Confrontos no Ciberespaço e o seu impacto na Segurança e Defesa Nacional – A alteração do paradigma estratégico internacional

Brigadeiro-general
Paulo Fernando Viegas Nunes

1. Introdução

A revolução tecnológica impulsionou a utilização da internet à escala planetária, aumentando a importância do funcionamento em rede, melhorando a estrutura de enquadramento e as condições de desenvolvimento das modernas sociedades. A densidade e profundidade das interligações daí decorrentes, reforçada pela adoção das comunicações de 5.ª Geração (5G), por sistemas de apoio à decisão suportados por ambientes de realidade virtual, pela supercomputação (quântica) e pela Inteligência Artificial (IA), alteraram os padrões de utilização do ciberespaço e são hoje uma realidade, influenciando cada vez mais os decisores humanos, disponibilizando recomendações, influenciando o presente e o futuro das organizações e dos Estados.

O World Economic Forum (WEF), num relatório recente[1], estima que, em 2025, 85 milhões de empregos sofrerão o impacto de uma alteração na divisão do trabalho entre seres humanos e máquinas. Uma parte significativa dos novos empregos terá uma relação direta com a área tecnológica e será criada em áreas ainda não existentes ou que já se encontram em transformação ao nível dos seus requisitos de competências. Neste

"novo mundo", complexo e interdependente, assistimos à adoção de modelos organizacionais híbridos onde a presença no mundo físico se estende para o ciberespaço, para uma interação virtual, onde a informação e o conhecimento se afirmam como os ativos mais críticos e valiosos.

A recente situação pandémica mundial, demonstrando que nenhuma instituição ou indivíduo pode enfrentar de forma isolada os desafios globais, tornou claro o enorme aumento da importância da internet e do ciberespaço na garantia da resiliência dos Estados, provando que as mudanças impostas pela transformação digital são inevitáveis, por vezes mesmo irreversíveis, em praticamente todas as áreas de atividade e domínios da sociedade.

Assistimos assim ao aprofundamento da vivência em rede, em que as interações do mundo real se transferem e dependem, cada vez mais, da disponibilidade e do acesso seguro ao ciberespaço. No entanto, importa assinalar que estes processos não são isentos de riscos, nomeadamente, porque subsistem ainda grandes diferenças ao nível da literacia e da transição digital, reforçando a importância da proteção da informação, dentro e fora das organizações. Explorando estas assimetrias funcionais e estruturais, atores mal-intencionados podem lançar ataques, através do ciberespaço e a partir dele, tanto no domínio social, político, económico como militar.

Ao serviço da consecução dos objetivos estratégicos de atores Estado e não-Estado, o ciberespaço passou também a ser utilizado como vetor de projeção de poder à escala global, apresentando, cada vez mais, um forte e inegável impacto, nomeadamente, enquanto espaço global comum, não limitado pela esfera pública ou privada, interna ou externa, civil ou militar.

2. Impacto militar do Ciberespaço

Um mundo mais interligado significa também a existência de um espetro mais alargado de ameaças e riscos. Os métodos tradicionais de conduzir a guerra, quando combinados com as novas tecnologias disruptivas e com novos elementos adjuntos como a desinformação online e os ciberataques, resultam muitas vezes em conflitos passíveis de ser considerados "guerra híbrida". Este fenómeno, explora a ambiguidade utilizada por atores Estados e não-Estado para infligir dano, pulverizar a linha entre a guerra e a paz, introduzir a dúvida e desestabilizar as sociedades. Estas zonas cinzentas, não lineares, têm vindo a ser promovidas pelas principais potencias mundiais, de forma a minar os esforços dos seus adversários, ao mesmo tempo que, paradoxalmente, se procura evitar uma declaração formal de guerra. A última década, marcada por uma utilização crescente do ciberespaço nas operações militares, acentuou esta tendência.

A crescente prevalência das ameaças e da "guerra híbrida" reflete assim uma ordem global em mudança. Conflitos que se podem negar e de natureza indireta, incluindo a guerra cibernética, onde a distância física e o poder militar convencional/cinético perdem

relevância, podem ser facilmente combinados com sanções económicas e comerciais. Também em áreas como o crime organizado e o terrorismo, o ciberespaço ocupa hoje uma posição central. Os beligerantes aprenderam todos a utilizar, alguns deles com um nível de sofisticação muito elevado, as capacidades oferecidas por este espaço global.

Face ao seu atual quadro de empenhamento e às características do ambiente operacional, existe um claro desajuste entre as capacidades e meios militares que equipavam as Forças Armadas da era industrial, predominantemente de atrito, e as requeridas pelos conflitos da era moderna. A tipologia da moderna conflitualidade requer, cada vez mais, a mobilização de capacidades de natureza não-cinética para a sua resolução, onde o desenvolvimento de operações no ciberespaço, funcionando como um multiplicador de força, permite projetar poder no e a partir do ciberespaço, afetando outros domínios operacionais, muitas vezes sem a utilização de meios cinéticos (Nunes, 2020).

