Conselho da
União Europeia

Bruxelas, 19 de novembro de 2018
(OR. en)

14413/18

CYBER 285
CSDP/PSDC 669
COPS 444
POLMIL 214
EUMC 193
RELEX 978
JAI 1154
TELECOM 415
CSC 328
CIS 13
COSI 290

RESULTADOS DOS TRABALHOS

de:	Secretariado-Geral do Conselho
data:	19 de novembro de 2018
para:	Delegações
Assunto:	Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018)

Envia-se em anexo, à atenção das delegações, o Quadro Estratégico da UE para a Ciberdefesa (atualização de 2018), adotado pelo Conselho na sua 3652.ª reunião, realizada em 19 de novembro de 2018.

ANEXO

QUADRO ESTRATÉGICO DA UE PARA A CIBERDEFESA

(na versão atualizada de 2018)

Âmbito de aplicação e objetivos

Para responder à evolução dos desafios em matéria de segurança, a UE e os seus Estados-Membros têm de reforçar a ciberresiliência e desenvolver capacidades sólidas em matéria de cibersegurança e de defesa.

O Quadro Estratégico da UE para a Ciberdefesa apoia o desenvolvimento das capacidades de ciberdefesa dos Estados-Membros da UE, bem como o reforço da ciberproteção das infraestruturas de segurança e de defesa da UE, sem prejuízo das legislações nacionais dos Estados-Membros e da legislação da UE, nomeadamente, quando definido, o âmbito de aplicação da ciberdefesa.

O ciberespaço é o quinto domínio da atividade militar, a par dos domínios terrestre, naval, aéreo e espacial: o êxito da execução das missões e operações da UE depende cada vez mais do acesso constante a um ciberespaço seguro, sendo assim necessário dispor cibercapacidades operacionais sólidas e resilientes.

O objetivo da atualização do Quadro Estratégico é prosseguir o desenvolvimento da política de ciberdefesa da UE, tendo em conta os desenvolvimentos relevantes noutras instâncias pertinentes e domínios estratégicos e a aplicação do referido Quadro desde 2014. O Quadro identifica as áreas prioritárias para a ciberdefesa e clarifica o papel dos diferentes intervenientes europeus, no pleno respeito das responsabilidades e competências dos intervenientes da União e dos Estados-Membros, bem como do quadro institucional da UE e da sua autonomia decisória.

Contexto

As conclusões do Conselho Europeu sobre a PCSD, de dezembro de 2013, juntamente com as conclusões do Conselho sobre a PCSD, de novembro de 2013, preconizavam a elaboração de um Quadro Estratégico da UE em matéria de Ciberdefesa, com base numa proposta da alta representante, em cooperação com a Comissão Europeia e a Agência Europeia de Defesa (AED). O Quadro Estratégico da UE em matéria de Ciberdefesa foi adotado pelo Conselho em 18 de novembro de 2014[1] e, desde dessa data, a sua aplicação produziu resultados concretos que têm contribuído para reforçar significativamente as capacidades de ciberdefesa dos Estados-Membros. No âmbito do relatório anual de 2017 sobre a aplicação do Quadro Estratégico da UE para a Ciberdefesa[2], e tendo em conta as iniciativas da UE no domínio da segurança e da defesa, nomeadamente a análise anual coordenada em matéria de defesa (AACD), a cooperação estruturada permanente (CEP), o Fundo Europeu de Defesa e o pacto sobre a vertente civil da PCSD, bem como a revisão de 2018 do Plano de Desenvolvimento de Capacidades (PDC) e o Plano de Desenvolvimento de Capacidades Civis, os Estados-Membros apelaram a que o Quadro Estratégico da UE para a Ciberdefesa fosse atualizado.

A cibersegurança é uma prioridade no âmbito da estratégia global para a política externa e de segurança da UE e do nível de ambição da UE[3]. A estratégia global sublinha a necessidade de se reforçar as capacidades a fim de proteger a UE e os seus cidadãos, e responder a crises externas. A estratégia global sublinha a necessidade de se reforçar a UE enquanto comunidade de segurança. Neste contexto, os esforços de segurança e de defesa deverão alargar o papel estratégico da UE e a sua capacidade para agir autonomamente, quando e onde necessário, e em conjunto com parceiros sempre que possível. Estes objetivos exigem uma maior cooperação no desenvolvimento de capacidades, promovendo a eficácia e da interoperabilidade das capacidades civis e militares.

---

1 Documento do Conselho 15585/14 de 18.11.2014.
2 Documento do Conselho 15870/17 de 19.12.2017.
3 Conclusões do Conselho sobre a execução da Estratégia Global da UE no domínio da Segurança e da Defesa, 14.11.2016

O conjunto comum de propostas para a implementação da Declaração Conjunta assinada pelo presidente do Conselho Europeu, pelo presidente da Comissão Europeia e pelo secretário-geral da Organização do Tratado do Atlântico Norte, em Varsóvia, a 8 de julho de 2016[4], inclui ações concretas para alargar a cooperação entre a UE e a OTAN em matéria de cibersegurança e ciberdefesa, inclusive no contexto das missões e operações, bem como no que respeita ao desenvolvimento de capacidades de ciberdefesa, de investigação e tecnologia, de formação, de educação e de exercícios e no que respeita à integração do ciberespaço no mecanismo de gestão de crises. Essa cooperação realiza-se no pleno respeito dos princípios da abertura, da transparência, da inclusividade, da reciprocidade e da autonomia decisória da UE. Um acordo técnico entre a Equipa de Resposta a Emergências Informáticas da UE (CERT-UE) e a Capacidade de Resposta a Incidentes Informáticos da OTAN (NCIRC), assinado em fevereiro de 2016, tem facilitado a partilha de informações técnicas para melhorar a prevenção, a deteção e a resposta a ciberincidentes em ambas as organizações.

