Conselho da
União Europeia

Bruxelas, 22 de maio de 2023
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
para:	Delegações
n.º doc. ant.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Assunto:	Conclusões do Conselho sobre a política de ciberdefesa da UE

Junto se enviam, à atenção das delegações, as Conclusões do Conselho sobre a política de ciberdefesa da UE, aprovadas pelo Conselho na sua reunião realizada a 22 de maio de 2023.

Conclusões do Conselho sobre a política de ciberdefesa da UE

1. Com base no Quadro Estratégico para a Ciberdefesa de 2014 e na sua atualização em 2018, o Conselho congratula-se com a ambiciosa comunicação conjunta sobre a política de ciberdefesa da UE para continuar a investir nas nossas forças armadas modernas e interoperáveis, nas tecnologias de ponta e nas capacidades de ciberdefesa mais avançadas, bem como para reforçar as parcerias a fim de enfrentar desafios comuns. O ciberespaço tornou-se um domínio de concorrência estratégica, numa época de crescente dependência das tecnologias digitais, pelo que é essencial mantê-lo aberto, livre, estável e seguro. O recurso às ciberoperações – que possibilitaram e acompanharam a guerra de agressão não provocada e injustificada da Rússia contra a Ucrânia – afeta a estabilidade e a segurança a nível mundial, representa um risco importante de escalada e vem somar-se ao aumento – já de si significativo – das ciberatividades maliciosas fora do contexto de conflitos armados que se tem verificado nos últimos anos.

2. A guerra na Ucrânia proporcionou um novo contexto estratégico e confirmou a necessidade de a UE, os seus Estados-Membros e os seus parceiros reforçarem ainda mais a resiliência da UE face às ciberameaças e aumentarem a nossa cibersegurança e ciberdefesa comuns contra comportamentos maliciosos e atos de agressão no ciberespaço. A comunicação conjunta sobre a política de ciberdefesa da UE expressa a nossa determinação em apresentar medidas, tanto imediatas como a longo prazo, para garantir a liberdade de ação no ciberespaço e a resposta aos autores de ameaças que procurem, nomeadamente, infiltrar, perturbar ou destruir as redes e os sistemas de informação da UE e dos seus parceiros. Complementando a Estratégia da UE para a Cibersegurança e em consonância com a Bússola Estratégica, a comunicação conjunta representa um passo significativo no sentido de uma abordagem abrangente da UE em matéria de resiliência, resposta, prevenção de conflitos, cooperação e estabilidade no ciberespaço. Neste contexto, o Conselho sublinha a necessidade de respostas adequadas e coerentes por parte da UE, dos seus Estados-Membros e dos seus parceiros, aguardando também com expectativa a revisão das orientações de execução do conjunto de instrumentos de ciberdiplomacia da UE, que constituirá mais um passo crucial na evolução da postura da UE no ciberespaço.

3. O Conselho salienta que os recentes ciberataques contra infraestruturas críticas europeias, a rápida evolução do panorama das ciberameaças e o ritmo acelerado do desenvolvimento tecnológico demonstram também a necessidade de reforçar a coordenação e a cooperação civil-militar, sublinhando ao mesmo tempo que não existe qualquer hierarquia entre as comunidades civil e militar. A política de ciberdefesa da UE permite que a UE e os seus Estados-Membros reforcem a capacidade de proteger, detetar, defender e dissuadir, utilizando de forma adequada toda a gama de opções defensivas à disposição das comunidades civil e militar para assegurar a segurança e a defesa alargadas da UE, em conformidade com o direito internacional, incluindo o direito em matéria de direitos humanos e o direito internacional humanitário.