Por outro lado, a tecnologia está também a transformar os conflitos de múltiplas e diversas formas, com inevitáveis e fortes consequências no domínio militar. Desde a utilização de sistemas robotizados, autónomos e não tripulados, até à integração de exoesqueletos e de sensores no corpo humano, passando pelas novas tecnologias e aplicações da realidade virtual e aumentada, surgem novos produtos considerados até muito recentemente ficção científica. Num futuro próximo, para além da melhoria das capacidades homem-máquina dos combatentes, será de esperar que estas venham a reduzir a sua presença física no campo de batalha, intervindo estes cada vez mais de forma remota. A integração e fusão destas novas tecnologias em rede, nos atuais e futuros sistemas militares, podem também criar sistemas de armas de grande letalidade e precisão, alterando os custos humanos, políticos e económicos da guerra.

Tradicionalmente, existia uma relação direta entre o custo dos sistemas de armas e a sua capacidade destrutiva, tendo sempre em consideração a distância física a que os equipamentos militares permitiam atingir os seus alvos. No entanto, as armas cibernéticas vieram inverter esta lógica da projeção de poder, nomeadamente, porque o seu custo é hoje substantivamente menor, mas o seu alcance é global, permitindo, através da sua elevada capacidade disruptiva e destrutiva, atingir alvos localizados em qualquer ponto do globo, bastando para tal que os mesmos se encontrem ligados em rede. Esta situação, com um forte impacto estratégico no domínio militar, tem originado uma verdadeira "corrida às ciberarmas" por parte de muitos Estados que, a um custo relativamente reduzido e explorando o forte impacto do ciberespaço numa sociedade de matriz marcadamente digital, procuram aumentar o seu potencial estratégico, a sua capacidade de projeção de poder e de dissuasão no atual ambiente de segurança internacional.

Com a proliferação de ciberarmas mas também de ferramentas informáticas de baixo custo, este tipo de capacidades passaram a estar disponíveis a praticamente todo o tipo de atores, nomeadamente, a indivíduos mal intencionados, ao crime organizado e a grupos terroristas. Há uma década, existia uma elevada probabilidade de ocorrência de ataques de pirataria informática (baixo poder disruptivo) e uma baixa probabilidade de

ocorrência de ciberataques patrocinados por Estados (alto poder disruptivo). Hoje, fruto da alteração do paradigma estratégico, assistimos a uma convergência do espetro da ameaça onde os piratas informáticos passam a ter a possibilidade de desenvolver ataques com elevado poder disruptivo (e elevada probabilidade) e os atores Estado, tradicionalmente com elevada capacidade disruptiva e destrutiva, passam a ser chamados a intervir também com elevada probabilidade.

A evolução do ciberespaço, observada ao longo dos últimos anos, não pode por esta razão ser dissociada da necessidade de ajustamento permanente às suas dinâmicas estratégicas, operacionais e tecnológicas, reforçando a necessidade de novos processos de cibersegurança e ciberdefesa.

3. Utilização operacional do Ciberespaço pelas Forças Armadas

O ciberespaço interseta transversalmente todos os vetores de projeção do poder nacional, incluindo os diversos domínios associados à segurança e defesa do Estado e, consequentemente, segundo uma lógica multidomínio, também todos os domínios operacionais das Forças Armadas (mar, terra, ar e espaço). A utilização do ciberespaço e do ambiente da informação assume assim um caráter transversal e multidisciplinar, sendo evidente o seu contributo para a definição dos diversos tipos de forças (tangíveis e intangíveis) de um País ou Aliança.

Segundo uma perspetiva operacional, a Organização do Tratado do Atlântico Norte (OTAN) entende o ciberespaço como "o domínio virtual, de natureza global e comum, dentro do ambiente da informação, composto pelos sistemas de comunicação, informação e outros sistemas de natureza eletrónica, incluindo a sua interação e a informação, de natureza digital, que é armazenada, processada e transmitida através desses sistemas" (OTAN, 2018c, p.A-1). Em termos nacionais, conforme assumido pela Estratégia Nacional de Segurança do Ciberespaço (ENSC, 2019), este é também entendido como "um ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação".

Importa assim reconhecer o carácter dual da informação (Nunes, 2020, p. 7), como recurso, no contexto dos processos de decisão, e/ou, como vetor de ataque, enquanto instrumento de exercício do poder. Na figura 1, a designada "pirâmide cognitiva", construída a partir dos seus quatro níveis de abstração (dados, informação, conhecimento e sabedoria), reflete a natureza dos efeitos produzidos (físicos, de sintaxe/lógicos e semânticos/cognitivos) e os diversos domínios onde os mesmos são aplicados.

