PRESIDÊNCIA DO CONSELHO DE MINISTROS

Resolução do Conselho de Ministros n.º 106/2022

Sumário: Aprova a Estratégia Nacional de Ciberdefesa.

O Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril, destaca a cibersegurança como uma prioridade nacional e recomenda a edificação de uma capacidade de ciberdefesa ao nível das Forças Armadas, tendo a Orientação para a política de Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, publicado no *Diário da República,* 2.ª série, n.º 208, de 28 de outubro de 2013, subsequentemente estabelecido os objetivos e as linhas de ação da política nacional de ciberdefesa.

A Lei de Bases da Organização das Forças Armadas, aprovada em anexo à Lei Orgânica n.º 2/2021, de 9 de agosto, dispõe que «o órgão de ciberdefesa destina-se a assegurar o exercício do comando de operações militares no e através do ciberespaço, pelo CEMGFA». Já a Lei Orgânica do Estado-Maior-General das Forças Armadas (EMGFA), na versão aprovada pelo Decreto-Lei n.º 19/2022, de 24 de janeiro, criou o Comando das Operações de Ciberdefesa, o qual é responsável por planear, dirigir, coordenar, controlar e executar operações no e através do ciberespaço em apoio a objetivos militares, garantindo a liberdade de ação das Forças Armadas neste domínio.

No entanto, nos termos do artigo 3.º da Lei Orgânica n.º 2/2021, de 9 de agosto, as normas relativas ao órgão de ciberdefesa apenas entram em vigor com a entrada em vigor da Lei Orgânica do EMGFA, mantendo-se, assim, em vigor, neste âmbito, a Lei Orgânica de Bases da Organização das Forças Armadas, aprovada pela Lei Orgânica n.º 1-A/2009, de 7 de julho, na sua redação atual. Acresce que a Lei Orgânica do EMGFA, na versão dada pelo Decreto-Lei n.º 19/2022, de 24 de janeiro, que revogou o Decreto-Lei n.º 184/2014, de 29 de dezembro, prevê que enquanto não for publicado o decreto regulamentar do EMGFA mantém-se em vigor o Decreto-Lei n.º 184/2014, de 29 de dezembro, pelo que, no momento presente, encontra-se ainda em funcionamento o Centro de Ciberdefesa, na dependência do Chefe do Estado-Maior-General das Forças Armadas, enquanto capacidade conjunta das Forças Armadas.

A Diretiva Ministerial de Orientação Política para o Investimento na Defesa, aprovada pelo Despacho n.º 4103/2018, publicado no *Diário da República,* 2.ª série, n.º 79, de 23 de abril de 2018, contempla, de forma inequívoca, o reforço do investimento na edificação da capacidade de ciberdefesa no âmbito da modernização das Forças Armadas, tendo esse investimento sido posteriormente consagrado na Lei de Programação Militar, aprovada pela Lei Orgânica n.º 2/2019, de 17 de junho, com a consequente atribuição de recursos financeiros próprios ao EMGFA para, no âmbito das suas competências, edificar essa capacidade.

Através do Despacho n.º 15/MDN/2020, de 6 de fevereiro, o Ministro da Defesa Nacional estabeleceu o Comité de Monitorização da Ciberdefesa, constituído pelo conjunto de entidades da defesa nacional com competências em matéria de ciberdefesa. Este Comité tem como missão assegurar a monitorização e a articulação de todos os assuntos relacionados com a ciberdefesa, com vista a manter informado o membro do Governo responsável pela área da defesa nacional, constituindo-se como a principal entidade responsável pelo acompanhamento destas matérias na defesa nacional e assegurando a coerência das iniciativas em curso.

A Estratégia Nacional de Segurança do Ciberespaço 2019-2023, aprovada pela Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, congrega seis eixos de intervenção, dos quais se extrai a atribuição de funções específicas à defesa nacional, nomeadamente, no âmbito da defesa dos interesses, dos valores e da soberania e independência nacionais e da integridade do território, incluindo o reforço da resiliência das Forças Armadas e restantes entidades que integram a defesa nacional, de forma a assegurar a defesa nacional no ciberespaço ou através dele, nomeadamente pelo emprego de capacidades ofensivas, quando necessário e sob orientação política. Refere, ainda, a necessidade de «aprofundar o emprego dual das capacidades de ciberdefesa, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão».