4. Embora a segurança nacional, inclusive no domínio do ciberespaço, continue a ser da exclusiva responsabilidade de cada Estado-Membro – como referido no artigo 4.º, n.º 2, do TUE –, o Conselho não quer deixar de salientar a necessidade de se fazerem investimentos substanciais, individual e colaborativamente, no reforço da resiliência e na projeção de uma gama completa de capacidades de ciberdefesa de natureza defensiva, bem como na mobilização dos quadros de cooperação e dos incentivos financeiros da UE. O Conselho salienta a necessidade de continuar a reforçar as ações dos Estados-Membros e das instituições, órgãos e organismos da UE, a fim de proteger a União, os nossos cidadãos, as instituições, órgãos e organismos da UE e as missões e operações da PCSD no ciberespaço. Mais sublinha a importância de reforçar a resiliência da UE no ciberespaço, mediante o desenvolvimento das capacidades de ciberdefesa e do reforço da cooperação com um ecossistema privado de confiança.

I. Agir em conjunto para uma ciberdefesa mais forte

5. O Conselho reafirma que um processo gradual, transparente e inclusivo é essencial para reforçar a confiança, o que é fundamental para o ulterior desenvolvimento de um quadro da UE em matéria de gestão de crises de cibersegurança, a realizar em consonância com o roteiro para a gestão de cibercrises desenvolvido no Conselho. O Conselho reitera a necessidade de continuarmos a reforçar a nossa capacidade de proteger, detetar, defender e dissuadir ciberataques através de um melhor conhecimento situacional, da capacitação, do desenvolvimento de capacidades, da formação, dos exercícios e do aumento da resiliência, e através de respostas firmes aos ciberataques perpetrados contra a UE, os seus Estados-Membros e instituições, órgãos e organismos e as missões e operações da PCSD, utilizando todos os meios adequados. Assim, o Conselho incentiva o alto representante e a Comissão a reduzirem a complexidade no domínio do ciberespaço, a evitarem duplicações desnecessárias e a assegurarem a cooperação e as sinergias com as iniciativas existentes. Deverá ser reforçada a cooperação e a coordenação entre os intervenientes na ciberdefesa da UE e dos Estados-Membros, bem como no seio da UE e dos Estados-Membros, entre as cibercomunidades militares e civis e entre um ecossistema público e um ecossistema privado de confiança. Neste contexto, o Conselho encoraja os Estados-Membros a continuar a explorar e a reforçar os mecanismos nacionais de coordenação civil-militar, a facilitar a partilha voluntária comum de informações, a partilhar os ensinamentos retirados, a contribuir para o desenvolvimento de normas interoperáveis, a realizar avaliações de risco e cenários de risco e a realizar exercícios conjuntos, em especial a nível europeu, no pleno respeito das disposições da Diretiva relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (SRI 2).

6. Reconhecendo os esforços destinados a reforçar ainda mais a resiliência da União por meio da Diretiva SRI 2 e da Diretiva Resiliência das Entidades Críticas (REC), o Conselho reitera a sua recomendação sobre uma abordagem coordenada à escala da UE no sentido de reforçar a resiliência das infraestruturas críticas[1]. Apela à adoção de medidas para reforçar ainda mais a resiliência das entidades críticas, das infraestruturas e dos produtos e serviços digitais, observando, ao mesmo tempo, que a correta aplicação da Diretiva SRI 2 continua a ser o passo mais importante. Embora seja predominantemente uma responsabilidade civil, isto contribui também para reforçar a ciberdefesa. Neste contexto, incentivam-se as instituições, órgãos e organismos da UE, bem como os Estados-Membros, a apoiar o desenvolvimento e a projeção de mecanismos de coordenação a nível da UE, tanto novos como existentes, bem como de avaliações e cenários de risco, partilha voluntária comum de informações e exercícios, de uma forma que acrescente valor e evite duplicações desnecessárias com iniciativas existentes.

7. A fim de reforçar ainda mais a confiança, consolidar a cooperação e facilitar a partilha atempada de informações sobre ciberincidentes significativos e de grande escala que afetem os sistemas de defesa, o Conselho congratula-se com a iniciativa de continuar a desenvolver a Conferência dos Cibercomandantes da UE, a organizar por cada Presidência do Conselho da UE, com o apoio da Agência Europeia de Defesa (AED) e a participação do Serviço Europeu para a Ação Externa (SEAE). O Conselho incentiva todos os Estados-Membros a participarem nestas reuniões. A fim de reforçar a resiliência da UE contra ciberincidentes em grande escala, o Conselho convida a Rede de Organizações de Coordenação de Cibercrises da UE (EU-CyCLONe) e a Conferência dos Cibercomandantes da UE a identificar possíveis formas de cooperar e de tirar benefício de uma perspetiva militar e civil conjunta.

