Cibersegurança e Defesa Nacional: Desafios e Estratégias na Nova Fronteira da Segurança em Portugal e na UE

Carlos Imbrosio Filho[1]

Resumo: O aumento das ameaças cibernéticas e híbridas no espaço euro-atlântico, intensificadas pelo conflito Rússia-Ucrânia, tem pressionado os Estados-membros da União Europeia, incluindo Portugal, a reforçar suas capacidades de ciberdefesa e a redefinir os conceitos de soberania e segurança nacional. Este trabalho, de natureza teórico-prática, fundamenta-se em dados quantitativos oriundos de organismos internacionais como a ENISA, a NATO e o CCDCOE, e analisa os principais desafios enfrentados por Portugal no desenvolvimento de uma resposta estratégica integrada no domínio da cibersegurança. Além disso, discute o papel das parcerias público-privadas e da cooperação europeia como vetores essenciais para a construção de uma resiliência digital eficaz e sustentável. O estudo visa contribuir para o fortalecimento da arquitetura de segurança nacional em articulação com os mecanismos europeus e internacionais de ciberdefesa.

Palavras-chave: Cibersegurança, Defesa Nacional, Soberania Digital, União Europeia, ENISA, Conflito Híbrido, NATO, Resiliência Cibernética

Abstract: *The rise of cyber and hybrid threats in the Euro-Atlantic space, intensified by the Russia-Ukraine conflict, has pushed European Union Member States, including Portugal, to enhance their cyber defence capabilities and rethink traditional concepts of sovereignty and national security. This theoretical-practical study, supported by quantitative data from international bodies such as ENISA, NATO, and the CCDCOE, analyses the main challenges faced by Portugal in developing a strategic and integrated response to cybersecurity threats. Furthermore, it explores the role of public-private partnerships and European cooperation as key drivers for building effective and sustainable digital resilience. The research aims to contribute to strengthening national security architecture in alignment with European and international cyber defence mechanisms.*

Keywords: *Cybersecurity, National Defence, Digital Sovereignty, European Union, ENISA, Hybrid Conflict, NATO, Cyber Resilience*

[1] Jurista, docente, investigador e consultor, Doutor em Direito pela Universidade Autónoma de Lisboa, especializado em segurança pública e anticorrupção. Fundador e consultor jurídico na Charles The Son, atua também como cientista-investigador no centro *Ratio Legis* - UAL, no *JusGov* - Universidade do Minho, e é fundador e cientista principal no *Education Beyond Science I&D Centre*. É Membro Associado da EuroDefense Portugal, ACJS-DC e Latina/o/x Criminology nos EUA.

Nota ao Leitor

O presente artigo resulta de um esforço investigativo contínuo que teve início em 2022, no âmbito do combate ao tráfico ilícito de pessoas e órgãos na região do Leste Europeu, com especial atenção aos países da Áustria, Bulgária e Polónia. Este estudo inicial permitiu aprofundar a análise sobre a obtenção e validação das provas criminais recolhidas por meio de comunicações encriptadas ponto a ponto, tecnologia que tem vindo a assumir um papel central nas estratégias de organizações criminosas transnacionais.

Posteriormente, a investigação expandiu-se para o exame do uso efetivo dessas provas no desmantelamento de redes criminosas complexas, considerando contextos diversos, nomeadamente nos Estados Unidos, na União Europeia e no Brasil, com enfoque no cenário latino-americano. Tal abordagem contribuiu para compreender as dinâmicas transnacionais da criminalidade organizada e os desafios inerentes à cooperação judicial internacional.

No contexto nacional, este estudo adquire particular relevância para as políticas de defesa e segurança de Portugal, dado o papel estratégico das forças de segurança e dos operadores jurídicos criminais na proteção do Estado e da sociedade contra ameaças híbridas e ciberataques. Assim, a investigação culmina na análise da aplicação da inteligência artificial como ferramenta de capacitação para oficiais de polícia e agentes jurídicos, visando aprimorar a eficácia operacional no combate à criminalidade organizada, bem como fortalecer a resiliência do sistema de segurança nacional frente a ameaças emergentes no ciberespaço.

Este trabalho pretende, assim, contribuir para o desenvolvimento de políticas públicas fundamentadas em evidências científicas, que promovam uma resposta integrada e inovadora no domínio da segurança e da defesa nacional.

Sumário

1. Introdução

O acelerado crescimento das ameaças cibernéticas e híbridas no espaço euro-atlântico, especialmente desde o início do conflito Rússia-Ucrânia, revelou a vulnerabilidade das infraestruturas críticas, sistemas de defesa e mecanismos de segurança nacional nos Estados-membros da União Europeia. No caso português, este cenário tem reforçado a urgência de reavaliar a sua política de defesa à luz de uma nova realidade digital, em que a cibersegurança deixa de ser apenas um tema tecnológico para se consolidar como uma dimensão estratégica essencial da soberania nacional na manutenção das liberdades e garantias democráticas.

A transição de conflitos convencionais para formas de guerra híbrida, que combinam ataques cibernéticos, desinformação, sabotagem digital e pressão geopolítica, exige das forças armadas e de segurança nacionais uma adaptação profunda das suas capacidades operacionais, da sua doutrina e dos seus modelos de cooperação internacional. Organismos como a ENISA (Agência da União Europeia para a Cibersegurança), a NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE) e a própria EUROPOL têm alertado para a tendência crescente da exploração de vulnerabilidades digitais por atores estatais e não estatais. Só em 2023, a ENISA (2023) registou um aumento de 84% nos ataques cibernéticos contra instituições públicas e infraestruturas críticas em solo europeu, reforçando o caráter sistémico, complexo e endémico dessas ameaças.

Nesse contexto, este artigo propõe uma investigação de natureza teórico-prática, apoiada em dados quantitativos e qualitativos, que analisa os principais desafios enfrentados por Portugal na construção de uma resposta integrada às ameaças cibernéticas e híbridas. O estudo enfatiza o papel das parcerias público-privadas, da coordenação interinstitucional, e da integração com as estruturas de ciberdefesa da União Europeia e da NATO, com o objetivo de identificar caminhos estratégicos para o reforço da resiliência digital e da soberania cibernética portuguesa.

A metodologia adotada é qualitativa e exploratória, com análise documental de políticas públicas, legislação, relatórios técnicos e estratégicos produzidos por entidades internacionais como a ENISA, NATO, EUROPOL, Eurostat e OCDE. A análise será complementada com dados estatísticos e estudos de caso representativos do impacto da guerra da informação e das campanhas de desinformação no ambiente de segurança europeu. Complementarmente, será conduzida uma leitura crítica e interpretativa de doutrina especializada, com base em obras, relatórios e excertos de especialistas da área — incluindo membros das forças armadas,

investigadores académicos e representantes do setor privado —, com o intuito de aprofundar a compreensão prática da aplicação dos instrumentos de defesa cibernética no contexto nacional e europeu.

1.1. Justificação da Investigação

A emergência de ameaças cibernéticas e híbridas como instrumentos de desestabilização no contexto europeu, intensificada pelo conflito Rússia-Ucrânia, tornou evidente a vulnerabilidade das infraestruturas críticas nacionais e a urgência de atualização dos mecanismos tradicionais de defesa. No caso português, essa realidade impõe um redimensionamento da sua estratégia de segurança, integrando a ciberdefesa como um domínio operacional essencial à soberania nacional, no seio de uma arquitetura de defesa europeia e atlântica cada vez mais interdependente.

A cibersegurança não se limita a uma resposta técnica às vulnerabilidades digitais; ela constitui uma frente estratégica que envolve capacidades militares, estruturas civis, entidades reguladoras e o setor privado. Portugal, na condição de Estado-membro da União Europeia e aliado ativo na NATO, desempenha um papel fundamental na consolidação de uma resposta integrada a essas ameaças, sobretudo no que se refere à resiliência digital, à interoperabilidade e à cooperação multilateral.

Diante deste cenário, justifica-se uma investigação que vá além da mera descrição de políticas públicas e busque compreender, de forma analítica e crítica, como Portugal tem respondido às ameaças cibernéticas e como se posiciona no esforço coletivo europeu de proteção e defesa digital. O presente estudo procura preencher essa lacuna, oferecendo uma análise multidisciplinar que poderá informar a formulação de políticas mais eficazes e adaptadas às exigências da nova fronteira tecnológica da defesa.