No âmbito da Organização do Tratado do Atlântico Norte (OTAN), os Chefes de Estado e de Governo dos Estados-Membros assumiram, em 2014, na declaração final da Cimeira de Gales que o direito internacional é aplicável ao ciberespaço e que a ciberdefesa faz parte dos objetivos de defesa coletiva da OTAN, estabelecendo um compromisso de os Estados-Membros desenvolverem as suas capacidades nessa área. Daí resultou a assunção formal, em 2016, na Cimeira de Varsóvia, do ciberespaço como o quarto domínio das operações, associando este novo espaço de condução de operações militares aos ambientes terrestre, naval e aéreo, e tendo estabelecido a melhoria das capacidades de ciberdefesa dos Estados aliados como uma prioridade, sustentada através do compromisso assumido no Cyber Defence Pledge. Mais recentemente, os Aliados, através do Conceito Estratégico da OTAN aprovado em junho de 2022, reafirmaram que a utilização segura e o acesso sem restrições ao ciberespaço são fundamentais para uma efetiva dissuasão e defesa coletivas. Neste contexto, instrumentos como o Defence Innovation Accelerator of the North Atlantic (DIANA) e o Fundo de Inovação da OTAN (NIF) concorrem para o desenvolvimento e modernização de capacidades, para uma melhor proteção das redes e para a promoção de uma comunidade de inovação transatlântica que consiga responder ao desafio de tecnologias emergentes disruptivas, incluindo no domínio ciber.

Também no plano europeu, a ciberdefesa é hoje uma área prioritária, tendo a Estratégia de Cibersegurança da União Europeia (UE), de dezembro de 2020, reafirmado o ciberespaço como um domínio da atividade militar e identificado como uma das iniciativas estratégicas a desenvolver pela UE a «facilitação do desenvolvimento de uma 'Visão e Estratégia Militar para o Ciberespaço como Domínio da Atividade Militar' para as missões e operações militares da [Política Comum de Segurança e Defesa]». A Bússola Estratégica aprovada em março de 2022 compromete-se, por sua vez, a desenvolver uma política de ciberdefesa de forma a melhor preparar e responder a eventuais ciberataques. A inclusão da ciberdefesa no Plano de Desenvolvimento de Capacidades da Agência Europeia de Defesa, bem como o reconhecimento pela Comissão Europeia da necessidade de criar sinergias para fomentar a inovação nas tecnologias de ciberdefesa, em conjunto com a economia civil, tem incentivado os Estados-Membros a incluir a ciberdefesa no âmbito da Cooperação Estruturada Permanente (PESCO) e do Fundo Europeu de Defesa. Em resposta a este desafio, Portugal apresentou, na terceira vaga de projetos PESCO, a Cyber Academia and Innovation Hub (CAIH), como um projeto sob sua liderança, com vista a estabelecer uma ligação entre a dimensão militar e civil da segurança do ciberespaço.

Por seu lado, o artigo 275.º da Constituição dispõe que incumbe às Forças Armadas a defesa militar da República. Concomitantemente, tanto a Lei de Defesa Nacional, aprovada pela Lei Orgânica n.º 1-B/2009, de 7 de julho, na sua redação atual, como a Lei Orgânica de Bases da Organização das Forças Armadas, aprovada pela Lei Orgânica n.º 1-A/2009, de 7 de julho, na sua redação atual, referem que incumbe às Forças Armadas desempenhar todas as missões militares necessárias para garantir a defesa dos interesses e valores e da soberania e independência nacionais, bem como a integridade territorial do Estado. Por último, extrai-se do Conceito Estratégico Militar, aprovado a 22 de julho de 2014, que as Forças Armadas, no caso de sujeição a ciberataques, serão chamadas a intervir para «garantir a salvaguarda da informação e a proteção das infraestruturas de comunicações e dos sistemas de informação das Forças Armadas, assim como o apoio na proteção e defesa das infraestruturas críticas nacionais e do Estado».

Decorre da própria orgânica do EMGFA que caberá às Forças Armadas, em obediência aos órgãos de soberania competentes, a execução de operações de natureza ofensiva e defensiva no ciberespaço ou através dele, como forma de salvaguardar a defesa dos interesses e valores fundamentais da ordem constitucional, a soberania e independência nacionais, bem como a integridade do território, devendo aplicar-se neste domínio os princípios da subordinação ao poder político e de estrita observância do direito nacional e internacional aplicável.

Compete, por seu lado, ao Governo assegurar que as Forças Armadas estejam adequadamente capacitadas para responder à sua missão, que estão perfeitamente integradas no sistema nacional de resiliência do ciberespaço, bem como nas iniciativas de inovação e capacitação nacionais e que o quadro normativo e jurídico nacional está adequado ao cumprimento dos objetivos politicamente definidos para a ciberdefesa.

A presente resolução visa, assim, caracterizar e densificar a visão estratégica, o enquadramento interorganizacional e assegurar o desenvolvimento desta capacidade, crucial para a soberania digital.

Assim:

Nos termos da alínea *a*) do n.º 1 do artigo 200.º da Constituição, o Conselho de Ministros resolve:

1 — Aprovar a Estratégia Nacional de Ciberdefesa (ENCD), que consta do anexo à presente resolução e da qual faz parte integrante.