Importa recordar que várias políticas da UE contribuem para os objetivos da estratégia de ciberdefesa tal como consta do presente documento, e o presente Quadro Estratégico tem igualmente em conta a regulamentação, as estratégias e o apoio tecnológico pertinentes no domínio civil. Por exemplo, em julho de 2016, o Parlamento Europeu e o Conselho adotaram a Diretiva Segurança das Redes e da Informação[5], que irá aumentar a preparação geral dos Estados-Membros contra ciberameaças, e intensificar a cooperação a nível da UE. Essa diretiva estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de se melhorar o funcionamento do mercado interno. O prazo de transposição desta diretiva terminou em 9 de maio de 2018.

---

4 Conclusões do Conselho sobre a implementação da Declaração Conjunta do presidente do Conselho Europeu, do presidente da Comissão Europeia e do secretário-geral da Organização do Tratado do Atlântico Norte (6 de dezembro de 2016, 15283/16; 5 de dezembro de 2017, 14802/17).

5 Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a um elevado nível comum de segurança das redes e da informação em toda a União (JO L 194 de 19.7.2016, p. 1).

O ato legislativo sobre a cibersegurança da UE, proposto em setembro de 2017, inclui o novo mandato para a Agência da União Europeia para a Cibersegurança (ENISA) e a criação de um quadro de certificação à escala da UE. Uma vez aplicado, esse quadro de certificação deverá favorecer normas elevadas em matéria de processos, produtos e serviços TIC, ser uma fonte de vantagem competitiva e aumentar a confiança por parte dos consumidores e compradores. Em setembro de 2017, a Comissão deu mais um passo para preparar a UE para a eventualidade de ciberincidentes transfronteiras em larga escala ("plano"), e está agora a trabalhar com os Estados-Membros e outras instituições, agências e organismos no sentido de desenvolver a cooperação europeia em matéria de cibercrises, estabelecendo a operacionalização prática e a documentação relativa a todos os intervenientes, processos e procedimentos pertinentes no contexto dos atuais mecanismos da UE de gestão de crises e de catástrofes, em particular o Mecanismo Integrado da UE de Resposta Política a Situações de Crise.

As conclusões do Conselho sobre o reforço da ciberresiliência, de novembro de 2016, definiram o objetivo comum de contribuir para a autonomia estratégica da Europa, como referido nas conclusões do Conselho, de novembro de 2016, sobre a Estratégia Global para a Política Externa e de Segurança da União Europeia, nomeadamente no que se refere ao ciberespaço. O Conselho Europeu reiterou esta mensagem em junho de 2018 e sublinhou também a necessidade de reforçar as capacidades contra as ameaças à cibersegurança provenientes do exterior da UE.

Em 2017, o Conselho adotou um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas ("instrumentos de ciberdiplomacia")[6]. O Quadro deverá incentivar a cooperação, facilitar a atenuação das ameaças e influenciar a longo prazo o comportamento dos potenciais agressores. O Quadro utiliza medidas do âmbito da PESC, designadamente medidas restritivas, para prevenir e responder a ciberatividades maliciosas. Os autores de ciberatividades maliciosas têm de ser responsabilizados pelos seus atos, e os Estados-Membros da UE são incentivados a prosseguir o desenvolvimento da sua capacidade de resposta às ciberatividades maliciosas, de forma coordenada, em conformidade com os instrumentos de ciberdiplomacia. Os Estados não deverão levar a cabo nem apoiar conscientemente atividades no domínio das tecnologias da informação e da comunicação contrárias às suas obrigações no âmbito do direito internacional e não deverão permitir com conhecimento de causa que os respetivos territórios sejam usados para cometer atos considerados ilícitos a nível internacional mediante a utilização das tecnologias da informação e da comunicação.

Foi apresentada pela Comissão e pela AR/VP, em setembro de 2017, uma comunicação conjunta[7] em matéria de cibersegurança destinada a atenuar os riscos decorrentes das novas ameaças. Nesse documento, a ciberdefesa figura como um dos principais domínios de ação e o Quadro Estratégico da UE para a Ciberdefesa é um dos pilares da sua aplicação concreta[8].

As conclusões do Conselho de novembro de 2017 sobre as questões do ciberespaço reconheceram os crescentes vínculos entre cibersegurança e ciberdefesa e apelaram à intensificação da cooperação em matéria de ciberdefesa, incentivando nomeadamente a cooperação entre as comunidades civis e militares de resposta a incidentes. Salientaram também que um ciberincidente ou uma cibercrise particularmente grave poderia constituir razão suficiente para um Estado-Membro invocar a cláusula de solidariedade e/ou a cláusula de assistência mútua da UE.

---

6 Conclusões do Conselho sobre um quadro para uma resposta diplomática conjunta da UE às ciberatividades maliciosas ("instrumentos de ciberdiplomacia"), doc. 9916/17, de 7 de junho de 2017.

7 Comunicação Conjunta ao Parlamento Europeu e ao Conselho intitulada: "Resiliência, dissuasão e defesa: reforçar a cibersegurança na UE "(13 de setembro de 2017, JOIN (2017) 450 final)).

