Portugal como Hub de Cibersegurança da União Europeia no Oceano Atlântico: Doutrina, Ameaças e Soberania Estratégica

Dr.ª
Catarina Isabel Pereira Leitão

Introdução*

Num mundo onde o ciberespaço se tornou um novo domínio de soberania e segurança, as fronteiras tradicionais são cada vez mais permeáveis às ameaças digitais. A digitalização acelerada das economias, a dependência crescente de infraestruturas tecnológicas críticas, e a emergência de novas potências digitais redefiniram a geopolítica global – e Portugal encontra-se numa encruzilhada estratégica. A União Europeia tem reforçado a sua ambição de soberania digital, procurando reduzir dependências externas e assegurar a resiliência das suas infraestruturas. Instrumentos como a Diretiva (UE) 2022/2555 (NIS2)1 e o AI Act2, bem como quadros estratégicos como a Estratégia Digital Nacional (EDN)3 dos Estados-Membros, refletem esta nova prioridade política [Comissão Europeia, 2022; República Portuguesa, 2020].

Todavia, a concretização plena desta visão europeia exige o envolvimento ativo dos Estados-Membros, nomeadamente daqueles com posições geoestratégicas singulares. Tal desiderato transcende a mera conectividade; implica, sobretudo, a consolidação de um polo de defesa avançada, monitorização proativa e cooperação digital multilateral. Este

desígnio exige uma abordagem integrada, articulando dimensões técnicas, institucionais, jurídicas e diplomáticas, numa lógica de segurança partilhada e cooperação europeia [ENISA, 2023]4.

Este artigo propõe-se a analisar esta possibilidade prospetiva, considerando criticamente:

- De que forma a posição geográfica e as infraestruturas críticas digitais permitem a Portugal assumir um papel de charneira na ciberdefesa europeia;
- As oportunidades decorrentes do novo enquadramento europeu e nacional, com destaque para a NIS2, AI Act e a EDN;
- E as responsabilidades soberanas, nacionais e europeias, que Portugal deve assumir no complexo xadrez da segurança híbrida e da diplomacia digital.

A abordagem metodológica adotada neste artigo assenta numa análise qualitativa, baseada na revisão de literatura e na análise documental de fontes primárias (legislação, estratégias nacionais) e secundárias (relatórios de agências, publicações académicas). A argumentação é enriquecida pela ponderação de estudos de caso ilustrativos, que contextualizam as ameaças e dão substância empírica à reflexão prospetiva.

A questão fundamental não reside apenas na capacidade de Portugal desempenhar este papel, mas na urgência e na determinação com que deve abraçar este desígnio, alicerçado em maturidade institucional, capacidade técnica robusta, e uma visão estratégica de longo alcance. Mais do que uma opção, a assunção deste papel constitui uma responsabilidade estratégica nacional.

1. Do Mar Profundo ao Ciberespaço: A Vantagem Geoestratégica da Conectividade Atlântica

A posição geográfica de Portugal constitui um dos seus ativos estratégicos mais valiosos e perenes no contexto da segurança e da soberania digital europeia. Localizado no ponto de confluência entre a Europa, as Américas e a África Ocidental, o país assume uma centralidade operacional na infraestrutura global de dados, consolidando-se como uma plataforma logística e tecnológica de alcance mundial.

Esta centralidade não é meramente conceptual: traduz-se materialmente através das rotas de cabos submarinos (CSs)5, estações de amarração, corredores marítimos e fluxos de dados que cruzam o território continental e os arquipélagos da Madeira e dos Açores. Particular destaque merecem os Açores, cuja localização estratégica entre a Europa e os Estados Unidos os torna um ponto natural de ligação, fator decisivo na captação de investimentos em sistemas de conectividade subaquática de elevada capacidade e em data centers de última geração6.

A infraestrutura de Sines, por exemplo, evoluiu para um dos principais gateways de tráfego internacional de dados para Portugal em para a Europa, com ligações diretas ao Brasil (via EllaLink) e à África Ocidental, projetando o país como elo ibero-americano essencial na arquitetura da conectividade transatlântica (Ella Link, 2021)7. Estima-se que mais de 95% do tráfego de dados intercontinental circule por estas autoestradas submarinas8, o que confere a Portugal uma responsabilidade acrescida na monitorização e proteção destes fluxos vitais.

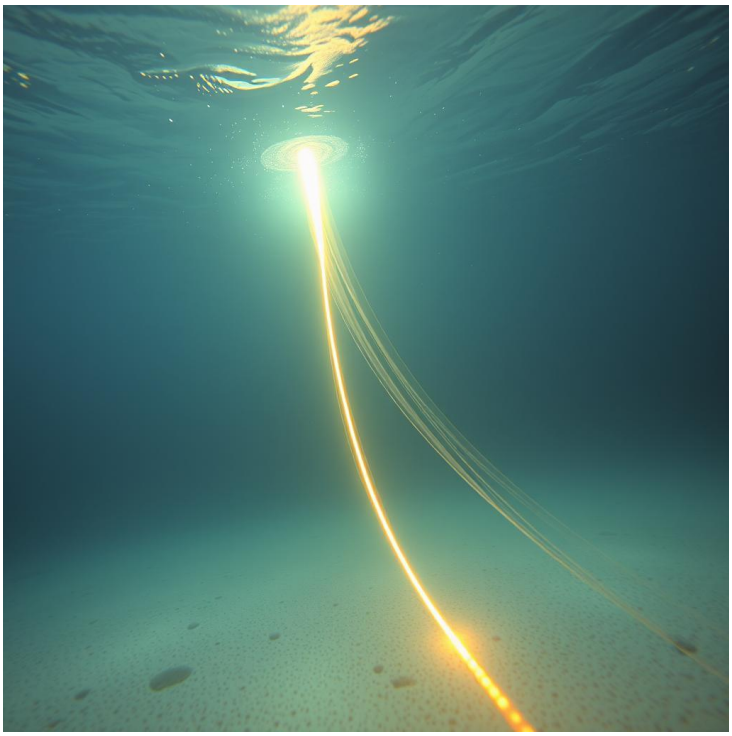

Figura 1 – Representação simbólica de um cabo submarino de comunicações transmitindo dados em alta velocidade no fundo do oceano. A imagem ilustra a dimensão invisível, porém crítica, da infraestrutura digital subaquática que sustenta a conectividade global e destaca a importância estratégica da sua proteção no contexto da segurança marítima e cibernética.

Simultaneamente, a extensa Zona Económica Exclusiva (ZEE) portuguesa – uma das maiores da União Europeia – confere a Portugal não só oportunidades económicas, mas também amplia o raio de responsabilidade nacional na proteção de infraestruturas críticas subaquáticas9. A monitorização, proteção e segurança destas artérias vitais da comunicação global são asseguradas por capacidades navais e tecnológicas que, em articulação com agências europeias como a EMSA (2023)10, reforçam o papel de Portugal como guardião dos fluxos de comunicação marítima e digital.

Infraestruturas marítimas como os portos de Sines, Lisboa e Ponta Delgada, aliadas às capacidades operacionais da Marinha Portuguesa11, permitem uma vigilância efetiva e eficaz, bem como a deteção e neutralização de ameaças híbridas, como ações hostis contra cabos submarinos – preocupação exponenciada por incidentes recentes em outras

geografias, designadamente na Escandinávia e no mar Báltico12. A integração das competências da Marinha Portuguesa, em articulação com agências europeias como a EMSA (Agência Europeia da Segurança Marítima) e com as capacidades de ciberdefesa nacional, pode constituir um diferencial estratégico único para Portugal e para a UE.

Como defende Luís Bernardino, "a segurança no Atlântico é hoje tão relevante no ciberespaço como no domínio físico tradicional, exigindo uma abordagem integrada entre capacidades marítimas, digitais e diplomáticas" (Bernardino, 2022)13.

Portugal situa-se na encruzilhada de rotas digitais fundamentais e críticas:

- Ligação direta entre a Europa e América Latina (ex.: SAT-3/WASC/AMC)14;
- Ligação com a África Ocidental (ex.: ACE, WACS, e futuros projetos como o 2Africa)15;
- Rede intra-europeia (ligações marítimas e terrestres dentro da UE).

Este posicionamento estratégico, e o papel de ponte digital entre continentes, coloca Portugal numa posição privilegiada para acolher centros de monitorização de tráfego internacional de dados, plataformas de resposta a ciberincidentes e hubs estratégicos de cibersegurança europeia (ENISA, 2023)16.

Contudo, a concretização deste potencial exige uma estratégia nacional integrada, envolvendo o Estado, o setor privado e o ecossistema de investigação e desenvolvimento tecnológico. A edificação de uma arquitetura de ciberdefesa sólida, ancorada na soberania digital e na segurança marítima, dependerá da capacidade do país em alinhar vantagens geográficas com políticas públicas consistentes e coerentes, bem como com investimentos sustentados em defesa, tecnologia e infraestruturas críticas.

2. Para Além dos Cabos: A Construção de um Ecossistema Digital Resiliente

A transformação digital global está a impulsionar uma nova onda de investimento em infraestruturas digitais críticas. Portugal, pela sua localização geoestratégica e estabilidade institucional, posiciona-se como um destino privilegiado e estratégico para a instalação de ativos digitais sensíveis, alavancando e propiciando a urgência de Portugal como um polo relevante na arquitetura da ciberdefesa atlântica.

A edificação de data centers de elevada capacidade, nomeadamente em zonas costeiras como Sines ou insulares como a Madeira, designadamente projetos como o Sines Data Center Park (Start Campus)17 ou o Atlantic Hub da WDC na Madeira18 ilustra esta tendência e reflete a aposta num modelo de infraestrutura alinhado com as exigências dos grandes players tecnológicos internacionais, como Microsoft, Google e Amazon Web

Services19 – alicerçados em quatro fatores-chave:

- Localização estratégica – perto de estações de desembarque de cabos submarinos;
- Condições favoráveis;
- Fontes de energia renovável;
- Baixo risco de desastres naturais20.

Estes centros não só respondem à crescente procura por capacidade de armazenamento e processamento de dados, mas também incorporam critérios e exigências de sustentabilidade, segurança física e cibersegurança21.

Segundo relatório da ANACOM (2024)22, o número de data centers Tier III e Tier IV em Portugal cresceu cerca de 40% em relação ao ano anterior, evidenciando uma rápida consolidação do país como hub tecnológico periférico.

Contudo, a infraestrutura digital não se resume aos data centers. A conectividade portuguesa assenta numa arquitetura híbrida e resiliente, combinando:

- As estações de amarração de cabos submarinos (Sines, Carcavelos, Açores), garantindo ligações diretas intercontinentais23;
- A modernização do Backbone terrestre nacional24;
- A conectividade via satélite, como redundância estratégica25.

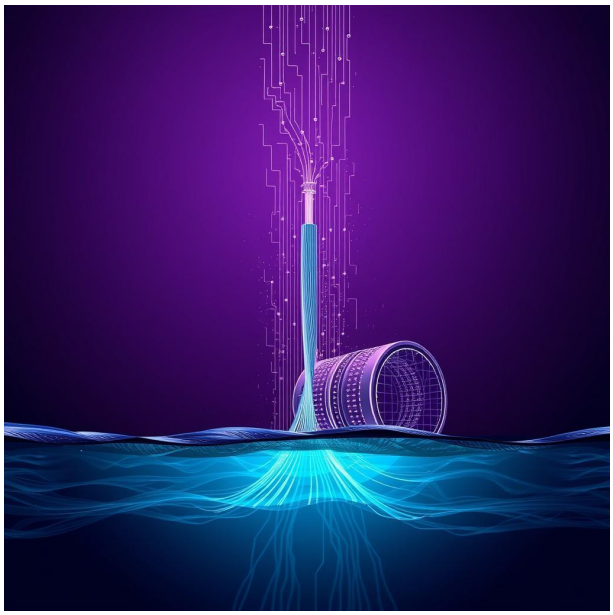

Figura 2 – Representação conceptual da infraestrutura de cabos submarinos como suporte fundamental da conetividade digital global. A imagem evoca a ascensão dos dados a partir do fundo oceânico, refletindo o

papel estrutural destas ligações na consolidação de um ecossistema digital resiliente e na projeção de Portugal como polo estratégico de armazenamento, processamento e segurança de informação.

Esta triangulação de meios (submarino, terrestre e espacial) é essencial para sistemas de comunicação seguros, especialmente para entidades estatais, Forças Armadas e operadores críticos. Neste contexto, Portugal encontra-se numa posição ímpar para implementar uma visão integrada de cibersegurança e soberania tecnológica, com potencial para liderar um novo paradigma europeu de ciberdefesa. Entre as iniciativas prioritárias destacam-se:

- Sistemas de monitorização contínua de tráfego e deteção de incidentes no tráfego internacional de dados;
- Operações conjuntas de defesa marítima e cibernética;
- Coordenação com a ENISA, NATO e CNCS para resposta a incidentes híbridos e internacionais[26].

À semelhança da Islândia, no Ártico, que integra centros de dados sustentáveis com capacidades de ciberdefesa, Portugal pode seguir este caminho, adaptando-o às suas especificidades geoestratégicas, reforçando simultaneamente a resiliência digital nacional e a solidariedade estratégica europeia (ENISA, 2023; NATO, 2022)[27].

A Irlanda, por exemplo, consolidou-se como um dos principais hubs de data centers da Europa, alavancando a sua densa rede de cabos transatlânticos num modelo focado na atração de investimento privado[28].

Contudo, a edificação deste ecossistema robusto não é apenas um desafio de capital e infraestrutura; é, fundamentalmente, um desafio de capital humano. A atração destes investimentos gera um efeito multiplicador na economia, estimado em vários pontos percentuais do PIB a médio prazo[29], mas expõe igualmente a necessidade crítica de formar, atrair e reter talento altamente qualificado em cibersegurança, engenharia de redes e gestão de dados[30]. A competição por estes profissionais é global, e Portugal deve criar condições para se afirmar não só como um hub de infraestruturas, mas também como um viveiro de competências digitais avançadas.

Esta abordagem deve integrar capacidades tecnológicas, doutrina de ciberdefesa e projeção internacional, garantindo simultaneamente a proteção do território nacional e dos seus interesses, mas também uma contribuição ativa e eficaz para a segurança coletiva da União Europeia no seu flanco atlântico.

3. Enquadramento Regulatório como Pilar Estratégico: Da NIS2 ao AI Act

A consolidação de um novo paradigma de cibersegurança na União Europeia não se esgota na edificação de infraestruturas tecnológicas. Requer, também, um enquadramento jurídico robusto, prospetivo e dinâmico que habilite as organizações e o Estado a responder com agilidade, eficácia e resiliência acrescida a ameaças cada vez mais complexas. Neste contexto, o enquadramento regulatório europeu – em particular a Diretiva NIS2 e o AI Act – representa um vetor essencial para o reforço da soberania tecnológica e da credibilidade internacional de Portugal.

A Diretiva NIS2 (Network and Information Security Directive) constitui um avanço significativo na arquitetura da cibersegurança europeia. Alarga o escopo de setores críticos abrangidos, impõe exigências mais rigorosas em matéria de gestão de risco, gestão de incidentes e cooperação internacional, além de fortalecer a proteção de infraestruturas digitais essenciais – como os cabos submarinos e data centers estratégicos (ENISA, 2023)31.

Portugal encontra-se num momento crucial para transformar este corpus legal em alavanca estratégica de soberania digital.

Para Portugal, com a sua crescente relevância enquanto hub digital atlântico, a implementação plena e eficaz da NIS2 é fundamental para garantir resiliência operacional e reforçar a confiança internacional. Esta diretiva não deve ser vista como um ónus, mas como uma oportunidade para elevar os padrões nacionais e consolidar a credibilidade de Portugal enquanto porto digital seguro. A NIS 2 é uma evolução estratégica, não uma metamorfose radical.

A articulação com estruturas europeias como a ENISA e o CERT-EU32, bem como a criação de capacidades nacionais de monitorização e resposta, são elementos críticos para garantir eficácia operacional e assegurar a integração operacional com os aliados da NATO e da UE.

Paralelamente, o AI Act, introduz um regime jurídico que regula a utilização da inteligência artificial. Assume-se, assim, como peça fundamental, particularmente no contexto da ciberdefesa e da monitorização de ameaças, ao classificar sistemas de IA por níveis de risco, impondo escrutínio apertado sobre aplicações de alto risco (infraestruturas críticas, segurança digital) (European Commission, 2024)33.

Esta abordagem estabelece parâmetros rigorosos de ética, transparência algorítmica e robustez técnica, prevenindo o uso abusivo de sistemas de IA em contextos sensíveis.

Para Portugal, a regulação da IA deve ser encarada como uma extensão da doutrina de ciberdefesa: tecnologias de monitorização de incidentes de tráfego, identificação antecipada de ameaças a cabos ou previsão de ciberataques são recursos críticos, desde que operem sob supervisão humana, com transparência algorítmica e em estrita

conformidade com os princípios do regulamento, particularmente no que respeita à ética, monitorização e proporcionalidade do risco.

A nível interno, a Estratégia Digital Nacional (EDN), publicada em 2024 pelo Conselho Nacional de Segurança[34], constitui a matriz operacional para a afirmação de Portugal no ciberespaço europeu e atlântico. Estruturada em quatro eixos – reforço da capacidade institucional de resposta a ameaças híbridas; desenvolvimento de um ecossistema tecnológico soberano e competitivo; proteção proativa de infraestruturas críticas; e fortalecimento da cooperação internacional em cibersegurança e ciberdefesa – esta estratégia reflete uma visão alinhada com os imperativos geoestratégicos já abordados.

A sua eficácia dependerá da capacidade do país em integrar dimensões jurídicas, técnicas e territoriais numa abordagem coordenada, holística e integrada. O reforço das capacidades institucionais, a descentralização operacional e a promoção de uma cultura de cibersegurança nos setores público e privado são pilares fundamentais para garantir uma resiliência contínua e integrada.

O atual enquadramento jurídico europeu e nacional não deve ser interpretado apenas como uma imposição normativa, mas como uma plataforma de projeção estratégica. A NIS2, o AI Act e a EDN convergem na edificação de um sistema normativo que, bem operacionalizado, permite a Portugal afirmar-se como um porto digital seguro do Atlântico, dotado de capacidades tecnológicas, doutrina estratégica e confiança internacional.

Esta arquitetura normativa, mais do que um conjunto de normas, é uma ferramenta de política pública, de poder digital e de soberania nacional. É um instrumento estratégico de projeção de poder, soberania e confiança que consolida o papel de Portugal como porto seguro digital do Atlântico, ancorado numa estrutura regulatória avançada e articulada com os seus recursos técnicos, humanos e geoestratégicos. Garante, assim, a proteção dos ativos críticos e contribui de forma relevante para a segurança coletiva da União Europeia e da Aliança Atlântica.

4. O Reverso da Medalha: Riscos, Vulnerabilidades e Desafios à Gestão Estratégica

A aspiração de Portugal a um papel estratégico proeminente na cibersegurança europeia e atlântica comporta, inevitavelmente, desafios estruturais, riscos operacionais e vulnerabilidades geoestratégicas que exigem uma avaliação criteriosa e mitigação proativa. Como ressalta a especialista Dr.ª Emily Parker, "a cibersegurança deixou de ser uma questão técnica para se tornar a linha de frente da defesa nacional e da geopolítica global – quem controla o ciberespaço controla o futuro" (Parker, 2024)[35]. Esta realidade torna urgente o desenvolvimento de capacidades robustas e coordenadas para a proteção das infraestruturas críticas nacionais.

A crescente centralidade geodigital do território português como nó de conectividade internacional – potenciada por cabos submarinos, data centers e hubs tecnológicos – implica uma maior vulnerabilidade a ameaças híbridas e cibernéticas, tanto por parte de atores estatais como não estatais (CERT.PT, 2023)[36].

Casos recentes, como os ataques a cabos submarinos no Mar Báltico, evidenciam a vulnerabilidade física e lógica destas infraestruturas. No contexto português, zonas como Sines, Açores e Madeira concentram ativos de elevado valor estratégico, cuja proteção exige não apenas vigilância contínua, mas também capacidade de resposta célere, coordenada e integrada.

Figura 3 – Centro de dados costeiro ligado a cabos submarinos, ilustrando a importância estratégica das infraestruturas digitais na articulação dos fluxos globais de informação e na soberania tecnológica.

Adicionalmente, a dependência de tecnologias emergentes e de fornecedores globais em áreas críticas como cloud computing, inteligência artificial e redes 5G coloca questões relevantes sobre a autonomia e soberania digital nacional. Tecnologias fundamentais para a ciberdefesa, como sistemas de IA aplicados à análise de tráfego de dados, estão sujeitas a decisões políticas, comerciais ou jurídicas fora do controlo nacional. O AI Act procura mitigar estes riscos através de requisitos de transparência e supervisão, mas a procura de um equilíbrio entre inovação participativa e autonomia estratégica continua a ser um desafio permanente[37].

A crescente complexidade dos domínios operacionais – que cruzam ciberespaço, mar, espaço e território – exige uma gestão sólida e coordenada em múltiplos níveis, com estruturas de comando e controlo bem definidas. A coexistência de múltiplas entidades com competências sobrepostas, aliada a uma articulação por vezes insuficiente entre organismos públicos (como o CERT.PT, ANACOM, Forças Armadas, GNS, entre outros),

tem evidenciado fragilidades de coordenação e respostas dispersas em cenários de crise digital. Em 2023, registou-se um aumento de 67% nos eventos relacionados com cibersegurança em Portugal, com particular incidência sobre infraestruturas críticas (CERT.PT, 2023)38, realçando a necessidade premente de soluções operacionais integradas.

Neste contexto, a criação de um Centro Nacional de Operações de Segurança (SOC), com uma visão integrada e capacidades técnicas, assim como estruturas de comando e controlo entre entidades estratégicas, constitui uma resposta estratégica prioritária. Esta estrutura deve articular capacidade de monitorização contínua e em tempo real das redes nacionais, resposta rápida e coordenação eficaz com os parceiros europeus e atlânticos, designadamente ENISA e NATO. Um incidente de larga escala nos Açores envolvendo cabos submarinos exigiria resposta imediata da Marinha, do CERT.PT, da ENISA e potencialmente da NATO.

No entanto, a ausência de protocolos claros e pré-estabelecidos, assim como de mecanismos de comando e controlo integrados, padronizados e pré-definidos para cenários de crise que envolvam infraestruturas digitais críticas, pode resultar em respostas fragmentadas e ineficazes.

Como sublinha Nassim Taleb, eventos raros e altamente disruptivos – os chamados "cisnes negros" – desafiam os modelos tradicionais de planeamento e gestão de risco, impondo a necessidade de desenvolver resiliência sistémica, e não apenas prevenção regulatória39.

Assim, a falta de mecanismos estruturados de coordenação em crises digitais constitui uma fragilidade e uma vulnerabilidade que Portugal não pode ignorar. A cibersegurança exige uma estratégia integrada em múltiplos níveis de atuação. Uma estratégia eficaz de cibersegurança depende de uma gestão ágil e de estruturas multidisciplinares aptas a operar num ambiente complexo e dinâmico. Apesar dos progressos legislativos, persistem fragilidades ao nível operacional e da coordenação institucional; é essencial assegurar a sua implementação coordenada e a integração estratégica.

O papel emergente de Portugal como gateway digital do Atlântico impõe, assim, uma consciência plena das ameaças inerentes. A exposição geoestratégica, as fragilidades operacionais internas, a dependência tecnológica e a complexidade da coordenação entre instituições exigem uma abordagem robusta, integrada, com visão, disciplina e investimento contínuo. A ambição digital portuguesa enfrenta o seu maior desafio: equilibrar protagonismo internacional com autonomia tecnológica e robustez defensiva.

Num cenário internacional caracterizado pela fragmentação do sistema digital, pela proliferação de ameaças híbridas e pela crescente complexidade geopolítica, a proteção das infraestruturas críticas nacionais é um imperativo de soberania. Como sublinha Armando Marques Guedes, "a soberania no século XXI não se exerce apenas com bandeiras no território, mas com controlo efetivo das redes que nos ligam ao mundo, sejam estas marítimas, digitais ou espaciais"40. Só uma abordagem holística, integrada,

multidisciplinar, pró-ativa e continuamente atualizada poderá garantir que o "lado sombrio" da conectividade não se transforme em vulnerabilidade estratégica.

O verdadeiro desafio estratégico não reside apenas na projeção de capacidade, mas na solidez da retaguarda.

5. Frente Comum Digital: A Arquitetura da Resiliência Coletiva

No complexo domínio da cibersegurança, nenhuma nação, por mais avançada que seja, pode garantir a sua segurança de forma isolada[41], isto é, não pode proteger isoladamente os seus ativos digitais. A natureza internacional e assimétrica das ciberameaças, aliada à multiplicidade de atores (estatais, não estatais e híbridos) e à complexidade dos riscos híbridos, requerem respostas integradas que articulem uma gestão diversificada, compatibilidade técnica, e cooperação entre os setores público e privado (ENISA, 2023)[42].

Para Portugal, a aspiração a um papel central na arquitetura da cibersegurança euro-atlântica é indissociável de uma capacidade robusta e proativa de cooperação multilateral, tanto a nível europeu como transatlântico. O aprofundamento de sinergias a nível europeu, atlântico, e lusófono é conditio sine qua non para a concretização de uma ciberdefesa robusta.

A Diretiva NIS2 impõe obrigações claras, mas também oferece oportunidades para liderança estratégica em áreas como:

- Monitorização conjunta de ameaças digitais;
- Resposta coordenada a incidentes críticos;
- Desenvolvimento conjunto de normas técnicas e operacionais.

Neste contexto, Portugal tem a oportunidade de assumir um papel ativo em domínios como a monitorização de ameaças entre países, o estabelecimento de normas técnicas partilhadas, e a resposta coordenada e articulada a ataques contra infraestruturas digitais.

A participação ativa em organismos europeus, como a ENISA e o CERT-EU, deve ser intensificada mediante propostas e iniciativas concretas, com impacto local no espaço atlântico e explorando a posição de Portugal como elo natural entre Europa, África e América Latina[43]. Um exemplo viável seria a criação de mecanismos conjuntos de vigilância em tempo real sobre o tráfego digital internacional nos pontos de aterragem dos cabos submarinos, em estreita cooperação entre o CERT.PT e as entidades europeias de cibersegurança, nomeadamente o CERT-EU. Tais iniciativas não apenas aumentariam

a resiliência nacional, como também reforçariam o posicionamento de Portugal como vetor de confiança digital no espaço atlântico.

A dimensão atlântica ganha particular relevo com o reconhecimento do ciberespaço como domínio operacional pela NATO. A articulação entre segurança marítima e ciberdefesa, sobretudo nos arquipélagos dos Açores e da Madeira, representa uma vantagem geoestratégica que deve ser plenamente explorada. Assim, o reforço da presença da NATO no Atlântico e a realização de exercícios conjuntos constituem oportunidades para Portugal se afirmar como um ponto de articulação entre a segurança marítima e a ciberdefesa, particularmente nas suas águas insulares.

Exercícios conjuntos, e a participação ativa em Centros de Excelência da NATO, como o CCDCOE, em Tallinn, são fundamentais para a partilha de conhecimento e o desenvolvimento de doutrina, reforçando essa ambição.

Em 2023, a NATO realizou o exercício "Cyber Coalition", com participação portuguesa, testando capacidades de resposta a ciberataques coordenados contra infraestruturas críticas (NATO, 2023)44.

Paralelamente, as parcerias público-privadas (PPP) constituem outro pilar essencial. Num cenário em que o setor privado detém e opera a maioria das infraestruturas digitais críticas, uma colaboração estreita e baseada na confiança entre o Estado e as empresas é crucial para a partilha de inteligência de ameaças, a coordenação de planos de contingência e a definição conjunta de estratégias de resiliência.

Iniciativas como o Fórum Nacional de Cibersegurança ou a coordenação entre a ANACOM e os operadores de telecomunicações demonstram o potencial desta abordagem, carecendo, contudo, de mecanismos legais e técnicos que garantam o equilíbrio entre segurança, privacidade e competitividade.

Finalmente, a Diplomacia Digital afirma-se como um dos pilares centrais da projeção de poder no século XXI, funcionando como instrumento estratégico de estabilização, influência e afirmação soberana no domínio cibernético.

Num contexto internacional marcado por uma crescente competição geoestratégica em torno dos fluxos digitais, das infraestruturas críticas e da regulação de tecnologias emergentes, a ciberdefesa deixou de ser apenas um exercício técnico-militar ou jurídico-administrativo. Tornou-se, cada vez mais, uma arena de negociação política, influência normativa e construção de alianças – é neste espaço que a diplomacia digital adquire relevância crítica.

Portugal deve alavancar e capitalizar a sua posição geográfica e os seus laços históricos com os países da CPLP, as nações Ibero-Americanas e os Estados costeiros da África Ocidental para fomentar parcerias estratégicas. Estas alianças podem ser instrumentais para estabelecer rotas de comunicação redundantes, promover padrões regionais de cibersegurança e desenvolver iniciativas conjuntas de formação e capacitação, reforçando um ecossistema digital mais seguro e resiliente em todo o espaço atlântico.

A valorização destes laços deve traduzir-se em iniciativas concretas e de alto impacto, tais como:

• A criação de um CERT Lusófono, uma estrutura para a partilha de inteligência sobre ameaças e resposta coordenada a incidentes no espaço da CPLP;

• A promoção de exercícios conjuntos de ciberdefesa com nações estratégicas como o Brasil, Espanha e os países costeiros de África, focados na proteção de infraestruturas marítimas e digitais partilhadas;

• O desenvolvimento de uma plataforma de diplomacia digital para a promoção de padrões de segurança e regulação tecnológica alinhados com os valores democráticos europeus.

Um exemplo é a cooperação entre Portugal e o Brasil no projeto EllaLink, que não se limita à infraestrutura física – podendo evoluir para iniciativas conjuntas de monitorização de tráfego e resposta a incidentes.

A construção de uma ciberdefesa coletiva exige, por isso, mais do que tecnologia: requer visão estratégica, gestão integrada e uma diplomacia proativa.

A segurança digital do futuro será, inequivocamente, um esforço coletivo, mútuo, descentralizado, integrado e contínuo. Portugal, ao reforçar a sua integração europeia, o seu compromisso atlântico e as suas alianças lusófonas e ibero-americanas, pode afirmar-se como um fornecedor sólido de cibersegurança no sistema internacional, contribuindo para uma arquitetura de defesa cibernética resiliente, credível e integrada a nível global.

O ciberespaço, enquanto novo domínio da soberania e da segurança, exige mais do que mera robustez tecnológica: requer visão estratégica, diplomacia dinâmica e ação coordenada.

Conclusões

A sua localização geográfica privilegiada, a posição central na conectividade atlântica e o papel cada vez mais decisivo na arquitetura das infraestruturas digitais críticas colocam Portugal diante de uma oportunidade histórica e de uma responsabilidade soberana: deixar de ser apenas um ponto de passagem e interligação de cabos submarinos e infraestruturas digitais para se afirmar como o centro nevrálgico da ciberdefesa estratégica da União Europeia no Atlântico.

Esta ambição não é meramente simbólica nem retórica – é uma exigência política, operacional e geoestratégica.

Não se trata de um título honorífico, mas sim de uma missão complexa e exigente que implica visão estratégica do Estado, investimento contínuo, reforço das capacidades

nacionais, maturidade institucional permanente e uma diplomacia digital assertiva, proativa e orientada para resultados.

Neste contexto, significa reconhecer que:

- A segurança digital não se limita a firewalls e criptografia – envolve também soberania territorial, proteção de cabos submarinos e defesa do espaço marítimo;

- As infraestruturas digitais são tão críticas quanto as redes elétricas e devem ser tratadas com idêntico grau de prioridade estratégica;

- A diplomacia digital é uma nova forma de projeção internacional, na qual Portugal detém vantagens únicas decorrentes da sua localização geográfica, da língua portuguesa e dos vínculos históricos que o ligam a diversos continentes.

A cibersegurança contemporânea ultrapassa o domínio técnico – exige controlo soberano de infraestruturas físicas e lógicas, proteção do espaço marítimo, capacidade de resposta eficaz a ameaças híbridas e articulação institucional robusta e coordenada.

A soberania digital é, hoje, indissociável da soberania territorial. Portugal, com a sua vasta Zona Económica Exclusiva e função estratégica nas redes globais de comunicação digital, deve assumir essa integração como trave-mestra da sua estratégia nacional.

O país precisa estabelecer uma arquitetura nacional integrada de comando e controlo, que inclua o GNS, o CNCS, as Forças Armadas, a ANACOM, os serviços de informação e os operadores críticos, operando sob uma lógica de ação coordenada e preventiva, capaz de responder aos novos domínios da guerra híbrida e da geopolítica digital.

Assumir este papel implica também um investimento contínuo na criação de centros de excelência em ciberdefesa no espaço atlântico, com especial foco nos Açores e na Madeira, promovendo e reforçando a integração entre os domínios marítimo e digital (CNCS, 2023)[45].

Esta criação não deve ser apenas desejável – deve ser prioritária. Estes polos devem reforçar a coordenação operacional com aliados europeus, atlânticos e lusófonos, posicionando Portugal como uma plataforma credível para operações conjuntas e resposta no espaço atlântico alargado.

A recente legislação europeia, nomeadamente a Diretiva NIS2 e o AI Act, oferece um quadro legal e normativo de referência, mas não é suficiente. A ciberdefesa não se edifica apenas com normas: as normas, por si só, não edificam fortalezas.

Como alerta Bruce Schneier, “security is not a product, but a process”[46], lembrando que a segurança digital eficaz não reside numa solução única ou documento regulatório, mas sim numa arquitetura viva de processos, pessoas e respostas articuladas.

Uma abordagem de cibersegurança baseada apenas em normas pode tornar-se numa

nova Linha Maginot digital: sólida na aparência, mas rígida; regulamentada, mas vulnerável; imponente, mas facilmente contornada.

Como alerta Lawrence Freedman, "a Linha Maginot simboliza as defesas que são cuidadosamente construídas para proteger o passado, mas que falham em enfrentar as ameaças do futuro"47, ressaltando a necessidade de uma postura flexível e adaptativa na ciberdefesa.

Construir uma postura estratégica de ciberdefesa exige muito mais do que um quadro regulamentar: impõe o reforço da cooperação institucional, agilidade estratégica, o desenvolvimento de capacidades operacionais tangíveis, mecanismos eficazes de coordenação em tempo real, partilha estruturada de inteligência estratégica e integração transversal da cibersegurança nas políticas públicas. Já não é suficiente reagir – é essencial antecipar, influenciar, moldar e liderar.

Num mundo onde as ameaças híbridas são cada vez mais difusas e persistentes, a geopolítica digital torna-se um novo campo de soberania – e Portugal está na linha da frente.

A sua posição central não pode limitar-se à mera contenção ou defesa: deve igualmente operar como vetor de projeção de valores, normas e alianças estratégicas. É neste teatro de operações que o soft power digital português – fundamentado na língua, na história, na diplomacia e na fiabilidade técnica – deve ser mobilizado como um instrumento de poder. Como observa Joseph Nye, "*soft power é a capacidade de influenciar outros por meio da atração e da persuasão, em vez do uso da força ou coerção*"48, realçando a importância da diplomacia digital como ferramenta estratégica. Assumir o comando da arquitetura da ciberdefesa atlântica exige não só proteger as linhas de comunicação e os fluxos, mas também moldar o rumo da transformação digital global, consolidando Portugal como uma potência digital de confiança no âmbito da União Europeia e além-fronteiras.

Portugal enfrenta, pois, um desafio: continuar como nó periférico de uma rede controlada por outros ou afirmar-se como potência digital estratégica, atlântica e segura, tornando-se o ponto nuclear da ciberdefesa no Atlântico, e o pilar da resiliência digital europeia, onde soberania, segurança e poder digital se cruzam. Trata-se de uma missão que depende de tecnologia, de estratégia, e, acima de tudo, de vontade política e da capacitação do seu maior ativo: as pessoas49.

Num contexto global em que os cabos submarinos funcionam como as artérias vitais do poder estratégico e os dados se tornam o recurso essencial da soberania, Portugal enfrenta uma decisão crítica: não pode limitar-se a ser uma linha defensiva estática, mas deve posicionar-se como força avançada, preparada para liderar operações de ciberdefesa e garantir o controlo proativo das infraestruturas estratégicas. Portugal não pode ser trincheira – tem de ser vanguarda.

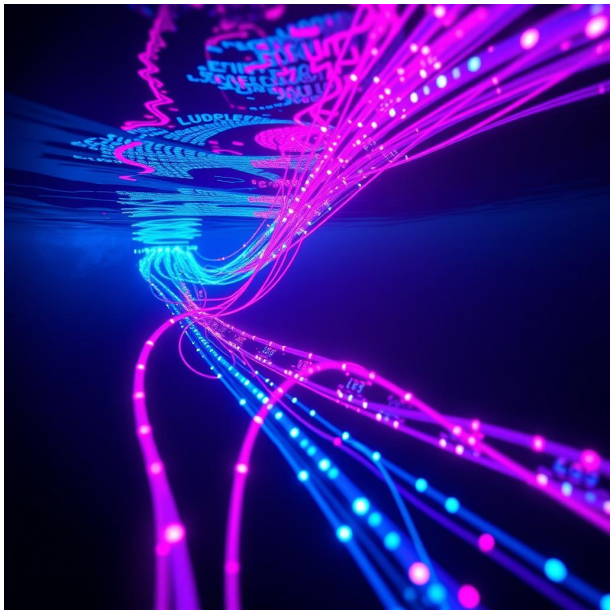

Figura 4 – A Vanguarda Digital Atlântica: o fluxo estratégico do poder. Esta imagem simboliza a missão de Portugal: transcender seu papel tradicional como mero nó de infraestruturas para se transformar em um protagonista ativo na modelagem dos fluxos de dados, inteligência e influência no Atlântico. A soberania digital deixa de ser uma postura defensiva e estática para se tornar uma capacidade dinâmica de projetar poder, liderança e inovação na vanguarda da geopolítica digital. Portugal afirma-se, assim, como uma potência emergente, capaz de comandar e influenciar os rumos estratégicos da nova era atlântica.

Ad victoriam et imperium.

Referências Bibliográficas

Agência da União Europeia para a Cibersegurança (ENISA). (2023). Panorama de ameaças da ENISA 2023. ENISA.

Autoridade Nacional de Comunicações (ANACOM). (2024). Relatório sobre o desenvolvimento de data centers em Portugal. ANACOM.

Bernardino, L. (2022). A geoestratégia do Atlântico na era digital. In A. Marques (Ed.), Segurança, defesa e o ciberespaço (pp. 45-62). Edições Sílabo.

Centro Nacional de Cibersegurança. (2024). Riscos & conflitos: Relatório 2023. https://www.cncs.gov.pt/recursos/reports-e-avisos/

Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas para um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) nº 910/2014 e a Diretiva (UE) 2018/1972 e que revoga a Diretiva (UE) 2016/1148 (Diretiva NIS 2). Jornal Oficial da União Europeia, L 333/80.

EllaLink. (2021). Conectando continentes: Relatório do projeto de cabo EllaLink. https://www.ellalink.com

Fórum Económico Mundial. (2024). Perspectivas globais de segurança cibernética 2024. https://www.weforum.org

Fórum Nacional de Cibersegurança. (2023). Estudo sobre o défice de talento em cibersegurança em Portugal. https://www.fnc.gov.pt

Freedman, L. (2013). Estratégia: Uma história. Imprensa da Universidade de Oxford.

Guedes, A. M. (2012). A soberania no pós-guerra fria: Teoria e práxis. Almedina.

Nye, J. S., Jr. (2004). Soft power: Os meios para o sucesso na política mundial. Relações Públicas.

Organização do Tratado do Atlântico Norte (NATO). (2022). Conceito estratégico da NATO 2022. https://www.nato.int

Organização do Tratado do Atlântico Norte (NATO). (2023). Relatório pós-ação da Cyber Coalition 2023. https://www.nato.int

Parker, E. (2024). A nova linha de frente: O poder cibernético e a geopolítica do século 21. Imprensa Pinguim.

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que estabelece regras harmonizadas em matéria de inteligência artificial e altera os Regulamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2006/42/CE, 2014/30/UE e 2014/53/UE (Regulamento Inteligência Artificial). Jornal Oficial da União Europeia, L 2024/1689.

República Portuguesa. (2024). Resolução do Conselho de Ministros n.º 43/2024, de 2 de abril de 2024. Aprova a Estratégia Nacional de Segurança do Ciberespaço 2024-2030. Diário da República, n.º 65/2024, Série I.

Schneier, B. (2000). Segredos e mentiras: Segurança digital em um mundo em rede. John Wiley & Sons. https://www.schneier.com/books/secrets-and-lies

Taleb, N. N. (2007). O cisne negro: O impacto do altamente improvável. Casa Aleatória.

---

* Trabalho Final realizado no âmbito da Pós-Graduação em Gestão de Cibersegurança | Nova SBE (2024-2025).

1 União Europeia. (2022). Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível

comum de cibersegurança em toda a União (reformulação). Jornal Oficial da União Europeia, L 333, 80-152. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2555 União Europeia. (2022). *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (reformulação)*. Jornal Oficial da União Europeia, L 333, 80-152. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2555

2 Comissão Europeia. (2021). Proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de inteligência artificial (Lei da Inteligência Artificial) e que altera determinados atos legislativos da União (COM/2021/206 final). https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206

3 República Portuguesa. (n.d.). Estratégia Digital Nacional (EDN). A EDN estabelece a visão nacional para a transformação digital até 2030, integrada no Plano de Ação para a Transição Digital. Define prioridades em cibersegurança, capacitação digital, administração pública digital e economia baseada em dados. https://www.transformacao-digital.pt

4 ENISA – Agência da União Europeia para a Cibersegurança. (2023). Threat Landscape Report & Strategic Outlook. A Agência publica anualmente este relatório, detalhando tendências, riscos emergentes e recomendações estratégicas para os Estados-Membros. Defende uma abordagem holística e partilhada da segurança digital na Europa. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

5 Autoridade Nacional de Comunicações (ANACOM). (n.d.). Cabos Submarinos de Comunicações (CSs). Representam a espinha dorsal do tráfego global de dados. Portugal possui mais de uma dezena de cabos ativos e previstos, incluindo ligações com África, América do Sul e Europa. A ANACOM disponibiliza mapas e informação técnica sobre os cabos que chegam ao território nacional. https://www.anacom.pt/render.jsp?contentId=1180515

6 Atlantis Data Center. (n.d.). Data Centers e Investimentos nos Açores. Projetos como o do "Atlantis Data Center" visam tirar partido da localização privilegiada dos Açores para criar hubs de dados seguros e resilientes, com baixa latência transatlântica. Atlantis Sea Cable System. https://www.atlantis-dc.com

7 EllaLink. (2021). Cabo submarino de alta capacidade que liga diretamente a Europa (Sines) ao Brasil (Fortaleza), reduzindo a latência transatlântica e reforçando a soberania digital da UE ao evitar rotas que passam pelos EUA. Site oficial do projeto EllaLink:

https://www.ellalink.com

8 ENISA – Agência da União Europeia para a Cibersegurança. (2023). Threat Landscape Report & Strategic Outlook. De acordo com a ENISA e a OCDE, cerca de 95% a 97% do tráfego internacional de dados circula por cabos submarinos, tornando-os ativos críticos de infraestrutura global. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

9 Direção-Geral de Política do Mar (DGPM). (n.d.). Zona Económica Exclusiva (ZEE) portuguesa. Portugal detém a maior Zona Económica Exclusiva da União Europeia, com cerca de 1,7 milhões de km². Este espaço inclui responsabilidades em matéria de segurança marítima, recursos e infraestruturas subaquáticas. https://www.dgpm.gov.pt

10 Agência Europeia da Segurança Marítima (EMSA). (n.d.). Sobre a EMSA. Sediada em Lisboa, a EMSA apoia os Estados-Membros na segurança marítima, proteção ambiental e vigilância das rotas marítimas e infraestruturas sensíveis. https://www.emsa.europa.eu

11 Estado-Maior da Armada. (n.d.). Capacidades operacionais da Marinha Portuguesa. A Marinha opera em estreita articulação com a NATO e entidades civis no âmbito da proteção de cabos submarinos, vigilância costeira e segurança de infraestruturas marítimas. https://www.marinha.pt

12 NATO. (2023). NATO statement on Baltic cable damage. Casos recentes, como o incidente nos cabos entre a Finlândia e a Estónia, evidenciam a vulnerabilidade de infraestruturas subaquáticas a ataques híbridos. https://www.nato.int

13 Bernardino, L. (2022). Geopolítica do Atlântico e segurança global. Instituto da Defesa Nacional. https://www.idn.gov.pt/publicacoes/geopolitica-do-atlantico-e-seguranca-global

14 Submarine Cable Map. (n.d.). SAT-3/WASC/AMC: Sistema de cabos submarinos ligando Portugal a África Ocidental e Brasil. https://www.submarinecablemap.com

15 2Africa Cable System. (n.d.). Projetos de cabos ACE, WACS e 2Africa ligando Europa e África. Detalhes do projeto 2Africa disponíveis em https://www.2africacable.net

16 ENISA – Agência da União Europeia para a Cibersegurança. (2023). Threat Landscape Report & Strategic Outlook. A ENISA identifica a necessidade de centros de monitorização regionais e nacionais para resposta rápida a incidentes de cibersegurança em redes transfronteiriças.

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

17 Start Campus. (n.d.). Sines Data Center Park: projeto de infraestrutura hiperescala. Projeto planeado para cobrir 495 MW em Sines, aproveitando a proximidade ao cabo EllaLink e a disponibilidade energética. Uma das maiores iniciativas do género na Península Ibérica. https://www.startcampus.pt

18 World Data Center Madeira. (n.d.). Atlantic Hub – WDC Madeira: projeto de data center resiliente. Localizado na Madeira, apoiado pelo Governo Regional, e parte de uma rede atlântica de dados. https://www.wdc-madeira.com

19 Amazon Web Services (AWS). (n.d.). Investimentos em Portugal e sul da Europa. Empresas como Microsoft, AWS e Google reforçam presença devido à posição geográfica e estabilidade regulatória.

20 Uptime Institute. (n.d.). Global Data Center Survey: critérios de localização. Principais fatores incluem acesso a cabos submarinos, clima ameno, fontes renováveis e baixo risco sísmico/inundação. https://uptimeinstitute.com

21 International Organization for Standardization (ISO). (n.d.). ISO/IEC 27001 – Informação de segurança e certificações. Inclui certificações ISO/IEC 27001, Tier III/IV Uptime Institute, compromissos com energia limpa, PUE baixo e neutralidade carbónica. https://www.iso.org/isoiec-27001-information-security.html

22 ANACOM – Autoridade Nacional de Comunicações. (2024). Relatório sobre o estado das comunicações eletrónicas em Portugal. O relatório destaca o crescimento dos data centers certificados Tier III e IV, alinhado com a estratégia de transformação digital e atração de investimentos tecnológicos em Portugal. https://www.anacom.pt/render.jsp?contentId=1737020

23 Submarine Cable Map. (n.d.). Estações de cabos submarinos em Portugal: Sines, Carcavelos, Açores e futuro Sesimbra. Pontos-chave de amarração para cabos como EllaLink, Equiano e 2Africa. https://www.submarinecablemap.com

24 IP Telecom. (n.d.). Modernização do backbone terrestre nacional de fibra e IP/MPLS. Promovida por operadores como Altice, NOS e IP Telecom. https://www.iptel.pt/pt

25 União Europeia. (2023). Programa IRIS²: sistema europeu de satélites seguros. Projetos como IRIS² e o envolvimento da Portugal Space reforçam a importância das

comunicações via satélite para redundância e resiliência. https://defence-industry-space.ec.europa.eu/eu-secure-connectivity-programme-iris2_en

26 European Union Agency for Cybersecurity (ENISA). (n.d.). Coordenação em cibersegurança na UE. Lidera a resposta a ciberameaças na UE. CNCS atua nacionalmente com planos de contingência e resposta a incidentes críticos. NATO promove exercícios conjuntos como o Cyber Coalition ENISA (https://www.enisa.europa.eu); CNCS (https://www.cncs.gov.pt); NATO Cyber Defence (https://www.nato.int/cps/en/natolive/topics_78170.htm); e NATO Cyber Defence (https://www.nato.int/cps/en/natolive/topics_78170.htm)

27 Advania. (n.d.). Modelo híbrido islandês de centros de dados sustentáveis. Centros alimentados por energia geotérmica com capacidades de soberania digital adaptadas ao Ártico; citados em relatórios da ENISA e OCDE – ENISA Threat Landscape Report 2023 (https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023) e Advania (https://www.advania.com)

28 IDA Ireland. (n.d.). Irlanda como hub digital europeu. Abriga mais de 70% dos data centers hiperescala da UE, com política fiscal atrativa, rede de cabos submarinos e estabilidade política. Modelo é referência na literatura de planeamento digital. https://www.idaireland.com

29 Organisation for Economic Co-operation and Development (OECD). (2022). Digital Economy Outlook 2022: impacto económico dos investimentos digitais. Estima-se que infraestruturas digitais possam representar 1,5% a 3% do PIB em crescimento acumulado a médio prazo. https://www.oecd.org/digital

30 (ISC)². (2023). Cybersecurity Workforce Study 2023: escassez de talento na UE. UE enfrenta um défice de cerca de 500.000 profissionais qualificados em cibersegurança, incluindo Portugal. https://www.isc2.org

31 European Union Agency for Cybersecurity (ENISA). (2023). NIS2 Directive overview. Documento que detalha as principais mudanças trazidas pela Diretiva NIS2, incluindo o alargamento dos setores críticos abrangidos e as exigências reforçadas em gestão de riscos, incidentes e cooperação internacional, com foco na proteção de infraestruturas digitais essenciais, como cabos submarinos e data centers. Disponível em: https://www.enisa.europa.eu/topics/nis-directive

32 Computer Emergency Response Team for the EU Institutions (CERT-EU). (2023). Relatório anual sobre operações e cooperação. Relatório que destaca as atividades de monitorização, resposta e cooperação entre as instituições europeias, NATO e Estados-

Membros para fortalecer a segurança cibernética integrada. Disponível em: https://cert.europa.eu/cert-en/operations/

33 European Commission. (2024). Artificial Intelligence Act – regulatory framework for AI. Documento da Comissão Europeia que propõe a regulamentação do uso da inteligência artificial, classificando sistemas de IA por níveis de risco e impondo obrigações rigorosas para aplicações em setores críticos, garantindo transparência, ética e proteção contra usos abusivos. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

34 Conselho Nacional de Segurança. (2024). Estratégia Digital Nacional – plano de cibersegurança e defesa. Documento estratégico que define a visão e as ações prioritárias para a proteção das infraestruturas críticas, desenvolvimento de capacidades tecnológicas soberanas e reforço da cooperação internacional no domínio da cibersegurança em Portugal. Disponível em: https://www.cnseguranca.pt/estrategia-digital-nacional

35 Parker, E. (2024). The new frontline: Cybersecurity and global power. Foreign Affairs. Discussão sobre o papel da cibersegurança na geopolítica global.

36 CERT.PT. (2023). Relatório anual de cibersegurança. Destaca a evolução das ameaças híbridas e cibernéticas a atores estatais e não-estatais, com ênfase na crescente centralidade digital de Portugal. Disponível em: https://www.cert.pt/relatorios/2023

37 European Commission. (2024). Artificial Intelligence Act – Regulatory framework for AI. Estabelece requisitos para sistemas de IA de alto risco, incluindo transparência, supervisão e ética, visando mitigar riscos à soberania digital. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

38 CERT.PT. (2023). Situação de incidentes em infraestruturas críticas – análise quantitativa. Revela um aumento de 67% nos eventos relatados em 2023, sublinhando a necessidade de respostas operacionais integradas. Disponível em: https://www.cert.pt/estatisticas/infraestruturas-criticas/2023

39 Taleb, N. N. (2007). The black swan: The impact of the highly improbable. Random House.

40 Guedes, A. M. (2022). Geopolítica das infraestruturas críticas: Redes, poder e soberania no século XXI. Lisboa: Instituto da Defesa Nacional. Disponível em: https://www.idn.gov.pt/publicacoes/geopolitica-infraestruturas-criticas

41 ENISA. (2023). Threat Landscape Report – International & Hybrid Threats. Analisa a natureza global das ciberameaças, destacando que nenhuma nação isolada está imune, e propõe modelos de resposta integrada. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

42 UNODA. (2023). Public private cooperation in cybersecurity: A European perspective. Examina a importância da colaboração entre setor público e privado para enfrentar ameaças híbridas e fortalecer a resiliência coletiva. Disponível em: https://www.un.org/disarmament/cybersecurity

43 CERT-EU. (2023). Roles and cooperation mechanisms. Descreve como o CERT-EU atua com Estados-Membros e agentes nacionais como o CERT.PT para resposta coordenada a ciberincidentes transfronteiriços. Disponível em: https://cert.europa.eu/cert-en/

44 NATO. (2023). Cyber Coalition Exercise – Annual Summary Report. Documento que explica o exercício "Cyber Coalition 2023", destacando a participação portuguesa e os resultados obtidos no ensaio de resposta a ataques coordenados. Disponível em: https://www.nato.int/cps/en/natohq/news

45 CNCS. (2023). Relatório anual de cibersegurança de Portugal. Documento que destaca a necessidade de centros regionais de ciberdefesa e coordenação entre entidades nacionais e internacionais, com recomendações específicas para os Açores e a Madeira. Disponível em: https://www.cncs.gov.pt/relatorio-anual

46 Schneier, B. (2000). Secrets and lies: Digital security in a networked world. Wiley. Obra fundamental sobre segurança digital e desafios em redes conectadas globalmente. https://www.schneier.com/books/secrets-and-lies

47 Freedman, L. (2013). Strategy: A history. Oxford University Press. Análise abrangente da evolução do pensamento estratégico ao longo da história.

48 Nye, J. (2004). Soft power: The means to success in world politics. PublicAffairs. Introduz o conceito de "soft power" e seu papel nas relações internacionais contemporâneas.

49 ENISA. (2023). ENISA Threat Landscape Report 2023. Destaca o papel central dos cabos submarinos como infraestruturas críticas e alerta para o novo paradigma da geopolítica digital, onde o controlo dos fluxos de dados é uma questão de soberania. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023