitem que os criminosos e terroristas comuniquem utilizando canais a que as autoridades competentes não podem ter acesso, tendo em conta a necessidade de respeitar os direitos humanos e as liberdades fundamentais e a proteção dos dados;

47. EXORTA a Comissão:

- a apresentar, até dezembro de 2017, um relatório intercalar sobre os progressos realizados na execução das medidas práticas para melhorar o acesso transfronteiras a meios de prova eletrónicos;

- a apresentar, no início de 2018, uma proposta legislativa destinada a melhorar o acesso transfronteiras a meios de prova eletrónicos;

48. CONVIDA a Europol, a ENISA e a Eurojust:

- a continuarem a reforçar a sua cooperação na luta contra a cibercriminalidade, quer entre si quer com outras partes interessadas, nomeadamente a comunidade das CSIRT, a Interpol, o setor privado e as universidades, assegurando sinergias e complementaridades, em conformidade com os respetivos mandatos e competências;

- a contribuírem, juntamente com os Estados-Membros, para uma abordagem coordenada da resposta da UE em matéria de aplicação da lei em caso de ciberincidentes e de cibercrises de grande escala, para complementar os procedimentos descritos nos quadros pertinentes[19];

49. CONVIDA a UE e os seus Estados-Membros a prosseguirem os trabalhos:

- para eliminarem os obstáculos à investigação de crimes e à aplicação da justiça penal no ciberespaço, bem como para reforçar a cooperação e a coordenação internacionais em matéria de luta contra a criminalidade no ciberespaço;

- para enfrentarem os desafios colocados pelas tecnologias de anonimização, sem perder de vista que uma cifragem forte e de confiança é de grande importância para a cibersegurança e para a confiança no Mercado Único Digital;

- para moldarem as decisões de governação da Internet, que têm impacto na capacidade de aplicação da lei, por forma a lutar contra a criminalidade no ciberespaço.

[19] 9916/17 e C/2017/6100 final.

Capítulo III

REFORÇAR A COOPERAÇÃO INTERNACIONAL PARA UM CIBERESPAÇO ABERTO, LIVRE, PACÍFICO E SEGURO A NÍVEL MUNDIAL

50. RECONHECE que assegurar a cibersegurança é um desafio mundial, que requer uma cooperação eficaz entre todos os intervenientes a nível mundial, e RECONHECE a necessidade de dar especial atenção ao respeito dos valores democráticos e dos princípios de um ciberespaço aberto, livre, pacífico e seguro a nível mundial; nesta perspetiva;

51. EXORTA a UE e os seus Estados-Membros a promoverem a criação de um quadro estratégico para a prevenção de conflitos, a cooperação e a estabilidade no ciberespaço, que se baseie na aplicação do direito internacional vigente – em particular, da Carta das Nações Unidas no seu todo – na elaboração e aplicação de normas universais de conduta responsável dos Estados e em medidas de reforço da confiança entre Estados;

52. RECONHECE o papel das Nações Unidas no aperfeiçoamento de normas para um comportamento responsável dos Estados no ciberespaço e recorda que os debates do Grupo de Peritos Governamentais das Nações Unidas ao longo dos anos têm resultado num conjunto de normas e recomendações consensuais[20], que a Assembleia Geral tem apoiado reiteradamente e que os Estados deverão tomar como base para o comportamento responsável dos Estados no ciberespaço;

53. RECONHECE que essas normas sobre o comportamento responsável dos Estados implicam que os Estados não permitam conscientemente que o seu território seja utilizado para atos ilícitos a nível internacional, que deem resposta aos pedidos de assistência adequados apresentados por outros Estados cujas infraestruturas críticas sejam alvo de atos informáticos maliciosos provenientes do território do seu Estado, e que os Estados tomem medidas adequadas para proteger as suas infraestruturas críticas de ameaças informáticas;

54. RECONHECE as ciberameaças e riscos comuns enfrentados pela UE, a OTAN e os respetivos Estados-Membros e REITERA a importância de continuar a cooperação entre a UE e a OTAN em matéria de cibersegurança e defesa, no pleno respeito dos princípios da inclusão, da reciprocidade e da autonomia de decisão da UE e em conformidade com as suas conclusões de 6 de dezembro de 2016 sobre a implementação da Declaração Conjunta do Presidente do Conselho Europeu, do Presidente da Comissão Europeia e do Secretário-Geral da Organização do Tratado do Atlântico Norte[20];