8 Conclusões do Conselho sobre a comunicação conjunta da Comissão ao Parlamento Europeu e ao Conselho intituladas: "Resiliência, dissuasão e defesa: Reforçar a cibersegurança na UE" (20 de novembro de 2017, doc. 14435/17)

Em 11 de dezembro de 2017 foi lançada a cooperação estruturada permanente (CEP). Este quadro de cooperação ambicioso, vinculativo e abrangente foi estabelecido entre 25 Estados-Membros e inclui um compromisso no sentido de intensificar os esforços na cooperação em matéria de ciberdefesa, bem como nos projetos CEP conexos. O primeiro conjunto de projetos da CEP, identificado pelos Estados-Membros que participam na CEP em 2017 inclui dois projetos relacionados com a ciberdefesa: as "Equipas de resposta rápida a ciberataques e assistência mútua no domínio da cibersegurança" e a "Plataforma de partilha de informações relativas às ciberameaças e à resposta a incidentes informáticos". Estão previstos novos conjuntos de projetos da CEP. A CEP desenvolverá capacidades de ciberdefesa, e, por conseguinte, reforçará a cooperação entre os Estados-Membros participantes e aumentará a interoperabilidade.

A versão atualizada do Plano de Desenvolvimento de Capacidades da UE (PDC) aprovada pelo Comité Diretor da AED em junho de 2018, identifica a ciberdefesa como um elemento fundamental, e reconhece a necessidade de ciberoperações defensivas em qualquer contexto operacional, baseado no sofisticado conhecimento atual e previsível da situação em matéria de ciberespaço, incluindo a capacidade de reunir grandes quantidades de dados e informações provenientes de várias fontes para contribuir para um processo decisório rápido e para o aumento da automatização da recolha de dados, da análise e do processo de apoio à decisão. O PDC de 2018 identifica as prioridades em matéria de capacidades de ciberdefesa nos seguintes domínios: cooperação e sinergias com os atores pertinentes em todas as áreas da ciberdefesa e da cibersegurança; atividades de investigação e de tecnologia em matéria de ciberdefesa; quadros de engenharia de sistemas para ciberoperações; educação, formação, avaliação e exercício (ETEE); resposta aos desafios em matéria de ciberdefesa nos domínios aéreo, espacial, naval e terrestre.

Por último, ao longo dos últimos anos, a necessidade de a comunidade internacional prevenir conflitos, cooperar e estabilizar o ciberespaço tornou-se evidente. A UE promove, em estreita cooperação com outras organizações internacionais, em especial a ONU, a OSCE e o Fórum Regional da ASEAN, um quadro estratégico para a prevenção de conflitos, a cooperação e a estabilidade no ciberespaço, que inclui (i) a aplicação no ciberespaço do direito internacional, em especial da Carta das Nações Unidas na sua integralidade; (ii) o respeito de normas, de regras e de princípios universais, não vinculativos para um comportamento responsável dos Estados; (iii) o desenvolvimento e aplicação de medidas regionais de criação de confiança. O Quadro Estratégico da UE para a Ciberdefesa deverá também contribuir para este esforço.

Prioridades

Foram identificados seis áreas prioritárias na versão atualizada do Quadro Estratégico da UE para a Ciberdefesa. Esse quadro estratégico tem como principais enfoques o desenvolvimento das capacidades de ciberdefesa, assim como a proteção das redes de comunicação e informação da PCSD da UE. Outras áreas prioritárias incluem, nomeadamente: a formação e os exercícios, a investigação e a tecnologia, a cooperação civil-militar e a cooperação internacional. Na área da formação, a tónica é colocada na melhoria da formação dos Estados-Membros sobre a ciberdefesa e na sensibilização da cadeia de comando da PCSD para o ciberespaço. É também importante que a ciberdimensão esteja devidamente contemplada nos exercícios, a fim de aumentar a capacidade de resposta da UE a cibercrises e a crises híbridas mediante a melhoria do processo de tomada de decisões estratégicas e da disponibilidade da informação. O ciberespaço é um domínio em rápido desenvolvimento e os novos avanços tecnológicos precisam de ser apoiados, tanto no domínio civil como no domínio militar. A cooperação civil-militar no domínio do ciberespaço é essencial para garantir uma resposta coerente às ciberameaças. Por último, mas não menos importante, o reforço da cooperação com os parceiros internacionais pode ajudar a melhorar a cibersegurança, tanto dentro como fora da UE, e a promover os princípios e os valores da UE.

O presente quadro apresenta propostas e oportunidades para a coordenação entre as instituições, organismos e agências pertinentes da UE. Reflete ainda o importante papel que o setor privado desempenha no desenvolvimento de tecnologias nas áreas da cibersegurança e da ciberdefesa.

Além disso, o Quadro Estratégico da UE para a Ciberdefesa apoia ainda a integração da ciberdefesa nos mecanismos de gestão de crises da União, quando, para lidar com os efeitos de uma cibercrise, sejam aplicáveis as disposições pertinentes do Tratado da UE e do Tratado sobre o Funcionamento da UE[9].

1. Apoio ao desenvolvimento das capacidades de ciberdefesa dos Estados-Membros

O desenvolvimento de capacidades e tecnologias de ciberdefesa deverá ter em conta todos os aspetos associados ao desenvolvimento de capacidades, incluindo a doutrina, a liderança, a organização, o pessoal, a formação, a indústria, a tecnologia, as infraestruturas, a logística e a interoperabilidade. Para o efeito, os Estados-Membros deverão intensificar os seus esforços para garantir uma capacidade de ciberdefesa eficaz. O SEAE, a Comissão e a AED deverão trabalhar em conjunto e apoiarem esses esforços.

É necessário avaliar continuamente as vulnerabilidades das infraestruturas de informação que apoiam as missões e operações da PCSD, e perceber em tempo quase real a eficácia da sua proteção. Do ponto de vista operacional, as atividades de ciberdefesa focar-se-ão em manter a operacionalidade das redes de comunicação e de informação da PCSD, salvo especificação em contrário no mandato das operações ou missões. Além disso, o SEAE, em cooperação com os Estados-Membros, irá integrar ainda mais as cibercapacidades nas missões e operações da PCSD.