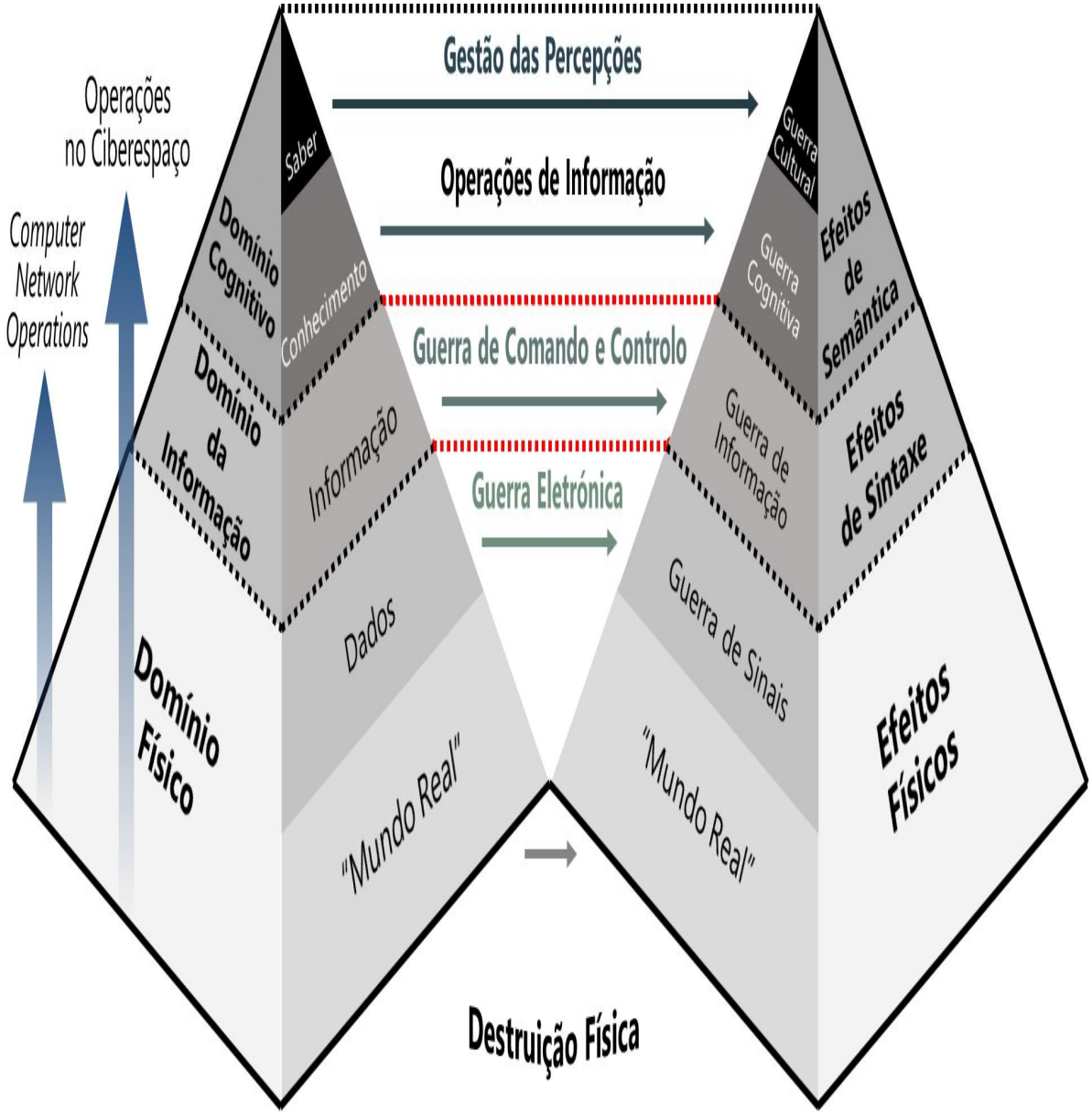

Figura 1 – "Pirâmide cognitiva" e a utilização operacional do ciberespaço.

Fonte: Nunes (2020, p. 7)

Face à doutrina existente, as Forças Armadas atuam de forma articulada no domínio: físico (destruição física e guerra eletrónica/guerra de sinais); da informação (guerra de comando e controlo/guerra de informação); e, cognitivo (operações de informação/guerra cognitiva e/ou gestão das perceções).

Relativamente às operações no ciberespaço, verifica-se que o seu enquadramento doutrinário, ainda em consolidação, é indissociável do ambiente da informação. Desta

forma, as operações em redes de computadores, de natureza iminentemente tática, produzem efeitos físicos e de sintaxe/lógica. As operações no ciberespaço (Allied Joint Publication [AJP]-3.20, 2020), conduzidas ao nível operacional, sem prejuízo de utilizarem efeitos físicos (e.g. negar o acesso ou exfiltrar informação do oponente), podem atingir efeitos de sintaxe e de semântica. Finalmente, as operações de informação (AJP-3.10, 2009), assumindo um papel de coordenação, planeiam essencialmente efeitos no domínio cognitivo, ao nível operacional/estratégico.