2 — Determinar que a execução da ENCD deve ser monitorizada pelo Estado-Maior-General das Forças Armadas (EMGFA), em articulação e estreita cooperação com todas as entidades relevantes, no sentido de a manter permanentemente atual e relevante.

3 — Cometer ao EMGFA a elaboração de um Plano de Ação da Estratégia Nacional de Ciberdefesa (PA-ENCD), a aprovar pelo membro do Governo responsável pela área da defesa nacional no prazo de 90 dias após a entrada em vigor da presente resolução.

4 — Determinar que o EMGFA deve produzir um relatório anual de execução da ENCD e do PA-ENCD, que deve ser submetido para aprovação do membro do Governo responsável pela área da defesa nacional.

5 — Determinar que o EMGFA deve auscultar o Comité de Monitorização da Ciberdefesa sobre o relatório de execução da ENCD e do PA-ENCD, previamente à sua submissão ao membro do Governo responsável pela área da defesa nacional.

6 — Determinar que a assunção de compromissos para a execução da ENCD depende da existência de fundos disponíveis por parte das entidades públicas competentes.

7 — Determinar a revisão, com periodicidade bienal, ou sempre que necessário, do PA-ENCD.

8 — Determinar que a presente resolução entra em vigor no dia seguinte ao da sua publicação.

Presidência do Conselho de Ministros, 20 de outubro de 2022. — Pelo Primeiro-Ministro, *Mariana Guimarães Vieira da Silva,* Ministra da Presidência.

ANEXO

(a que se refere o n.º 1)

Estratégia Nacional de Ciberdefesa

1 — Nota de abertura

Portugal, pela sua posição no continente europeu, tem no mar, no espaço e no ciberespaço novas centralidades geoestratégicas e geoeconómicas que, a par da história e da cultura lusófona, são pilares relevantes ao desenvolvimento e à inserção global do País no mundo, bem como da defesa ativa dos seus interesses e valores.

Na Estratégia Nacional de Segurança do Ciberespaço (ENSC), o ciberespaço é definido como sendo o ambiente de valores e interesses complexo, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.

Num mundo globalizado, marcado por um ritmo acelerado da transformação digital e interdependência, a capacidade de usufruir do ciberespaço em segurança e em liberdade está a tornar-se cada vez mais relevante e central para o desenvolvimento das sociedades modernas.

Apesar de o ciberespaço se ter tornado um domínio central ao desenvolvimento humano, social, cultural e económico, entre outros, é, contudo, um espaço onde operam indivíduos, entidades e Estados com agendas desestabilizadoras, realizando ações de natureza encoberta, assimétrica e híbrida. Estas atividades, com forte impacto negativo no ciberespaço, mas também, e por via deste, no normal funcionamento dos Estados, das economias e das sociedades, comprometem a segurança, a confiança e a liberdade do uso — justo, equilibrado, partilhado e global — desse espaço coletivo da humanidade. É também nesta perspetiva, de defesa e reação, entre outras, às ameaças que comprometem o uso legítimo e livre do ciberespaço, que Portugal estabeleceu a ENSC.

Na ENSC a ciberdefesa vem definida como sendo a «atividade que visa assegurar a Defesa Nacional no, ou através do, ciberespaço», o que requer um esforço de densificação conceptual ao nível estratégico, da resiliência operacional e de geração de uma verdadeira capacidade.

A mesma estratégia privilegia uma perspetiva colaborativa, estabelecendo que a «segurança do Ciberespaço é uma responsabilidade partilhada entre os diferentes atores, sejam eles públicos ou privados, coletivos ou individuais». O reforço de uma responsabilidade partilhada, de forma colaborativa, materializar-se-á necessariamente numa coordenação próxima e regular entre os agentes centrais à segurança do ciberespaço em Portugal, onde se inclui o Centro de Ciberdefesa e incluirá o Comando das Operações de Ciberdefesa quando for constituído em substituição daquele, com a plena entrada em vigor da Lei de Bases da Organização das Forças Armadas, aprovada pela Lei Orgânica n.º 2/2021, de 9 de agosto, mas deverá ser também estendida a aliados e parceiros internacionais — civis e militares — para o reforço da capacidade nacional.

O desenvolvimento das capacidades de ciberdefesa, com a correspondente atribuição de verbas em sede da Lei de Programação Militar, aprovada pela Lei Orgânica n.º 2/2019, de 17 de junho, materializa um reforço importante nesse caminho, por parte do Governo.