55. EXORTA a UE e os seus Estados-Membros a apoiarem e incentivarem a tomada de medidas de desenvolvimento de confiança a nível regional, já que estas são um aspeto essencial para aumentar a cooperação e a transparência e reduzir os riscos de conflito. A aplicação de medidas de reforço da confiança no domínio da cibersegurança no âmbito da OSCE e de outros contextos regionais aumentará a previsibilidade do comportamento dos Estados e contribuirá para estabilizar o ciberespaço;

56. REAFIRMA que a UE continuará a respeitar os seus valores fundamentais, protegendo os direitos humanos e as liberdades fundamentais e desenvolvendo as diretrizes da UE em matéria de direitos humanos relativas à liberdade em linha. A UE salienta igualmente a importância de todas as partes interessadas participarem na governação da Internet, incluindo o mundo académico, a sociedade civil e o setor privado;

57. EXORTA a UE e os seus Estados-Membros a promoverem o desenvolvimento de capacidades de cibersegurança em países terceiros, dando especial prioridade aos países vizinhos da UE e aos países em desenvolvimento que têm conhecido um forte crescimento da conectividade, para que combatam a cibercriminalidade e desenvolvam a resiliência do seu ciberespaço, em conformidade com os valores fundamentais da UE. Para fazer avançar os esforços da UE neste domínio, há que desenvolver uma rede da UE dedicada ao reforço das capacidades em matéria de cibersegurança, bem como diretrizes da UE para esse efeito, devendo estes dois instrumentos complementar os mecanismos e estruturas já existentes;

[20] Doc. 15283/16.

58. DESTACA os progressos alcançados na cooperação entre a UE e a OTAN em matéria de ciberdefesa e cibersegurança e o desenvolvimento dessa cooperação nos domínios da formação, da educação e dos conceitos, ao mesmo tempo que se tem evitado a duplicação desnecessária de esforços, nos casos em que as necessidades coincidem, e se tem promovido a interoperabilidade através de normas e requisitos de ciberdefesa; APELA a que se continue a cooperar no domínio dos exercícios de ciberdefesa (a nível do pessoal) e na partilha de boas práticas relativas à gestão de crises, evitando simultaneamente a duplicação desnecessária de esforços, nos casos em que as necessidades coincidem, e respeitando plenamente a política de exercícios da UE e os princípios da inclusão, da reciprocidade e da autonomia de decisão da UE;

59. RECONHECE que a Convenção do Conselho da Europa sobre o Cibercrime (a Convenção de Budapeste) proporciona uma norma jurídica eficaz para inspirar a legislação nacional sobre a cibercriminalidade. APELA a todos os países para que elaborem quadros jurídicos nacionais adequados e cooperem no âmbito deste quadro jurídico internacional em vigor proporcionado pela Convenção de Budapeste;

60. RECORDA os resultados obtidos na realização de diálogos bilaterais da UE sobre cibersegurança e apela a novos esforços para facilitar a cooperação com os países terceiros neste domínio;

61. RECORDA que a UE dispõe de um mecanismo de controlo das exportações robusto e juridicamente vinculativo, baseado nas decisões e boas práticas desenvolvidas no âmbito de regimes internacionais de não-proliferação, e REGISTA os debates em curso no Conselho destinados a encontrar as melhores formas de continuar a melhorar o funcionamento desses controlos; CONVIDA os Estados-Membros a continuarem a abordar, nos regimes internacionais relevantes de controlo das exportações (p. ex., Acordo de Wassenaar), as aplicações críticas das novas tecnologias ao domínio da cibersegurança, a fim de garantir um controlo eficaz das tecnologias de cibersegurança críticas do futuro;

62. No seguimento das conclusões do Conselho Europeu de 19 de outubro de 2017[21], as presentes conclusões serão postas em prática através de um plano de ação, que deverá ser adotado pelo Conselho antes do final de 2017. O plano de ação é um documento evolutivo, que será regularmente revisto e atualizado pelo Conselho.

---

[21] EUCO 14/17.