Reconhecendo que o ciberespaço constitui um domínio global, dentro do ambiente da informação, na taxonomia relativa às operações no ciberespaço (AJP-3.20, 2020), a OTAN refere que estas podem ser de natureza defensiva ou ofensiva. Estes dois tipos de operações, fruto das dinâmicas de poder geradas à escala global, têm vindo a assumir uma importância crescente, no e através do ciberespaço, para salvaguardar a liberdade de ação das forças amigas e/ou para atingir objetivos operacionais e estratégicos.

4. Ciberespaço: um domínio estratégico para Portugal

A designada "era da informação", permitiu atingir patamares de progresso e bem-estar social sem precedentes. Abraçando as vantagens oferecidas pela transformação digital e afirmando o desígnio político de aumento da competitividade num contexto europeu e mundial, a economia nacional, passou a estar cada vez mais centrada em rede. Sobretudo a partir do princípio da década de 1990 e no início deste século, Portugal investiu fortemente na melhoria das suas infraestruturas de comunicações, apresentando uma elevada taxa de penetração na adoção de novas aplicações e serviços digitais. Em consequência desta aposta, enquanto economia de serviços, a geração de riqueza nacional tornou-se cada vez mais dependente da internet, passando a estar mais exposta e vulnerável a um leque alargado de novos riscos de segurança.

O nível de sofisticação tecnológica, que caracteriza os vários vetores de ataque emergentes do ciberespaço, faz crescer exponencialmente o nível da ameaça e os riscos sociais, colocando em risco as infraestruturas críticas, os processos de administração e governação eletrónica do Estado e, de uma forma geral, a própria resiliência nacional. Indissociável destas, levanta-se também uma outra questão ao nível da "soberania digital", nomeadamente, porque atualmente um Estado já não consegue, por si só, refazer/reajustar a sua infraestrutura de comunicações nacional sem a ajuda dos grandes fabricantes de equipamentos que, inevitavelmente, se encontram associados aos seus países de origem.

Assumindo um papel determinante, tanto na geração de valor como no exercício do poder, o ciberespaço tem vindo também a ser utilizado como elemento de desinformação, de manipulação de ideias e de influência política. Acontecimentos recentes como a "primavera árabe", as eleições norte-americanas, o "Brexit", ou até a própria pandemia COVID-19 e o atual conflito na Ucrânia, evidenciam bem o poder das redes sociais e o impacto da desinformação na geopolítica mundial.

O ciberespaço facilita o lançamento de ataques a partir de qualquer local, tornando difícil distinguir todos os atores envolvidos e clarificar o que é interno e externo. Ao longo das últimas décadas, também em áreas como o ativismo social, o crime organizado e o terrorismo, alguns atores têm vindo a utilizar o ciberespaço como vetor de ataque. Estas novas ameaças, incluindo ações desenvolvidas por atores Estado e não-Estado, devido à sua natureza assimétrica e efeitos potencialmente disruptivos e destrutivos, levaram a que este espaço global seja hoje assumido como um novo domínio das operações militares.

Só muito dificilmente será possível explorar todo o valor que o ambiente de informação e o ciberespaço oferecem às modernas sociedades sem que este desígnio seja acompanhado pela garantia da sua segurança e defesa. Por essa razão, este constitui reconhecidamente um domínio estratégico para Portugal, necessitando de ser pensado como uma área prioritária de defesa de interesses e afirmação de soberania. De forma a melhor definir os fundamentos da visão político-estratégica nacional associada à segurança e defesa do ciberespaço, importa assim, contextualizar, enquadrar e identificar os esforços em curso neste domínio.

5. Enquadramento estratégico nacional do Ciberespaço

Refletindo a evolução das políticas de defesa nacional, tanto no domínio da cibersegurança como da ciberdefesa, Portugal tem vindo, desde 2010, a desenvolver um conjunto de iniciativas destinadas a garantir uma utilização mais livre, fiável e segura do ciberespaço. Em linha com esta orientação político-estratégica, o Conceito Estratégico de Defesa Nacional ([CEDN], 2013), reconheceu a "informação e a segurança do ciberespaço" como um dos seus pilares estratégicos. Atendendo às questões emergentes da segurança do ciberespaço, o CEDN determinou, entre outras medidas, a criação de uma estrutura nacional de cibersegurança e, ao nível das Forças Armadas, a edificação de uma capacidade de ciberdefesa. Refletindo uma visão conceptual e cronológica, a figura 2 ilustra o processo de desenvolvimento da capacidade nacional de defesa do ciberespaço.