Assim, a Estratégia Nacional de Ciberdefesa (ENCD) vem estabelecer uma visão que visa densificar conceitos e promover o desenvolvimento das capacidades de ciberdefesa nacional, no âmbito das Forças Armadas, devidamente articulada com as estruturas civis da defesa nacional, bem como com outras áreas de governação e entidades com responsabilidade pela segurança do ciberespaço, contribuindo para uma maior resiliência e soberania nacional no ciberespaço.

2 — Natureza, missão e âmbito de atuação da ciberdefesa

O desenvolvimento da capacidade nacional de ciberdefesa requer a ação concertada do País, sob orientação política do Governo e em particular da Ministra da Defesa Nacional, com vista à edificação de uma capacidade de natureza militar, conjunta, de âmbito estratégico e operacional, na dependência do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), plenamente integrada no ecossistema nacional e internacional de segurança do ciberespaço, garantindo desta forma a máxima interoperabilidade.

O ciberespaço constitui-se, assim, como um domínio de operações militares à semelhança da terra, do mar, do ar e do espaço, sendo um elemento integrante do processo de planeamento estratégico e operacional das Forças Armadas portuguesas numa perspetiva multidomínio.

Nesse sentido, deverá o desenvolvimento dessa capacidade ser alinhado com o Conceito Estratégico de Defesa Nacional e outros documentos relevantes e deve ser integrado no Planeamento de Defesa Militar, em conjugação, designadamente, com o Defence Planning Process da Organização do Tratado do Atlântico Norte (OTAN) e o Capability Defence Plan da União Europeia (UE). Adicionalmente, para edificar e sustentar esta capacidade, devem-se desenvolver iniciativas dedicadas a alavancar a capacidade tecnológica e económica nacional, contribuindo para a coesão e resiliência nacional e para projetar os interesses nacionais nas áreas consideradas estratégicas para Portugal.

A missão da ciberdefesa é assegurar a defesa nacional no ciberespaço ou através dele, consubstanciada na capacidade de garantir o direito soberano de Portugal de aceder e utilizar o ciberespaço, de forma livre, segura e em igualdade de circunstâncias com os outros Estados da comunidade internacional, contribuindo para a promoção do desenvolvimento, do progresso e dos legítimos interesses nacionais e contribuindo para a segurança cooperativa do ciberespaço no seio das entidades internacionais que Portugal integra.

A capacidade para assegurar a defesa nacional no ciberespaço ou através dele realizar-se-á pela conjugação de ações defensivas e ofensivas, que serão suportadas pelo relevante enquadramento jurídico e político, bem como pelo apoio operacional, logístico e técnico considerado necessário e adequado, nomeadamente no que concerne aos recursos humanos e à capacidade tecnológica e de recolha de informação.

Através de ações defensivas, a ciberdefesa deve ser capaz de assegurar em permanência um perímetro de proteção dinâmico e avançado das redes e dos sistemas de informação considerados críticos para a defesa nacional e, ao abrigo do direito internacional, quando necessário, para a defesa aliada.

Decorrente da legislação em vigor, cumpre, ainda, às Forças Armadas a exclusividade de executar ações de natureza ofensiva no ciberespaço ou através dele, como forma de assegurar a defesa e os interesses nacionais, em conformidade com o quadro constitucional e o direito internacional aplicável, designadamente no quadro da Carta das Nações Unidas.

Estas ações são entendidas como aquelas que materializam operações reativas, preventivas e outras deliberadas para, nomeadamente: neutralizar, manipular, negar, romper, degradar ou destruir a capacidade de uma entidade em aceder livremente ao ciberespaço, nas situações em que uma ação ou omissão que lhe seja imputável constitua uma ameaça à segurança daquele domínio; utilizar as suas redes e sistemas de informação, atacando a disponibilidade, a integridade e a confidencialidade dessa informação comprometendo a perceção e cognição daí resultantes; e ou a capacidade física para prosseguir atividades e operações cinéticas e não cinéticas em curso, entre outras.

A atividade ofensiva, em resposta à ação de entidades que comprometam a segurança da informação, a disponibilidade dos sistemas e o legítimo acesso ao ciberespaço por parte do Estado português, serão regulados por normas próprias, na forma de regras de empenhamento, com autorizações que podem ir do âmbito tático ao estratégico, sendo essas normas autorizadas pelo poder político instituído e verificada a sua correta utilização, sempre também em linha com a moldura constitucional e jurídico-internacional aplicável.

No contexto das entidades que contribuem para a segurança do ciberespaço em Portugal, e assegurando a necessária articulação com os demais atores pertinentes neste domínio, é atribuída à ciberdefesa a liderança das ações militares que respondam a ameaças originárias de Estados ou entidades não estatais, direta ou indiretamente, nomeadamente quando sejam promovidas de forma encoberta por Estados, ou que, pela sua dimensão crítica e capacidades, os seus efeitos coloquem em risco a soberania nacional, a independência nacional, a integridade do território, a liberdade e segurança das populações, bem como a proteção dos valores fundamentais da ordem constitucional, independentemente da sua origem.