Para isso, a análise será orientada por um conjunto de questões centrais que visam captar os elementos estruturantes da ciberdefesa nacional em articulação com os compromissos europeus e atlânticos. Procura-se compreender, antes de mais, *quais são os principais riscos e ameaças cibernéticas atualmente enfrentados por Portugal, à luz das transformações no panorama geopolítico europeu.* Seguidamente, investiga-se *de que forma o país tem integrado a sua política de ciberdefesa nos quadros institucionais e estratégicos da União Europeia e da NATO*, avaliando o grau de alinhamento e cooperação operacional.

A análise incidirá também sobre a *eficácia da articulação entre o setor público e o setor privado no combate às ameaças híbridas e cibernéticas*, elemento essencial para o

desenvolvimento de uma resiliência digital robusta. Em paralelo, pretende-se avaliar *em que medida as recomendações técnicas e estratégicas da ENISA e de outros organismos de defesa europeus têm sido incorporadas no contexto nacional*, influenciando a arquitetura normativa e as práticas institucionais. Por fim, o estudo interroga-se sobre *os principais desafios que Portugal deverá enfrentar nos próximos cinco a dez anos para garantir a sua soberania digital*, numa era em que o domínio cibernético se afirma como dimensão estruturante da segurança nacional.

1.2 Relevância Estratégica para Portugal e para a União Europeia

A relevância da cibersegurança como dimensão estruturante da defesa nacional tornou-se inquestionável no panorama europeu contemporâneo. Desde 2022, com a intensificação do conflito Rússia-Ucrânia, a União Europeia passou a considerar os ciberataques como potenciais gatilhos para aplicação das cláusulas de defesa coletiva previstas no artigo 42.º, n.º 7 do Tratado da União Europeia (TUE), e no artigo 5.º da Carta da NATO (European Commission, 2023; NATO, 2023). Neste novo cenário, Portugal encontra-se numa posição geoestratégica sensível, com responsabilidades no Atlântico Norte e como ponto de ligação entre a Europa, a África Ocidental e o espaço lusófono.

O Relatório *ENISA Threat Landscape 2023* identificou que mais de 65% dos ciberataques registados na UE tiveram como alvo instituições públicas, infraestruturas críticas e sistemas governamentais (ENISA, 2023). Em Portugal, o Centro Nacional de Cibersegurança (CNCS) registou um aumento de 38% nas ocorrências de incidentes cibernéticos entre 2022 e 2023, com destaque para ataques de ransomware, phishing direcionado e tentativas de intrusão em sistemas do setor da saúde, energia e defesa (CNCS, 2024).

Do ponto de vista europeu, a *resiliência cibernética coletiva* tornou-se uma prioridade da Comissão Europeia, que alocou mais de €1,6 mil milhões para o financiamento de programas de cibersegurança no período 2021–2027, através do *Mecanismo Interligar a Europa* e do programa *Europa Digital* (European Commission, 2022). Portugal, como beneficiário desses mecanismos, integra atualmente diversas redes de cooperação e centros de resposta, como o *EU CyberNet*, o Centro de Cibersegurança da União Europeia (ECCC) e participa regularmente de exercícios como o *Cyber Europe* e o *Locked Shields* (CCDCOE, 2023).

Além disso, a Estratégia Nacional de Defesa para o Ciberespaço (2023–2027) reforça o compromisso do país com uma abordagem multidimensional da ciberdefesa, reconhecendo

o ciberespaço como *"um domínio operacional prioritário da Defesa Nacional"* e propondo ações estruturadas em torno da prevenção, deteção, resposta e recuperação de incidentes (Ministério da Defesa Nacional, 2023).

Neste quadro, a relevância estratégica de Portugal manifesta-se tanto pela necessidade de proteger o seu ecossistema digital e infraestruturas críticas, como pelo seu papel ativo na construção de uma política europeia de defesa cibernética robusta, interoperável e alinhada com os princípios do Estado de Direito e da soberania tecnológica. Como sublinha Nye (2010), no novo equilíbrio global de poder, os Estados que controlarem melhor os seus recursos digitais e souberem responder eficazmente a ameaças híbridas terão vantagem decisiva não só militar, mas também económica e institucional.

Assim, compreender como Portugal está a adaptar as suas estruturas de segurança e defesa ao contexto europeu de ciberameaças não é apenas uma necessidade acadêmica, mas uma contribuição direta para o fortalecimento da arquitetura estratégica europeia.

2. Quadro Teórico

A crescente interdependência entre os sistemas digitais e os domínios tradicionais da segurança pública e da defesa nacional exige um novo olhar teórico sobre os conceitos de soberania, ameaça e resposta estratégica. A cibersegurança deixou de ser uma dimensão exclusivamente técnica e passou a integrar os fundamentos da segurança estatal, exigindo a mobilização coordenada de forças armadas, estruturas civis e parcerias internacionais (Nye, 2010; Rid, 2013). Neste capítulo, serão exploradas as noções fundamentais que sustentam a análise das políticas de ciberdefesa no contexto português e europeu, com base em literatura especializada e orientações de organismos internacionais.

2.1 Cibersegurança e Ciberdefesa: Conceitos e Abordagens

O conceito de *cibersegurança* refere-se à proteção dos sistemas de informação, redes e infraestruturas digitais contra acessos não autorizados, ataques, danos ou interrupções (ENISA, 2023). Já a *ciberdefesa* diz respeito à resposta estatal — especialmente no domínio da defesa nacional — a ameaças de origem cibernética, envolvendo a atuação direta das forças armadas, estruturas de comando e controlo e alianças militares, como a NATO (NATO, 2024).

Enquanto a cibersegurança tem uma aplicação transversal, englobando tanto o setor público quanto o privado, a ciberdefesa situa-se num plano estratégico-militar, vinculado à

preservação da soberania e à capacidade de dissuasão e resposta ofensiva e defensiva do Estado (Schmitt, 2013). Para Arquilla e Ronfeldt (1997), a guerra informacional e os conflitos no ciberespaço representam uma nova fase das operações militares, exigindo doutrinas adaptadas à realidade digital.

De acordo com Nye (2010), o poder cibernético está relacionado não apenas à capacidade de ataque e defesa, mas também ao controle da informação e à resiliência dos sistemas estatais e sociais. Isso implica a criação de estruturas normativas e institucionais capazes de sustentar uma postura de segurança coletiva e interoperabilidade internacional.

2.2 Soberania Digital e Segurança Nacional

A noção de *soberania digital* surge como resposta à crescente dependência tecnológica das infraestruturas críticas e à exposição de Estados e cidadãos a ataques externos, sabotagem e vigilância ilícita. Segundo Deibert (2019), a soberania digital implica a capacidade de um Estado de controlar seus próprios recursos informacionais, garantir a integridade dos seus sistemas e proteger os dados sensíveis de sua população.

No domínio da *segurança nacional*, a digitalização trouxe novos desafios à atuação das forças armadas e das estruturas de segurança pública, incluindo a necessidade de novos protocolos de vigilância, inteligência e neutralização de ameaças digitais (Liff, 2012). Como aponta Betz (2011), o ciberespaço tornou-se um novo teatro estratégico, onde os conflitos assumem formas assimétricas e persistentes, muitas vezes sem declaração formal de guerra ou envolvimento direto de forças convencionais.

Em Portugal, a Estratégia Nacional de Segurança do Ciberespaço (Governo de Portugal, 2019) e a Estratégia Nacional de Defesa para o Ciberespaço (2023-2027) consolidam esse entendimento, reconhecendo o ciberespaço como um *domínio operacional autónomo* e uma prioridade na agenda de segurança e defesa.

2.3 Ameaças Híbridas e Guerra Cognitiva

O conceito de *ameaças híbridas* refere-se à combinação de métodos convencionais e não convencionais — como ataques cibernéticos, desinformação, sabotagem digital, manipulação de redes sociais e pressão económica — utilizados para desestabilizar Estados sem recorrer à força militar direta (Mumford, 2013; EUROPOL, 2023). A *guerra cognitiva*, uma evolução dessa lógica, explora as vulnerabilidades humanas e sociais através da manipulação da informação e do comportamento (NATO Innovation Hub, 2021).

Essas formas de conflito afetam diretamente a legitimidade das instituições democráticas e a coesão social, exigindo respostas intersetoriais e interinstitucionais coordenadas, em que as forças armadas, a sociedade civil e o setor privado atuem de forma complementar. Como apontam Thomas e Raska (2016), o combate às ameaças híbridas exige uma arquitetura de segurança que vá além da defesa física do território e integre a defesa dos sistemas de informação, da reputação institucional e da estabilidade social.

2.4 Cooperação Internacional e Estruturas Europeias

No contexto europeu, diversas entidades desempenham um papel fundamental na construção de uma resposta coletiva às ameaças digitais. A Agência da União Europeia para a Cibersegurança (ENISA) atua como órgão técnico de referência, responsável por produzir relatórios estratégicos, definir boas práticas e coordenar respostas entre os Estados-membros (ENISA, 2023). Por sua vez, o NATO CCDCOE funciona como centro de excelência em ciberdefesa cooperativa, promovendo exercícios, formações e pesquisa aplicada.

A EUROPOL, por meio do *Internet Organised Crime Threat Assessment* (IOCTA), tem documentado o aumento das atividades criminosas no ambiente digital, destacando a importância de estratégias conjuntas entre segurança interna e defesa externa (EUROPOL, 2023). A articulação entre essas estruturas reforça a necessidade de interoperabilidade jurídica, técnica e operacional entre os Estados europeus.

Como observa Choucri (2012), a segurança no ciberespaço só poderá ser alcançada por meio da governança multilateral, que una esforços estatais, privados e científicos em torno de objetivos comuns. Nesse sentido, Portugal tem procurado desempenhar um papel ativo, integrando iniciativas como o *EU CyberNet*, participando de ciberexercícios conjuntos (*Cyber Europe, Locked Shields*) e adaptando sua legislação às normativas europeias.

3. Contextualização Geopolítica

3.1 Impactos do Conflito Rússia-Ucrânia na Segurança Cibernética Europeia

O conflito em curso entre a Rússia e a Ucrânia, iniciado em fevereiro de 2022 com a invasão russa, marcou uma viragem paradigmática na compreensão das ameaças à segurança europeia. Pela primeira vez, um conflito militar tradicional foi amplamente precedido e

acompanhado por ações cibernéticas ofensivas em larga escala, demonstrando a integração estratégica do ciberespaço nas campanhas de guerra híbrida contemporânea (EU Cyber Direct, 2023).

Segundo a ENISA (2023), os primeiros 12 meses do conflito observaram um aumento sem precedentes de ataques cibernéticos com motivação geopolítica em solo europeu. A agência registou um crescimento de mais de 200% nas campanhas de desinformação e ataques DDoS (*Distributed Denial of Service*) direcionados a instituições públicas, empresas de telecomunicações, operadores de energia e infraestruturas críticas em Estados-membros da UE. Esses ataques foram atribuídos a grupos alinhados com os interesses estratégicos russos, como o KillNet e o Sandworm (ENISA, 2023).

Relatórios do NATO CCDCOE indicam que a Rússia utilizou o ciberespaço como instrumento tático para desestabilizar a opinião pública, comprometer sistemas logísticos militares ucranianos e criar disrupções em cadeias de abastecimento europeias. Um dos exemplos mais notórios foi o ataque à rede de satélites KA-SAT (operada pela Viasat), que afetou não apenas as comunicações militares ucranianas, mas também serviços civis em vários países da Europa Central e Oriental (CCDCOE, 2022).

Em termos doutrinários, essa realidade confirma o que autores como Thomas Rid (2013) e Betz (2011) já anunciavam: o ciberconflito moderno não substitui a guerra tradicional, mas atua como seu prolongamento e amplificador, permitindo atingir alvos estratégicos e psicológicos com menor custo e maior alcance. O ciberespaço torna-se, assim, um campo operacional integrado, simultaneamente tático e simbólico, em que o objetivo não é apenas destruir, mas desorganizar, confundir e desmobilizar.

Para além da desinformação e dos ataques técnicos, a *guerra cognitiva* — que visa influenciar perceções, comportamentos e decisões políticas — ganhou destaque no contexto do conflito. A NATO Innovation Hub (2021) destacou que a Rússia tem investido de forma sistemática em campanhas de manipulação da informação, com recurso a redes sociais, bots e inteligência artificial para gerar narrativas falsas e dividir a opinião pública nos países ocidentais.

A União Europeia respondeu com medidas coordenadas, como a ativação da *EU Rapid Alert System* para combate à desinformação, o reforço das capacidades do Centro Europeu de Cibercriminalidade da EUROPOL (EC3) e o financiamento de exercícios conjuntos de ciberdefesa por meio do programa Europa Digital (European Commission, 2023). Em termos

legislativos, destaca-se a revisão da Diretiva NIS (Diretiva (UE) 2022/2555), que amplia os requisitos de segurança para operadores de serviços essenciais e entidades digitais.

Em Portugal, embora o país não tenha sido alvo direto de ataques com impacto estrutural, o Centro Nacional de Cibersegurança (CNCS) registou um aumento expressivo na sofisticação e frequência de tentativas de intrusão em sistemas públicos e privados, alinhando-se à tendência europeia (CNCS, 2024). O envolvimento português em exercícios como o Locked Shields 2023, promovido pelo NATO CCDCOE, demonstra o reconhecimento crescente da ciberdefesa como um eixo prioritário da política de segurança nacional.

Deste modo, os impactos do conflito Rússia-Ucrânia na segurança cibernética europeia vão muito além do contexto militar: redesenham as prioridades da segurança coletiva, forçam a integração operacional entre setores civis e militares, e acentuam a necessidade de soberania digital e resiliência conjunta no espaço europeu.

3.2 O Novo Papel da NATO e da UE na Ciberdefesa

A intensificação dos ataques cibernéticos de natureza estratégica no contexto da guerra Rússia-Ucrânia consolidou uma transformação já em curso: a incorporação formal do ciberespaço como um domínio operacional autónomo tanto pela NATO quanto pela União Europeia (UE). Essa transição assinala uma mudança doutrinária profunda, que reposiciona o ciberespaço no centro da Reforma do Setor de Segurança (RSS) e redefine os mecanismos de cooperação entre Estados, forças armadas, estruturas policiais e entidades judiciais.

No âmbito da NATO, desde 2016 o ciberespaço é reconhecido como o "quarto domínio" da guerra, ao lado da terra, do mar e do ar (NATO, 2016). Contudo, foi a partir de 2022 que a Aliança passou a integrar capacidades cibernéticas ofensivas nos seus planos operacionais de defesa coletiva, incluindo no novo Concepto Estratégico de Madrid (2022). Este documento sublinha a necessidade de resposta coordenada a ciberataques significativos, inclusive com recurso a meios convencionais, nos termos do artigo 5.º do Tratado do Atlântico Norte (NATO, 2022).

Paralelamente, a União Europeia tem reforçado o seu papel enquanto ator normativo e estratégico na área da ciberdefesa, particularmente através da Política Comum de Segurança e Defesa (PCSD) e do desenvolvimento do Quadro de Política de Ciberdefesa da UE.[2] O

[2] O Ato Único Europeu (1986) representou um marco na consolidação do projeto de integração europeia ao estabelecer, entre outros objetivos, a criação progressiva de um espaço sem fronteiras internas, alicerçado nos princípios da liberdade, segurança e justiça. Este compromisso, posteriormente reforçado pela criação

documento de 2022 propõe a criação de capacidades operacionais conjuntas, a partilha de inteligência estratégica e o reforço das relações civis-militares, enfatizando a importância da interoperabilidade entre os sistemas de defesa digital dos Estados-membros (European Commission, 2022).

Essa transformação institucional no plano europeu deve ser lida à luz das orientações do Conselho de Segurança das Nações Unidas sobre Reforma do Setor de Segurança (RSS), que define a segurança como um bem público e preconiza a necessidade de instituições eficazes, transparentes, profissionais e sujeitas ao primado do direito (UNSG, 2008). Neste sentido, tanto a NATO quanto a UE têm incorporado elementos da RSS em suas agendas cibernéticas, com foco em governança, *accountability*, capacitação técnica e controle democrático das forças de segurança digitalizadas.

A cooperação policial e judicial internacional, por sua vez, tornou-se um pilar indispensável no enfrentamento das ameaças cibernéticas transfronteiriças. Organismos como a EUROPOL, por meio do seu Centro Europeu de Cibercriminalidade (EC3), atuam em estreita colaboração com agências de segurança dos Estados-membros, promovendo operações conjuntas, partilha de dados em tempo real, harmonização de normas processuais e capacitação técnica para investigação digital (EUROPOL, 2023). O mecanismo Eurojust desempenha igualmente um papel crucial ao facilitar a cooperação entre Ministérios Públicos em casos de crimes cibernéticos complexos e com implicações transnacionais.

Além disso, a NATO CCDCOE tem-se consolidado como um hub de excelência em doutrina, formação e simulação de conflitos cibernéticos, incluindo exercícios internacionais como o Locked Shields, que simulam situações de cibercrise em tempo real com envolvimento de forças militares, civis e entidades privadas (CCDCOE, 2023). A presença portuguesa nestas estruturas e exercícios reforça o compromisso do país com a construção de uma cultura de ciberdefesa cooperativa e interoperável, alinhada aos princípios da segurança coletiva e ao imperativo da soberania digital.

---

do espaço Schengen, resultou na supressão sistemática dos controlos de fronteira interna entre os Estados-Membros. Contudo, num cenário contemporâneo fortemente marcado pela digitalização de ameaças, pela proliferação de riscos transnacionais e pelo uso estratégico das redes como instrumentos de guerra híbrida, coloca-se a necessidade de revisão e atualização deste modelo à luz da segurança coletiva europeia. Nesse sentido, a Política Comum de Segurança e Defesa (PCSD) tem vindo a assumir um papel fundamental no reconhecimento do ciberespaço como domínio operacional, propondo mecanismos de intervenção coordenada entre as dimensões civil, militar e digital da segurança europeia (European Commission, 2022).

Nesse novo ecossistema de defesa, os desafios da guerra híbrida e da ciberameaça exigem mais do que resposta militar: demandam a integração plena entre defesa, segurança interna e justiça penal, num esforço comum que só será eficaz se ancorado em mecanismos institucionais robustos, profissionalizados e orientados por normas comuns de proteção de direitos e garantias fundamentais. O caminho passa, portanto, pela europeização da resposta cibernética, dentro de um quadro jurídico e operacional partilhado, que respeite as especificidades nacionais mas garanta uma resposta supranacional eficaz e tempestiva.

4. Cenário Português

4.1 Políticas Nacionais de Cibersegurança e Defesa

Em resposta ao crescimento exponencial das ameaças digitais e à crescente interdependência tecnológica dos setores público e privado, Portugal tem vindo a consolidar, desde a última década, um arcabouço normativo e institucional robusto no domínio da cibersegurança e da ciberdefesa. Essa evolução está alinhada tanto com os compromissos internacionais assumidos no seio da União Europeia e da NATO, como com a necessidade interna de proteção das infraestruturas críticas e da salvaguarda da soberania digital.

A Estratégia Nacional de Segurança do Ciberespaço (2019–2023), aprovada pelo Conselho de Ministros, estabeleceu como prioridades a resiliência das infraestruturas críticas, a ciber-higiene institucional, a capacitação técnica nacional e a cooperação internacional multissetorial (CNCS, 2019). Em linha com esta orientação, foi criada a Estrutura de Missão para a Cibersegurança, coordenada pelo Centro Nacional de Cibersegurança (CNCS), entidade responsável pela articulação entre entidades civis, militares e privadas no tratamento de incidentes e na gestão do risco cibernético.

Complementarmente, o Ministério da Defesa Nacional publicou, em 2023, a nova Estratégia Nacional de Defesa para o Ciberespaço (2023–2027), que reconhece o ciberespaço como "domínio operacional prioritário" e define a capacidade de resposta militar a ameaças cibernéticas como um vetor essencial para a defesa nacional (Ministério da Defesa Nacional, 2023).[3] Essa estratégia inclui medidas específicas para reforçar o Comando de

[3] A consolidação do ciberespaço como domínio estratégico da defesa nacional tem suscitado intenso debate académico e institucional, refletido em diversas publicações e iniciativas científicas no contexto europeu. Em Portugal, destaca-se o esforço reiterado da EuroDefense-Portugal na promoção deste debate, por meio de conferências temáticas, estudos estratégicos e grupos de reflexão interinstitucional, que visam integrar os desafios da ciberdefesa na formulação de políticas públicas e doutrinas operacionais nacionais. Estas

Comunicações e Sistemas de Informação das Forças Armadas (CCSIFA) e a formação de equipas militares especializadas em ciberdefesa ativa, além de prever exercícios conjuntos com parceiros da NATO.

Em termos quantitativos, o CNCS reportou um total de 2.432 incidentes de cibersegurança em 2023, um aumento de 38% em relação ao ano anterior, com predominância de ataques de *ransomware*, *phishing* direcionado e tentativas de intrusão em sistemas de entidades públicas, universidades e prestadores de serviços essenciais (CNCS, 2024). Estes dados estão em consonância com o ENISA Threat Landscape Report (2023), que classifica Portugal entre os países da UE com nível médio-alto de exposição a ameaças digitais.

De forma preocupante, a EUROPOL (2023) alerta que as redes de crime organizado transnacional têm adaptado as suas operações à lógica digital, explorando a fragmentação das políticas nacionais e a lentidão na partilha de dados entre autoridades de diferentes Estados-membros. A INTERPOL, por sua vez, tem identificado padrões de criminalidade cibernética que cruzam fronteiras físicas e jurídicas, colocando em evidência a urgência de protocolos padronizados de resposta e investigação, como aqueles promovidos pelo Protocolo de Budapeste e pelas redes de cooperação do Eurojust (INTERPOL, 2023).

Nesse contexto, as políticas nacionais portuguesas revelam avanços significativos na integração entre cibersegurança civil e ciberdefesa militar, embora desafios estruturais persistam. Como observa Pereira (2022), ainda é necessário melhorar a interoperabilidade entre organismos do Estado, a capacidade de resposta técnica em tempo real e o investimento contínuo na qualificação de recursos humanos especializados.[4] Além disso, a cooperação público-privada carece de regulamentação mais clara e incentivos para partilha de informação sensível em tempo útil (Silva & Rocha, 2021).

---

iniciativas, como se observa na conferência "*A Guerra no Ciberespaço: Desafios à Defesa e à Segurança*" (EuroDefense-Portugal, 2022), reforçam o papel da sociedade civil, da academia e das forças armadas na construção de uma cultura nacional de segurança digital partilhada.

[4] Um dos instrumentos mais relevantes no fortalecimento da interoperabilidade e da resposta transfronteiriça a ameaças complexas, como os crimes cibernéticos, são as Equipas de Investigação Conjuntas (EIC), também conhecidas como *Joint Investigation Teams* (JITs). Criadas sob os auspícios do Eurojust, em cooperação com a EUROPOL e, quando aplicável, com o apoio da INTERPOL, essas equipas permitem que autoridades judiciais e policiais de diferentes Estados-Membros conduzam investigações criminais de forma coordenada e partilhem provas em tempo real. No domínio da cibercriminalidade, as JITs têm sido fundamentais para desmantelar redes de *ransomware*, infraestruturas de *botnets* e operações de fraude digital de grande escala, como evidenciado no desmantelamento do grupo Emotet em 2021 (Eurojust & Europol, 2021). A consolidação deste modelo colaborativo é estratégica para Estados como Portugal, cuja integração nos mecanismos europeus de investigação representa um multiplicador de capacidade operativa e uma ferramenta para acelerar a resposta nacional a incidentes cibernéticos com origem externa.

Portugal tem participado ativamente de exercícios como o Locked Shields e o Cyber Europe, mas enfrenta limitações no que respeita à capacidade ofensiva digital e à resiliência das pequenas e médias empresas (PME), frequentemente alvos fáceis de ciberataques e pontos de entrada para cadeias de ataque mais amplas. Como alerta a ENISA (2023), 75% dos ataques bem-sucedidos em 2022 exploraram falhas em fornecedores de menor porte dentro das cadeias de fornecimento digital.

Assim, embora o enquadramento normativo português esteja em conformidade com os referenciais europeus, a eficácia prática das políticas públicas de cibersegurança e defesa depende da sua operacionalização em rede, da cooperação internacional efetiva, e da consolidação de uma cultura de segurança transversal à administração pública e ao setor privado.

4.2 – Papel da Defesa Nacional e das Forças Armadas

O papel da Defesa Nacional e das Forças Armadas insere-se num quadro jurídico e estratégico mais amplo, que conjuga a salvaguarda da soberania estatal com a promoção da paz, da estabilidade interna e da cooperação internacional. A conceção moderna de segurança, sobretudo a partir do pós-Guerra Fria, deslocou o eixo da defesa de uma lógica exclusivamente militar para uma abordagem mais abrangente, integradora e multidimensional (Matlary, 2009; Williams, 2008).[5] Nesse contexto, as Forças Armadas passam a desempenhar funções que ultrapassam o paradigma clássico da defesa territorial contra ameaças externas.

Do ponto de vista constitucional, a Defesa Nacional representa uma função essencial do Estado, estruturada com base nos princípios da legalidade, da subordinação do poder militar ao poder civil e da prossecução do interesse público (Cottey, Edmunds & Forster, 2002). As Forças Armadas, como braço operativo dessa política, estão vinculadas a objetivos definidos democraticamente e operam sob rígido escrutínio institucional, de forma a garantir o respeito pelos direitos fundamentais e pelos compromissos internacionais assumidos pelo Estado (Born, Leigh & Wills, 2016).[6]

---

[5] Conforme sublinha Bacelar Gouveia, a segurança internacional contemporânea deixou de estar exclusivamente subordinada à lógica militarista da soberania armada para passar a integrar dimensões políticas, sociais, ambientais e jurídicas, sendo objeto de uma abordagem holística e interdependente entre atores estatais e não estatais. Tal visão está em consonância com a evolução do Direito Internacional da Paz e da Segurança e com os princípios constitucionais que regem a inserção externa do Estado democrático de direito (Bacelar Gouveia, *Direito Constitucional Internacional e da União Europeia*, 2022, p. 387).

[6] A doutrina constitucionalista portuguesa reconhece que a Defesa Nacional, enquanto função essencial do Estado, deve ser orientada pelos princípios do Estado de Direito democrático, estando as Forças Armadas sujeitas ao poder civil e aos objetivos constitucionais de preservação da paz, da independência nacional e

A crescente interdependência entre segurança interna e externa exige, hoje, uma articulação eficaz entre os setores da Defesa, da Segurança Interna e da Política Externa. Essa articulação materializa-se em cenários diversos, como missões de paz sob égide da ONU ou da UE, operações de resposta a catástrofes, apoio logístico em situações de emergência nacional, e, em casos determinados, o combate ao crime organizado transnacional, nomeadamente em zonas de fronteira (Kaldor, 2012). Neste ponto, destaca-se a relevância da doutrina da segurança cooperativa e da resiliência estratégica, como conceitos operacionais fundamentais para a atuação contemporânea das Forças Armadas (NATO, 2010; Bueger & Edmunds, 2017).

Importa ainda referir que, no quadro das reformas do setor de segurança (*Security Sector Reform – SSR*), a redefinição do papel das Forças Armadas deve estar alinhada com os princípios do Estado de Direito, da boa governação e da transparência. O emprego militar deve ser sempre subsidiário, proporcional e legalmente enquadrado, sendo inadmissível a sua instrumentalização para fins de repressão política ou controlo social (OECD, 2007; DCAF, 2020). A doutrina internacional sobre SSR reforça a ideia de que a transformação das instituições militares deve privilegiar a profissionalização, o controlo civil democrático, a integração dos direitos humanos na formação e na doutrina militar, bem como a cooperação com atores não estatais legítimos (Sedra, 2010; Bryden & Hänggi, 2005).

Finalmente, o papel das Forças Armadas na defesa dos interesses estratégicos do Estado, incluindo os domínios marítimo, aéreo e cibernético, impõe um *aggiornamento* constante das suas capacidades operacionais. A emergência das ameaças híbridas, como a guerra informacional, os ciberataques e as campanhas de desinformação, exige uma reconfiguração das estruturas clássicas de defesa, incorporando capacidades tecnológicas e competências interdisciplinares (Hoffman, 2009; Rid, 2012). Esse esforço deve ser orientado por uma política nacional de defesa robusta, sustentada em diagnósticos realistas, planeamento de longo prazo e investimentos consistentes em inovação e capacitação (Council of the EU, 2020).

---

da integridade do território. Jorge Miranda destaca que a Constituição da República Portuguesa impõe limites claros ao exercício da força militar, proibindo a sua instrumentalização política e assegurando o seu enquadramento sob a direção superior do Presidente da República, do Governo e da Assembleia da República (Miranda, *Manual de Direito Constitucional*, 2020, pp. 344–346). De igual modo, Bacelar Gouveia sublinha que o exercício da função militar se encontra subordinado ao princípio democrático, devendo ser compatível com os direitos fundamentais e os compromissos internacionais do Estado português (Gouveia, *Direito Constitucional*, 2022, pp. 517–519).

Assim, o papel da Defesa Nacional e das Forças Armadas revela-se como uma dimensão crítica do sistema democrático contemporâneo, cuja legitimidade depende do equilíbrio entre eficácia operacional e conformidade jurídica, entre poder e responsabilidade, entre soberania e solidariedade internacional.

5. Integração Europeia e Cooperação Internacional

A crescente interdependência dos Estados europeus em matéria de segurança exige respostas que superem os limites da soberania clássica e incorporem lógicas de partilha de informação, interoperabilidade tecnológica e confiança institucional mútua. Nesse sentido, a integração europeia no domínio da segurança e defesa, especialmente no ciberespaço e na prevenção do crime organizado transnacional, tem dado origem a mecanismos de cooperação institucional altamente especializados, entre os quais se destacam a ENISA, o CCDCOE, a EUROPOL e as estruturas conjuntas de resposta a incidentes de segurança. Estes organismos representam um esforço conjunto de coordenação estratégica e operacional entre os Estados-Membros da União Europeia (UE) e, em alguns casos, da NATO, no sentido de proteger infraestruturas críticas, reforçar a ciber-resiliência e responder a ameaças híbridas em tempo real.

5.1 ENISA, CCDCOE, EUROPOL e mecanismos de resposta conjunta

A ENISA – European Union Agency for Cybersecurity atua como ponto focal da UE para a promoção da cibersegurança entre os Estados-Membros, com funções que incluem a formação técnica, a elaboração de orientações normativas, e a coordenação de exercícios conjuntos de resposta a incidentes (ENISA, 2022). A agência opera também como facilitadora de redes entre CSIRTs (Computer Security Incident Response Teams), promovendo a interoperabilidade entre equipas nacionais e garantindo que boas práticas sejam disseminadas por toda a União.

Por outro lado, o CCDCOE – Cooperative Cyber Defence Centre of Excellence, estabelecido em Tallinn sob a égide da NATO, representa um centro internacional de excelência em doutrina, treino e investigação em ciberdefesa, com membros de ambos os lados do Atlântico. Ainda que não seja uma instituição da UE, o CCDCOE coopera estreitamente com agências e Estados europeus, participando em exercícios como o Locked Shields e contribuindo para o desenvolvimento de normas operacionais e quadros jurídicos para a atuação em conflitos cibernéticos (CCDCOE, 2021).

No plano do policiamento europeu, a EUROPOL desempenha um papel central na cooperação transnacional de combate ao crime organizado, terrorismo e cibercrime. Através do seu European Cybercrime Centre (EC3), sediado em Haia, a Europol atua como plataforma de partilha de informação estratégica, coordenação de operações transfronteiriças, e apoio técnico aos Estados-Membros em investigações complexas. A Europol também promove grupos de trabalho permanentes e centros de especialização conjunta, como o Joint Cybercrime Action Taskforce (J-CAT), permitindo uma resposta ágil e concertada a ameaças digitais (Europol, 2023).

Estes mecanismos são reforçados pelo EU CSIRTs Network e pelo Cyber Crisis Liaison Organisation Network (CyCLONe), estruturas europeias que integram autoridades nacionais e organismos técnicos para assegurar respostas coordenadas a crises de cibersegurança de larga escala, nomeadamente nos termos do Regulamento (UE) 2022/2554 – Cybersecurity Act.

Assim, verifica-se a existência de um ecossistema institucional interconectado, baseado na lógica da partilha de soberania funcional, com canais permanentes de comunicação e protocolos previamente definidos para cenários de crise (Pernice & Weidenfeld, 2020). Essa arquitetura permite que a integração europeia transcenda o plano normativo, assumindo contornos operacionais com impacto direto na segurança nacional e na resiliência institucional de cada Estado-Membro.

5.2 Ciberexercícios, simulações e estratégias coordenadas

A operacionalização da ciberdefesa e da prevenção criminal transnacional exige mais do que tratados e protocolos formais: requer capacitação prática, adaptação constante a novas ameaças e testes reais de resposta em ambiente simulado. Nesse contexto, os ciberexercícios e simulações interinstitucionais assumem papel estratégico tanto na validação das capacidades técnicas como na avaliação da coordenação política e institucional.

Entre os exercícios mais relevantes, destacam-se:

- **EU CYBER RAPID RESPONSE TEAMS (CRRTs)**, uma iniciativa cooperativa financiada pela UE que permite a constituição de equipas técnicas de resposta rápida compostas por especialistas dos Estados participantes, sendo frequentemente ativadas em casos de ciberataques de impacto elevado;

- **Cyber Europe**, liderado pela ENISA, um exercício bienal que simula ataques massivos e em cadeia contra infraestruturas críticas, envolvendo tanto autoridades públicas quanto operadores privados;
- **Locked Shields**, promovido pelo CCDCOE, o maior exercício internacional de defesa cibernética em tempo real, envolvendo mais de 30 países com cenários altamente complexos, focando aspectos técnicos, legais e estratégicos da resposta conjunta.

Tais iniciativas não apenas melhoram a resiliência coletiva, como também ajudam a identificar lacunas nos planos nacionais, a calibrar as responsabilidades institucionais e a criar confiança mútua entre os atores participantes (Carrapico & Barrinha, 2018).

Além disso, a Estratégia da União Europeia para a Cibersegurança (2020) e a Bussola Estratégica da UE (2022) consagram formalmente o papel dos ciberexercícios como parte integrante da política de segurança comum. A simulação de cenários híbridos e multivetoriais, como a interferência eleitoral, sabotagem de redes de energia e campanhas de desinformação, permite preparar as instituições não apenas para as ameaças técnicas, mas também para os impactos sociais e políticos de um ataque (European Commission, 2020).

Neste contexto, verifica-se uma crescente valorização das capacidades partilhadas, da formação conjunta e da integração doutrinária, em que os exercícios e simulações assumem o duplo papel de treino e diplomacia, fortalecendo o sentimento de pertença a uma comunidade de segurança europeia.

6. Parcerias Estratégicas - *A reforma do setor de segurança na Europa e os novos paradigmas colaborativos*

A reforma do setor de segurança na Europa tem sido moldada não apenas pela reconfiguração das ameaças contemporâneas — cibercrime, desinformação, terrorismo híbrido, sabotagem digital —, mas também pela necessidade de superar os limites das abordagens estatais isoladas. A lógica atual da *Security Sector Reform* (SSR) europeia passa por construir estruturas inclusivas, resilientes e interoperáveis, nas quais a cooperação público-privada se torna um dos pilares centrais da capacidade de resposta e prevenção.

A segurança deixou de ser monopólio exclusivo das forças públicas e passou a depender da articulação com atores não estatais, empresas de tecnologia, centros de investigação,

operadores de infraestruturas críticas e organizações da sociedade civil. Este modelo híbrido, legitimado por políticas europeias como a Cybersecurity Strategy for the Digital Decade (European Commission, 2020), reforça o entendimento de que a resiliência coletiva exige parcerias estratégicas sustentadas e adaptáveis.

6.1 Cooperação público-privada na defesa cibernética

No contexto da reforma europeia do setor de segurança, a cooperação público-privada (CPP) é uma dimensão operacional da governança da cibersegurança. Esta cooperação visa garantir que os setores público e privado partilham dados, capacidades e responsabilidades para prevenir, responder e recuperar de incidentes críticos (ENISA, 2022).

A ENISA, por exemplo, promove fóruns CPP regulares e lidera o EU Public-Private Partnership on Cybersecurity (cPPP), lançado em 2016 com o objetivo de mobilizar investimentos em investigação, inovação e segurança digital. Através dessa parceria, empresas privadas (grandes e PME), universidades, centros tecnológicos e autoridades públicas desenvolvem conjuntamente standards técnicos, sistemas de alerta precoce e metodologias de mitigação de risco.

O setor das infraestruturas críticas é particularmente relevante neste domínio. As empresas que gerem redes elétricas, telecomunicações, sistemas bancários ou transporte público são alvos frequentes de ataques cibernéticos e, por isso, integram os Planos Nacionais de Cibersegurança dos Estados-Membros, como elementos essenciais da arquitetura de defesa nacional (Carrapico & Farrand, 2021).

As Joint Cybersecurity Units, criadas no âmbito da Bússola Estratégica da UE, preveem explicitamente a participação de atores privados em estruturas de resposta conjunta. A ideia é garantir conectividade em tempo real entre o setor público (forças armadas, polícia, autoridades de proteção de dados) e o privado (tecnologia, cibersegurança, telecomunicações), formando redes de cooperação ágeis e tecnicamente capazes de enfrentar crises complexas.

Além disso, projetos financiados pelo programa Horizon Europe e pelo Digital Europe Programme têm incentivado *testbeds* conjuntos, ciberlaboratórios de simulação, partilha de *threat intelligence* e formação integrada entre empresas tecnológicas e entidades governamentais.

6.2 Casos de sucesso e boas práticas em Portugal

Portugal tem vindo a posicionar-se como referência emergente na articulação público-privada em cibersegurança, integrando-se nas dinâmicas da reforma europeia do setor de segurança com iniciativas concretas.

Um dos principais exemplos é o trabalho desenvolvido pelo Centro Nacional de Cibersegurança (CNCS), que opera sob a tutela do Gabinete Nacional de Segurança e está alinhado com a Estratégia Nacional de Segurança do Ciberespaço. O CNCS promove relações sistemáticas com operadores privados através de múltiplas iniciativas, entre as quais se destacam o Programa C-Academy, desenvolvido em parceria com universidades e empresas para a formação técnica especializada em cibersegurança; o Observatório de Cibersegurança, responsável pela elaboração de estudos e pela promoção de encontros multissetoriais; a certificação de competências e a homologação de boas práticas para entidades privadas; e, ainda, a participação ativa no Conselho Consultivo de Cibersegurança, que integra representantes de setores estratégicos como o financeiro, telecomunicações, energia e tecnologia.

Outro exemplo de boa prática é o exercício nacional "Ciber Perseu", organizado pelas Forças Armadas Portuguesas com o envolvimento de entidades públicas e privadas, como a REN (energia), a NOS (telecomunicações), o Banco de Portugal e operadores do setor da saúde. Estes exercícios testam a capacidade de resposta colaborativa a ciberincidentes, simulando ataques de larga escala e promovendo uma cultura de segurança partilhada.

A nível europeu, Portugal tem estado ativo no EU Cybersecurity Competence Centre, sediado em Bucareste, e na European Cybercrime Training and Education Group (ECTEG), onde forças policiais portuguesas, incluindo a PJ e a GNR, participam em formações e no desenvolvimento de materiais de treino conjunto com parceiros europeus.[7]

Também no domínio académico, o país destaca-se com instituições como o INESC TEC, a Universidade do Porto, o Instituto Superior Técnico e a Universidade de Coimbra, que

[7] A Polícia Judiciária tem desempenhado um papel relevante no reforço da cooperação policial e judiciária europeia, nomeadamente através da sua Unidade de Cooperação Internacional (UCI), que assegura a articulação com os mecanismos da UE e a operacionalização de instrumentos como o Mandado de Detenção Europeu, as ordens europeias de investigação e o apoio direto a agências como a Europol e Eurojust. A UCI funciona como ponto de contacto privilegiado entre a PJ e as restantes autoridades europeias e internacionais, promovendo a eficácia da colaboração transfronteiriça em matéria criminal (Polícia Judiciária, s.d.). Disponível em: https://www.policiajudiciaria.pt/uci/

mantêm colaborações com a ENISA e com empresas tecnológicas em projetos europeus de investigação aplicada em segurança digital.

Essas boas práticas mostram como a reforma do setor de segurança, para ser eficaz, precisa ser multinível, participativa e tecnicamente robusta, incorporando os diferentes atores que operam e protegem o ciberespaço nacional e europeu.

7. Desafios e Propostas - *A cibersegurança como frente estratégica da soberania digital e da defesa nacional*

A defesa nacional em Portugal, ao integrar o ciberespaço como novo domínio estratégico de atuação, enfrenta desafios estruturais e dinâmicos que testam os limites da sua arquitetura jurídica, das capacidades operacionais e da prontidão tecnológica. No atual contexto de reformas do setor de segurança e da transformação digital da soberania, a cibersegurança já não pode ser tratada como uma extensão técnica da informática, mas sim como expressão real da segurança coletiva, da ordem constitucional e da legitimidade democrática do Estado (Gouveia, 2022; Rebelo, 2023).

Portugal, apesar de progressos relevantes — como a Estratégia Nacional de Segurança do Ciberespaço, o funcionamento do CNCS e os exercícios militares como o "Ciber Perseu" —, continua a enfrentar lacunas que exigem não apenas investimento, mas sobretudo visão estratégica e sinergias institucionais. A soberania cibernética portuguesa depende da capacidade de adaptar o seu modelo jurídico, operacional e educativo às novas ameaças que emergem de forma assimétrica, invisível e, frequentemente, transnacional.

7.1 Barreiras jurídicas, operacionais e tecnológicas

As *barreiras jurídicas* estão fortemente ligadas à falta de um regime normativo específico e transversal para o ciberespaço no contexto da defesa e da segurança. Embora a Constituição da República Portuguesa consagre a paz, a segurança coletiva e a proteção da soberania como fins do Estado (CRP, art. 5.º e 273.º), não existe uma delimitação clara da atuação das Forças Armadas e das forças de segurança em cenários híbridos, especialmente no domínio cibernético. Como refere Jorge Miranda (2020), a Constituição portuguesa prevê mecanismos de defesa em tempo de guerra ou ameaça externa, mas a fluidez das ameaças digitais levanta dúvidas sobre a sua qualificação e o acionamento legítimo dos meios de resposta.

No plano operacional, a dispersão de competências entre diferentes entidades — GNS, PJ, CNCS, SIRP, Forças Armadas — cria obstáculos à interoperabilidade, partilha de informação e liderança unificada em tempo de crise. A ausência de um comando técnico centralizado para o ciberespaço compromete a eficácia e celeridade da resposta. Além disso, o esforço conjunto entre entidades civis e militares carece de uma doutrina comum de ciberdefesa, como apontam estudos recentes do Instituto da Defesa Nacional (IDN, 2022), defendendo uma clarificação do papel das Forças Armadas no apoio à cibersegurança nacional, especialmente em estado de exceção constitucional.

Já as *barreiras tecnológicas* decorrem de múltiplos fatores: a dependência de fornecedores estrangeiros para *software* e infraestruturas críticas, a escassez de profissionais altamente especializados em cibersegurança, e a ausência de um ecossistema de inovação tecnológica orientado à segurança nacional. O Relatório Anual de Segurança Interna (RASI, 2023) identificou a crescente sofisticação dos ataques cibernéticos a entidades públicas e a carência de sistemas de resposta automatizada, o que evidencia fragilidades sistémicas e riscos à soberania digital do país.

7.2 Recomendações para reforçar a resiliência nacional

Diante dos desafios identificados, propõe-se um conjunto articulado de recomendações estratégicas visando reforçar a resiliência cibernética de Portugal sob uma perspectiva integrada que abrange a defesa nacional, a reforma do setor de segurança e a inovação institucional. Em primeiro lugar, destaca-se a necessidade da criação de uma Lei de Ciberdefesa Nacional, dotada de estatuto jurídico próprio, que estabeleça claramente as competências, os limites de atuação e os cenários de intervenção das várias entidades envolvidas. Essa legislação deve ainda regular a articulação entre as Forças Armadas, as forças de segurança, o Centro Nacional de Cibersegurança (CNCS) e demais órgãos públicos e privados, assegurando sempre o respeito pelos direitos fundamentais e o controlo democrático das ações.

Além disso, recomenda-se o estabelecimento de um Comando Nacional de Ciberdefesa, que funcione sob uma coordenação conjunta do Ministério da Defesa Nacional e da Presidência do Conselho de Ministros. Esse comando teria a responsabilidade de atuar de forma transversal em situações de crise cibernética, garantindo uma resposta ágil e integrada, espelhando modelos já existentes em outros países da União Europeia.

Outra recomendação essencial refere-se à integração obrigatória de componentes relativos à cibersegurança e à defesa cibernética nos currículos das academias militares, das escolas de polícia e da formação contínua do funcionalismo público. Essa medida visa promover uma cultura transversal de segurança digital, fundamentada nos princípios constitucionais e na defesa da legalidade democrática, conforme destacado por Loureiro dos Santos (2015).

No âmbito da inovação tecnológica, propõe-se o fomento de um polo nacional dedicado à cibersegurança, estruturado com base em parcerias público-privadas. Tal polo estimularia a colaboração entre startups, universidades e centros tecnológicos para o desenvolvimento de soluções críticas que garantam a proteção de dados, infraestrutura e a aplicação de inteligência artificial voltada para a segurança nacional.

Por fim, destaca-se a importância da implementação de uma doutrina nacional de ciber-resiliência, que se apoie em cenários de simulação interinstitucional e esteja alinhada com as melhores práticas da União Europeia e da NATO. Essa doutrina deve privilegiar os princípios da antecipação, redundância, resposta coordenada e recuperação ágil, assegurando que Portugal esteja preparado para enfrentar os desafios do ambiente digital em constante transformação.

Essas recomendações transcendem o mero reforço técnico das capacidades nacionais, pois objetivam consolidar uma visão constitucional e estratégica da ciberdefesa, compreendendo a segurança como um direito e uma responsabilidade compartilhada, fundamentada nos valores do Estado de direito democrático e na proteção efetiva dos cidadãos.

Conclusão

O presente estudo demonstrou a complexidade e a importância crescente da ciberdefesa no contexto da segurança nacional e europeia, ressaltando a necessidade de Portugal adotar uma abordagem integrada, multidimensional e alinhada com os padrões e políticas europeias. A análise das barreiras jurídicas, operacionais e tecnológicas, bem como das práticas institucionais existentes, evidenciou lacunas que demandam ações estratégicas concretas para reforçar a resiliência cibernética do país.

Nesse sentido, as recomendações propostas — incluindo a criação de uma Lei de Ciberdefesa Nacional, o estabelecimento de um Comando Nacional de Ciberdefesa, a incorporação da cibersegurança nos currículos das academias militares e forças de segurança, o fomento da inovação em parcerias público-privadas, e a adoção de uma doutrina nacional de

ciber-resiliência — formam um conjunto articulado de medidas que podem garantir uma resposta eficaz e coordenada aos desafios contemporâneos. Essas medidas não se limitam à modernização técnica, mas buscam ancorar a ciberdefesa nos princípios constitucionais do Estado de direito democrático, assegurando o respeito aos direitos fundamentais e o controlo democrático das instituições (Loureiro dos Santos, 2015).

O fortalecimento da agenda nacional de ciberdefesa permitirá a Portugal contribuir de forma mais decisiva para os objetivos estratégicos da União Europeia e da NATO no domínio da segurança digital, reforçando sua presença e papel nos mecanismos europeus de cooperação e resposta conjunta (European Commission, 2020; NATO CCDCOE, 2022). A articulação entre atores públicos e privados, bem como o incentivo ao diálogo com a sociedade civil, facilitará a construção de uma cultura nacional de soberania digital e resiliência coletiva, conforme orientado pelas diretrizes do Centro Europeu de Competência em Cibersegurança e da Agência Europeia para a Cibersegurança (ENISA, 2021; EU Cybersecurity Competence Centre, 2023).