Os autores de ciberatividades maliciosas têm de ser responsabilizados pelos seus atos. É importante que os Estados-Membros da UE, com o apoio do SEAE, promovam a cooperação mútua a fim de responder às ciberatividades maliciosas. Os instrumentos de ciberdiplomacia foram desenvolvidos tendo em vista contribuírem para lograr essa resposta mútua. O SEAE e a AED irão organizar exercícios regulares baseados nos instrumentos de ciberdiplomacia, durante os quais os Estados-Membros da UE poderão exercitar-se com os referidos instrumentos.

---

[9] Artigo 222.º do TFUE e artigo 42.º, n.º 7, do TUE, tendo devidamente em conta o artigo 17.º do TUE.

Tendo em conta que, tanto na legislação nacional dos Estados-Membros como na legislação da UE, o âmbito da ciberdefesa, nos casos em que é definido, é amplo e diversificado, é necessário chegar a um conceito comum agregado sobre o âmbito da de aplicação da ciberdefesa.

Uma vez que as operações militares da PCSD têm por base uma infraestrutura de comando, controlo, comunicações e computadores (C4) disponibilizada pelos Estados-Membros, é necessário estabelecer um certo grau de convergência estratégica durante o planeamento das necessidades em matéria de ciberdefesa para a infraestrutura de informação.

Com base no trabalho desenvolvido pela equipa do projeto de ciberdefesa da AED no sentido de desenvolver as capacidades de ciberdefesa, a AED e os Estados-Membros:

- Utilizarão o Plano de Desenvolvimento de Capacidades (PDC) e outros instrumentos como a análise anual coordenada da defesa (AACD), que facilitam e apoiam a cooperação entre os Estados-Membros, a fim de melhorar o grau de convergência no planeamento das necessidades em matéria de ciberdefesa dos Estados-Membros a nível estratégico, nomeadamente no que diz respeito à monitorização, conhecimento da situação, prevenção, deteção e proteção, partilha de informações, capacidade de análise forense e de análise de software mal-intencionado (malware), ensinamentos colhidos, contenção de danos, capacidades de recuperação dinâmica, armazenamento de dados distribuído e de ficheiros de segurança.
- Apoiarão os projetos atuais e futuros de recolha e partilha de dados de ciberdefesa no âmbito de operações militares (por exemplo, nos domínios da análise forense, do desenvolvimento de interoperabilidade e da normalização).
- Definirão um conjunto normalizado de objetivos e requisitos que estabeleçam o nível mínimo de cibersegurança e de confiança a atingir pelos Estados-Membros, com base na experiência existente em toda a UE.

O SEAE e a AED:

- Promoverão intercâmbios entre Estados-Membros sobre doutrinas nacionais de ciberdefesa, bem como programas de recrutamento, conservação e constituição de reservas no domínio da ciberdefesa.

A AED:

- Estudará os diferentes âmbitos de aplicação das necessidades militares em matéria de ciberdefesa na legislação nacional e nas melhores práticas dos Estados-Membros. O principal objetivo do estudo será a criação de uma arquitetura institucional para a ciberdefesa que inclua o âmbito de aplicação, as funcionalidades e os requisitos utilizados neste domínio pelos Estados-Membros na legislação nacional e da UE.

A título voluntário, os Estados-Membros:

- Aumentarão a cooperação entre as equipas militares de resposta a emergências informáticas (CERT) para melhorar a prevenção e o tratamento de incidentes.
- Tirarão partido da CEP para reforçar a cooperação em matéria de ciberdefesa, inclusive para desenvolver novos projetos.
- Tirarão partido do Fundo Europeu de Defesa para desenvolver conjuntamente as capacidades de ciberdefesa.
- Desenvolverão um conceito comum sobre a aplicação da cláusula de assistência mútua no domínio do ciberespaço, preservando simultaneamente a sua flexibilidade.
- Estabelecerão os requisitos de base em matéria de ciberdefesa para a infraestrutura de informação.
- Na medida em que a melhoria das capacidades de ciberdefesa depende de conhecimentos especializados civis em matéria de segurança das redes e da informação, tirarão partido dos conhecimentos especializados da ENISA, das autoridades dos Estados-Membros reunidas no grupo de cooperação SRI e de outras entidades a nível da UE que disponham de conhecimentos especializados sobre cibersegurança civil.

Os Estados-Membros, o SEAE/Estado-Maior da UE, a AESD, e a AED:

- Terão em conta a necessidade de desenvolverem programas de formação sobre ciberdefesa, tendo em vista a certificação dos agrupamentos táticos da UE.

A Comissão, em cooperação com os Estados-Membros:

- Terá em conta a ciberdefesa nos programas de trabalho do Programa Europeu de Desenvolvimento Industrial no domínio da Defesa e do Fundo Europeu de Defesa.

2. Maior proteção dos sistemas de comunicação e de informação da PCSD utilizadas por entidades da UE

Sem prejuízo do papel da Equipa de Resposta a Emergências Informáticas para as instituições e agências da UE (CERT-UE) como estrutura de coordenação central da UE da resposta a ciberincidentes entre todas as instituições, órgãos e organismos da União, e no quadro das regras pertinentes relativas ao orçamento da União, o SEAE desenvolverá uma análise adequada e autónoma das questões de segurança e defesa das redes e desenvolverá as suas próprias capacidades em matéria de segurança das tecnologias da informação (TI). Terá como objetivo melhorar a resiliência das redes do SEAE no domínio da PCSD, com particular enfoque na prevenção, deteção, resposta a incidentes, conhecimento da situação, intercâmbio de informações e mecanismos de alerta precoce.