Consequentemente, devem ser asseguradas a partilha de informação, por todas as entidades técnicas com responsabilidades na segurança do ciberespaço, e a avaliação conjunta da natureza e extensão das ameaças, em linha com o princípio de cooperação, garantindo uma identificação precisa de todos os incidentes e ataques de natureza estatal ou não estatal no ciberespaço ou através dele, ou com impacto na soberania e/ou na resiliência estrutural do Estado.

3 — Princípios de atuação da ciberdefesa

A ciberdefesa dever-se-á reger pelos seguintes princípios:

Proteção e sustentação

A capacidade defensiva da ciberdefesa deve ser capaz de detetar e se possível antecipar ciberataques, evitar ou retardar a sua progressão e contribuir para a recuperação dos sistemas que tenham sido comprometidos, garantindo dessa forma a proteção das redes e sistemas de informação do universo da defesa e/ou sob sua responsabilidade.

Deve contribuir com alertas e recomendações para que as áreas responsáveis pela arquitetura e pela administração de redes e sistemas de informação possam evitar vulnerabilidades, corrigir rapidamente as detetadas, especialmente as que estejam a ser um veículo de penetração pelos ciberataques em curso. Deste modo, a ciberdefesa deve constituir-se como uma referência técnica permanente para o universo da defesa nacional, no âmbito dos sistemas de proteção e resiliência das redes e dos sistemas de informação. Para o efeito, deve a ciberdefesa desenvolver os mecanismos e processos necessários a uma capacidade que deve ser prospetiva, mas simultaneamente reativa, esta última em situações de urgência e complexidade elevada.

Para garantir a defesa, de forma contínua e sem interrupções, esta capacidade terá necessariamente de ser sustentável e por isso deve: estar permanentemente disponível 24 horas todos os dias; incorporar nos seus recursos humanos os conhecimentos técnicos suficientes para a tarefa; e cobrir o universo defensivo e ofensivo determinado e necessário à missão da ciberdefesa. Pretende-se que a ciberdefesa seja capaz de garantir a resiliência necessária contra ataques sofisticados, de saturação e prolongados no tempo.

Proporcionalidade e credibilidade

As ações e operações militares conduzidas no âmbito da ciberdefesa devem ser executadas no respeito do quadro legal em vigor, obedecendo à mesma lógica e fundamentos que caracterizam a atuação em operações cinéticas, tendo como objetivo atingir com sucesso a desejada dissuasão no ciberespaço. Para isso, segundo uma lógica multidomínio, deverá existir a flexibilidade operacional necessária para ajustar, de forma proporcional, a resposta a cada tipo de situação, sempre em linha com o direito nacional e internacional aplicável, tendo por base uma adequada análise de risco e um processo credível de imputação da entidade responsável pelo ataque, assegurando, assim, a necessária legitimidade e credibilidade.

A utilização de capacidades ofensivas deverá reger-se sobretudo pelos princípios da proporcionalidade e da necessidade, aplicando-se, em situação de conflito armado, os princípios regentes do direito internacional humanitário.

A decisão e controlo pelo poder político devem ser assegurados no âmbito da estrutura hierárquica governamental e coadjuvados por um mecanismo de fiscalização que garanta um escrutínio eficaz, dentro de um quadro normativo e legal adequado, bem como a manutenção e o efetivo exercício do poder de direção e superintendência. Para isso, deve ser garantida, nomeadamente, a permanente disponibilidade dos dados da ciberdefesa, devidamente classificados ao abrigo do regime da informação classificada.

Parceria e cooperação

A segurança do ciberespaço deve ser abordada de forma inclusiva, alargada e integradora, promovendo a indispensável cooperação entre instituições civis e militares, para o benefício do interesse comum e para uma segurança eficiente e eficaz.

A partilha de informação, de exercícios e de boas práticas e a existência de uma estrutura de comando clara, fortemente apostada no desenvolvimento da capacidade de resiliência nacional, em parceria com empresas e centros científicos e tecnológicos nacionais, afiguram-se como contributos de primeira linha que a defesa nacional poderá dar para a segurança do ciberespaço de interesse nacional.

A ciberdefesa integra o núcleo das capacidades do Estado português definidas na ENSC, através de mecanismos de cooperação e troca de informação com as entidades relevantes, e constituir-se-á como o ponto de contacto único para todas as entidades militares das alianças e coligações a que o País pertence, contribuindo para uma perceção o mais completa possível dos fenómenos desestabilizadores do uso ilegítimo do ciberespaço e para a ação externa do Estado.