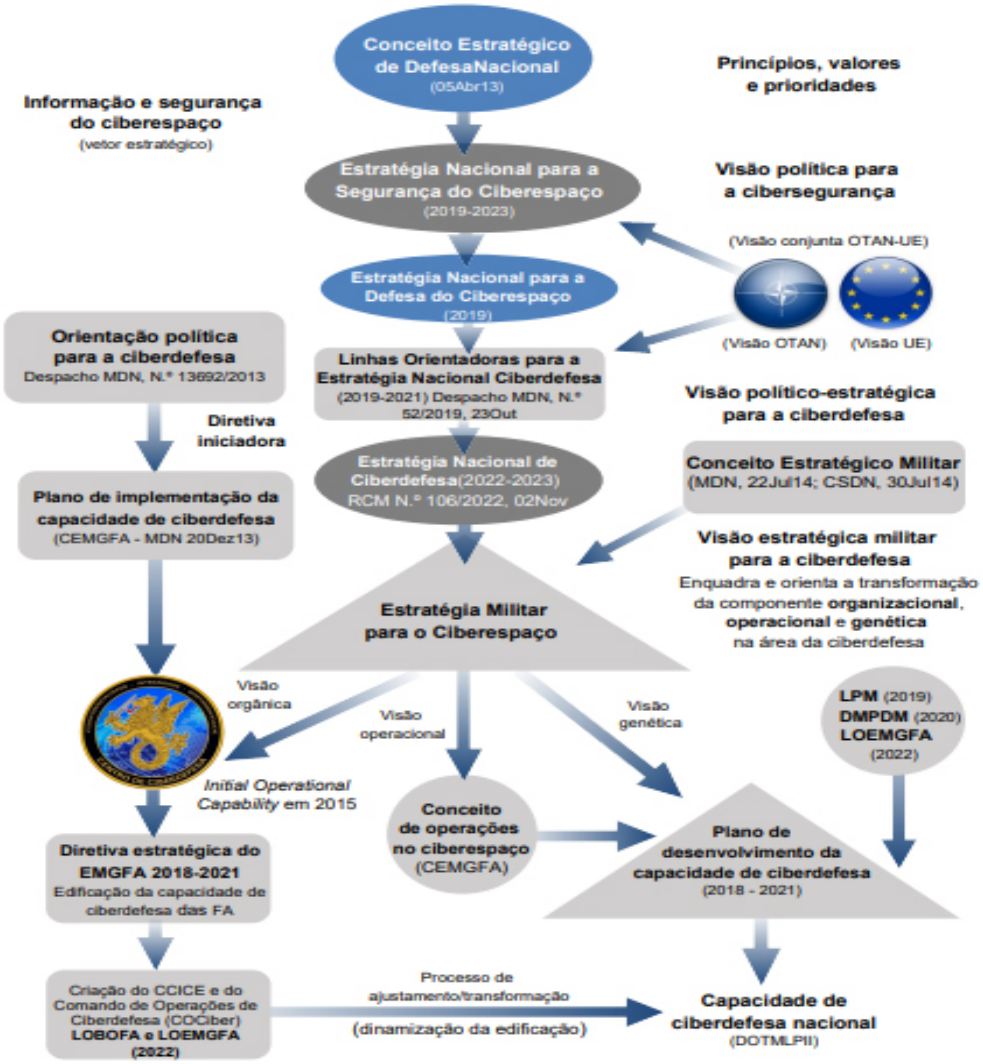

Figura 2 – Enquadramento da política de defesa e da estratégia militar para o ciberespaço.

Fonte: Adaptado de (Nunes, 2020, p. 17; Nunes, 2018, p. 94)

Neste âmbito, salienta-se que a transversalidade das áreas relacionadas com o ciberespaço e a complexidade associada à coordenação e condução de operações de cibersegurança e ciberdefesa, obriga a uma permanente adaptação da visão estratégica nacional à contínua evolução do ambiente estratégico internacional (OTAN e União Europeia [UE]).

6. Segurança e Defesa do Ciberespaço: situação atual

Requerendo mecanismos de governação transversais, capazes de garantir a necessária articulação entre a cibersegurança e a ciberdefesa nacional, a atuação eficaz das várias

entidades responsáveis só será possível através da criação de uma articulação civil-militar coordenada e integrada no ciberespaço, capaz de explorar sinergias nacionais e a cooperação internacional.

Apesar de a resiliência das tecnologias digitais ter vindo a aumentar, subsistem ainda algumas fragilidades ao nível dos processos associados à gestão de crises no ciberespaço e à partilha de informação situacional em tempo real. Esta situação limita a capacidade nacional para garantir uma atempada fusão e difusão da análise das ciberameaças emergentes num ambiente de segurança de complexidade crescente. Esta lacuna conduz potencialmente a uma falta de articulação operacional e à adoção de políticas não coordenadas, impedindo a partilha de informação crítica, resultando, por vezes, numa gestão inadequada dos riscos sociais, deixando o País vulnerável. Esta fragilidade estratégica poderá vir a ser explorada por potenciais adversários, sejam eles atores Estado ou não-Estado.