Em suma, a consolidação da ciberdefesa nacional representa não apenas um investimento em capacidades tecnológicas e operacionais, mas um compromisso estratégico com a proteção da democracia, da soberania e dos cidadãos portugueses. Ao assumir uma posição ativa e inovadora nos fóruns internacionais de segurança cibernética, Portugal estará melhor preparado para enfrentar os desafios futuros, contribuindo para a estabilidade do espaço digital europeu e global.

Referências

BETZ, D. (2011). Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed. *Journal of Strategic Studies, 34*(5), 705–728.

BORN, H., LEIGH, I., & WILLS, A. (2016). *Intelligence oversight in the twenty-first century: Accountability in a changing world.* Routledge.

BRYDEN, A., & HÄNGGI, H. (Eds.) (2005). *Security governance in post-conflict peacebuilding.* Geneva Centre for the Democratic Control of Armed Forces (DCAF).

BUEGER, C., & EDMUNDS, T. (2017). Beyond seablindness: A new agenda for maritime security studies. *International Affairs, 93*(6), 1293–1311.

CARRAPICO, H., & BARRINHA, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society, 19*(3), 299–312. https://doi.org/10.1080/23745118.2018.1430712

CCDCOE. (2021). Locked Shields 2021: Technical Summary. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

CCDCOE. (2022). Viasat Hack: Lessons from the Russian Cyber Campaign in Ukraine. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

CCDCOE. (2023). Locked Shields 2023 After Action Report. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

CCDCOE. (2024). Annual Report 2023: Cyber Defence Cooperation and Operational Preparedness. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org

CNCS. (2019). Estratégia Nacional de Segurança do Ciberespaço 2019–2023. Centro Nacional de Cibersegurança. https://www.cncs.gov.pt

CNCS. (2024). Relatório Anual de Cibersegurança em Portugal – 2023. Centro Nacional de Cibersegurança. https://www.cncs.gov.pt

CONSTITUIÇÃO DA REPÚBLICA PORTUGUESA (VII Revisão Constitucional). (2005). Diário da República, 1.ª série-A, n.º 178.

COUNCIL OF THE EUROPEAN UNION. (2020). A Strategic Compass for Security and Defence. Brussels.

COTTETY, A., EDMUNDS, T., & FORSTER, A. (2002). The second generation problematic: Rethinking democracy and civil-military relations. *Armed Forces & Society, 29*(1), 31–56.

DCAF – GENEVA CENTRE FOR SECURITY SECTOR GOVERNANCE. (2020). Security Sector Reform Backgrounder Series. Geneva.

EU CYBER DIRECT. (2023). Cyber Operations in the War Against Ukraine: Lessons for Europe. European Union Cyber Diplomacy Initiative.

EURODEFENSE-PORTUGAL. (2022). A Guerra no Ciberespaço: Desafios à Defesa e à Segurança [Conferência]. EuroDefense-Portugal. https://www.eurodefense.pt

EUROPOL. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. European Cybercrime Centre. https://www.europol.europa.eu

EUROPOL. (2023). IOCTA – Internet Organised Crime Threat Assessment. European Union Agency for Law Enforcement Cooperation. https://www.europol.europa.eu

EUROJUST & EUROPOL. (2021). Major international operation targets Emotet malware infrastructure [Joint Press Release]. https://www.europol.europa.eu

EUROPEAN COMMISSION. (2020). Shaping Europe's digital future. https://ec.europa.eu/digital-strategy

EUROPEAN COMMISSION. (2020). The EU's Cybersecurity Strategy for the Digital Decade. Brussels.

EUROPEAN COMMISSION. (2021). EU Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

EUROPEAN COMMISSION. (2022). Digital Europe Programme – Cybersecurity Calls Overview. https://digital-strategy.ec.europa.eu

EUROPEAN COMMISSION. (2023). Joint Communication on the EU Cyber Defence Policy. https://ec.europa.eu

EUROPEAN COMMISSION. (2023). Joint Communication on the EU Cyber Defence Policy Framework. https://ec.europa.eu

EUROPEAN CYBERSECURITY COMPETENCE CENTRE. (2023). Annual Report. https://cybercompetence.eu/

EUROPEAN EXTERNAL ACTION SERVICE (EEAS). (2024). Strategic Compass for Security and Defence – Progress Report. https://www.eeas.europa.eu

EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). (2021). Threat Landscape Report 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ENISA. (2022). Annual Report 2022. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

ENISA. (2023). ENISA Threat Landscape Report 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

ENISA. (2023a). ENISA Threat Landscape 2023 – Executive Summary. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

ENISA. (2023b). Cybersecurity Threat Landscape: Critical Sectors Focus. ENISA Report Series.

GOUVEIA, J. B. (2022). Direito constitucional (6.ª ed.). Almedina.

GOUVEIA, J. B. (2022). Direito constitucional internacional e da União Europeia (7.ª ed.). Almedina.

GOVERNO DE PORTUGAL. (2023). Estratégia Nacional de Defesa para o Ciberespaço 2023-2027. Ministério da Defesa Nacional.

HOFFMAN, F. (2009). Hybrid threats: Reconceptualizing the evolving character of modern conflict. *Strategic Forum, 240*.

INSTITUTO DA DEFESA NACIONAL. (2022). Cibersegurança e Defesa Nacional: Desafios e Perspetivas. Lisboa: IDN.

INTERPOL. (2023). Cybercrime Strategy 2023–2026. International Criminal Police Organization. https://www.interpol.int

KALDOR, M. (2012). *New and old wars: Organized violence in a global era* (3rd ed.). Polity Press.

LOUREIRO DOS SANTOS, J. (2015). Portugal e a Nova Estratégia de Defesa Nacional. Lisboa: Prefácio.

LOUREIRO DOS SANTOS, S. (2015). A defesa nacional e a legalidade democrática. Coimbra: Almedina.

MATLARY, J. H. (2009). *European Union Security Dynamics: In the New National Interest.* Palgrave Macmillan.

MINISTÉRIO DA DEFESA NACIONAL. (2023). Estratégia Nacional de Defesa para o Ciberespaço 2023–2027. República Portuguesa. https://www.defesa.gov.pt

MIRANDA, J. (2020). *Manual de direito constitucional* (Tomo IV, 7.ª ed.). Coimbra Editora.

NATO. (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation: Active Engagement, Modern Defence.* Lisbon.

NATO. (2023). Cyber Defence Pledge Progress Report. North Atlantic Treaty Organization. https://www.nato.int

NATO. (2024). Cyber Defence Policy: NATO's Strategic Adaptation in a Changing Threat Environment. NATO Public Diplomacy Division. https://www.nato.int

NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE (NATO CCDCOE). (2022). Annual Review 2022. https://ccdcoe.org/annual-review-2022/

NATO INNOVATION HUB. (2021). Cognitive Warfare: The Battle for the Human Mind. NATO Allied Command Transformation.

NYE, J. S. (2010). Cyber Power. Harvard Kennedy School, Belfer Center for Science and International Affairs.

OECD. (2007). *OECD DAC Handbook on Security System Reform: Supporting Security and Justice.* Paris: OECD Publishing.

PEREIRA, M. (2022). Ciberdefesa Nacional: Entre a Doutrina e a Capacidade. *Revista Militar, 2742*, 65–80.

PERNICE, I., & WEIDENFELD, W. (2020). Europe's Capacity to Act in the 21st Century: European Security and Strategic Autonomy. Bertelsmann Stiftung.

POLÍCIA JUDICIÁRIA. (s.d.). Unidade de Cooperação Internacional. https://www.policiajudiciaria.pt/uci/

RASI – RELATÓRIO ANUAL DE SEGURANÇA INTERNA. (2023). Ministério da Administração Interna.

REBELO, A. (2023). A defesa cibernética como função de soberania: o desafio jurídico-constitucional da guerra digital. *Revista do Instituto de Defesa Nacional, 158*, 45–63.

RID, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32.

RID, T. (2013). *Cyber War Will Not Take Place.* Oxford University Press.

SILVA, L., & ROCHA, D. (2021). Cibersegurança em Portugal: Desafios à Cooperação Público-Privada. *Revista de Estudos de Segurança, 12*(1), 33–49.

SEDRA, M. (Ed.) (2010). *The Future of Security Sector Reform.* Centre for International Governance Innovation.

WILLIAMS, P. D. (2008). *Security studies: An introduction.* Routledge.