P8_TA(2018)0258

Ciberdefesa

Resolução do Parlamento Europeu, de 13 de junho de 2018, sobre ciberdefesa (2018/2004(INI))

(2020/C 28/06)

O Parlamento Europeu,

— Tendo em conta o Tratado da União Europeia (TUE) e o Tratado sobre o Funcionamento da União Europeia (TFUE),

— Tendo em conta o documento intitulado «Visão partilhada, ação comum: uma Europa mais forte – Estratégia global para a política externa e de segurança da União Europeia», apresentado pela Vice-Presidente da Comissão Europeia/Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança (VP/AR) em 28 de junho de 2016,

— Tendo em conta as Conclusões do Conselho Europeu de 20 de dezembro de 2013, 26 de junho de 2015, 15 de dezembro de 2016, 9 de março de 2017, 22 de junho de 2017, 20 de novembro de 2017 e 15 de dezembro de 2017,

— Tendo em conta a Comunicação da Comissão, de 7 de junho de 2017, intitulada «Documento de reflexão sobre o futuro da defesa europeia» (COM(2017)0315),

— Tendo em conta a Comunicação da Comissão, de 7 de junho de 2017, intitulada «Lançar o Fundo Europeu de Defesa» (COM(2017)0295),

— Tendo em conta a Comunicação da Comissão, de 30 de novembro de 2016, relativa ao Plano de Ação Europeu no Domínio da Defesa (COM(2016)0950),

— Tendo em conta a comunicação conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, de 7 de fevereiro de 2013, intitulada «Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido» (JOIN(2013)0001),

— Tendo em conta o documento de trabalho dos serviços da Comissão, de 13 de setembro de 2017, intitulado «Avaliação da Estratégia de Cibersegurança da UE para 2013» (SWD(2017)0295),

— Tendo em conta o Quadro Estratégico da UE para a Ciberdefesa, de 18 de novembro de 2014,

— Tendo em conta as Conclusões do Conselho, de 10 de fevereiro de 2015, sobre ciberdiplomacia,

— Tendo em conta as Conclusões do Conselho, de 19 de junho de 2017, sobre um quadro para uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas («instrumentos de ciberdiplomacia»),

— Tendo em conta a comunicação conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança ao Parlamento Europeu e ao Conselho, de 13 de setembro de 2017, intitulada «Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE» (JOIN(2017)0450),

— Tendo em conta o «Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations» (Manual de Taline sobre o direito internacional aplicável às ciberoperações) ([1]),

— Tendo em conta a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União ([2]),

— Tendo em conta os trabalhos da Comissão Mundial sobre a Estabilidade do Ciberespaço,

— Tendo em conta a Comunicação da Comissão, de 28 de abril de 2015, intitulada «Agenda Europeia para a Segurança» (COM(2015)0185),

— Tendo em conta a comunicação conjunta da Comissão e da Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança ao Parlamento Europeu e ao Conselho, de 6 de abril de 2016, intitulada «Quadro comum em matéria de luta contra as ameaças híbridas: uma resposta da União Europeia» (JOIN(2016)18),

— Tendo em conta a sua Resolução, de 3 de outubro de 2017, sobre a luta contra a cibercriminalidade ([3]),

— Tendo em conta a declaração conjunta, de 8 de julho de 2016, dos Presidentes do Conselho Europeu e da Comissão e do Secretário-Geral da NATO, sobre os conjuntos comuns de propostas relativas à aplicação da declaração conjunta aprovada pelos Conselhos da NATO e da UE, em 6 de dezembro de 2016 e 5 de dezembro de 2017, e os relatórios intercalares sobre a sua aplicação, de 14 de junho e 5 de dezembro de 2017,

— Tendo em conta a sua Resolução, de 22 de novembro de 2012, sobre Cibersegurança e Ciberdefesa ([4]),

— Tendo em conta a sua Resolução, de 22 de novembro de 2016, sobre a União Europeia da Defesa ([5]),

— Tendo em conta a proposta da Comissão de um regulamento do Parlamento Europeu e do Conselho, de 13 de setembro de 2017, relativo à ENISA, a «Agência da União Europeia para a Segurança das Redes e da Informação», e à certificação da cibersegurança das tecnologias da informação e comunicação, e que revoga o Regulamento (UE) n.º 526/2013 («Regulamento Cibersegurança») (COM(2017)0477),

— Tendo em conta a sua Resolução, de 13 de dezembro de 2017, sobre o relatório anual sobre a execução da Política Externa e de Segurança Comum (PESC) ([6]),

— Tendo em conta a sua Resolução, de 13 de dezembro de 2017, sobre o relatório anual sobre a execução da Política Comum de Segurança e Defesa (PCSD) ([7]),

— Tendo em conta o artigo 52.º do seu Regimento,

— Tendo em conta o relatório da Comissão dos Assuntos Externos (A8-0189/2018),

A. Considerando que os desafios, as ameaças e os ataques híbridos e cibernéticos constituem uma séria ameaça à segurança, defesa, estabilidade e competitividade da UE, dos seus Estados-Membros e dos seus cidadãos; que a ciberdefesa comporta manifestamente tanto a dimensão militar como a civil;

([1]) Cambridge University Press, fevereiro de 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
([2]) JO L 194 de 19.7.2016, p. 1.
([3]) Textos Aprovados, P8_TA(2017)0366.
([4]) JO C 419 de 16.12.2015, p. 145.
([5]) Textos Aprovados, P8_TA(2016)0435.
([6]) Textos Aprovados, P8_TA(2017)0493.
([7]) Textos Aprovados, P8_TA(2017)0492.

B. Considerando que a UE e os seus Estados-Membros enfrentam uma ameaça sem precedentes sob a forma de ciberataques patrocinados por Estados e com motivações políticas, bem como sob a forma de cibercriminalidade e ciberterrorismo;

C. Considerando que o ciberespaço é amplamente reconhecido pelas forças armadas como o quinto domínio operacional, permitindo o desenvolvimento de capacidades de ciberdefesa; que está a ser debatida a possibilidade de reconhecer o ciberespaço como o quinto campo de batalha;

D. Considerando que a cláusula de defesa mútua, consagrada no artigo 42.º, n.º 7, do Tratado da União Europeia (TUE), prevê a obrigação mútua de prestar auxílio e assistência por todos os meios ao alcance, caso um Estado-Membro seja alvo de agressão armada no seu território; que tal não afeta o caráter específico da política de segurança e defesa de determinados Estados-Membros; que a cláusula de solidariedade, consagrada no artigo 222.º do Tratado sobre o Funcionamento da União Europeia (TFUE), complementa a cláusula de defesa mútua, prevendo a obrigação dos Estados-Membros da UE de atuarem em conjunto se um Estado-Membro for alvo de um ataque terrorista ou vítima de uma catástrofe natural ou de origem humana; que a mesma cláusula implica a mobilização de meios civis e militares;