Atendendo ao contexto nacional e ao seu enquadramento internacional, importa salientar que o percurso nacional no domínio da cibersegurança e da ciberdefesa, reflete um desenvolvimento assimétrico destas duas áreas, tanto ao nível estrutural como operacional e genético, tornando difícil uma conceptualização estratégica integrada e consistente destas duas realidades.

Na área da cibersegurança, no final de 2022, Portugal dispunha de uma Estratégia Nacional para a Segurança do Ciberespaço (ENSC), aprovada em 2015 e atualizada/revista em 2020. Alinhada com esta visão estratégica, foi edificada uma estrutura nacional de cibersegurança, articulada: ao nível político-estratégico, através do Conselho Superior para a Segurança do Ciberespaço; ao nível da coordenação operacional, através do Centro Nacional de Cibersegurança; e, ao nível operacional/tático, através da rede nacional de Computer Emergency Response Teams.

Contrastando com esta situação, após quase uma década de preparação e muitos esforços desenvolvidos, a Estratégia Nacional de Ciberdefesa (ENCD) só muito recentemente foi aprovada (2022). Apesar da nova Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA, 2021) e da nova Lei Orgânica do Estado-Maior-General das Forças Armadas (LOEMGFA, 2022) terem aprovado a criação do Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE) e do Comando de Operações de Ciberdefesa (COCiber), na dependência do CCICE, a estrutura de ciberdefesa implementada assenta ainda apenas no Centro de Ciberdefesa das Forças Armadas (coordenação operacional/tática) e na rede de Computer Incident Response Capability dos vários Ramos das Forças Armadas (nível tático/técnico). Neste âmbito, salienta-se a necessidade de definição urgente de uma estratégia militar para o ciberespaço e para a dinamização da edificação da capacidade de ciberdefesa nacional. Entre outras medidas apresentadas para mitigar o impacto dos riscos desta situação (Nunes, 2020), é proposta a criação de um Conselho Superior de Defesa do Ciberespaço (CSDC), na dependência da Ministra da Defesa Nacional (MDN) e de um Comando Operacional para o Ciberespaço e domínio da informação, na dependência direta do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA) e não apenas um

Comando subsidiário deste, através do CCICE. Estes órgãos, garantindo respetivamente o enquadramento político-estratégico e operacional da ciberdefesa e do ambiente de informação, não só contribuirão decisivamente para reforçar a unidade de comando e esforço das Forças Armadas na sua utilização operacional do ciberespaço mas também para melhorar a ligação com a estrutura nacional de cibersegurança, colmatando desta forma muitas das fragilidades existentes no processo de gestão de crises nacional, reforçando a resiliência cibernética do País.

Com a adoção destas medidas, a coordenação politico-estratégica e a operacionalização da cooperação internacional no domínio da ciberdefesa (e.g. com a OTAN e UE) serão, desde logo, institucionalmente reforçadas, alinhando vertical e transversalmente as responsabilidades e competências das estruturas existentes e a levantar. Tal permitirá também ultrapassar os constrangimentos operacionais decorrentes do facto de a tutela política da Ciberdefesa (MDN) ser diferente do enquadramento político da Cibersegurança (Gabinete Nacional de Segurança/Presidência do Conselho de Ministros) e porque passará a existir um Comando Operacional, tal como nos restantes domínios das operações militares, capaz de garantir uma efetiva atuação multidomínio e a articulação internacional das Forças Armadas ao nível das operações de ciberdefesa da Aliança.

A gestão de crises no ciberespaço, obrigando a uma avaliação permanente das ameaças, vulnerabilidades e riscos, exige assim uma resposta nacional coerente e articulada. Esta, respeitando os limites de competências dos vários atores, deverá envolver toda a sociedade, explorando sinergias nacionais e a cooperação internacional. Este objetivo só será alcançável através do desenvolvimento de uma estratégia nacional de segurança e defesa do ciberespaço, transversal, equilibrada e integradora das suas áreas estruturantes.

7. Políticas de Defesa no Ciberespaço: perspetivas de evolução

À medida que os avanços tecnológicos e a interconetividade global aceleraram exponencialmente, assistimos a um crescimento sem precedentes das ameaças e dos riscos de segurança sistémicos, pondo em causa o desenvolvimento das sociedades de matriz digital. No início de 2022, foram tornados públicos sete ciberataques sucessivos a empresas e instituições nacionais, com grande impacto disruptivo em vários setores da economia do País. Esta onda de ciberataques, acentuando-se desde o início da guerra na Ucrânia, tem vindo a afetar redes e sistemas de várias instituições públicas e privadas atingindo, nomeadamente, as designadas áreas de soberania do Estado.