A avaliação do impacto das ações desestabilizadoras, ilegais e ilegítimas, constitui-se o elemento crítico para uma clara atuação dos organismos com responsabilidades nacionais no ciberespaço, devendo ser promovidos os processos e mecanismos que garantam uma rápida e eficaz classificação das ameaças pela ciberdefesa, articulada com todas as entidades com responsabilidades nesta matéria.

Para isso, nomeadamente para fazer face a situações de crise ou estados de exceção, importará reforçar os sistemas de partilha de informação e de classificação de incidentes já existentes, promovendo, em coordenação com o Secretário-Geral do Sistema de Segurança Interna, a interoperabilidade técnica e funcional entre o Centro de Ciberdefesa, que será sucedido pelo Comando das Operações de Ciberdefesa, o Centro Nacional de Cibersegurança, a Polícia Judiciária e o Sistema de Informações da República Portuguesa, sem prejuízo do recurso a outros canais tidos como necessários para a efetivação desta partilha.

No âmbito das atividades de informação, que contribuam para o mapeamento das ameaças, o princípio a seguir será o da necessidade de partilhar, quer os parceiros sejam nacionais ou estrangeiros. Este princípio está naturalmente enquadrado pelos interesses nacionais, condicionado e submetido à necessária cobertura legal para colaborar com essas entidades, resultante quer da legislação nacional, quer da legislação da UE, quer ainda dos tratados internacionais regularmente ratificados ou aprovados pelo Estado português, bem como às necessidades operacionais, tendo em consideração também o princípio da confiança e das relações de reciprocidade estabelecidas.

4 — Objetivos estratégicos

A ciberdefesa deve assegurar a liberdade de ação do País no ciberespaço através da capacidade de conduzir operações militares e, quando necessário e determinado, a exploração reativa, preventiva ou deliberada do ciberespaço para impedir ou dificultar o seu uso hostil contra os interesses nacionais e para promover os mesmos através da prossecução dos seguintes objetivos estratégicos:

a) Consolidar a capacidade de ciberdefesa;
b) Maximizar a resiliência e a coesão da ação nacional;
c) Promover a investigação, desenvolvimento e inovação;
d) Garantir recursos qualificados.

5 — Eixos de desenvolvimento da ciberdefesa

O desenvolvimento de uma capacidade nacional de ciberdefesa deverá assentar numa abordagem cooperativa, alavancada por um ecossistema nacional de segurança do ciberespaço que agrega as vertentes defensiva e ofensiva. Para isso, deverá garantir-se a articulação entre as estruturas da defesa nacional e as das restantes áreas governativas, mas também entre a comunidade académica, os setores público e privado, em particular o setor empresarial, a base tecnológica e industrial de defesa e as demais entidades com responsabilidade na segurança do ciberespaço de interesse nacional.

Definem-se, assim, seis eixos orientadores para a edificação de um plano de ação concreto, a ser desenvolvido pela defesa nacional, destinado a potenciar a capacidade de ciberdefesa e a contribuir para o reforço das capacidades sinérgicas e as relações de cooperação entre organismos do Estado e das diferentes entidades relevantes, bem como fomentar o desenvolvimento industrial, científico e tecnológico nacional, euro-atlântico e no espaço da Comunidade de Países de Língua Portuguesa.

E1 — Utilizar o ciberespaço como um domínio de operações

Decorrente das grandes revoluções tecnológicas e da tipologia e diversidade de ameaças a que os países são sujeitos, a capacidade autónoma de conduzir operações no ciberespaço ou através dele deve tornar-se parte integrante da capacidade militar global das Forças Armadas Portuguesas, em linha com as decisões tomadas no âmbito da OTAN e da UE, assim como as que decorrem da Orientação para a política para a Ciberdefesa, aprovada pelo Despacho n.º 13692/2013, publicado no *Diário da República,* 2.ª série, n.º 208, de 28 de outubro de 2013, da Diretiva Ministerial de Orientação Política para o Investimento na Defesa, aprovada pelo Despacho n.º 4103/2018, publicado no *Diário da República,* 2.ª série, n.º 79, de 23 de abril de 2018, e da Lei de Programação Militar, em estreita ligação com as diferentes entidades que garantem, quer a orientação política, quer o apoio logístico e técnico relevante.

O ciberespaço constitui-se, assim, um elemento integrante do processo de planeamento estratégico e operacional, onde deverá ser dada especial atenção à sua potencial influência nas missões nos outros domínios de operações. Desta forma, a ciberdefesa participa no conjunto das operações da defesa numa perspetiva multidomínio (terra, mar, ar, espaço e ciberespaço), constituindo-se igualmente como um elemento de dissuasão.

A ciberdefesa, em resultado da sua componente ofensiva, é eminentemente uma capacidade do âmbito estratégico, dependente de autorização política, onde devem ser plenamente entendidas a ponderação do alcance, tempo e efeitos, assim como as prováveis reações e implicações que possam resultar da sua atuação, nomeadamente no posicionamento internacional do País.