[1] Proposta de recomendação do Conselho relativa a uma abordagem coordenada da União para reforçar a resiliência das infraestruturas críticas, COM(2022) 551.

8. A fim de promover uma resposta mais robusta e coordenada a nível da UE, o Conselho congratula-se com a criação e aguarda com expectativa a capacidade operacional inicial da Rede Operacional de Equipas Militares de Resposta a Emergências Informáticas da UE (MICNET) até meados de 2024, a fim de reforçar a partilha de informações técnicas sobre ciberincidentes que afetem os sistemas de defesa entre os Estados-Membros participantes. O Conselho incentiva todos os Estados-Membros a participarem na MICNET, a fim de assegurar a eficácia da rede. Além disso, o Conselho convida os Estados-Membros a tirarem partido dos ensinamentos retirados da Rede de Equipas de Resposta a Incidentes de Segurança Informática (CSIRT) e incentiva vivamente a criação, em momento oportuno, de um mecanismo eficaz de cooperação e coordenação entre as duas redes, no pleno respeito dos mecanismos de governação e da composição de cada uma das entidades.

9. Tendo em conta o aumento das ciberatividades maliciosas por parte de intervenientes estatais e não estatais contra as missões e operações da UE no âmbito da PCSD, o Conselho convida a UE e os seus Estados-Membros a reforçarem as suas capacidades de defesa e segurança das missões e operações da PCSD. A este respeito, o Conselho congratula-se com os objetivos de continuar a promover a proteção das redes e estruturas militares da UE, em consonância, nomeadamente, com a Visão e Estratégia Militar da UE para o Ciberespaço como Domínio de Atividade[2].

[2] EEAS(2021) 706 REV4 (não traduzido para português)

10. O Conselho reitera as conclusões do Conselho de maio de 2022[3] e a necessidade de investir na nossa assistência mútua nos termos do artigo 42.º, n.º 7, do TUE, bem como da cláusula de solidariedade prevista no artigo 222.º do TFUE. O Conselho salienta a importância de se continuar a aprofundar o entendimento comum, por parte da UE e dos Estados-Membros, da aplicação do artigo 42.º, n.º 7, inclusivamente em cenários complexos que impliquem um ciberataque, no respeito dos princípios pertinentes do direito internacional. Congratula-se com a possibilidade de apoio por parte da UE quando ocorre um ciberataque, a pedido expresso do(s) Estado(s)-Membro(s) em causa, sem prejuízo do caráter específico da política de segurança e defesa de determinados Estados-Membros.

11. O Conselho sublinha os progressos alcançados no projeto CEP de Equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança (CRRT) e a sua disponibilidade para agir, mediante pedido, como capacidade de resposta às necessidades dos Estados-Membros e da UE, em apoio das missões e operações da PCSD e para prestar assistência aos parceiros da UE. O Conselho acolhe favoravelmente a continuação do desenvolvimento da capacidade das CRRT constituídas no âmbito da CEP, das equipas nacionais de resposta a ciberataques e, se adequado, das capacidades adicionais de resposta a incidentes, tais como as futuras equipas de resposta rápida às ameaças híbridas previstas na Bússola Estratégica, nomeadamente através da promoção da sua coordenação e cooperação a nível da UE.

[3] Conclusões do Conselho sobre o desenvolvimento da postura da União Europeia no ciberespaço, 23 de maio de 2022, documento 9364/22.