E. Considerando que, embora a ciberdefesa continue a ser fundamentalmente uma competência dos Estados-Membros, a UE tem um papel essencial a desempenhar na criação de uma plataforma de cooperação europeia e na garantia de que estas novas iniciativas sejam estreitamente coordenadas, a nível internacional e no quadro da arquitetura de segurança transatlântica, desde o início para evitar as lacunas e ineficiências que caracterizam muitos dos esforços envidados no âmbito tradicional da defesa; que é necessário ir além do reforço da cooperação e coordenação; que importa garantir uma prevenção eficaz através do reforço da capacidade da UE para detetar, defender e dissuadir; que uma ciberdefesa e uma ciberdissuasão credíveis são necessárias para alcançar uma cibersegurança eficaz da UE, assegurando em simultâneo que esses Estados estão pelo menos preparados para não serem facilmente alvo de ciberataques, e que uma considerável capacidade de ciberdefesa é uma componente necessária da PCSD e do desenvolvimento da União Europeia da Defesa; que nos encontramos numa situação de escassez permanente de especialistas em cibersegurança altamente qualificados; que a estreita coordenação para a proteção das forças armadas contra ciberataques é uma componente necessária para o desenvolvimento de uma PCSD eficaz;

F. Considerando que os Estados-Membros da UE são frequentemente objeto de ciberataques realizados por agentes estatais e não estatais, hostis e perigosos, contra alvos civis ou militares; que a atual vulnerabilidade se deve em grande parte à fragmentação das estratégias e capacidades de defesa europeias, que permite aos serviços estrangeiros de informações explorar repetidamente as vulnerabilidades de segurança das redes e sistemas informáticos essenciais para a segurança europeia; que os governos dos Estados-Membros muitas vezes não informam as partes interessadas pertinentes em tempo útil de forma a permitir-lhes resolver as vulnerabilidades nos seus produtos e serviços; que estes ataques requerem reforços urgentes e o desenvolvimento de capacidades europeias ofensivas e defensivas a nível civil e militar, a fim de evitar o eventual impacto económico e social transfronteiras dos ciberincidentes;

G. Considerando que a fronteira entre a interferência civil e militar se torna menos nítida no ciberespaço;

H. Considerando que muitos ciberincidentes são possíveis devido à falta de resiliência e robustez das infraestruturas públicas e privadas de rede, por má proteção ou segurança das bases de dados e por causa de outras deficiências nas infraestruturas críticas de informação; que apenas poucos Estados-Membros assumem a responsabilidade pela proteção da sua rede e dos sistemas de informação e dados associados como parte integrante do seu dever de diligência, o que explica a falta geral de investimento em formação, em tecnologias de segurança avançadas e no desenvolvimento de orientações adequadas;

I. Considerando que os direitos à privacidade e à proteção dos dados estão previstos na Carta dos Direitos Fundamentais da União Europeia e no artigo 16.º do TFUE, e são regulados pelo Regulamento Geral sobre a Proteção de Dados, que entrou em vigor em 25 de maio de 2018;

J. Considerando que uma política cibernética ativa e eficaz se caracteriza por ser capaz de dissuadir inimigos, bem como de perturbar as suas capacidades, condicionando e diminuindo a sua capacidade para atacar;

K. Considerando que vários grupos e organizações terroristas utilizam o ciberespaço como uma ferramenta de baixo custo para recrutar, radicalizar e disseminar propaganda terrorista; que os grupos terroristas, os agentes não estatais e as redes de criminalidade transnacionais recorrem a operações cibernéticas para angariar fundos anonimamente, recolher informações e desenvolver armas cibernéticas para realizar campanhas de ciberterrorismo, condicionar, danificar ou destruir infraestruturas críticas, atacar os sistemas financeiros e praticar outras atividades ilícitas que têm implicações para a segurança dos cidadãos europeus;

L. Considerando que a ciberdissuasão e a ciberdefesa das forças armadas e da infraestrutura crítica da Europa se tornaram questões cruciais nos debates sobre a modernização da defesa, os esforços comuns de defesa da Europa, o desenvolvimento futuro das forças armadas e das suas operações, e a autonomia estratégica da União Europeia;

M. Considerando que vários Estados-Membros investiram consideravelmente na criação de comandos cibernéticos dotados de pessoal suficiente para dar resposta a estes novos desafios e melhorar a sua ciber-resiliência, mas que é necessário fazer muito mais, dado que o combate aos ciberataques está a tornar-se cada vez mais difícil de efetuar a nível dos Estados-Membros; que os comandos cibernéticos de cada Estado-Membro variam em termos dos seus mandatos ofensivos e defensivos; que outras estruturas de ciberdefesa variam muito entre os Estados-Membros e com frequência permanecem fragmentadas; que a melhor forma de abordar a ciberdefesa e a ciberdissuasão é através da cooperação a nível europeu e em cooperação com os parceiros e aliados, já que o seu âmbito operacional ultrapassa as fronteiras nacionais e os limites das organizações; que a cibersegurança militar e a cibersegurança civil estão estreitamente relacionadas e que é necessária, por conseguinte, uma maior sinergia entre especialistas civis e militares; que as empresas privadas têm importantes conhecimentos especializados neste domínio, o que levanta questões fundamentais sobre governação e segurança, e sobre a capacidade de os Estados defenderem os seus cidadãos;

N. Considerando que existe uma necessidade imperiosa de reforçar as capacidades da UE no domínio da ciberdefesa dada a falta da resposta atempada às alterações no panorama da cibersegurança; que a rapidez de resposta e um estado de preparação adequado constituem elementos-chave para a garantia de segurança neste domínio;

O. Considerando que tanto a Cooperação Estruturada Permanente (CEP) como o Fundo Europeu de Defesa (FED) são novas iniciativas com a margem de manobra necessária para fomentar um ecossistema que pode proporcionar oportunidades para as PME e as empresas em fase de arranque, e para promover projetos de cooperação no domínio da ciberdefesa, e que ambas contribuirão para dar forma ao quadro regulamentar e institucional;

P. Considerando que os Estados-Membros que participam na CEP se comprometeram a garantir que os esforços de cooperação no domínio da ciberdefesa, como a partilha de informações, a formação e o apoio operacional, continuarão ser cada vez mais desenvolvidos;

Q. Considerando que, dos 17 projetos selecionados no âmbito da CEP, dois projetos são no domínio da ciberdefesa;

R. Considerando que o Fundo Europeu da Defesa deve apoiar a competitividade e a capacidade de inovação globais da indústria europeia de defesa, investindo nas tecnologias digitais e cibernéticas, bem como promover o desenvolvimento de soluções inteligentes proporcionando oportunidades para a participação das PME e das empresas em fase de arranque neste esforço;

S. Considerando que a Agência Europeia de Defesa (AED) lançou uma série de projetos para dar resposta à necessidade de os Estados-Membros desenvolverem as suas capacidades de ciberdefesa, nomeadamente projetos nos domínios da educação e da formação, tais como a Plataforma de Coordenação da Formação e Exercícios em Ciberdefesa (CD TEXP), o agrupamento de procura para o apoio de formação e exercícios em ciberdefesa do setor privado (DePoCyTE) e o projeto sobre plataformas virtuais de formação cibernética;

T. Considerando que existem outros projetos da UE em curso sobre o conhecimento da situação, a deteção e partilha de informações sobre software mal-intencionado (Plataforma para a Partilha de Informações sobre Software Mal-intencionado (MISP) e o Sistema Multiagente para a Deteção Avançada de Ameaças Persistentes (MASFAD));

U. Considerando que as necessidades de formação e de desenvolvimento de capacidades no domínio da ciberdefesa são consideráveis e crescentes, e que a maneira mais eficaz de as satisfazer é de forma cooperativa a nível da UE e da NATO;

V. Considerando que as missões e operações no âmbito da PCSD, como todas as iniciativas contemporâneas de organização, dependem profundamente de sistemas informáticos funcionais; que as ciberameaças às missões e operações da PCSD podem existir em vários níveis, desde o nível tático (missões e operações no âmbito da PCSD), passando pelo nível operacional (redes da UE) até um nível mais amplo da infraestrutura informática global;