O desenvolvimento desta capacidade militar conjunta deverá ter em conta as competências das diferentes entidades da defesa e restantes áreas governativas, devendo as Forças Armadas, sob autoridade do CEMGFA, assegurar todas as capacidades de comando e controlo relevantes a este novo domínio de operações, incluindo aquelas requeridas no âmbito da cooperação nacional e internacional militar, devendo proceder-se ao desenvolvimento gradual das estruturas conducentes à futura criação de um comando da ciberdefesa.

E2 — Reforçar a capacidade de ciberdefesa nacional

Com vista a prosseguir o desenvolvimento da capacidade de ciberdefesa, incrementando a capacidade de assegurar a defesa nacional no ciberespaço ou através dele, devem ser prosseguidas três linhas de ação principais:

a) Incrementar o conhecimento e o número de operacionais da ciberdefesa para uma dimensão suficiente, de modo a que seja garantida a missão e os princípios definidos para esta capacidade, devendo os serviços centrais do Ministério da Defesa Nacional, em articulação com as entidades relevantes, identificar recursos disponíveis e necessidades, bem como desenvolver propostas legislativas ou de outra natureza que permitam alavancar este novo âmbito de atividade operacional, associado ao quarto domínio das operações militares;

b) Assegurar permanentemente uma infraestrutura tecnologicamente avançada — sofisticada, robusta e resiliente — que permita um potencial diferenciador para operar com vantagem no ciberespaço, devendo os serviços centrais do Ministério da Defesa Nacional, em apoio ao EMGFA e às Forças Armadas e em articulação com outras entidades relevantes, participar na identificação de requisitos técnicos transversais que respondam às necessidades tecnológicas da ciberdefesa;

c) Garantir, na máxima extensão possível, a independência tecnológica, pela criteriosa combinação de sistemas abertos e comerciais e pelo incremento das capacidades nacionais fomentando o desenvolvimento de parcerias com o tecido económico e académico nacional, devendo a idD-Portugal Defence, S. A., em articulação com outras áreas governativas, no âmbito da sua missão, proporcionar o desenvolvimento de parcerias com o ecossistema tecnológico nacional, por forma a assegurar um adequado nível de capacidades.

Deste modo, e tendo em consideração que a ciberdefesa é uma atividade de conhecimento intensivo, fortemente especializado, deve ser dada uma importância elevada ao recrutamento, seleção, retenção e capacitação da componente humana, sendo esta uma prioridade.

E3 — Criar a escola de ciberdefesa

Assegurar o constante incremento e a adaptação das qualificações necessárias para que os recursos humanos da defesa possam desenvolver operações num ambiente multidomínio e especificamente no ciberespaço, com vantagem sobre os agentes de ameaça, numa atuação segura, dinâmica e capaz.

A edificação de uma entidade formadora conjunta, no âmbito das Forças Armadas e em colaboração com outras entidades nacionais e internacionais de referência, deverá ser entendida como um instrumento crucial para a resiliência e soberania digital do País, servindo também para promover a ligação à comunidade académica e empresarial nacional e estimular o conhecimento dos cidadãos sobre a missão da ciberdefesa.

Antecipando a execução do projeto apresentado por Portugal na terceira vaga de candidaturas PESCO, a escola de ciberdefesa deverá articular-se com a Cyber Academia and Innovation Hub (CAIH), explorando sinergias, estabelecendo para esse efeito uma estreita articulação com outras iniciativas de capacitação de recursos humanos na área da cibersegurança, nacionais e internacionais, contribuindo com os seus conhecimentos específicos para a capacitação tecnológica dos recursos humanos das entidades com responsabilidade na segurança do ciberespaço.

Deverá também tornar-se um centro de referência internacional, aberto à cooperação no seio das alianças e coligações militares de que o País faz parte, nomeadamente potenciando a participação de Portugal no Cooperative Cyber Defence Centre of Excellence da OTAN, e tornando-se um instrumento de projeção de influência do País no exterior e de reforço do compromisso de Portugal enquanto coprodutor de segurança internacional.

Deverão as Forças Armadas, sob orientação do EMGFA e em articulação com as restantes entidades da defesa nacional, desenvolver o projeto desta escola, assegurando a sua operacionalização e permanente adequação às necessidades do País.

E4 — Intensificar a cooperação nacional e internacional

Ao nível estratégico, a cooperação nacional e internacional reveste-se de particular importância para os objetivos transversais da ciberdefesa, assegurando a ligação estreita entre o desenvolvimento de capacidades nacionais e a participação na defesa europeia, bem como nas alianças militares e organizações regionais que Portugal integra.