A proteção dos sistemas de comunicação e informação do SEAE e o desenvolvimento das capacidades de segurança das TI estão a cargo da Direção-Geral do Orçamento e da Administração (DGOE) do SEAE. O Estado-Maior da União Europeia (EMUE), a Direção da Gestão de Crises e Planeamento (DGCP) e a Capacidade Civil de Planeamento e Condução (CPCC) disponibilizarão igualmente apoio e recursos adicionais específicos. A capacidade de segurança das TI abrangerá tanto os sistemas de informações classificadas como os de informações não classificadas e será parte integrante das entidades operacionais existentes.

Haverá igualmente que simplificar as regras de segurança dos sistemas de informações definidas pelos vários intervenientes institucionais da UE durante a condução das missões e operações da PCSD. Neste contexto, dever-se-á considerar a possibilidade de desenvolver uma cadeia de comando unificada para melhorar a resiliência das redes utilizadas no âmbito da PCSD.

A fim de melhorar a coordenação e reforçar a proteção e a resiliência das redes e dos sistemas de comunicação e de informação da PCSD, foi criado em 2017 no SEAE um conselho interno de cibergovernação sob a direção do secretário-geral do SEAE.

O SEAE/DGOE:

- Reforçarão a capacidade de segurança das TI no SEAE com base nas capacidades e procedimentos técnicos existentes, atribuindo particular atenção à prevenção, deteção, resposta a incidentes, conhecimento da situação, intercâmbio de informações e mecanismo de alerta precoce. Uma estratégia de cooperação com a CERT-UE e as atuais capacidades de cibersegurança serão melhoradas.

O SEAE/DGOE, em conjunto com o EMUE, o CMPC, a DGCP e a CPCC:

- Definirão políticas e orientações coerentes em matéria de segurança das TI, tendo igualmente em conta os requisitos técnicos da ciberdefesa no contexto da PCSD, para as estruturas, missões e operações, tendo presentes os quadros e as estratégias de cooperação existentes na UE com vista à convergência de regras, políticas e modalidades de organização.

O SEAE/Capacidade Única de Análise de Informações (SIAC):

- Reforçará, com base nas estruturas existentes, a avaliação das ciberameaças e a capacidade dos serviços de informações para identificar novos ciberriscos e disponibilizar regularmente avaliações dos riscos, com base na avaliação estratégica das ameaças e em informações quase em tempo real sobre os incidentes, coordenadas entre as estruturas pertinentes da UE e tornadas acessíveis em diferentes níveis de classificação.

O SEAE/SIAC e a CERT-UE:

- Promoverão a partilha em tempo real de informações sobre ciberameaças entre os Estados-Membros e as entidades pertinentes da UE. Para o efeito, serão desenvolvidos mecanismos de partilha de informações e medidas geradoras de confiança entre as autoridades competentes a nível nacional e europeu, através de uma abordagem voluntária assente na cooperação existente.

O SEAE/EMUE e a CMPC:

- Reforçarão o desenvolvimento, e a sua integração num planeamento a nível estratégico, de um conceito de ciberdefesa para as missões e as operações militares da PCSD.
- Desenvolverão, em cooperação com o Quartel-General de Operações, um procedimento operativo normalizado em matéria de ciberespaço.

O SEAE/CCPC e a DGCP:

- Reforçarão o desenvolvimento, e a respetiva integração num planeamento estratégico, de um conceito de ciberdefesa para as missões civis da PCSD.
- Reforçarão as capacidades de ciberdefesa das missões civis da PCSD, partindo das infraestruturas existentes, e promoverão a normalização e a harmonização das tecnologias utilizadas nas missões e operações da PCSD, tirando partido, se for caso disso, dos conhecimentos especializados da CERT-UE, da ENISA e da AED.
- No processo de reforço da vertente civil da PCSD, estudarão com mais detalhe o eventual apoio das missões civis da PCSD aos países de acolhimento em matéria de cibersegurança.

O SEAE:

- Reforçará o desenvolvimento dos requisitos comuns para as missões e as operações militares da PCSD.
- Reforçará coordenação da ciberdefesa para concretizar os objetivos relacionados com a proteção das redes de apoio à PCSD utilizadas pelos intervenientes institucionais da UE, com base nas experiências existentes em toda a União.
- Analisará periodicamente as necessidades de recursos e outras decisões estratégicas relevantes com base na evolução do clima de ameaça, em consulta com os Estados-Membros e outras instituições da UE.

3. Promoção da cooperação civil-militar

O ciberespaço é um domínio em rápido desenvolvimento: a evolução tecnológica precisa de ser reforçada por sistemas de segurança, tanto no domínio civil como no domínio militar. Na medida do possível, os domínios civil e militar deverão coordenar-se nos casos em que progressos tecnológicos semelhantes apresentem soluções tanto para aplicações civis como militares. Noutros casos, as capacidades militares e os sistemas de armas são tão específicos que não há possibilidade de partilhar com tecnologias civis. Sem prejuízo da organização interna e da legislação dos Estados--Membros, a cooperação civil-militar no domínio da cibernética poderá servir não só para partilhar boas práticas, trocar informações e criar mecanismos de alerta precoce, proceder a avaliações de risco da resposta a incidentes e desenvolver ações de sensibilização, como para desenvolver ações de formação e realizar exercícios.

Melhorar a cibersegurança civil é um fator importante que contribui para a resiliência global da segurança das redes e da informação. A Diretiva SRI aumenta o grau de preparação à escala nacional e reforça a cooperação entre os Estados-Membros ao nível da União, tanto no plano estratégico como no plano operacional. Esta cooperação envolve as autoridades nacionais que supervisionam as políticas de cibersegurança, bem como as CERT nacionais e a CERT-UE. A cooperação entre as CERT civis e militares deverá ser reforçada tendo devidamente em conta a evolução registada. O novo Regulamento Europeu sobre Cibersegurança visa melhorar a resiliência da Europa aos ciberataques e fornecer um quadro de certificação em matéria de cibersegurança dos produtos e serviços, aumentando assim a confiança na esfera digital civil.