12. O Conselho congratula-se com o trabalho do projeto CEP "Centro de Coordenação no Domínio da Cibernética e da Informação" (CIDCC), que visa proporcionar uma capacidade militar para recolher e analisar informações pertinentes para a formação de uma imagem operacional comum do ciberespaço. O Conselho saúda igualmente a proposta de integração da prova de conceito – desde que seja bem sucedida como centro de coordenação das informações – num centro de coordenação da ciberdefesa da UE (EUCDCC) a partir de 2025, a fim de melhorar a coordenação e o conhecimento situacional, em especial por parte dos comandantes das missões e operações da UE no âmbito da PCSD, bem como de reforçar a arquitetura de comando e controlo da UE no seu todo. O Conselho exorta o alto representante a apresentar um conceito e um roteiro para a criação do EUCDCC, baseando-se na experiência de entidades internacionais semelhantes, identificando os recursos necessários, evitando duplicações desnecessárias e procurando a complementaridade com o quadro de cibersegurança da UE no sentido lato.

13. O Conselho salienta a importância da cooperação estratégica em matéria de informações sobre ciberameaças e ciberatividades, e convida os Estados-Membros, através das respetivas autoridades competentes, a continuarem a contribuir para o trabalho do INTCEN da UE, da Direção de Informações do EMUE e dos Estados-Membros no âmbito da Capacidade Única de Análise de Informações (SIAC). O Conselho salienta ainda a importância de reforçarmos as nossas capacidades de ciberinformação no intuito de reforçar a nossa ciber-resiliência e as nossas respostas e de prestar um apoio eficaz às missões e operações civis e militares da PCSD, bem como às nossas forças armadas e à capacidade da SIAC no domínio do ciberespaço, com base em contributos voluntários dos Estados-Membros em matéria de informações e sem prejuízo das suas competências.

14. O Conselho toma nota do centro de situação e de análise cibernética da Comissão Europeia, cujo objetivo é reforçar o conhecimento situacional por parte da Comissão. O Conselho salienta a importância de se estabelecer uma cooperação mutuamente benéfica entre este centro e outras instituições, órgãos e organismos da UE, em especial a ENISA e a CERT-UE. O Conselho sublinha a importância de, ao desenvolver o conhecimento situacional, se estabelecer uma estreita colaboração com as redes de cooperação da UE, bem como de se respeitar a confidencialidade. O Conselho regista a necessidade de reforçar o conhecimento situacional comum a nível da UE e de prosseguir o desenvolvimento do quadro de resposta da UE a crises de cibersegurança, evitando ao mesmo tempo a duplicação desnecessária de esforços.

15. O Conselho recorda que a educação, a formação e os exercícios em matéria de cibersegurança são essenciais para garantir a preparação e a eficácia, e congratula-se com as atividades nacionais e com as realizadas pela UE através da Academia Europeia de Segurança e Defesa (AESD), da AED, da ENISA e dos projetos em curso no âmbito da CEP, como as federações de centros virtuais de treino e a Academia e Plataforma de Inovação da UE no Domínio da Cibernética (CAIH). Com vista a intensificar estes esforços, o Conselho aguarda com expectativa a criação do projeto-quadro CyDef-X da AED para sincronizar e apoiar os exercícios de ciberdefesa. O Conselho incentiva a AED a explorar, em estreita cooperação com os Estados-Membros e o SEAE, de que forma o CyDef-X poderá reforçar o apoio a exercícios como o CYBER PHALANX – nomeadamente em matéria de assistência mútua nos termos do artigo 42.º, n.º 7, do TUE e em matéria de cláusula de solidariedade nos termos do artigo 222.º do TFUE –, e em estreita cooperação com a Comissão e a ENISA no que diz respeito aos exercícios civis. O Conselho incentiva ainda a utilização e o desenvolvimento ulterior, no âmbito do CyDef-X, dos ambientes existentes dedicados a testes e a exercícios de ciberdefesa, como as federações de centros virtuais de treino. A fim de assegurar a agilidade e a eficiência do processo decisório em matéria de cibercrises, o Conselho sublinha a importância de se realizarem regularmente exercícios teóricos de simulação para o nível de tomada de decisão dos Estados-Membros.

16. O Conselho toma nota da proposta de regulamento em matéria de cibersolidariedade e da intenção de reforçar as capacidades de deteção e resposta a ameaças e incidentes de cibersegurança na UE. O Conselho sublinha que as propostas neste domínio só podem ser eficazes se forem alinhadas com os quadros e as necessidades dos Estados-Membros em matéria de gestão de crises. O Conselho sublinha a importância de se testarem as infraestruturas críticas para detetar potenciais vulnerabilidades, se tal for considerado benéfico, enquanto competência nacional, tendo em conta as avaliações de risco disponíveis a nível da UE.

17. O Conselho regista a proposta da Comissão no sentido de criar um mecanismo de ciberemergência, que poderá favorecer a disponibilidade de serviços de cibersegurança por parte de prestadores privados de confiança, os quais poderiam, mediante pedido, prestar assistência aos Estados-Membros em caso de incidentes de cibersegurança em grande escala; o Conselho sublinha, ao mesmo tempo, a necessidade de reforçar a indústria europeia da cibersegurança com o apoio do Centro Europeu de Competências em Cibersegurança (ECCC) como pilar essencial para que o referido mecanismo fique operacional. O Conselho sublinha o papel fundamental de cada Estado-Membro no acompanhamento e avaliação das suas necessidades nacionais.

II. Proteger o ecossistema de defesa da UE

18. O Conselho recorda o seu incentivo aos Estados-Membros para que continuem a desenvolver as suas próprias capacidades para realizar operações de ciberdefesa, incluindo, se for caso disso, medidas defensivas proativas destinadas a proteger, detetar, defender e dissuadir os ciberataques. Tendo em conta que a SRI 2 não se aplica às entidades da administração pública que exercem as suas atividades no domínio da defesa, o Conselho convida a AED, com o apoio da Comissão e do SEAE, conforme adequado, a ajudar os Estados-Membros a elaborar recomendações voluntárias não vinculativas, inspiradas na SRI 2, a fim de aumentar a cibersegurança na comunidade da defesa, e convida todos os Estados-Membros a empenhar-se ativamente neste esforço. Estas recomendações devem ter em conta esforços semelhantes envidados noutros quadros.

19. Como admite a Bússola Estratégica, a capacidade de ação da UE depende da capacidade de reduzir as dependências estratégicas em todas as suas capacidades de ciberdefesa e cadeias de abastecimento, bem como de desenvolver e dominar tecnologias de ponta no domínio da ciberdefesa. Isto inclui o reforço da base tecnológica e industrial de defesa europeia (BTIDE) em toda a UE e a sua capacidade para cooperar com parceiros que partilham as mesmas ideias no resto do mundo, na base da reciprocidade, a fim de assegurar benefícios mútuos. O Conselho apela assim a que as indústrias da cibersegurança e da ciberdefesa cooperem estreitamente por forma a criar sinergias, com o objetivo de desenvolver e disponibilizar capacidades de ciberdefesa que abranjam todo o espetro. O Conselho convida a Comissão, em estreita colaboração com o ECCC, se adequado, a continuar a apoiar o desenvolvimento de uma base tecnológica e industrial de ciberdefesa europeia que seja forte, ágil, competitiva a nível mundial e inovadora e que inclua as pequenas e médias empresas (PME), através de novos investimentos e de ações estratégicas.

20. Considerando a importância da interoperabilidade e da uniformidade das capacidades de ciberdefesa, inclusive no que diz respeito ao desenvolvimento colaborativo das capacidades de ciberdefesa da próxima geração, o Conselho convida a AED e o Estado-Maior da UE a trabalhar sobre um conjunto de requisitos de interoperabilidade da ciberdefesa da UE que se baseiem nos princípios, processos e normas existentes – estabelecidos, em especial, no quadro da Organização do Tratado do Atlântico Norte (OTAN) – e que sejam compatíveis com os mesmos. O Conselho convida ainda os Estados-Membros a analisar, no âmbito do Comité Europeu de Normalização no domínio da Defesa, se poderão ser necessárias normas voluntárias específicas para os sistemas de defesa, em estreita cooperação com todas as partes interessadas pertinentes, incluindo as organizações europeias de normalização e a OTAN, conforme adequado.