Tendo em conta a partilha de responsabilidades prevista na ENSC e os quadros cooperativos existentes, devem ser desenvolvidos esforços que garantam, para além das necessidades de cada área, a partilha atempada de informação, a monitorização, avaliação e definição conjunta da natureza da ameaça e o desenvolvimento de procedimentos e regras de empenhamento partilhados, sempre que relevante, e que garantam respostas em tempo útil e eficazes.

A participação ativa nos mecanismos de gestão de crises, em exercícios e organismos internacionais com responsabilidades na segurança do ciberespaço, deve ser ativamente promovida e formalizada quando relevante.

A promoção dos objetivos da ciberdefesa exige uma estreita colaboração entre as estruturas do universo da Defesa Nacional, incluindo o Ministério da Defesa Nacional, as Forças Armadas e a idD-Portugal Defence, S. A., em articulação com as áreas governativas com responsabilidades em matéria de cooperação internacional e em matéria de segurança do ciberespaço.

E5 — Promover a investigação, desenvolvimento e inovação no ciberespaço, incentivando o desenvolvimento de soluções de duplo uso

Os agentes de ameaça no domínio do ciberespaço podem ter como veículo as tecnologias emergentes e disruptivas, da supercomputação, da robótica e da inteligência artificial, sendo fundamental o desenvolvimento das melhores ferramentas e capacidades para as contrariar, nomeadamente através de parcerias com centros de investigação e desenvolvimento, universidades e empresas.

A sensibilização e a capitalização do conhecimento nacional e dos cidadãos nesta área assumem especial importância para uma maior segurança no ciberespaço, autonomia tecnológica e formulação de doutrina, políticas, normas e procedimentos indispensáveis a este novo domínio de operações, assumindo o Instituto da Defesa Nacional um papel fundamental a esse respeito.

A ciberdefesa deverá ter, por isso, um papel importante na promoção da indústria 4.0, utilizando as suas necessidades para alavancar o arranque e sustentação de nichos de competências nacionais, que possam eventualmente vir a constituir-se como fundamentais no tecido económico e académico nacional e que promovam o reforço da autonomia nacional. Ao nível da defesa nacional destaca-se o papel da idD-Portugal Defence, S. A., do Instituto Universitário Militar e das suas unidades orgânicas autónomas universitárias, no âmbito das suas respetivas competências.

Garantindo a plena interação dos esforços da defesa nacional no conjunto das ações do Estado e procurando traduzir os incentivos para o desenvolvimento industrial da defesa em inovação de duplo uso, deverá ser assegurada a cooperação entre as áreas governativas responsáveis pela defesa nacional, a administração interna, economia e mar, ciência e tecnologia e o ambiente, entre outras.

E6 — Assegurar as capacidades necessárias da ciberdefesa em contextos de estado de exceção

Nas situações de estado de sítio e de estado de emergência previstas na legislação nacional, o emprego da ciberdefesa será enquadrado à luz do estabelecido na lei em vigor. A ciberdefesa desenvolverá também uma capacidade de coordenação e gestão centralizada de ações no ciberespaço, estando preparada para integrar os esforços de outras organizações nacionais e internacionais para situações de exceção, ou conflito armado.

Esta última componente deverá ser apoiada por um Estado-Maior e um serviço de informações dedicado, que manterá um quadro de situação atualizado das ameaças promovidas por Estados, alianças ou coligações destes, incluindo fenómenos patrocinados por atores não estatais como o terrorismo, a insurgência, a intolerância radical e a guerra híbrida.

Estas capacidades e responsabilidades devem estar perfeitamente integradas no sistema nacional de resiliência do ciberespaço, através de canais de comunicação claros, articulados e de mecanismos de ação conjunta, sempre que se justifique, garantindo as necessidades da defesa nacional e o seu pleno contributo para a segurança do ciberespaço de interesse nacional.

6 — Avaliação e revisão da Estratégia

A execução da presente Estratégia e correspondente plano de ação serão objeto de monitorização e revisão pelo EMGFA, em estreita articulação com o Comité de Monitorização da Ciberdefesa.

Essa avaliação incluirá uma verificação do cumprimento dos objetivos e do plano de ação definidos, bem como da sua adequação em função dos vetores político-estratégicos considerados em razão da evolução das circunstâncias. De acordo com a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, deverá o EMGFA assegurar o reporte relevante sobre a implementação da ENCD ao Conselho Superior de Segurança do Ciberespaço.

Por outro lado, a rápida evolução intrínseca ao ciberespaço exige que a presente Estratégia seja objeto de revisão regular e periódica, em alinhamento com o ciclo de vigência da ENSC, considerando-se que, sem prejuízo de processos de revisão extraordinários sempre que as circunstâncias o exijam, esta deve ocorrer num prazo máximo de cinco anos.

115826042