A AED, a Agência da União Europeia para a Segurança das Redes e da Informação (ENISA) e o Centro Europeu da Cibercriminalidade (EC3), juntamente com outros organismos e agências competentes da UE, são incentivados, no âmbito dos respetivos mandatos e sem interferirem com as competências dos Estados-Membros, a intensificar a cooperação nas seguintes áreas:

- Desenvolver perfis de competências comuns em cibersegurança e ciberdefesa com base nas boas práticas internacionais e na certificação utilizada pelas instituições, órgãos e organismos da UE, tendo igualmente em conta as normas de certificação do setor privado.
- Contribuir para o desenvolvimento e adaptação das normas técnicas e organizacionais do setor público em matéria de cibersegurança e ciberdefesa a utilizar no setor da defesa e da segurança. Sempre que necessário, dar continuidade ao trabalho desenvolvido pela ENISA e pela AED.
- Criar ou desenvolver mecanismos e métodos de trabalho que permitam o intercâmbio de boas práticas, nomeadamente em matéria de educação, formação e realização de exercícios, bem como em matéria de investigação e tecnologia, e outras áreas que apresentem sinergias civilo-militares.
- Tirar partido das atuais experiências da UE em matéria de prevenção da cibercriminalidade, bem como das suas capacidades de investigação forense e do reforço da sua utilização, no desenvolvimento de capacidades de ciberdefesa.

A título voluntário, os Estados-Membros:

- Intensificarão a cooperação entre as CERT civis e militares dos Estados-Membros.

O SEAE, a Comissão e os Estados-Membros:

- Incluirão a ciberdefesa nos procedimentos da UE em matéria de gestão de crises e catástrofes (através de um processo matricial).

4. Investigação e tecnologia

Uma vez que os requisitos estabelecidos em termos de tecnologia e capacidade operacional são comuns, os operadores de infraestruturas e serviços de tecnologias da informação e comunicação (TIC) para fins civis e de defesa veem-se confrontados com desafios semelhantes em matéria de cibersegurança. As necessidades comuns em matéria de I&T e os requisitos comuns aplicáveis aos sistemas são previstos antecipadamente a fim de melhorar a interoperabilidade dos sistemas a longo prazo e reduzir os custos de desenvolvimento de soluções. Para fazer face ao número cada vez maior de ameaças e vulnerabilidades, será necessário realizar economias de escala. Tal deverá, por seu turno, facilitar a preservação e o crescimento de uma indústria de ciberdefesa competitiva na Europa.

O desenvolvimento de capacidades de ciberdefesa envolve uma importante dimensão de I&T. No quadro da agenda de investigação em matéria de ciberdefesa, a AED proporcionou uma base sólida para se definirem prioridades em termos de financiamento futuro da I&T dentro do quadro intergovernamental. A Agenda de Investigação Estratégica desenvolvida no seio do grupo *ad hoc* competente da AED estabelece, com conhecimento de causa, as prioridades em matéria de tecnologias relacionadas com o ciberespaço necessárias ao setor militar, identificando simultaneamente as oportunidades de investimento e desenvolvimento de esforços no domínio da dupla utilização, sejam eles desenvolvidos em contextos nacionais, multinacionais ou financiados pela UE.

Para fazer face às ameaças e vulnerabilidades, será essencial desenvolver as capacidades tecnológicas na Europa. A indústria continuará a ser o principal motor da tecnologia e da inovação relacionadas com a ciberdefesa. A criptografia, os sistemas securizados integrados, a deteção de *software* mal intencionado, as técnicas de simulação e visualização, a proteção das redes e dos sistemas de comunicação e as tecnologias de identificação e autenticação são algumas das áreas que mais atenção merecem. Importará também promover a criação de uma cadeia europeia de abastecimento industrial competitiva em matéria de cibersegurança, apoiando para tal o envolvimento das pequenas e médias empresas (PME).

Garantir que a Europa seja capaz de competir com os concorrentes internacionais em matéria de capacidades tecnológicas no domínio da cibersegurança depende também da nossa capacidade de impulsionar a inovação radical através de instrumentos nacionais e da UE, como o Conselho Europeu da Inovação.

Para facilitar a cooperação civil-militar no desenvolvimento de capacidades de ciberdefesa, reforçar a base industrial e tecnológica de defesa europeia[10] e contribuir para a autonomia estratégica da UE também na área do ciberespaço, quando e onde necessário e, sempre que possível, juntamente com os parceiros**,**

A AED, a Comissão e os Estados-Membros:

- Procurarão criar sinergias entre os esforços desenvolvidos em matéria de I&T no setor militar e os programas civis de investigação e desenvolvimento, em particular os que digam respeito às inovações radicais, e terão em conta os aspetos relacionados com a cibersegurança e a ciberdefesa ao porem em prática a ação preparatória em matéria de investigação no domínio da defesa.
- Partilharão as agendas de investigação sobre cibersegurança (como a Agenda de Investigação Estratégica em matéria de Cibersegurança da Agência Europeia de Defesa) e os roteiros e ações que delas resultem; para o efeito, será desenvolvida, em estreita cooperação com a Comissão e os Estados-Membros, uma agenda de investigação transetorial em matéria de ciberdefesa.
- Contribuirão para uma melhor integração dos aspetos atinentes à cibersegurança e à ciberdefesa nos programas com uma dupla dimensão de segurança e defesa, como, por exemplo, o programa de investigação sobre a gestão do tráfego aéreo no Céu Único Europeu (SESAR).

[10] Comunicação intitulada:"Para um setor da defesa e da segurança mais competitivo e eficiente", COM (2013) 542.

A Comissão:

- Ponderará a possibilidade de criar um centro europeu de competências industriais, tecnológicas e de investigação em matéria de cibersegurança dotado de uma rede de centros nacionais de coordenação a fim de apoiar as capacidades tecnológicas e industriais em matéria de cibersegurança e de aumentar a competitividade do setor da cibersegurança da União, garantindo a complementaridade e evitando duplicações de esforços tanto dentro da rede de centros de competências em matéria de cibersegurança como com outras agências da UE. O Centro deverá, nomeadamente, contribuir para reforçar a cooperação entre as tecnologias e aplicações civis e de defesa, trabalhando em estreita colaboração e plena complementaridade com a Agência Europeia de Defesa no domínio da ciberdefesa.
- Apoiará o desenvolvimento de ecossistemas industriais e de polos de inovação que abranjam toda a cadeia de valor da segurança com base nos conhecimentos académicos, na inovação das PME e na produção industrial.

A Comissão, em cooperação com os Estados-Membros:

- Repercutirá as questões ligadas à ciberdefesa nos convites à apresentação de propostas respeitantes à ação preparatória em matéria de investigação no domínio da defesa.
- Analisará a possibilidade de incluir a ciberdefesa entre as áreas contempladas pelo Fundo Europeu de Defesa.
- Apoiará a coerência das políticas da UE por forma a garantir que os aspetos políticos e técnicos da proteção da UE contra ciberataques continuam na vanguarda da inovação tecnológica e estão harmonizados em toda a UE (capacidade de análise e avaliação de ciberameaças, iniciativas de "segurança desde a conceção", gestão da dependência em termos de acesso às tecnologias, etc.).

5. Melhorar as oportunidades de educação, formação e realização de exercícios

Para aumentar o grau de preparação para enfrentar as ciberameaças e desenvolver uma cultura de ciberdefesa comum em toda a UE, também em benefício das missões e operações da UE, será necessário aumentar e melhorar as oportunidades de formação em ciberdefesa. É essencial que os orçamentos dedicados à educação e à formação sejam utilizados de forma eficiente, garantindo simultaneamente a melhor qualidade possível. A mutualização e a partilha na área da educação e da formação em ciberdefesa a nível europeu serão de importância fundamental.

A Academia Europeia de Segurança e Defesa (AESD), o SEAE, a AED, a Comissão e os Estados-Membros:

- Com base na análise das necessidades da AED em termos de formação em ciberdefesa e na experiência adquirida pela AESD com a formação em cibersegurança, instituirão programas de formação e educação no âmbito da PCSD destinados a públicos diversos, como o SEAE, pessoal das missões e operações da PCSD e funcionários dos Estados-Membros, que deverão também focar questões de conservação de pessoal qualificado a curto, médio e longo prazo.
- Proporão o estabelecimento de um diálogo sobre ciberdefesa relativo às normas de formação e certificação com os Estados-Membros, as instituições da UE, países terceiros e outras organizações internacionais, bem como com o setor privado.
- Colaborarão com os formadores do setor privado europeu e com as instituições académicas para aumentar as competências e aptidões do pessoal envolvido nas missões e operações da PCSD.

A AESD:

- Continuará a desenvolver a plataforma de educação, formação, avaliação e realização de exercícios criada no seu seio (plataforma ETEE em matéria de cibersegurança e ciberdefesa).
- Criará sinergias com os programas de formação de outros intervenientes, como a ENISA, a Europol, a Agência da União Europeia para a Formação Policial (CEPOL) e o Centro de Excelência Cooperativo da OTAN para a Ciberdefesa.
- Estudará a possibilidade de desenvolver programas de formação conjuntos AESD-OTAN sobre ciberdefesa, abertos a todos os Estados-Membros da UE, de forma a promover uma cultura de ciberdefesa partilhada.

A Comissão:

- Analisará as opções para aumentar nos Estados-Membros as oportunidades de formação e educação identificadas pela plataforma ETEE em matéria de cibersegurança e ciberdefesa.

A AED:

- Desenvolverá no seu seio, em colaboração com a AESD, novos cursos que vão ao encontro das necessidades dos Estados-Membros em matéria de educação, formação e realização de exercícios de ciberdefesa.
- Apoiará a plataforma ETEE em matéria de cibersegurança e ciberdefesa, nomeadamente integrando progressivamente a educação, formação, avaliação e realização de módulos de exercícios de cibersegurança e ciberdefesa desenvolvidos no quadro da AED.

O SEAE e os Estados-Membros:

- Servir-se-ão dos mecanismos de certificação instituídos pela AESD para os programas de formação em estreita cooperação com os serviços competentes das instituições, órgãos e organismos s da UE, com base nas normas e conhecimentos existentes. Considerarão a possibilidade de criar módulos de cibernética específicos no quadro da iniciativa Erasmus Militar.

É necessário melhorar as oportunidades de exercícios de ciberdefesa para os intervenientes militares e civis da PCSD. Os exercícios conjuntos funcionam como um instrumento para desenvolver o conhecimento e o entendimento comuns da ciberdefesa. Estes exercícios permitirão que as forças nacionais reforcem a sua preparação para operar num ambiente multinacional. A realização de exercícios comuns de ciberdefesa contribuirá também para desenvolver a interoperabilidade e a confiança.

O SEAE, a AED, a CERT-UE e os Estados-Membros centrar-se-ão na promoção de elementos de ciberdefesa no âmbito da PCSD e noutros exercícios:

- Integrar a dimensão de ciberdefesa nos atuais cenários de exercício para o *MILEX* e o *MULTILAYER*;
- Organizar regularmente exercícios estratégicos/políticos como o *CYBRID 2017* em coordenação com o exercício paralelo e coordenado conduzido pela UE (PACE), e exercícios técnico-operacionais como o *DEFNET*.
- Desenvolver, conforme for adequado, um exercício de ciberdefesa específico no âmbito da PCSD da UE e explorar a eventual coordenação com ciberexercícios pan-europeus como o *CiberEuropa*, organizado pela ENISA.
- Continuar a participar noutros exercícios multinacionais de ciberdefesa, como o *Locked Shields*.
- Convidar os parceiros internacionais pertinentes, como a OTAN, para os exercícios em conformidade com o quadro de política de exercícios da UE.
- Organizar exercícios regulares com base no conjunto de instrumentos de ciberdiplomacia que permitem aos Estados-Membros da UE treinar-se para dar resposta a ciberatividades maliciosas.

6. Reforçar a cooperação com os parceiros internacionais pertinentes

No quadro da cooperação internacional, é necessário garantir um diálogo com os parceiros internacionais, nomeadamente a OTAN e outras organizações internacionais, para contribuir para o desenvolvimento de capacidades efetivas de ciberdefesa. Deve procurar-se um maior envolvimento com o trabalho realizado no quadro da Organização para a Segurança e a Cooperação na Europa (OSCE) e as Nações Unidas (ONU), com vista a apresentar um quadro estratégico para a prevenção de conflitos, a cooperação e a estabilidade no ciberespaço.

Existe vontade política na UE para cooperar ainda mais com a OTAN em matéria de ciberdefesa para desenvolver capacidades de ciberdefesa sólidas e resilientes conforme prescrito na Declaração Conjunta assinada pelo Presidente do Conselho Europeu, pelo Presidente da Comissão Europeia e pelo Secretário-Geral da Organização do Tratado do Atlântico Norte em Varsóvia a 8 de julho de 2016. Consultas regulares entre agentes e o cruzamento de informações, assim como possíveis reuniões entre o Grupo Político-Militar e os comités pertinentes da OTAN, contribuirão para evitar duplicações desnecessária e assegurar a coerência e complementaridade dos esforços, de acordo com o quadro acima referido.

O SEAE e a AED, juntamente com os Estados-Membros, continuarão a desenvolver a cooperação em matéria de ciberdefesa entre a UE e a OTAN, respeitando devidamente o quadro institucional e a respetiva autonomia de decisão destas organizações:

- Intensificam as atividades em curso no quadro da implementação da Declaração Conjunta do Presidente do Conselho Europeu, do Presidente da Comissão Europeia e do Secretário-Geral da Organização do Tratado do Atlântico Norte;
- Procedem ao intercâmbio de boas práticas em matéria de gestão de crises, bem em matéria de ciberdefesa e no quadro de missões e operações militares e civis;
- Aumentam a coerência dos resultados no desenvolvimento de requisitos em matéria de capacidades de ciberdefesa onde existe sobreposição, especialmente no desenvolvimento de capacidades de ciberdefesa a longo prazo;
- Utilizam mais o quadro de cooperação da AED com o Centro de Excelência Cooperativo para a Ciberdefesa, da OTAN, como uma plataforma inicial para uma colaboração reforçada em projetos multinacionais de ciberdefesa, com base em avaliações adequadas;

A AESD, o SEAE e a AED:

- Reforçarão a cooperação em matéria de conceitos para a formação e ensino em matéria de ciberdefesa, bem como para os exercícios;
- Assegurarão a participação recíproca do pessoal em exercícios, em conformidade com o quadro acordado.

A CERT-UE:

- Continuará a explorar o acordo técnico entre a CERT-UE e os organismos competentes da UE em matéria de ciberdefesa e a NCIRC (capacidade de resposta a incidentes informáticos da NATO) para melhorar o conhecimento da situação, a partilha de informação e os mecanismos de alerta rápido, e antecipar as ameaças que possam afetar ambas as organizações.

No que diz respeito a outras organizações internacionais e aos parceiros internacionais pertinentes da UE, o SEAE e os Estados-Membros, conforme for adequado:

- Acompanharão os desenvolvimentos estratégicos e realizarão consultas sobre questões relacionadas com a ciberdefesa com os parceiros internacionais (organizações internacionais e países terceiros);
- Explorarão as possibilidades de cooperação no domínio da ciberdefesa, nomeadamente com países terceiros que participem em missões e operações da PCSD;
- Promoverão nas organizações internacionais relevantes, em particular a ONU, a OSCE e o Fórum Regional da ASEAN, a aplicação, no ciberespaço, do direito internacional em vigor, em especial a Carta da ONU na íntegra, a elaboração e a aplicação de normas universais não vinculativas que definam um comportamento responsável dos Estados, bem como medidas geradoras de confiança (MGC) a nível regional entre Estados para aumentar a transparência e reduzir o risco de mal-entendidos no comportamento de um Estado.

A Comissão e o SEAE:

- Apoiarão, sempre que necessário , o desenvolvimento de cibercapacidades para os parceiros da UE através do Instrumento para a estabilidade e a paz (IcSP) alterado.

Acompanhamento

No quadro da coordenação, por parte do SEAE, da aplicação do CDPF, o SEAE / a AED / a Comissão deverão apresentar ao Grupo Político-Militar, com a participação dos membros do Grupo Horizontal das Questões do Ciberespaço, e ao Comité Político e de Segurança um relatório intercalar anual sobre os seis domínios acima expostos, a fim de avaliar a aplicação do CDPF. Será feita igualmente uma apresentação oral de seis em seis meses.

Tendo em conta o desenvolvimento da ciberameaça, é essencial identificar novos requisitos em matéria de ciberdefesa e incluí-los posteriormente no Quadro Estratégico em matéria de Ciberdefesa. A próxima versão revista do Quadro Estratégico da UE para a Ciberdefesa deverá ser apresentada o mais tardar em meados de 2022, em estreita concertação com os Estados-Membros.