W. Considerando que os sistemas de comando e controlo, de intercâmbio de informações e de logística dependem de infraestruturas informáticas classificadas e não classificadas, especialmente a nível tático e operacional; que estes sistemas constituem alvos atrativos para agentes mal-intencionados cujo objetivo seja atacar as missões; que os ciberataques podem ter repercussões graves nas infraestruturas da UE; que os ciberataques contra, nomeadamente, a infraestrutura energética da UE teriam graves consequências, pelo que deve ser protegida desses ataques;

X. Considerando amplamente reconhecido que a ciberdefesa deve ser devidamente tida em conta em todas as fases do processo de planeamento de missões e operações da PCSD, que exige um constante acompanhamento e que é necessário dispor das capacidades adequadas para a integrar plenamente no planeamento de missões e prestar continuamente o necessário apoio crítico;

Y. Considerando que a rede da Academia Europeia de Segurança e Defesa (AESD) é o único organismo de formação europeu para as estruturas, missões e operações da PCSD; que, de acordo com os planos atuais, o seu papel na partilha das capacidades de formação europeias no domínio cibernético deverá ser aumentado substancialmente;

Z. Considerando que a Declaração da NATO por ocasião da Cimeira de Varsóvia, em 2016, reconheceu o ciberespaço como um âmbito de operações no qual a NATO se deve defender com eficácia comparável à sua defesa no ar, na terra e no mar;

AA. Considerando que a UE e a NATO têm contribuído para melhorar as capacidades de ciberdefesa dos Estados-Membros, através de projetos de investigação de dupla utilização coordenados pela AED e pela NATO, e do reforço da ciber-resiliência dos Estados-Membros, através do apoio prestado pela Agência da UE para a Segurança das Redes e da Informação (ENISA);

AB. Considerando que, em 2014, a NATO criou operações de ciberdefesa integradas na sua defesa coletiva e que, em 2016, reconheceu o ciberespaço como um domínio operacional, a par da terra, do ar e do mar; que a UE e a NATO são parceiros que se complementam na criação da respetiva ciber-resiliência e de capacidades de ciberdefesa; que a cibersegurança e ciberdefesa são atualmente um dos mais importantes pilares da cooperação entre ambos e um domínio crítico no qual os dois possuem capacidades únicas; que, na Declaração Conjunta UE-NATO, de 8 de julho de 2016, a UE e a NATO chegaram a acordo quanto a uma ampla agenda de cooperação; que quatro das 42 propostas tendentes a uma cooperação mais estreita dizem respeito à cibersegurança e à ciberdefesa, e que existem outras propostas que visam resolver as ameaças híbridas, num sentido mais amplo; que este quadro foi complementado por mais uma proposta relativa à cibersegurança e à ciberdefesa, apresentada em 5 de dezembro de 2017;

AC. Considerando que o Grupo de Peritos Estatais da ONU sobre a Segurança da Informação (UNGGE) concluiu a sua última ronda de deliberações; que, apesar de não ter conseguido elaborar um relatório de consenso em 2017, os relatórios de 2015 e 2013 são aplicáveis, incluindo o reconhecimento de que o direito internacional, e em especial a Carta das Nações Unidas, é aplicável e essencial para manter a paz e a estabilidade, bem como para promover um ambiente aberto, seguro, pacífico e acessível para as TIC;

AD. Considerando que o quadro recentemente lançado para uma resposta diplomática conjunta da UE às atividades informáticas dolosas, os «instrumentos de ciberdiplomacia» da União Europeia, destinados a desenvolver as capacidades da UE e dos Estados-Membros no sentido de influenciar a conduta dos potenciais agressores, prevê o recurso a medidas proporcionadas no âmbito da PESC, incluindo a adoção de medidas restritivas;

AE. Considerando que diferentes intervenientes estatais – a Rússia, a China e a Coreia do Norte, entre outros, mas também intervenientes não estatais (incluindo grupos de criminalidade organizada) inspirados, contratados ou patrocinados por Estados, agências de segurança ou empresas privadas – participaram em atividades informáticas dolosas na prossecução de objetivos políticos, económicos ou de segurança que incluem ataques a infraestruturas críticas, espionagem cibernética e vigilância em larga escala dos cidadãos da UE, ajudando campanhas de desinformação e distribuindo software mal-intencionado (Wannacry e NotPetya, etc.) que limita o acesso à Internet e o funcionamento dos sistemas informáticos; que tais atividades ignoram e violam o direito internacional, os direitos humanos e os direitos fundamentais da UE, pondo simultaneamente em causa a democracia, a segurança, a ordem pública e a autonomia estratégica da UE, e que, por conseguinte, devem conduzir a uma resposta conjunta da UE, como o recurso ao quadro para uma resposta diplomática conjunta da UE, incluindo a utilização de medidas restritivas previstas nos instrumentos de ciberdiplomacia da UE, por exemplo, no caso de empresas privadas, a aplicação de multas e a restrição do acesso ao mercado interno;

AF. Considerando que este tipo de ataques em larga escala contra infraestruturas TIC foi levado a cabo várias vezes no passado, incluindo na Estónia em 2007, na Geórgia em 2008 e, atualmente, quase todos os dias na Ucrânia; que as capacidades cibernéticas ofensivas estão também a ser utilizadas contra os Estados-Membros da UE e os países da NATO numa escala inédita;

AG. Considerando que as tecnologias de cibersegurança, pertinentes para a esfera civil e para a esfera militar, são tecnologias de dupla utilização que proporcionam muitas oportunidades para criar sinergias entre intervenientes civis e militares num conjunto de áreas, tais como a cifragem, os instrumentos de gestão da segurança e da vulnerabilidade, a deteção de intrusões e os sistemas de prevenção;

AH. Considerando que o desenvolvimento de tecnologias cibernéticas nos próximos anos irá afetar novas áreas, como a inteligência artificial, a Internet das coisas, a robótica e os dispositivos portáteis, e que todos estes elementos podem igualmente ter implicações em matéria de segurança para o domínio da defesa;

AI. Considerando que os comandos cibernéticos criados por vários Estados-Membros podem contribuir significativamente para a proteção das infraestruturas civis vitais, e que os conhecimentos em matéria de ciberdefesa são, muitas vezes, igualmente úteis no domínio civil;

Desenvolvimento de capacidades de ciberdefesa e ciberdissuasão

1. Sublinha que a política comum em matéria de ciberdefesa e um nível significativo de capacidades de ciberdefesa devem ser elementos centrais do desenvolvimento da União Europeia da Defesa;

2. Congratula-se com a iniciativa da Comissão de apresentar um pacote em matéria de cibersegurança, com vista a promover a ciber-resiliência, a ciberdissuasão e a ciberdefesa da UE;

3. Recorda que a ciberdefesa possui dimensões militares e civis, e que tal significa que é necessária uma abordagem política integrada e uma estreita cooperação entre as partes interessadas militares e civis;

4. Apela ao desenvolvimento coerente de capacidades cibernéticas em todas as instituições e órgãos da UE, bem como nos Estados-Membros, e para que se encontrem as necessárias soluções políticas e práticas que permitam superar as remanescentes barreiras políticas, legislativas e organizativas à cooperação em matéria de ciberdefesa; entende que a cooperação e o intercâmbio periódicos e reforçados entre os intervenientes públicos pertinentes no domínio da ciberdefesa, a nível nacional e da UE, são cruciais;

5. Insiste vivamente em que, no âmbito da emergente União Europeia de Defesa, as capacidades de ciberdefesa dos Estados-Membros estejam na linha da frente e, na medida do possível, integradas desde o início, a fim de garantir a máxima eficácia; insta, por conseguinte, os Estados-Membros a cooperarem estreitamente no desenvolvimento da respetiva ciberdefesa, com um roteiro claro, contribuindo assim para um processo coordenado pela Comissão, pelo Serviço Europeu para a Ação Externa (SEAE) e pela AED com vista a uma melhor racionalização das estruturas de ciberdefesa nos Estados-Membros, aplicando medidas disponíveis de curto prazo com urgência e promovendo o intercâmbio de conhecimentos especializados; entende que deve ser criada uma rede europeia segura para informações e infraestruturas críticas; reconhece igualmente que uma robusta capacidade de atribuição da autoria é uma componente essencial de uma ciberdefesa e uma ciberdissuasão eficazes, e que uma prevenção eficaz exigirá o desenvolvimento substancial de novos conhecimentos tecnológicos especializados; insta os Estados-Membros a aumentarem os recursos financeiros e humanos, em especial os peritos no domínio da informática forense, a fim de melhorar a capacidade de atribuição da autoria dos ciberataques; sublinha que essa cooperação deve igualmente ser implementada através do reforço da ENISA;

6. Reconhece que muitos Estados-Membros consideram que a detenção de capacidades de ciberdefesa próprias deve estar no cerne da sua estratégia de segurança nacional e constituir uma parte essencial da sua soberania nacional; salienta, no entanto, que devido à natureza sem fronteiras do ciberespaço, a escala e os conhecimentos necessários para a instalação de forças verdadeiramente abrangentes e eficazes que assegurem o objetivo de autonomia estratégica da UE no ciberespaço está fora do alcance de qualquer Estado-Membro isolado, exigindo, portanto, uma resposta coordenada e reforçada da parte de todos os Estados-Membros a nível da UE; assinala, neste contexto, que a UE e os seus Estados-Membros se encontram pressionados pelo tempo no que se refere à criação dessas forças e têm de tomar medidas imediatamente; observa que, devido a algumas iniciativas da UE, como o mercado único digital, a UE está bem colocada para assumir um papel de liderança no desenvolvimento de estratégias europeias de ciberdefesa; recorda que o desenvolvimento da ciberdefesa a nível da UE deve favorecer a capacidade da União para se proteger a si própria; congratula-se, a este respeito, com a proposta no sentido de confiar um mandato permanente à ENISA e de reforçar o seu papel;

7. Exorta, neste contexto, os Estados-Membros a utilizarem da melhor forma possível o quadro estabelecido pela CEP e pelo Fundo Europeu de Defesa para propor projetos de cooperação;

8. Salienta o árduo trabalho realizado pela UE e pelos Estados-Membros no domínio da ciberdefesa; assinala, em especial, os projetos da AED sobre plataformas virtuais de formação cibernética, a Agenda Estratégica de Investigação em Ciberdefesa e o desenvolvimento de pacotes mobilizáveis de sensibilização sobre situações no domínio da cibersegurança para os centros de operação;

9. Acolhe com agrado os dois projetos informáticos que serão lançados no quadro da CEP, a saber, uma plataforma de intercâmbio de informações relativas a ciberameaças e à resposta a ciberincidentes e equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança; destaca que estes dois projetos se centram numa política cibernética defensiva que se baseia na partilha de informações relativas a ciberameaças, através de uma plataforma em rede dos Estados-Membros e da criação de equipas de resposta rápida a ciberataques (ERRC), permitindo aos Estados-Membros entreajudarem-se para garantir um nível mais elevado de ciber-resiliência e, em conjunto, detetar, identificar e atenuar as ciberameaças; insta a Comissão e os Estados-Membros a desenvolverem os projetos da CEP relativos às equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança, através da criação de uma ERRC europeia encarregada de coordenar, detetar e combater ciberameaças coletivas, apoiando os esforços dos Estados-Membros participantes;

10. Observa que a capacidade da UE de desenvolver projetos de ciberdefesa se baseia no domínio das tecnologias, dos equipamentos, dos serviços e dos dados e do seu tratamento, requerendo uma base de agentes industriais fidedignos;

11. Recorda que um dos objetivos dos esforços envidados para melhorar a homogeneidade dos sistemas de comando consiste em garantir que os ativos de comando disponíveis sejam interoperáveis com os dos países da NATO não membros da UE, bem como com os dos parceiros apropriados, e garantir a fluidez dos intercâmbios de informações, a fim de acelerar a tomada de decisões, e manter o controlo das informações num contexto de risco cibernético;

12. Recomenda que se encontrem formas de complementar os projetos de defesa inteligente da NATO (por exemplo, os projetos de desenvolvimento de capacidades de ciberdefesa multinacionais, a Plataforma para a Partilha de Informações sobre Software Mal-intencionado (MISP) e a Educação e Formação em Ciberdefesa Multinacional (MNCDE&T));

13. Reconhece os progressos que estão a ser feitos em áreas como a nanotecnologia, a inteligência artificial, os megadados, a robótica avançada e a área dos resíduos de equipamentos elétricos e eletrónicos; insta os Estados-Membros e a UE a prestarem especial atenção à eventual exploração destas áreas por intervenientes não estatais hostis e por grupos de criminalidade organizada; apela ao desenvolvimento de formação e capacidades que visem proteger contra o surgimento de métodos sofisticados de criminalidade, tais como fraudes complexas de identidade e a contrafação de bens;

14. Salienta a necessidade de uma maior clareza terminológica sobre segurança no ciberespaço, bem como de uma abordagem abrangente e integrada e esforços conjuntos para combater as ciberameaças e as ameaças híbridas, para detetar e erradicar refúgios em linha da criminalidade e das entidades extremistas, reforçando e intensificando a partilha de informações entre a UE e as agências da UE, como a Europol, a Eurojust, a AED e a ENISA;

15. Sublinha o crescente papel da inteligência artificial, tanto na componente de ciberataque como na de ciberdefesa; insta a UE e os Estados-Membros a prestarem especial atenção a esta área, tanto ao longo da investigação como no desenvolvimento prático das suas capacidades de ciberdefesa;

16. Salienta categoricamente que devem ser tomadas medidas para reduzir o potencial de vulnerabilidades cibernéticas no âmbito da mobilização de veículos aéreos não tripulados, sejam eles armados ou não;

Ciberdefesa das missões e operações da PCSD

17. Salienta que a ciberdefesa deve ser considerada uma tarefa operacional das missões e operações da PCSD e que a mesma deve ser incluída em todos os processos de planeamento da PCSD, tendo sempre em conta a cibersegurança durante a fase de planeamento, reduzindo, deste modo, as lacunas de vulnerabilidade cibernética;

18. Reconhece que o planeamento de uma missão ou operação bem-sucedida da PCSD requer importantes conhecimentos especializados em matéria de ciberdefesa e infraestruturas e redes informáticas seguras, tanto a nível do centro de operações como a nível da missão propriamente dita, para se poder efetuar uma avaliação exaustiva da ameaça e garantir uma proteção adequada neste domínio; insta o SEAE e os Estados-Membros a disponibilizarem centros de comando para as operações da PCSD, a fim de reforçar os conhecimentos especializados em matéria de ciberdefesa das missões e operações da UE; assinala o facto de haver um limite até o qual as missões da PCSD poderão estar preparadas para se protegerem a si mesmas de ciberataques;

19. Salienta que o planeamento de todas as missões e operações da PCSD tem de ser acompanhado de uma avaliação pormenorizada do contexto de ciberameaças; assinala que a classificação das ameaças elaborada pela ENISA proporciona um modelo adequado para essa avaliação; recomenda a criação de capacidades de avaliação da ciber-resiliência dos centros de operação da PCSD;

20. Reconhece, nomeadamente, a importância de reduzir ao mínimo necessário a pegada cibernética e as superfícies de ataque das missões e operações da PCSD; insta os responsáveis pelo planeamento a terem este aspeto em conta desde o início do processo de planeamento;

21. Regista a Avaliação das Necessidades de Formação da AED, que revelou graves insuficiências em matéria de competências e aptidões no domínio da ciberdefesa entre os decisores, não apenas nos Estados-Membros, e congratula-se com as iniciativas da AED relativas aos cursos para os altos decisores nos Estados-Membros, para apoiar o planeamento das missões e operações da PCSD;

Educação e formação em ciberdefesa

22. Assinala que a racionalização do panorama da educação e formação em ciberdefesa da UE atenuaria significativamente as ameaças e insta a UE e os Estados-Membros a intensificarem a cooperação na educação, formação e realização de exercícios;

23. Apoia com convicção o programa Erasmus Militar e outras iniciativas comuns de formação e intercâmbio que visam reforçar a interoperabilidade das forças armadas dos Estados-Membros e o desenvolvimento de uma cultura estratégica comum através de um maior intercâmbio de jovens militares, tendo presente que essa interoperabilidade é necessária entre todos os Estados-Membros e aliados da NATO; entende, todavia, que os intercâmbios de formação e educação no domínio da ciberdefesa devem ir além desta iniciativa e incluir pessoal militar de todas as idades e patentes, bem como estudantes de todos os centros de estudos académicos com programas educativos em matéria de cibersegurança;

24. Salienta que são necessários mais peritos no domínio da ciberdefesa; insta os Estados-Membros a promoverem a cooperação entre instituições académicas civis e academias militares para colmatar esta lacuna, tendo em vista a criação de mais possibilidades de educação e formação no domínio da ciberdefesa, bem como a consagrarem mais recursos à formação operacional cibernética especializada, incluindo sobre inteligência artificial; insta as academias militares a integrarem o ensino em matéria de ciberdefesa nos seus programas curriculares, contribuindo assim para aumentar a reserva de talentos no domínio da cibernética disponíveis para satisfazer as necessidades das missões de PCSD;

25. Insta os Estados-Membros a informarem, sensibilizarem e aconselharem, de forma satisfatória e proativa, as empresas, as escolas e os cidadãos no que se refere à cibersegurança e às principais ameaças digitais; acolhe favoravelmente, a este respeito, a elaboração de manuais cibernéticos como instrumento de orientação dos cidadãos e das organizações rumo a uma melhor estratégia de cibersegurança, de promoção do conhecimento no domínio da cibersegurança e de reforço da ciber-resiliência a todos os níveis;

26. Assinala que, dada a necessidade de um maior número de pessoal especializado, os Estados-Membros devem concentrar-se não apenas no recrutamento de pessoal competente para as forças armadas, mas também na retenção dos especialistas necessários;

27. Congratula-se com a execução – por 11 Estados-Membros (Áustria, Bélgica, Alemanha, Estónia, Grécia, Finlândia, Irlanda, Letónia, Países Baixos, Portugal e Suécia) do projeto de federação sobre plataformas virtuais de formação cibernética – do primeiro de quatro projetos de ciberdefesa lançados no quadro da agenda de Mutualização e Partilha da AED; exorta os restantes Estados-Membros a juntarem-se a esta iniciativa; insta os Estados-Membros a promoverem uma maior disponibilidade mútua de ações de formação em ciberdefesa virtual e de plataformas virtuais de formação cibernética; observa que, a este respeito, deve ser tido em conta o papel e o conhecimento especializado da ENISA;

28. Considera que estas iniciativas contribuem para melhorar a qualidade da educação no domínio da ciberdefesa à escala da UE, em especial através da criação de plataformas técnicas de amplo alcance e do estabelecimento de uma comunidade de peritos da UE; considera que as forças armadas europeias podem tornar-se mais atrativas proporcionando uma formação abrangente em ciberdefesa para atrair e reter talentos no domínio cibernético; sublinha a necessidade de identificar as fragilidades dos sistemas informáticos, tanto dos Estados-Membros como das instituições da UE; reconhece que o erro humano é uma das fragilidades mais frequentemente identificadas nos sistemas de cibersegurança, pelo que insta à organização de ações periódicas de formação para pessoal militar e civil que trabalha nas instituições da UE;

29. Exorta a AED a lançar a Plataforma de Coordenação da Formação, Educação e Treino em Ciberdefesa para apoiar a federação sobre plataformas virtuais de formação cibernética o mais rapidamente possível, concentrando-se no reforço da cooperação em matéria de requisitos harmonizados, na promoção da investigação e das inovações tecnológicas no domínio da ciberdefesa, e na prestação de assistência conjunta a países terceiros no reforço das suas capacidades de criação de resiliência no domínio da ciberdefesa; insta a Comissão e os Estados-Membros a complementarem estas iniciativas com a criação de um centro de excelência europeu para a formação em ciberdefesa, que preste formação especializada aos recrutas mais promissores, em complemento da formação no domínio cibernético prestada pelos Estados-Membros participantes;

30. Encoraja a criação, no âmbito da AESD, de uma Plataforma de Formação, Educação, Treino e Avaliação em Ciberdefesa com vista a alargar as oportunidades de formação e educação nos Estados-Membros;

31. Incentiva a realização de mais intercâmbios para a sensibilização sobre situações, através de exercícios cibernéticos de gabinete e da coordenação dos respetivos esforços de desenvolvimento de capacidades, destinados a alcançar uma maior interoperabilidade e uma melhor prevenção e resposta a ataques futuros; apela para que esses projetos sejam realizados com aliados da NATO, as forças armadas dos Estados-Membros da UE e outros parceiros com uma ampla experiência no combate a ciberataques, a fim de desenvolver a preparação operacional, procedimentos e normas comuns para dar uma resposta abrangente a diferentes ciberameaças; congratula-se, a este título, com a participação da UE em determinados exercícios cibernéticos, tal como o exercício de ciberataque e ciberdefesa (CODE);

32. Recorda que um ciberespaço resiliente exige uma ciber-higiene irrepreensível; exorta todos os intervenientes públicos e privados a realizarem formações periódicas no domínio da ciber-higiene para todos os membros do seu pessoal;

33. Recomenda o reforço do intercâmbio de conhecimentos especializados e de ensinamentos entre as forças armadas, as forças policiais e outros organismos estatais dos Estados-Membros ativamente envolvidos na luta contra ciberameaças;

A cooperação UE-NATO no domínio da ciberdefesa

34. Reitera que, com base nos seus valores e interesses estratégicos comuns, a UE a NATO têm uma responsabilidade e capacidade especiais de abordar mais eficientemente, e em estreita cooperação, os crescentes desafios no domínio da cibersegurança e ciberdefesa, através da procura de eventuais complementaridades, evitando a duplicação de ações e assumindo as suas respetivas responsabilidades;