21. O Conselho congratula-se com os esforços envidados pela Comissão para apresentar um plano destinado a promover a utilização das normas existentes para fins de cibersegurança civil e de ciberdefesa, bem como o desenvolvimento de novas normas voluntárias. O Conselho salienta a necessidade de alinhar, na medida do necessário, as normas de cibersegurança e de ciberdefesa. O Conselho reconhece que essas normas voluntárias poderão ser úteis para as indústrias da cibersegurança e da ciberdefesa da UE e apela a uma colaboração mais estreita entre os organismos de normalização civis e de defesa.

22. O Conselho apela a que sejam rapidamente desenvolvidas recomendações baseadas no levantamento das ferramentas existentes para a comunicação segura no ciberespaço, realizado pela Comissão e pelas instituições pertinentes. Sempre que possível, as recomendações deverão ser alinhadas com as iniciativas existentes em matéria de partilha de informações, e deverão igualmente ter em conta os riscos colocados pelas tecnologias emergentes e disruptivas aos atuais métodos de cifragem.

23. O Conselho congratula-se também com o trabalho inicial sobre a avaliação e os cenários de risco que está a ser desenvolvido pela Comissão, pelo alto representante e pelo Grupo de Cooperação da SRI em relação aos setores da energia e das telecomunicações – para começar –, a pedido do Conselho. O Conselho reconhece que estão também a ser preparadas avaliações específicas dos riscos de cibersegurança para as infraestruturas e redes de comunicações na UE. O Conselho reafirma que é da maior importância que haja um entendimento comum dos possíveis impactos dos ciberincidentes entre os Estados-Membros, mas também entre as instituições, órgãos e organismos da UE. Assim, o Conselho convida os intervenientes acima referidos a assegurarem que as avaliações de risco, os cenários e as recomendações subsequentes sejam tidos em conta na definição e priorização das medidas e do apoio, a nível da UE e, se for caso disso, a nível nacional. Além disso, o Conselho apela a que os cenários de risco sejam tidos em conta por todos os intervenientes pertinentes nos processos de avaliação dos riscos, bem como no desenvolvimento de ciberexercícios.

III. Investir em capacidades de ciberdefesa

24. O Conselho incentiva os Estados-Membros a aumentarem os seus investimentos no sentido de criar, manter e continuar a desenvolver capacidades interoperáveis de ciberdefesa. O Conselho apoia o desenvolvimento de um conjunto de compromissos voluntários para o desenvolvimento das capacidades nacionais de ciberdefesa, tendo em conta os esforços da mesma ordem envidados noutros quadros.

25. O Conselho exorta os Estados-Membros e a AED a aproveitarem a oportunidade da revisão do Plano de Desenvolvimento de Capacidades para estabelecer um elevado nível de ambição no que toca ao desenvolvimento da ciberdefesa colaborativa a nível da UE. O Conselho incentiva ainda os Estados-Membros a basearem-se no conjunto atualizado de prioridades e nos seus compromissos no âmbito da CEP para aumentarem o seu nível de participação em projetos colaborativos de desenvolvimento de capacidades de ciberdefesa da UE, reconhecendo o benefício direto dos projetos colaborativos a nível da UE para apoiar o desenvolvimento de capacidades nacionais de ciberdefesa.

26. O Conselho congratula-se com os esforços colaborativos de investigação a nível da UE para explorar as possíveis aplicações, em sistemas relacionados com a defesa, das tecnologias emergentes e disruptivas, fazendo igualmente notar a necessidade de assegurar que esses desenvolvimentos tecnológicos sejam rapidamente incorporados nas capacidades existentes e futuras. O Conselho incentiva os Estados-Membros e a indústria da UE a aproveitar da melhor forma as oportunidades de investigação colaborativa a nível da UE, por exemplo no quadro da AED, dos projetos em curso no âmbito da CEP – como por exemplo a Academia e Plataforma de Inovação da UE no Domínio da Cibernética (CAIH) –, do Fundo Europeu de Defesa e, se adequado, do Horizonte Europa e do Programa Europa Digital para projetos relativos aos bens de dupla utilização. Ademais, o Conselho congratula-se com a mobilização de quadros específicos para apoiar a inovação no domínio da defesa, recorrendo a aplicações derivadas do domínio civil ("spin-ins"), nomeadamente o Programa de Inovação no domínio da Defesa da UE e o polo de inovação no domínio da defesa europeia. O Conselho incentiva ainda o Centro Europeu de Competências em Cibersegurança (ECCC) e a AED a desenvolverem modalidades de trabalho destinadas a facilitar a partilha de informações entre o respetivo pessoal sobre as prioridades em matéria de tecnologias civis, de dupla utilização e de defesa, a fim de criar sinergias e de evitar duplicações.

27. O Conselho congratula-se com a intenção de desenvolver um roteiro tecnológico para as cibertecnologias críticas, a cargo da Comissão em cooperação com a AED e o ECCC, em conformidade com os respetivos mandatos, com os Estados-Membros e em consulta com as partes interessadas pertinentes, tais como a indústria, que, ao identificar as cibertecnologias críticas, ao proceder ao levantamento da evolução tecnológica e das dependências estratégicas, proporciona formas de as reduzir, favorecendo a autonomia estratégica e a soberania tecnológica da UE e preservando simultaneamente uma economia aberta. O Conselho regista que o roteiro tecnológico para as cibertecnologias críticas poderá ajudar a definir as prioridades estratégicas para os instrumentos de financiamento da UE, sem deixar de respeitar as modalidades em vigor para estes instrumentos. O Conselho recorda que a UE deverá seguir uma política industrial europeia ambiciosa e assertiva, com o objetivo de criar um ambiente empresarial sustentável, atrativo e competitivo, que possa também permitir a expansão das entidades europeias no domínio cibernético.

28. O Conselho saúda a intenção de colmatar o significativo défice de competências em matéria de cibersegurança, atraindo novos profissionais, incluindo as mulheres, visando a melhoria de competências e a requalificação e investindo na organização de formações e de exercícios, a fim de constituir uma mão de obra diversificada e inclusiva no domínio cibernético. Reconhecendo os desafios que a UE enfrenta no que diz respeito ao capital humano no âmbito da cibersegurança e da ciberdefesa, o Conselho congratula-se com a iniciativa da Academia de Competências em Cibersegurança, que poderá também beneficiar a mão de obra no setor da ciberdefesa.

29. O Conselho convida os Estados-Membros a trocarem informações sobre boas práticas para formar profissionais qualificados no domínio da cibersegurança, tirando partido das sinergias entre as iniciativas militares, civis e policiais, e apela à AESD, com o apoio e os conhecimentos especializados da AED e da ENISA, a estudarem opções para reforçar o intercâmbio de boas práticas e promover novas sinergias entre os domínios militar e civil no que toca à formação e ao desenvolvimento de competências especificamente cibernéticas no setor da defesa.

30. O Conselho sublinha a importância de um entendimento comum da composição da mão de obra no domínio da cibersegurança e das competências conexas, a fim de identificar e colmatar as lacunas do mercado de trabalho no domínio da cibersegurança, bem como a necessidade de envolver todas as partes interessadas, incluindo os Estados-Membros e a indústria. O Conselho reconhece que o estabelecimento de indicadores para monitorizar o mercado de trabalho no domínio da cibersegurança ajudaria a identificar as necessidades em matéria de competências em cibersegurança e a canalizar adequadamente os fundos, contribuindo ao mesmo tempo para o cumprimento das obrigações decorrentes das políticas existentes, nomeadamente da SRI 2. O Conselho acolhe com agrado a proposta de um quadro de certificação de competências em ciberdefesa e convida o alto representante, na qualidade de chefe da AESD, a desenvolver esse quadro, em cooperação com o SEAE, a Comissão e os Estados-Membros, mobilizando iniciativas civis.

IV. Parcerias para dar resposta aos desafios comuns

31. O Conselho apela ao alto representante e à Comissão para que reforcem e façam avançar a cooperação e explorem parcerias mutuamente benéficas e adaptadas em matéria de políticas de ciberdefesa, nomeadamente no que diz respeito ao reforço das capacidades de ciberdefesa através do Mecanismo Europeu de Apoio à Paz (MEAP). Para o efeito, a ciberdefesa deverá ser acrescentada como ponto a abordar nos diálogos da UE, e as consultas em matéria cibernética deverão ser acrescentadas às consultas globais em matéria de segurança e defesa com os parceiros. Deverão, ademais, ser reforçados os diálogos e a colaboração com o setor privado. O Conselho sublinha que a colaboração internacional em matéria de normas e certificação de cibersegurança constituiria um valor acrescentado para a indústria europeia. Assim sendo, congratula-se com o facto de a Comissão se comprometer a tornar este aspeto uma parte essencial dos diálogos em matéria cibernética entre a UE os países terceiros e organizações internacionais.

32. O Conselho salienta a importância da cooperação internacional para prevenir ou reduzir os riscos de conflito no ciberespaço, especialmente através de um maior desenvolvimento e operacionalização de medidas geradoras de confiança a nível regional e internacional, inclusive no âmbito da ONU; salienta ainda a importância de se continuar a incentivar o recurso às medidas geradoras de confiança existentes, como por exemplo no âmbito da Organização para a Segurança e a Cooperação na Europa (OSCE), nomeadamente em tempos de tensões internacionais. A UE e os seus Estados-Membros salientam que o direito internacional em vigor se aplica no ciberespaço, e realçam a importância dos esforços tendentes a defender e a promover o quadro das Nações Unidas para um comportamento responsável dos Estados e a trabalhar no sentido da sua aplicação, nomeadamente através da criação do Programa de Ação para promover o comportamento responsável dos Estados no ciberespaço.

33. Em consonância com as declarações conjuntas sobre a cooperação UE-OTAN, o Conselho convida o alto representante, designadamente na qualidade de chefe da AED, bem como a Comissão, a fortalecerem, aprofundarem e expandirem ainda mais a parceria com a OTAN no domínio cibernético, na plena observância dos princípios da inclusividade, da reciprocidade, da abertura mútua e da transparência, bem como da autonomia decisória de cada uma das organizações. Sem deixar de ter em conta a necessidade de envidar esforços complementares e coordenados com a maior participação possível dos Estados-Membros que não fazem parte da OTAN e de evitar duplicações desnecessárias, o Conselho apela ao estabelecimento de ligações aos níveis pertinentes entre a UE e a OTAN em matéria de formação, educação, conhecimento situacional, exercícios e plataformas de I&D, e à procura de potenciais sinergias entre os respetivos compromissos voluntários para o desenvolvimento das capacidades nacionais de ciberdefesa e dos quadros de gestão de crises, a proteção das infraestruturas críticas e o reforço das trocas de conhecimentos situacionais, as respostas coordenadas a ciberatividades maliciosas, bem como as ações em prol do reforço das capacidades em países terceiros. Inclui-se aqui o acordo técnico entre a Capacidade de Resposta a Incidentes Informáticos da NATO (NCIRC) e a Equipa de Resposta a Emergências Informáticas da UE (CERT-UE), bem como o reforço do diálogo político sobre questões de ciberdefesa a todos os níveis.

V. Conclusão

34. Com base nas conclusões do Conselho sobre a política de ciberdefesa da UE, o Conselho apela ao alto representante e à Comissão para que elaborem um plano de execução dessa política até ao segundo trimestre de 2023, para aprovação pelos Estados-Membros. O Conselho convida igualmente os Estados-Membros a declararem voluntariamente a sua ambição e as suas ações em matéria de ciberdefesa no contexto da política de ciberdefesa da UE, e a tirarem pleno partido de recomendações e compromissos voluntários não vinculativos a fim de intensificarem os seus esforços nacionais e multinacionais em matéria de ciberdefesa, com o objetivo de maximizarem o seu impacto a nível da UE. O Conselho convida o alto representante, a Comissão e os Estados-Membros a apresentar um relatório e a debater anualmente os progressos realizados na execução dos elementos da comunicação conjunta e do seu plano de execução, começando no segundo trimestre de 2024, o mais tardar.