Face ao número crescente de ciberataques, o desenvolvimento das relações internacionais requer uma postura cooperativa da comunidade internacional, assente numa capacidade acrescida de diálogo e num alinhamento estratégico permanente, para garantir a cibersegurança e ciberdefesa do ecossistema digital. Na formulação das suas

políticas de segurança, os Estados devem estar cada vez mais atentos aos principais desafios estratégicos e competitivos associados ao fenómeno da digitalização, da adoção generalizada de aplicações de inteligência artificial e da robotização, salientando-se a aceleração destes processos nos últimos anos e o facto de a transformação digital transcender, em muito, o processo de digitalização. Neste contexto, surgem inevitavelmente novos padrões de utilização competitiva do ambiente de informação, quer ao nível das ferramentas tecnológicas quer no que se refere aos processos e ao modelo de governo das empresas e das organizações do futuro.

Antecipando as dinâmicas de mudança do ambiente de segurança internacional, no caso específico da segurança da informação e do ciberespaço, a UE (2020b; 2022) propõe que a evolução das políticas de segurança e defesa dos seus Estados-Membros (EM) decorra de forma a integrar, num todo coerente, as várias áreas políticas com um impacto direto na segurança e defesa do ciberespaço, reforçando a segurança do ecossistema digital. Procura-se assim, ao nível dos diversos EM, contribuir para a construção de uma resiliência nacional, sustentável no longo prazo.

Tendo consciência que a defesa do ciberespaço nacional depende da atuação sinérgica e "em rede" da sociedade portuguesa, em linha com a visão da UE e da OTAN, com caráter supletivo e complementar, considera-se também necessário fortalecer as sinergias nacionais e aumentar a cooperação internacional nestes domínios, de forma a facilitar o combate ao cibercrime e a reduzir as barreiras (ainda existentes) à cooperação no domínio da cibersegurança e ciberdefesa. Através da colaboração entre o sector público e privado, será possível melhorar o conhecimento transversal, fazendo face aos riscos associados a um contexto social de rápida inovação tecnológica. Adicionalmente, importa promover a adoção de soluções de cibersegurança escaláveis, capazes de acelerar a adoção das melhores práticas e aumentar a ciber resiliência nacional.

A implementação desta visão estratégica, articulada nas diversas dimensões, dependerá muito da capacidade nacional para congregar esforços e gerar uma atuação concertada por parte das várias entidades que contribuem para a cibersegurança e ciberdefesa do Estado.

8. Conclusões

Na formulação de uma visão política para o ciberespaço, surgem descontinuidades, desafios emergentes e sinais de uma alteração substantiva do ambiente de segurança internacional. Neste contexto, importa compreender a influência do ciberespaço, contextualizando o seu papel transformador das organizações e sociedades do futuro, projetando possíveis cenários de evolução competitiva e de confrontação estratégica.

À medida que a tecnologia se torna cada vez mais central na condução dos conflitos da era moderna, a fronteira entre a sua dimensão militar e civil tem vindo a diluir-se. Esta situação, oferecendo uma vantagem estratégica aos atores que detenham uma

vantagem/supremacia tecnológica poderá contribuir para estimular a ocorrência de novos conflitos no ciberespaço ou mesmo até originar a sua proliferação.

Consubstanciando-se neste domínio global sérios riscos para a salvaguarda dos interesses e para a defesa da soberania nacional, esta realidade não pode ser dissociada da necessidade de ajustamento permanente das políticas de defesa à envolvente estratégica e ao desenvolvimento de novos processos e capacidades. Uma continua observação do horizonte estratégico permitirá aos diversos atores, Estado e não-Estado, a possibilidade de agir com vantagem e gerar valor, a tempo de mitigar as vulnerabilidades e aproveitar as oportunidades.

O ecosistema digital nacional, permanentemente ligado ao ciberespaço, desempenha também um papel relevante para a cibersegurança da UE, para a ciberdefesa OTAN e até para a cibersegurança global. Esta articulação e interdependência, impõe a Portugal a necessidade de honrar os compromissos políticos assumidos no quadro das organizações internacionais a que pertence, garantindo o alinhamento estratégico necessário para assegurar a segurança cooperativa e a defesa coletiva no ciberespaço, afirmando-se como parceiro relevante, num esforço conjunto destinado a assegurar a estabilidade do ambiente de segurança internacional. Tal exige a definição de políticas consistentes e estratégias coerentes com esta realidade, assentes numa edificação de capacidades credível.

Tanto ao nível da conceptualização como da operacionalização, Portugal tem vindo a amadurecer a sua visão estratégica para o ciberespaço. No entanto, face aos atuais e futuros desafios da segurança e defesa nacional, promovendo uma visão estratégica integrada para o ciberespaço, importa restabelecer e alargar o conceito de resiliência nacional, clarificar o enquadramento político e o papel a desempenhar pela defesa na gestão de crises no ciberespaço, reforçando a estrutura e acelerando o desenvolvimento da capacidade de ciberdefesa das Forças Armadas. Estes imperativos, contrariando a adoção de uma abordagem estratégica errática, exigem uma política de defesa para o ciberespaço, estruturada e afirmativa, evitando assim que a consecução dos objetivos políticos formulados seja perspetivada sem a existência de uma estratégia coerente e sem um plano de ação consistente, articulado nos seus domínios operacional, estrutural e genético.