35. Exorta o Conselho, em colaboração com outras instituições e estruturas pertinentes da UE, a estudar formas de apoiar a nível da União, o mais rapidamente possível, a integração do domínio cibernético nas doutrinas militares dos Estados-Membros, de modo harmonizado e em estreita cooperação com a NATO;

36. Apela à aplicação das medidas que já foram objeto de acordo; solicita que sejam identificadas novas iniciativas para uma maior cooperação entre a UE e a NATO, tendo igualmente em conta as possibilidades de cooperação no âmbito do Centro de Excelência Cooperativo para a Ciberdefesa da NATO (CCD COE) e da Academia das Comunicações e da Informação da NATO, que visam reforçar as capacidades de formação em matéria de ciberdefesa nos sistemas informáticos e cibernéticos, tanto na sua componente de software como na de hardware; observa que tal poderia incluir um diálogo com a NATO sobre a possibilidade de a UE aderir ao CCD COE com vista a uma maior complementaridade e colaboração; congratula-se com a recente criação do Centro de Excelência Europeu de Luta contra as Ameaças Híbridas; exorta todas as instituições e os aliados pertinentes a reunirem-se periodicamente para debater as suas atividades, a fim de evitar sobreposições e promover uma abordagem coordenada para a ciberdefesa; entende que é crucial incentivar, com base na confiança mútua, o intercâmbio de informações sobre ciberameaças entre os Estados-Membros e com a NATO;

37. Manifesta convicção de que o reforço da cooperação entre a UE e a NATO no domínio da ciberdefesa é importante e útil como meio para prevenir, detetar e dissuadir ciberataques; insta, por conseguinte, ambas as organizações a reforçar a sua cooperação e coordenação operacionais e a alargar os seus esforços conjuntos de desenvolvimento de capacidades, em particular em termos de exercícios e formação conjuntos de pessoal civil e militar de ciberdefesa e através da participação dos Estados-Membros em projetos de defesa inteligente da NATO; considera fundamental que a UE e a NATO intensifiquem a partilha de informações de modo a permitir a atribuição formal de ciberataques e, consequentemente, a imposição de sanções restritivas aos responsáveis pelos mesmos; exorta ambas as organizações a também cooperarem mais estreitamente no que se refere aos aspetos cibernéticos da gestão de crises;

38. Congratula-se com o intercâmbio de conceitos no sentido de integrar os requisitos e as normas no domínio da ciberdefesa no planeamento e na execução das missões e operações para estimular a interoperabilidade, e exprime o desejo de que seja seguido de uma maior cooperação operacional para assegurar a ciberdefesa das respetivas missões e a sincronia das abordagens operacionais;

39. Acolhe favoravelmente o acordo entre a equipa de resposta a emergências informáticas da União Europeia (CERT-UE) e a Capacidade de Resposta a Incidentes Informáticos da NATO (NCIRC) que visa facilitar o intercâmbio de informações, o apoio logístico, a avaliação das ameaças comuns, o recrutamento de pessoal e a partilha das melhores práticas, aspetos que asseguram a capacidade de dar resposta imediata às ameaças; salienta que é importante incentivar o intercâmbio de informações entre a CERT-UE e a NCIRC e diligenciar no sentido de um aumento do nível de confiança; entende que se presume que as informações detidas pela CERT-UE poderão ser úteis para efeitos de investigação em ciberdefesa e para a NATO, e que estas informações deverão, por conseguinte, ser partilhadas, desde que esteja assegurada a plena conformidade com a legislação da UE em matéria de proteção dos dados;

40. Congratula-se com a cooperação entre as duas organizações em matéria de exercícios de ciberdefesa; regista a participação de representantes da União no exercício anual da Coligação Cibernética; reconhece os progressos que representa a participação da UE através de exercícios paralelos e coordenados (PACE) 17 no Exercício de Gestão de Crises da NATO 17, e congratula-se, em particular, com a inclusão de uma componente de ciberdefesa; insta ambas as organizações a intensificar esses esforços;

41. Insta a UE e a NATO a organizarem periodicamente exercícios a nível estratégico, com a participação dos principais dirigentes políticos de ambas as organizações; congratula-se, neste contexto, com o exercício EU CYBRID 2017 organizado pela Estónia, o qual registou, pela primeira vez, a participação do Secretário-Geral da NATO num exercício da UE;

42. Assinala que existe uma margem significativa para estabelecer um programa de cooperação mais ambicioso e concreto em matéria de ciberdefesa que vá além do nível concetual de cooperação no âmbito das operações específicas; insta ambas as organizações a aplicarem, na prática e de forma eficaz, tudo o que já existe, e a apresentarem propostas mais ambiciosas no próximo exame da aplicação da Declaração Conjunta;

43. Congratula-se com a Parceria Cibernética da Indústria da NATO (NICP), instituída em 2014, e insta a UE a empenhar-se nos esforços cooperativos da NICP para ligar o esforço de cooperação NATO-UE ao dos líderes da indústria especializados nas tecnologias cibernéticas, a fim de fazer progredir a cibersegurança através de uma colaboração continuada com especial incidência: na formação, nos exercícios e na educação para a NATO, a UE e representantes da indústria; na inclusão da UE e da indústria nos projetos de defesa inteligente da NATO; na partilha colaborativa de informações e melhores práticas em matéria de preparação e recuperação entre a NATO, a UE e a indústria; na prossecução do desenvolvimento conjunto de capacidades no domínio da ciberdefesa; e em respostas conjuntas a incidentes informáticos, se for caso disso;

44. Assinala os trabalhos em curso no âmbito da proposta de regulamento que altera o Regulamento ENISA (Regulamento (UE) n.º 526/2013) e que institui um quadro europeu para a certificação e rotulagem da segurança das TIC; insta a ENISA a celebrar um acordo com a NATO para reforçar a sua cooperação prática, incluindo a partilha de informações e a participação em exercícios no domínio da ciberdefesa;

Normas internacionais aplicáveis ao ciberespaço

45. Solicita a integração das capacidades de ciberdefesa na PESC e na ação externa da UE e dos seus Estados-Membros como uma tarefa transversal, e insta a uma coordenação mais estreita no domínio da ciberdefesa entre os Estados-Membros, as instituições da UE, a NATO, as Nações Unidas, os Estados Unidos e outros parceiros estratégicos, nomeadamente no que diz respeito às regras, normas e medidas coercivas no ciberespaço;

46. Lamenta que, após vários meses de negociações, o Grupo de Peritos Governamentais da ONU 2016-2017 (UNGGE) não tenha conseguido elaborar um novo relatório de consenso; recorda que, tal como reconhece o relatório de 2013, o direito internacional em vigor e a Carta das Nações Unidas, em particular – que proíbe a ameaça ou o uso da força contra a independência política de qualquer Estado, incluindo as ciberoperações coercivas destinadas a perturbar a infraestrutura técnica essencial para a realização de processos participativos oficiais, incluindo eleições, noutro Estado – são aplicáveis e devem ser aplicados no ciberespaço; recorda que o relatório de 2015 da UNGGE enumera um conjunto de normas para a conduta responsável dos Estados, incluindo a proibição de os Estados levarem a cabo ou apoiarem deliberadamente atividades cibernéticas contrárias às suas obrigações decorrentes do direito internacional; apela à UE para que assuma uma posição de liderança nos debates em curso e futuros relativos às normas internacionais no ciberespaço e à sua aplicação;

47. Assinala a importância do Manual de Taline 2.0, como ponto de partida para um debate e uma análise das possíveis modalidades de aplicação do direito internacional em vigor ao ciberespaço; exorta os Estados-Membros a iniciarem a análise e aplicação dos elementos indicados pelos peritos no Manual de Taline e a chegarem a acordo sobre outras normas voluntárias em matéria de conduta internacional; assinala em especial que toda a utilização ofensiva de capacidades cibernéticas deve ter por base o direito internacional;

48. Reitera o seu pleno compromisso para com um ciberespaço aberto, livre, estável e seguro, que respeite os valores fundamentais da democracia, os direitos humanos e o Estado de direito, e em que os diferendos internacionais sejam resolvidos por meios pacíficos, tendo por base a Carta das Nações Unidas e os princípios do direito internacional; exorta os Estados-Membros a promoverem uma melhor aplicação da abordagem global e comum da UE no domínio da ciberdiplomacia e das normas cibernéticas em vigor, e a elaborarem, em conjunto com a NATO, critérios e definições a nível da UE do que constitui um ciberataque, a fim de melhorar a capacidade da UE de chegar rapidamente a uma posição comum na sequência de um ato ilícito a nível internacional sob a forma de ciberataque; apoia firmemente a aplicação de normas voluntárias e não vinculativas de conduta responsável dos Estados no ciberespaço, referidas no relatório de 2015 da UNGGE, abrangendo o respeito da privacidade e dos direitos fundamentais dos cidadãos, bem como a criação de medidas regionais de reforço da confiança; apoia, neste contexto, o trabalho da Comissão Mundial sobre a Estabilidade do Ciberespaço no sentido de elaborar propostas de normas e políticas para reforçar a segurança e a estabilidade internacionais e orientar a conduta responsável dos agentes estatais e não estatais no ciberespaço; subscreve a proposta que defende que os agentes estatais e não estatais não devem realizar ou permitir deliberadamente a realização de atividades que prejudiquem intencional e substancialmente a integridade ou disponibilidade geral do núcleo público da Internet e, por conseguinte, a estabilidade do ciberespaço;

49. Reconhece que a maioria das infraestruturas tecnológicas é detida ou explorada pelo setor privado, e que uma estreita cooperação com o setor privado e os grupos da sociedade civil, assim como a sua consulta e inclusão, através de um diálogo entre as diversas partes interessadas, é por conseguinte essencial para garantir um ciberespaço aberto, livre e estável;

50. Reconhece que, devido a dificuldades na sua aplicação, os acordos bilaterais entre Estados nem sempre dão os resultados esperados; considera, por conseguinte, que a formação de coligações dentro de grupos de países com valores semelhantes dispostos a criar consensos constitui um meio eficaz para complementar os esforços das diversas partes interessadas; sublinha o papel importante que as autoridades locais desempenham no processo de inovação tecnológica e partilha de dados, no que toca a reforçar a luta contra a criminalidade e o terrorismo;

51. Congratula-se com a adoção, pelo Conselho, do quadro para uma resposta diplomática conjunta da UE às ciberatividades mal-intencionadas, os chamados instrumentos de ciberdiplomacia da UE; apoia a possibilidade de a UE tomar medidas restritivas contra adversários que atacam os seus Estados-Membros no ciberespaço, incluindo a imposição de sanções;

52. Insta a uma abordagem proativa clara no domínio da cibersegurança e da ciberdefesa, e ao reforço da ciberdiplomacia da UE, como uma tarefa transversal na política externa da União, e das suas capacidades e instrumentos a todos os níveis, de modo a que estes possam reforçar eficazmente as normas e valores da UE, bem como abrir caminho para um consenso sobre regras, normas e medidas de execução no ciberespaço a nível mundial; observa que a criação de ciber-resiliência em países terceiros contribui para a paz e a segurança internacionais e, em última análise, dá uma maior segurança aos cidadãos europeus;

53. Considera que os ciberataques como o NotPetya ou o WannaCry são dirigidos por Estados ou realizados com o conhecimento e aprovação de um Estado; assinala que estes ciberataques, que provocam prejuízos económicos graves e duradouros, além de representarem uma ameaça à vida, são claramente violações do direito internacional e das normas jurídicas internacionais; entende, por conseguinte, que os incidentes NotPetya e WannaCry representam violações do direito internacional, respetivamente pela Federação da Rússia e pela Coreia do Norte, e que os dois países devem enfrentar uma resposta proporcional e adequada da UE e da NATO;

54. Insta a que o Centro Europeu da Cibercriminalidade da Europol se torne um ponto focal para as unidades das forças de aplicação da lei e as agências governamentais dedicadas à cibercriminalidade, cuja principal responsabilidade seria gerir a defesa dos domínios .eu e das infraestruturas críticas das redes da UE durante um ataque; salienta que esse ponto focal deve também ter competência para proceder ao intercâmbio de informações e prestar assistência aos Estados-Membros;

55. Salienta a importância do desenvolvimento de normas em matéria de privacidade e segurança, cifragem, discurso de ódio, desinformação e ameaças de terrorismo;

56. Recomenda que cada Estado-Membro aceite a obrigação de prestar assistência a outros Estados-Membros sob ciberataque e de garantir a responsabilidade cibernética nacional em estreita cooperação com a NATO;

Cooperação civil e militar

57. Insta todas as partes interessadas a reforçarem as parcerias no domínio da transferência de conhecimentos, a aplicarem modelos empresariais adequados e a reforçarem a confiança entre empresas e utilizadores finais da esfera civil e do setor da defesa, bem como a melhorarem a transferência dos conhecimentos académicos para soluções práticas, a fim de criar sinergias e transferir soluções entre o mercado civil e o mercado militar – essencialmente um mercado único europeu para a cibersegurança e produtos de cibersegurança, tendo por base procedimentos transparentes e respeitando o direito internacional e da União, com vista a preservar e reforçar a autonomia estratégica da UE; assinala o papel fulcral que as empresas privadas de cibersegurança desempenham no alerta precoce e na atribuição da autoria dos ciberataques;

58. Salienta vivamente a importância da I&D, em particular à luz dos requisitos de segurança de alto nível no mercado da defesa; insta a UE e os Estados-Membros a darem mais apoio prático à indústria europeia da cibersegurança e a outros intervenientes económicos pertinentes, a reduzirem os encargos burocráticos, em especial para as PME e as empresas em fase de arranque (principais fontes de soluções inovadoras no domínio da ciberdefesa), e a promoverem uma cooperação mais estreita com as grandes organizações de investigação universitárias, com vista a reduzir a dependência dos produtos de cibersegurança de fontes externas e a criar uma cadeia de abastecimento estratégica no interior da UE que aumente a sua autonomia estratégica; assinala, neste contexto, o valioso contributo que pode ser dado pelo Fundo Europeu de Defesa e outros instrumentos do Quadro Financeiro Plurianual (QFP);

59. Incentiva a Comissão a integrar aspetos de ciberdefesa numa rede de centros europeus de investigação e de competências em cibersegurança, tendo igualmente em vista atribuir um nível adequado de recursos às capacidades e tecnologias cibernéticas de dupla utilização no próximo QFP;

60. Regista que a proteção de ativos de infraestruturas públicas e outras infraestruturas críticas civis, nomeadamente sistemas de informação e dados associados, é uma tarefa essencial de defesa para os Estados-Membros e, nomeadamente para as autoridades encarregadas da segurança dos sistemas de informação, e deve fazer parte das funções atribuídas às estruturas nacionais de ciberdefesa ou às referidas autoridades; realça que isto irá exigir um nível de confiança e uma cooperação o mais estreita possível entre os militares, agências de ciberdefesa, outras autoridades pertinentes e os setores afetados, o que só poderá ser alcançado através da definição clara dos deveres, dos papéis e das responsabilidades dos agentes civis e militares, e exorta todas as partes interessadas a terem em conta este aspeto nos seus processos de planeamento; insta a uma maior cooperação transfronteiras, respeitando plenamente a legislação da UE em matéria de proteção de dados, no que se refere à aplicação da lei relativa ao combate às ciberatividades mal-intencionadas;

61. Apela a todos os Estados-Membros para que centrem as suas estratégias nacionais em matéria de cibersegurança na proteção dos sistemas de informação e dos dados associados e que considerem a proteção destas infraestruturas críticas como parte integrante do seu dever de diligência; insta os Estados-Membros a adotarem e executarem estratégias, orientações e instrumentos que garantam um nível razoável de proteção contra níveis de ameaça razoavelmente identificáveis, devendo os custos e o encargo da proteção ser proporcionais aos eventuais prejuízos suscetíveis de serem sofridos pelas partes em causa; exorta os Estados-Membros a tomarem as medidas adequadas para obrigar as pessoas coletivas sob a sua jurisdição a protegerem os dados pessoais que estão ao seu cuidado;

62. Reconhece que, devido ao contexto em mutação das ciberameaças, poderá ser aconselhável uma cooperação mais estruturada e reforçada, em especial em algumas áreas críticas, por exemplo a localização de ameaças relacionadas com a *jihad* cibernética, o ciberterrorismo, a radicalização em linha e o financiamento de organizações extremistas ou radicais;

63. Incentiva uma estreita cooperação entre as agências da UE, tais como a AED, a ENISA e o Centro Europeu da Cibercriminalidade, numa abordagem intersetorial, a fim de promover sinergias e evitar sobreposições;

64. Insta a Comissão a elaborar um roteiro para uma abordagem coordenada à ciberdefesa europeia que inclua uma atualização do Quadro de Política de Ciberdefesa da UE, a fim de garantir que o mesmo continue a ser adequado aos fins que persegue enquanto mecanismo de intervenção pertinente para atingir os objetivos de ciberdefesa da UE, em estreita cooperação com os Estados-Membros, a AED, o Parlamento e o SEAE; assinala que este processo tem de fazer parte de uma abordagem estratégica mais ampla para a PCSD;

65. Apela ao reforço das capacidades em matéria de cibersegurança através da cooperação para o desenvolvimento, bem como da educação e formação contínuas para a sensibilização no domínio cibernético, tendo em conta que, nos próximos anos, haverá milhões de novos utilizadores da Internet, na sua maioria localizados nos países em desenvolvimento, reforçando, assim, a resiliência dos países e das sociedades face às ciberameaças e às ameaças híbridas;

66. Apela para que haja uma cooperação internacional e sejam promovidas iniciativas multilaterais para criar quadros exigentes nos domínios da ciberdefesa e cibersegurança que combatam a captura do Estado pela corrupção, pela fraude financeira, pelo branqueamento de capitais e pelo financiamento do terrorismo, e dar resposta aos desafios colocados pelo ciberterrorismo e pelas criptomoedas e outros métodos de pagamento alternativos;

67. Assinala que os ciberataques como o NotPetya se propagam rapidamente, provocando, assim, prejuízos de modo indiscriminado, a menos que haja uma ampla resiliência a nível mundial; entende que a formação e a educação no domínio da ciberdefesa devem fazer parte da ação externa da UE e que criar ciber-resiliência em países terceiros contribui para a paz e a segurança internacionais, proporcionando, em última análise, maior segurança aos cidadãos europeus;

Reforço institucional

68. Insta os Estados-Membros a cooperarem de forma ambiciosa no domínio do ciberespaço no âmbito da CEP; sugere que os Estados-Membros lancem um novo programa de cooperação no domínio cibernético no âmbito da CEP com vista a apoiar o planeamento, o comando e o controlo rápidos e eficazes das missões e operações em curso e futuras da UE; assinala que este programa deve proporcionar uma melhor coordenação das capacidades operacionais no ciberespaço e pode conduzir ao desenvolvimento de um comando comum de ciberdefesa, quando o Conselho Europeu assim decidir;

69. Reitera o seu apelo aos Estados-Membros e à VP/AR para que apresentem um livro branco da UE sobre a segurança e a defesa; insta os Estados-Membros e a VP/AR a fazerem da ciberdefesa e da ciberdissuasão uma pedra angular do livro branco, abrangendo a proteção do ciberespaço no que se refere às operações previstas no artigo 43.º do TUE e a defesa comum prevista no artigo 42.º, n.º 7, do TUE;

70. Assinala que o novo programa de cooperação da CEP no domínio cibernético deve ser liderado por militares de alta patente e por pessoal civil de cada Estado-Membro, numa base rotativa, e deve prestar contas perante os ministros da defesa da UE, no formato CEP, e a VP/AR, a fim de promover o princípio da confiança entre os Estados-Membros e as instituições e agências da UE no que se refere ao intercâmbio de informações;

71. Renova o apelo para a criação de um Conselho de Defesa da UE, com base no Comité Diretor ministerial da AED e no formato CEP com os ministros da defesa da UE, a fim de garantir que é dada prioridade e operacionalidade aos recursos e à integração e cooperação eficazes entre os Estados-Membros;

72. Recorda a necessidade de garantir a manutenção, ou até o reforço, do Fundo Europeu de Defesa no próximo QFP, prevendo meios orçamentais suficientes para a ciberdefesa;

73. Insta a um aumento dos recursos para a modernização e agilização da cibersegurança e da disseminação das informações entre o SEAE/Centro de Situação e de Informações da UE (INTCEN), o Conselho e a Comissão;

Parcerias público-privadas

74. Reconhece que as empresas privadas desempenham um papel fundamental na prevenção, deteção, contenção e resposta a incidentes de cibersegurança, não apenas na qualidade de fornecedores de tecnologia, mas também enquanto prestadores de serviços fora do âmbito informático;

75. Reconhece o papel do setor privado na prevenção, deteção, contenção e resposta a incidentes de cibersegurança, além do seu papel de promoção da inovação no domínio da ciberdefesa, e, por conseguinte, insta a uma cooperação reforçada com o setor privado para garantir a troca de impressões sobre os requisitos da UE e da NATO e a prestação de assistência para encontrar soluções conjuntas;

76. Insta a UE a proceder a uma ampla revisão do software, das infraestruturas e dos equipamentos informáticos e de comunicações utilizados nas instituições, a fim de excluir programas e dispositivos potencialmente perigosos e proibir os que tenham sido confirmados como mal-intencionados, tal como o Kaspersky Lab;

o

o o

77. Encarrega o seu Presidente de transmitir a presente resolução ao Conselho Europeu, ao Conselho, à Comissão, à Vice-Presidente da Comissão/Alta Representante da União para os Negócios Estrangeiros e a Política de Segurança, às agências da UE nos domínios da defesa e da cibersegurança, ao Secretário-Geral da NATO e aos parlamentos nacionais dos Estados-Membros.