O ciberespaço, materializa um domínio de exercício de cidadania, afirmação de valores, defesa de interesses e soberania nacional. Atendendo aos objetivos políticos traçados, às melhores práticas e aos projetos já em curso, tanto no plano nacional como internacional, num momento em que se perspetiva a revisão do conceito estratégico de defesa nacional, definido em 2013, as políticas de segurança e defesa nacional não podem deixar de integrar esta realidade.

Referências Bibliográficas

AJP-3.10. (2009). Allied Joint Doctrine for Information Operations. Bruxelas: NATO Standardization Office.

AJP-3.20. (2020). Allied Joint Doctrine for Cyberspace Operations (Edition A), Version 1. Bruxelas: NATO Standardization Office.

CEDN (2013). Resolução do Conselho de Ministros n.º 19/2013, de 21 de março. Aprova o Conceito Estratégico de Defesa Nacional. Diário da República, 1.ª Série, 67, 1981–1995. Lisboa: Presidência do Conselho de Ministros.

CEM (2014). Conceito Estratégico Militar. Conselho Superior de Defesa Nacional. Retirado de https://www.fd.unl.pt/docentes_docs/ma/FPG_MA_27255.pdf

CNCS (2014). Decreto-Lei n.º 69/2014, de 9 de maio. Cria o Centro Nacional de Cibersegurança. Diário da República, 1.ª Série, 89, 2712-2719. Lisboa: Presidência do Conselho de Ministros.

CSSC (2017). Resolução do Conselho de Ministros n.º 115/2017, de 13 de julho de 2017. Cria o grupo de projeto denominado "Conselho Superior de Segurança do Ciberespaço". Diário da República, 1.ª Série, 163/2017, 5035-5037. Lisboa: Presidência do Conselho de Ministros.

DMPDM (2020). Diretiva Ministerial de Planeamento de Defesa Militar (Despacho n.º 2536/MDN, de 24 de fevereiro). Lisboa: Ministro da Defesa Nacional.

EMGFA (2018). Diretiva Estratégica do EMGFA 2018-2021, de 18 abril de 2018. Lisboa: Chefe do Estado-Maior-General das Forças Armadas.

EMGFA (2019). Proposta de Estratégia Nacional para a Ciberdefesa 2019-2023. Lisboa: Grupo de Trabalho-Capacidade Ciberdefesa das FFAA.

ENCD (2022). Resolução do Conselho de Ministros n.º 106/2022, de 2 de novembro. Aprova a Estratégia Nacional de Ciberdefesa. Diário da República, 1.ª Série, 211, 13–22. Lisboa: Presidência do Conselho de Ministros.

ENSC (2019). Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. Diário da República, 1ª Série, 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.

ENSC (2019). Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. Diário da República, 1ª Série, 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.

MDN (2013). Orientação para a Política de Ciberdefesa (Despacho n.º 13692/MDN, de 11 de outubro). Lisboa: Ministro da Defesa Nacional.

MDN (2018). Diretiva Ministerial de Orientação Política para o Investimento na Defesa (Despacho n.º 4103/MDN, de 12 de abril). Lisboa: Ministro da Defesa Nacional.

MDN (2019). Linhas Orientadoras para a Estratégia Nacional de Ciberdefesa-Horizonte 2019-23 (Despacho n.º 52/MDN, de 23 de outubro). Lisboa: Ministro da Defesa Nacional.

MDN (2020). Criação do Comité de Monitorização da Ciberdefesa (Despacho n.º 15/2020, de 6 de fevereiro). Lisboa: Ministro da Defesa Nacional.

NUNES, P. F.V. (2020). A Edificação da Capacidade de Ciberdefesa Nacional: Contributos para a Definição de uma Estratégia Militar para o Ciberespaço. Coleção "ARES", 36. Lisboa: Instituto Universitário Militar.

NUNES, P. F.V. (Coord.). (2018). Contributos para uma Estratégia Nacional de Ciberdefesa. IDN Cadernos, 28. Lisboa: Instituto da Defesa Nacional.

OTAN (2018). High Level Taxonomy of Cyberspace Operations (Taxonomia IMSM-0222-2018). Bruxelas: Organização do Tratado do Atlântico Norte. NATO International Military Staff.

Resolução do Conselho de Ministros n.º 26/2013, de 11 de abril. (2013). Aprova a reforma "Defesa 2020". Diário da República, 1.ª Série, 77, 2285-2289. Lisboa: Presidência do Conselho de Ministros.

UE (2020). Estratégia de Cibersegurança da União Europeia [Página online]. Retirado de https://ec.europa.eu/digital-single-market/en/cybersecurity-strategy

UE (2022). Bússola Estratégica para a Segurança e a Defesa da EU [Página online]. Retirado de https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf