A CPLP 3.0: Inteligência Artificial e Cibersegurança como Novos Domínios da Cooperação Lusófona*

Paulo Henrique Montini dos Santos Ribeiro
Membro do grupo SOCIATOS (Sociabilidades e Conflitos Contemporâneos) – UFCG.

José Almir da Luz Júnior
Laboratório de Estudos e Pesquisas em Direito Internacional Ambiental (LEPADIA).

Resumo

A emergência do ciberespaço como domínio operacional constitui simultaneamente uma oportunidade e um desafio para os Estados-membros da Comunidade dos Países de Língua Portuguesa (CPLP). O presente artigo argumenta que a partilha linguística representa um ativo estratégico singular para a construção de capacidades conjuntas em cibersegurança e inteligência artificial (IA), conferindo ao espaço lusófono uma vantagem competitiva diante de outras comunidades linguísticas. Partindo de uma análise crítica do estado atual da cooperação no ciberespaço na CPLP, identifica-se um conjunto de lacunas estruturais que comprometem a eficácia da resposta coletiva às ciberameaças transnacionais. Propõe-se um modelo integrado de cooperação designado "CPLP 3.0", baseado em quatro pilares: (i) um Centro de Cibersegurança Lusófono; (ii) uma Academia de Ciberdefesa comum; (iii) um laboratório de IA em Português; (iv) e um quadro normativo harmonizado. Portugal, por sua inserção em estruturas europeias e atlânticas e pelo capital relacional acumulado no espaço lusófono, surge como catalisador natural dessa arquitetura de cooperação. Analisa-se ainda o caso particular da Guiné Equatorial, cuja adesão à CPLP em 2014 representa uma oportunidade estratégica para a expansão da língua portuguesa e o aprofundamento da cooperação no Golfo da Guiné.

Palavras-chave: Ciberespaço; CPLP; IA; PALOP.

* Este artigo está redigido na norma linguística do português do Brasil (PB).

Abstract

The emergence of cyberspace as an operational domain presents both opportunities and challenges for the member states of the Community of Portuguese Language Countries (CPLP). This article argues that linguistic sharing represents a unique strategic asset for building joint capabilities in cybersecurity and artificial intelligence (AI), giving the Lusophone space a competitive advantage over other linguistic communities. Based on a critical analysis of the current state of cyberspace cooperation in the CPLP, a set of structural gaps that compromise the effectiveness of the collective response to transnational cyber threats is identified. An integrated cooperation model designated "CPLP 3.0" is proposed, based on four pillars: (i) a Lusophone Cybersecurity Centre; (ii) a common Cyberdefense Academy; (iii) a Portuguese Language AI Laboratory; and (iv) a harmonized normative framework. Portugal, due to its integration in European and Atlantic structures and the relational capital accumulated in the Lusophone space, emerges as a natural catalyst for this cooperation architecture. The particular case of Equatorial Guinea is also analyzed, whose accession to the CPLP in 2014 represents a strategic opportunity for the expansion of the Portuguese language and the deepening of cooperation in the Gulf of Guinea.

Keywords: *AI; CPLP; cyberspace; Lusophone PALOP.*

https://doi.org/10.47906/ND2026.173.01

Introdução

A revolução tecnológica que marca as primeiras décadas do século XXI redesenha profundamente os contornos da segurança internacional. O ciberespaço, reconhecido como o "quinto domínio" das operações militares pela OTAN (Organização do Tratado do Atlântico Norte) em 2016, tornou-se simultaneamente um teatro de conflito e um multiplicador de ameaças tradicionais, do terrorismo ao crime organizado transnacional (Kello, 2017). Nesse contexto, garantir a segurança das infraestruturas que sustentam o ciberespaço tornou-se um imperativo estratégico. Isso vale para o desenvolvimento de tecnologias soberanas, especialmente no campo da inteligência artificial, condição cada vez mais relevante para a preservação da autonomia estatal no sistema internacional contemporâneo.[1]

Para os países de língua portuguesa, essa transformação traz uma oportunidade singular. Pela primeira vez na história, a partilha de um idioma comum transcende a dimensão meramente cultural ou diplomática para se tornar um ativo estratégico operacional. Num domínio no qual a velocidade de comunicação, a confiança entre parceiros e a capacidade de compartilhar informações sensíveis são determinantes, a homogeneidade linguística oferece vantagens competitivas que outras potências – a China, a Rússia ou mesmo a França e a Turquia – dificilmente conseguem replicar junto dos Estados lusófonos (Moreira, 2020).

A Comunidade dos Países de Língua Portuguesa (CPLP), que em 2026 celebra três décadas de existência, tem vindo a consolidar, de forma progressiva, mecanismos de cooperação em diversos domínios, entre os quais se destaca a defesa.[2] A adesão da Guiné Equatorial em 2014 – único país membro em que o português não constitui a língua materna predominante – evidencia o potencial de alargamento e de afirmação da comunidade lusófona e levanta questões pertinentes sobre o papel da língua portuguesa como vetor de integração regional no Golfo da Guiné.[3] Contudo, o ciberespaço permanece amplamente inexplorado como vetor de cooperação estruturada. Essa lacuna é ainda mais significativa considerando que os Estados-membros enfrentam ciberameaças crescentes – do cibercrime financeiro que afeta economias frágeis às campanhas de desinformação que ameaçam processos democráticos – sem dispor de capacidades de resposta proporcionais ou de mecanismos eficazes de assistência mútua.

1 União Europeia (2019) *Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação.* Jornal Oficial da União Europeia.

2 Comunidade dos Países de Língua Portuguesa (1996) Declaração Constitutiva da Comunidade dos Países de Língua Portuguesa. Lisboa, 17 de julho.

3 Comunidade dos Países de Língua Portuguesa (2014) *Resolução sobre a Adesão da República da Guiné Equatorial à Comunidade dos Países de Língua Portuguesa.* Díli, 23 de julho de 2014.

O presente artigo busca responder à seguinte pergunta de investigação: de que forma Portugal pode liderar uma estratégia integrada de cibersegurança e inteligência artificial no espaço lusófono, transformando a partilha linguística em vantagem competitiva diante de outras potências? Para responder a essa questão, adota-se uma metodologia qualitativa baseada na análise documental de fontes primárias, incluindo legislação nacional e instrumentos jurídicos da CPLP, e na revisão crítica da literatura especializada em cibersegurança, relações internacionais e cooperação lusófona. O artigo estrutura-se em cinco secções principais: após esta introdução, procede-se ao enquadramento teórico que sustenta a análise; segue-se um diagnóstico do estado atual da cooperação no ciberespaço na CPLP; examina-se posteriormente o papel de Portugal como potencial catalisador; apresentam-se propostas concretas para uma estratégia integrada; e, finalmente, discutem-se os desafios e formulam-se as considerações finais.

Importa sublinhar que o presente artigo adota a terminologia consolidada na doutrina estratégica, distinguindo rigorosamente o ciberespaço – enquanto domínio operacional – dos conceitos de digital (codificação binária), virtual (categoria ontológica) e informacional (fluxos de dados e dimensão cognitiva). Essa precisão terminológica, frequentemente negligenciada na literatura não especializada, reveste-se de importância analítica, visto que cada conceito remete a problemáticas e respostas políticas distintas.

A relevância deste estudo justifica-se não somente pela atualidade do tema, mas também pela escassez de produção acadêmica que articule, de forma sistemática, as questões da cibersegurança e da inteligência artificial com as dinâmicas específicas da cooperação lusófona. Pretende-se, assim, contribuir para o debate estratégico em curso e oferecer pistas concretas aos decisores políticos dos Estados-membros da CPLP.[4]

1. Enquadramento teórico-conceptual

1.1. O ciberespaço como domínio estratégico

O conceito de cibersegurança evoluiu significativamente desde as primeiras formulações, centradas na proteção de sistemas informáticos, até às conceituações contemporâneas que o enquadram como dimensão fundamental da segurança nacional e internacional (Nye, 2011). Essa evolução reflete, por um lado, a crescente dependência dos Estados face a infraestruturas que sustentam o espaço cibernético e a

4 Portugal (2019) *Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023.*

proliferação de agentes, estatais ou não estatais, capazes de explorar vulnerabilidades e sensibilidades nesse domínio para fins hostis, políticos e económicos (Krepinevich, 2012).

Cabe aqui uma distinção conceptual importante. O ciberespaço constitui um domínio operacional, designadamente o ambiente formado por redes interdependentes de infraestruturas de tecnologia da informação, incluindo a Internet, redes de telecomunicações e sistemas computacionais. Distingue-se, portanto, do conceito de digital, que se refere especificamente à codificação binária da informação, ou seja, à representação de dados em sequências de zeros (0) e uns (1). Embora as infraestruturas do ciberespaço sejam predominantemente digitais, os termos não são sinônimos: o ciberespaço é um domínio estratégico de atuação, ao passo que o digital é uma característica técnica de codificação. Da mesma forma, o termo informacional remete aos fluxos de dados e à dimensão cognitiva das operações, incluindo a guerra de informação, constituindo categoria analítica distinta das anteriores.[5]

A literatura identifica três características distintivas do ciberespaço que o diferenciam dos teatros tradicionais de conflito (Libicki, 2009). A primeira delas é a assimetria estrutural, pela qual atores com recursos limitados podem infligir danos significativos a adversários tecnologicamente superiores, reduzindo as barreiras de entrada no campo da conflitualidade internacional (Devanny e Stevens 2024). A segunda característica consiste no problema da atribuição, ou seja, a dificuldade em identificar inequivocamente a origem de um ataque cibernético, complicando a aplicação dos mecanismos tradicionais de dissuasão e resposta (Hoffman, 2007). A terceira diz respeito à velocidade operacional, uma vez que os ataques cibernéticos se desenvolvem numa escala temporal que frequentemente ultrapassa a capacidade de reação das estruturas de decisão convencionais (Grant, 2008).[6]

Para os países em desenvolvimento – categoria que abrange a maioria dos Estados-membros da CPLP, com exceção de Portugal e, em certa medida, do Brasil – essas características traduzem-se em vulnerabilidades acrescidas. A rápida informatização de serviços públicos e sistemas financeiros, frequentemente desacompanhada de investimentos proporcionais em segurança, cria superfícies de ataque extensas e mal protegidas. Ao mesmo tempo, a escassez de recursos humanos qualificados e a dependência de tecnologias estrangeiras limitam a capacidade de resposta autônoma a incidentes (Calandro e Berglund, 2019).

5 A distinção entre ciberespaço, digital, virtual e informacional é desenvolvida em Libicki (2009) e consolidada em documentos doutrinários da OTAN. O ciberespaço é definido como domínio operacional; digital refere-se à codificação binária; informacional remete aos fluxos de dados e à dimensão cognitiva das operações.

6 União Europeia (2016) *Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir elevado nível comum de segurança das redes e da informação em toda a União (Diretiva NIS).*

O reconhecimento do ciberespaço como "quinto domínio" pela OTAN, em 2016, formalizou uma realidade que a prática internacional já evidenciava: os ataques cibernéticos podem constituir atos de guerra e, como tal, justificar respostas no âmbito da defesa coletiva.[7] Esse desenvolvimento doutrinário tem implicações significativas para Estados que, como os membros da CPLP, não integram a Aliança Atlântica, mas mantêm relações de cooperação com países que dela fazem parte.

1.2. A língua como ativo estratégico

A literatura sobre *soft power* tem tradicionalmente enfatizado a dimensão cultural e diplomática das línguas internacionais (Nye, 2004). Contudo, no contexto específico da cibersegurança e da inteligência artificial, a partilha linguística assume uma relevância operacional que transcende essas funções convencionais.

A homogeneidade linguística facilita, em primeiro lugar, o compartilhamento de informações sensíveis entre serviços de *intelligence* e centros de resposta a incidentes. Num domínio no qual a velocidade de comunicação pode determinar a eficácia da resposta a uma ameaça, a eliminação de barreiras linguísticas representa uma vantagem competitiva significativa. Diferentemente do que ocorre em fóruns multilaterais genéricos, nos quais a tradução é prática rotineira, a cooperação em cibersegurança exige frequentemente comunicação em tempo real e acesso a documentação técnica que perderia precisão se traduzida (Klimburg, 2012).

Em segundo lugar, o desenvolvimento de tecnologias de inteligência artificial – particularmente no campo do processamento de linguagem natural – depende criticamente da disponibilidade de comandos linguísticos de qualidade. A língua portuguesa, falada por mais de 250 milhões de pessoas em quatro continentes, constitui um mercado linguístico de dimensão suficiente para justificar investimentos em pesquisa e desenvolvimento. Contudo, a fragmentação dos esforços entre os países lusófonos tem resultado numa sub-representação do português no panorama global da IA, comparativamente a línguas com número semelhante ou inferior de falantes (Pires et al., 2019).[8]

Em terceiro lugar, a partilha linguística potencializa a formação conjunta de recursos humanos especializados. Num contexto de escassez global de profissionais de cibersegurança, a possibilidade de desenvolver programas de formação em português, acessíveis sem barreiras linguísticas a nacionais de nove países, representa economia de escala com implicações estratégicas significativas.

7 NATO (2016) Warsaw Summit Communiqué, 8-9 de julho, para. 70. Reconhecimento do ciberespaço como domínio de operações.

8 Portugal (2021) Decreto-Lei n.º 65/2021, de 30 de julho, que estabelece o regime jurídico da segurança do ciberespaço.

1.3. O caso particular da Guiné Equatorial

A adesão da Guiné Equatorial à CPLP, formalizada na Cimeira de Díli em 2014, constitui um caso singular que merece análise aprofundada no contexto da cooperação lusófona no ciberespaço.[9] Trata-se do único Estado-membro no qual o português não é a língua materna da maioria da população, embora tenha sido adotado como terceira língua oficial, ao lado do espanhol e do francês.[10]

A singularidade equato-guineense reside em múltiplos fatores. Do ponto de vista histórico, o território da atual Guiné Equatorial – compreendendo a região continental de Río Muni e a ilha de Bioco (antiga ilha de Fernando Pó) – esteve sob soberania portuguesa entre 1471 e 1778, quando foi cedido à Espanha pelo Tratado de El Pardo.[11] Esse legado histórico, ainda que distante, confere uma legitimidade simbólica à presença da Guiné Equatorial no espaço lusófono que transcende considerações meramente pragmáticas.

Do ponto de vista geopolítico, a Guiné Equatorial ocupa uma posição estratégica no Golfo da Guiné, região que concentra reservas significativas de hidrocarbonetos e enfrenta desafios crescentes de segurança marítima, incluindo pirataria e tráfico ilícito. A sua integração na arquitetura de cooperação lusófona poderia facilitar a articulação entre os PALOP do Golfo da Guiné – São Tomé e Príncipe, especialmente – e estruturas regionais mais amplas, como a Comissão do Golfo da Guiné.[12]

No domínio específico da cibersegurança, a Guiné Equatorial apresenta um perfil particular. A economia petrolífera gerou recursos financeiros que permitiram investimentos significativos em infraestruturas de telecomunicações, conferindo ao país um nível de conectividade superior ao de vários PALOP. Entretanto, a dependência de tecnologia estrangeira – predominantemente chinesa e europeia – e a escassez de recursos humanos qualificados criam vulnerabilidades que poderiam ser mitigadas através da cooperação lusófona.

A promoção da língua portuguesa na Guiné Equatorial, compromisso assumido quando da adesão à CPLP, abre perspetivas interessantes para a cooperação no ciberespaço.[13] A formação de quadros equato-guineenses em cibersegurança, utilizando o português como língua de instrução, poderia simultaneamente reforçar as

9 Comunidade dos Países de Língua Portuguesa (2014) *Resolução sobre a Adesão da República da Guiné Equatorial à Comunidade dos Países de Língua Portuguesa*. Díli.

10 Guiné Equatorial (2012) *Ley Fundamental de Guinea Ecuatorial (Constitución)*, artigo 4.º. Alterações que consagraram o português e o francês como línguas co-oficiais.

11 Espanha e Portugal (1778) *Tratado Preliminar de Límites en América Meridional entre España y Portugal (Tratado de El Pardo)*, 11 de março.

12 Comissão do Golfo da Guiné (2001) *Tratado da Comissão do Golfo da Guiné*. Libreville, 3 de julho.

13 Nações Unidas, Conselho de Direitos Humanos (2017) *Report of the Special Rapporteur on the situation of human rights defenders on his mission to Equatorial Guinea*, A/HRC/34/52/Add.2.

capacidades nacionais e consolidar os laços com a comunidade lusófona. Iniciativas como a criação de um centro de formação técnica em Malabo, com o apoio de Portugal e do Brasil, permitiriam materializar essa visão.

Importa, contudo, reconhecer os desafios que essa integração enfrenta. A situação dos direitos humanos no país tem sido objeto de críticas por parte de organizações internacionais, suscitando reservas quanto ao aprofundamento de certas dimensões da cooperação.[14] O compartilhamento de informações sensíveis em matéria de cibersegurança exige níveis de confiança mútua que se constroem progressivamente e que dependem, em última instância, da convergência em torno de valores fundamentais.

Não obstante essas reservas, o potencial estratégico da Guiné Equatorial para a comunidade lusófona permanece significativo. A sua posição como ponte entre o espaço lusófono e o espaço hispanófono, na África Central, a disponibilidade de recursos financeiros e a vontade política demonstrada em promover a língua portuguesa constituem ativos que não devem ser negligenciados. Uma estratégia inteligente de cooperação no ciberespaço deveria contemplar mecanismos diferenciados que permitam à Guiné Equatorial participar progressivamente nas iniciativas lusófonas, à medida que se consolidem os requisitos de confiança e a capacidade institucional.

1.4. Modelos de cooperação multilateral no ciberespaço

A análise comparada oferece pontos relevantes para a conceituação de uma estratégia lusófona de cooperação no ciberespaço. A *Commonwealth*, que agrupa 56 Estados, com uma população cuja soma ascende a 2,5 bilhões de pessoas, desenvolveu desde 2002 abordagem estruturada à cibersegurança, consubstanciada na *Commonwealth Cybergovernance Model* (CCM) e em programas de assistência técnica aos Estados-membros menos desenvolvidos (*Commonwealth Secretariat*, 2020). A criação do *Commonwealth Cybercrime Initiative* (CCI), em 2014, ilustra a possibilidade de articular esforços entre países com níveis de desenvolvimento muito díspares, em torno de objetivos comuns de segurança no ciberespaço.

A Organização Internacional da Francofonia (OIF), por sua vez, tem privilegiado uma abordagem centrada na soberania e no desenvolvimento de conteúdos em língua francesa, com menor ênfase nas dimensões securitárias. A *Stratégie de la Francophonie Numérique*, adotada em 2012 e atualizada em 2022, estabelece objetivos ambiciosos em matéria de literacia e governança da Internet, mas revela lacunas significativas no que se refere à cooperação em ciberdefesa (OIF, 2022).

14 Comunidade dos Países de Língua Portuguesa (2018) *Plano de Ação de Lisboa para a Promoção, Difusão e Projeção da Língua Portuguesa*. Lisboa, 17 de julho.

A União Africana constitui uma referência incontornável para os PALOP e para a Guiné Equatorial, funcionando como principal enquadramento regional para seis dos dez Estados-membros e Estados com o *status* de observadores da CPLP no continente africano. A Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais, adotada em Malabo em 2014, coincidentemente na capital equato-guineense, estabelece um quadro normativo ambicioso, cuja implementação, contudo, permanece incipiente.[15] Apenas 15 dos 55 Estados-membros ratificaram a Convenção até 2026, evidenciando os desafios de coordenação que caracterizam a cooperação africana nesse domínio.

A análise desses modelos sugere que a eficácia da cooperação multilateral no ciberespaço depende de três fatores críticos. O primeiro é a existência de um Estado-âncora com capacidades técnicas e financeiras para liderar os esforços. O segundo consiste na definição de objetivos concretos e mensuráveis que transcendam declarações de intenções. O terceiro reside na articulação com estruturas regionais e globais que potencializem sinergias e evitem duplicações.

2. A cooperação no ciberespaço na CPLP: estado da arte

2.1. Iniciativas existentes

O quadro institucional da cooperação em defesa e segurança na CPLP assenta em dois instrumentos fundamentais: o Protocolo de Cooperação da CPLP no Domínio da Defesa, assinado em 2006, e os Programas-Quadro de Cooperação que dele decorrem.[16] Esses instrumentos estabelecem um enquadramento genérico para a cooperação militar e de segurança, mas não contemplam disposições específicas relativas ao ciberespaço como domínio operacional.

No plano bilateral, Portugal tem desenvolvido acordos de cooperação no domínio de defesa (CDD) com todos os PALOP, incluindo componentes de formação que, em alguns casos, abrangem aspectos de segurança da informação. O Instituto da Defesa Nacional (IDN), o Instituto Universitário Militar (IUM) e a Academia Militar (AM) têm acolhido oficiais dos países lusófonos em cursos nos quais as temáticas da cibersegurança são abordadas, ainda que de forma não sistemática.[17] O Centro

15 União Africana (2014) Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais (Convenção de Malabo). Malabo, 27 de junho.

16 Comunidade dos Países de Língua Portuguesa (2006) *Protocolo de Cooperação da CPLP no Domínio da Defesa*. Bissau, 17 de julho.

17 Portugal (1996) Decreto-Lei n.º 238/96, de 13 de dezembro, que cria o Instituto da Defesa Nacional.

Nacional de Cibersegurança (CNCS), criado em 2014, tem igualmente participado em ações pontuais de cooperação com congêneres lusófonos.[18]

O Brasil, por sua vez, desenvolveu capacidades significativas em ciberdefesa, materializadas no Comando de Defesa Cibernética, criado em 2010, e na Escola Nacional de Defesa Cibernética.[19] A cooperação bilateral Brasil-Portugal nesse domínio tem se intensificado, incluindo a participação conjunta em exercícios de cibersegurança e intercâmbio de experiências doutrinárias. Contudo, a extensão sistemática dessa cooperação aos demais membros da CPLP permanece incipiente.

No plano multilateral, a CPLP tem abordado as questões do ciberespaço, sobretudo na perspectiva da inclusão e do desenvolvimento, com menor ênfase nas dimensões securitárias A Declaração de Brasília sobre a Sociedade da Informação, adotada em 2002, e iniciativas subsequentes como a Rede de Conhecimento de Língua Portuguesa centram-se no acesso às tecnologias e na promoção de conteúdos em português, sem articular uma visão integrada de cibersegurança.[20]

2.2. Lacunas identificadas

O diagnóstico do estado atual da cooperação no ciberespaço, na CPLP, revela conjunto de lacunas estruturais que comprometem a eficácia da resposta coletiva às ciberameaças. A primeira e mais evidente dessas lacunas é a fragmentação institucional. A ausência de órgão especializado em cibersegurança no seio da CPLP resulta na dispersão de esforços e na impossibilidade de coordenar respostas a incidentes transnacionais. Diferentemente do que ocorre na União Europeia, onde a Agência Europeia para a Segurança das Redes e da Informação (European Union Agency for Cybersecurity – ENISA) desempenha funções de coordenação e apoio técnico, a CPLP carece de uma estrutura equivalente que possa centralizar informações, padronizar procedimentos e mobilizar recursos de forma ágil.[21]

A segunda lacuna diz respeito às assimetrias de capacidade entre os Estados-membros. Enquanto Portugal dispõe de um ecossistema relativamente maduro,

18 Portugal (2014) Decreto-Lei n.º 69/2014, de 9 de maio, que cria o Centro Nacional de Cibersegurança.

19 Brasil (2020) Decreto n.º 10222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética (Brasil); Brasil (2012) Portaria Normativa n.º 3389/MD, de 21 de dezembro de 2012, que dispõe sobre a Política Cibernética de Defesa.

20 Comunidade dos Países de Língua Portuguesa (2002) Declaração de Brasília sobre a Sociedade da Informação, adotada pela IV Conferência de Chefes de Estado e de Governo da CPLP, Brasília, 1 de agosto.

21 União Europeia (2019) *Regulamento (UE) 2019/881 (Regulamento Cibersegurança)*, artigos 3.º a 12.º. Artigos relativos às atribuições da ENISA.

com Computer Security Incident Response Team (CSIRT) nacional, quadro legislativo desenvolvido e integração em estruturas europeias, vários PALOP carecem das capacidades mínimas para detetar e responder a incidentes básicos. A Guiné Equatorial, não obstante os recursos financeiros disponíveis, apresenta igualmente défices significativos nesse domínio, refletindo a ausência de tradição institucional e de massa crítica de profissionais qualificados.

A terceira lacuna consiste na ausência de doutrina comum que oriente a cooperação lusófona em cibersegurança. Conceitos fundamentais como a definição de incidente de segurança, os limiares para compartilhamento de informações ou os procedimentos de assistência mútua carecem de harmonização, dificultando a interoperabilidade entre os diferentes sistemas nacionais e comprometendo a eficácia de eventuais respostas coordenadas.

Por fim, o défice de recursos humanos constitui um problema transversal que afeta de forma particularmente aguda os PALOP. A escassez de profissionais qualificados em cibersegurança é um fenômeno global, mas assume contornos dramáticos em países onde os sistemas de ensino superior ainda não desenvolveram programas específicos nessa área. A inexistência de oferta formativa de nível internacional em língua portuguesa obriga os quadros africanos a buscar qualificação no estrangeiro, frequentemente em língua inglesa, com custos financeiros e de integração significativos.

2.3. Ameaças compartilhadas

A análise das ameaças cibernéticas que afetam o espaço lusófono evidencia padrões comuns que reforçam a racionalidade de uma resposta coordenada. O cibercrime financeiro constitui talvez a ameaça mais disseminada. Os países lusófonos têm sido alvo de campanhas de *phishing*, fraude bancária e *ransomware* frequentemente operadas por grupos criminosos que exploram a língua portuguesa para conferir credibilidade às suas comunicações. O fato de esses ataques utilizarem o português como vetor sugere uma especialização criminosa que transcende fronteiras nacionais e que, paradoxalmente, poderia ser melhor combatida através de cooperação lusófona.[22]

As campanhas de desinformação em língua portuguesa representam uma ameaça crescente à integridade dos processos democráticos no espaço lusófono. Operações de influência, frequentemente originadas em plataformas estrangeiras, têm afetado eleições e polarizado o debate público em vários Estados-membros. A dificuldade em monitorar e responder a essas campanhas de forma isolada reforça a

22 Portugal (2009) *Lei n.º 109/2009, de 15 de setembro (Lei do Cibercrime).*

necessidade de mecanismos compartilhados de deteção e alerta que permitam respostas coordenadas em tempo útil.

A crescente informatização de setores críticos como energia, transportes e telecomunicações expõe infraestruturas essenciais a ataques cibernéticos potencialmente devastadores. Essa vulnerabilidade é particularmente preocupante nos PALOP e na Guiné Equatorial, onde a concentração de investimentos chineses em infraestruturas de tecnologia da informação suscita questões quanto à segurança das cadeias de fornecimento e à eventual existência de vulnerabilidades deliberadamente inseridas em equipamentos críticos.[23]

3. Portugal como catalisador

3.1. Ecossistema nacional de cibersegurança

Portugal desenvolveu, na última década, um ecossistema de cibersegurança que, embora modesto em termos de dimensão absoluta, apresenta níveis de maturidade comparáveis aos dos seus parceiros europeus. O Centro Nacional de Cibersegurança, criado pelo Decreto-Lei n.º 69/2014, de 9 de maio, constitui a autoridade nacional nessa matéria.[24] Essa estrutura coordena a implementação da Estratégia Nacional de Segurança do Ciberespaço, atualizada em 2019, que estabelece objetivos em matéria de proteção das infraestruturas críticas, capacitação de recursos humanos e cooperação internacional.[25]

No plano acadêmico, várias instituições de ensino superior portuguesas desenvolveram competências de relevo em cibersegurança. O Instituto Superior Técnico, a Universidade do Minho, a Universidade de Coimbra e a Universidade Nova de Lisboa oferecem programas de formação avançada e desenvolvem pesquisa em áreas como criptografia, segurança de redes e análise de *malware*. Essa capacidade instalada poderia ser mobilizada para programas de formação em benefício de nacionais dos demais países da CPLP.

Para além das capacidades institucionais e acadêmicas, o ecossistema português de cibersegurança pode ser diferenciado por um modelo de governação relativamente integrado, que articula estruturas civis e militares sob coordenação central, favorecendo a interoperabilidade entre a defesa, segurança interna e administração

23 Portugal (2014) *Decreto-Lei n.º 69/2014, de 9 de maio (criação do CNCS);* Portugal (2021) *Decreto-Lei n.º 65/2021, de 30 de julho (regime jurídico da segurança do ciberespaço)*.

24 Portugal (2014) *Decreto-Lei n.º 69/2014, de 9 de maio (criação do CNCS);* Portugal (2021) *Decreto-Lei n.º 65/2021, de 30 de julho (regime jurídico da segurança do ciberespaço)*.

25 Portugal (2019) *Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho, que aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*.

pública. Essa arquitetura permite respostas mais coordenadas a incidentes e maior alinhamento com os padrões europeus em matéria de segurança cibernética, conforme definido na Estratégia Nacional de Segurança do Ciberespaço de 2019-2023 (Portugal, 2019).

Não obstante esses avanços, o ecossistema nacional apresenta limitações estruturais. A escassez de recursos humanos altamente especializados, a dependência de tecnologias e fornecedores estrangeiros e a capacidade limitada de projeção externa constituem desafios persistentes. Em paralelo, essas restrições reforçam o racional da cooperação lusófona, já que tornam essa articulação com parceiros membros da CPLP mais estratégicas.

O setor privado português inclui igualmente empresas com capacidades relevantes em cibersegurança, desde multinacionais com operações no país até *startups* especializadas. Essas empresas poderiam desempenhar papel relevante na transferência de conhecimento para o espaço lusófono, mediante incentivos adequados e enquadramento institucional apropriado.

3.2. Inserção em estruturas europeias e atlânticas

A pertença de Portugal à União Europeia e à OTAN confere-lhe acesso a capacidades, conhecimentos e recursos que podem ser mobilizados – dentro dos limites legais aplicáveis – em benefício da cooperação lusófona. No âmbito europeu, Portugal participa das estruturas da ENISA e beneficia dos programas de capacitação e de financiamento disponíveis aos Estados-membros.[26] A transposição da Diretiva Network and Information Security (NIS) e, mais recentemente, a implementação do Regulamento relativo à Cibersegurança conferiram robustez ao quadro normativo nacional.[27]

No contexto atlântico, Portugal integra a OTAN através do *Cooperative Cyber Defence Centre of Excellence*, sediado em Tallinn, e participa em exercícios de ciberdefesa da Aliança como o *Locked Shields*.[28] Essa inserção confere acesso a doutrina, melhores práticas e capacidades de treino que não estão disponíveis a Estados não membros da OTAN, mas que poderiam ser parcialmente transferidas para parceiros lusófonos no âmbito de programas de cooperação bilaterais (Štrucl, 2021).

26 União Europeia (2019) *Regulamento (UE) 2019/881 (Regulamento de Cibersegurança)*, Cap. III.

27 União Europeia (2022) *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 (Diretiva NIS 2).*

28 NATO Cooperative Cyber Defence Centre of Excellence (2017*) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

3.3. Legitimidade e capital relacional no espaço lusófono

Para além das capacidades técnicas, Portugal dispõe de capital relacional no espaço lusófono que lhe confere legitimidade para liderar iniciativas de cooperação. A tradição diplomática portuguesa, caracterizada por uma abordagem não hegemônica e pelo respeito à soberania dos parceiros, constitui um ativo intangível de valor significativo.

A rede de CDD estabelecida ao longo de décadas criou laços de confiança entre as Forças Armadas portuguesas e as dos PALOP que facilitam a cooperação em domínios sensíveis. Os milhares de oficiais africanos formados em Portugal constituem uma rede de contatos e reserva de boa vontade que podem ser mobilizadas para a cooperação em cibersegurança. No que se refere especificamente à Guiné Equatorial, Portugal tem desenvolvido iniciativas de promoção da língua portuguesa que constituem uma base para um relacionamento mais amplo. O estabelecimento de um Camões – Centro de Língua Portuguesa em Malabo, na Universidade Nacional da Guiné Equatorial, e a oferta de bolsas de estudo a estudantes equato-guineenses ilustram uma abordagem pragmática, que reconhece as especificidades desse membro mais recente da CPLP.[29]

4. Propostas para uma estratégia integrada: CPLP 3.0

4.1. Centro de cibersegurança lusófono

A criação de um Centro de Cibersegurança Lusófono constitui a pedra angular da proposta de cooperação avançada no ciberespaço. Esse centro, que se propõe seja sediado em Lisboa, desempenharia funções de coordenação, apoio técnico e capacitação em benefício de todos os Estados-membros da CPLP.

O referido centro teria como missão reforçar a resiliência do espaço lusófono no ciberespaço através da partilha de informações sobre ameaças, da coordenação de respostas a incidentes transnacionais e do apoio à capacitação dos Estados-membros com menores recursos. A sua estrutura contemplaria três divisões principais: uma voltada à inteligência de ameaças, responsável pela recolha, análise e disseminação de informações sobre ameaças cibernéticas relevantes para o espaço lusófono; outra dedicada à resposta a incidentes, funcionando como um CSIRT regional que prestaria apoio técnico aos Estados-membros na resposta a incidentes significativos; e uma terceira, focada na capacitação, coordenando os programas de formação e assistência técnica em benefício dos PALOP e da Guiné Equatorial.

29 Portugal e Guiné Equatorial (2015) *Memorando de Entendimento entre a República Portuguesa e a República da Guiné Equatorial no Domínio do Ensino da Língua Portuguesa.*

A governança do Centro seria assegurada por um Conselho de Administração composto por representantes de todos os Estados-membros, com presidência rotativa. O financiamento seria baseado em contribuições proporcionais às capacidades de cada Estado, complementadas por financiamento europeu mobilizado por Portugal. A escolha de Lisboa como sede justifica-se pela concentração de competências técnicas, pela facilidade de acesso a partir de todos os países lusófonos e pela possibilidade de articulação com as estruturas europeias de cibersegurança.[30]

4.2. Academia de defesa cibernética lusófona

A formação de recursos humanos qualificados constitui, porventura, o investimento com maior potencial de retorno a longo prazo. A criação de uma Academia de Ciberdefesa Lusófona ofereceria formação de excelência em língua portuguesa, acessível a nacionais de todos os Estados-membros. A oferta formativa da Academia abrangeria desde sensibilização básica para usuários finais até formação técnica avançada para especialistas. Seriam privilegiados cursos em áreas como análise de *malware* e engenharia reversa, resposta a incidentes e análise forense, segurança de redes e infraestruturas, criptografia aplicada, e governança e gestão de riscos no espaço cibernético.

A formação seria ministrada em modalidade híbrida, combinando módulos *on-line* – acessíveis a partir de qualquer localização – com períodos presenciais intensivos em Lisboa ou noutras capitais lusófonas. Essa abordagem maximizaria o alcance da formação enquanto minimiza os custos de deslocação. Os certificados emitidos pela Academia seriam reconhecidos mutuamente por todos os Estados-membros, criando um padrão lusófono de qualificação em cibersegurança.

A inclusão de quadros equato-guineenses nos programas de formação da Academia constituiria instrumento poderoso para a consolidação dos laços linguísticos e técnicos. A formação em português desses profissionais contribuiria para o objetivo mais amplo de difusão da língua no país, simultaneamente criando rede de especialistas familiarizados com as práticas e a doutrina lusófonas.[31]

30 Modelo inspirado no Cooperative Cyber Defence Centre of Excellence da Organização do Tratado do Atlântico Norte e no European Cybersecurity Competence Centre da União Europeia (2021).

31 European Union Agency for Cybersecurity (2022) *European Cybersecurity Skills Framework*. Atenas: ENISA.

4.3. Laboratório de IA em português

O desenvolvimento de capacidades próprias em inteligência artificial, particularmente no processamento de linguagem natural, reveste-se de importância estratégica para a soberania do espaço lusófono no ciberespaço. A criação de um laboratório de IA em português coordenaria esforços de pesquisa e desenvolvimento nesse domínio.

O laboratório teria como objetivos principais o desenvolvimento de modelos de linguagem otimizados para o português, contemplando as variantes brasileira, europeia e africanas; a criação de comandos linguísticos de qualidade para treinamento de modelos de IA; a aplicação de técnicas de IA à análise de ciberameaças em língua portuguesa; e o desenvolvimento de ferramentas de deteção de desinformação adaptadas ao contexto lusófono. O laboratório funcionaria em rede, articulando centros de pesquisa em Portugal, Brasil e outras instituições lusófonas que desenvolvam capacidades nesse domínio. A coordenação seria assegurada por uma secretaria técnica sediada em Lisboa. Para além das contribuições dos Estados-membros, o laboratório buscaria financiamento junto a programas europeus e fundações privadas interessadas no desenvolvimento de IA multilíngue.

O controle sobre as tecnologias de processamento de linguagem natural tem implicações que transcendem o domínio técnico. Modelos de IA treinados exclusivamente em dados anglófonos ou sinófonos incorporam inevitavelmente vieses culturais e linguísticos que podem afetar a sua utilidade – ou mesmo a sua segurança – quando aplicados ao contexto lusófono. O desenvolvimento de capacidades próprias mitiga essa dependência e cria oportunidades econômicas significativas.[32]

4.4. Quadro normativo harmonizado

A cooperação eficaz em cibersegurança exige um quadro normativo harmonizado que facilite a assistência mútua, o compartilhamento de informações e a persecução transnacional de cibercrimes. A negociação de uma Convenção da CPLP sobre Cibersegurança e Cibercrime estabeleceria esse enquadramento.

A Convenção regularia a definição harmonizada de cibercrimes e as respectivas penas, os procedimentos de consultoria jurídica mútua em matéria de cibercrime, os mecanismos de compartilhamento de informações sobre ameaças entre autoridades competentes, as obrigações de notificação de incidentes de segurança, a proteção de infraestruturas críticas de informação e as salvaguardas para proteção de dados pessoais e direitos fundamentais.

32 União Europeia (2024) *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho*, de 13 de junho (Regulamento da IA).

A Convenção da CPLP articular-se-ia com instrumentos já em vigor, nomeadamente a Convenção de Budapeste sobre Cibercrime, à qual Portugal aderiu, e a Convenção de Malabo da União Africana.[33] Para os Estados que não são parte desses instrumentos, a Convenção da CPLP poderia constituir um primeiro passo de aproximação a padrões internacionais. Um Comitê de Peritos seria responsável pelo acompanhamento da implementação e pela formulação de recomendações aos Estados-Partes.

A inclusão da Guiné Equatorial nesse quadro normativo suscita questões delicadas, tendo em conta as preocupações relativas ao estado de direito e aos direitos humanos no país. Uma abordagem pragmática poderia contemplar mecanismos de integração progressiva, condicionada ao cumprimento de salvaguardas específicas em matéria de proteção de dados e garantias processuais.[34]

5. Desafios e considerações finais

5.1. Obstáculos à implementação

A materialização da visão proposta para uma "CPLP 3.0" enfrenta obstáculos significativos que importa identificar e endereçar. As assimetrias de desenvolvimento constituem o primeiro e mais evidente desses obstáculos. As disparidades entre Portugal e o Brasil, por um lado, e os demais Estados-membros, por outro, em matéria de capacidades no ciberespaço são substanciais. A implementação de estratégia comum exigirá investimentos significativos em capacitação que transcendem, em muito, os recursos atualmente disponíveis para a cooperação lusófona. A mobilização de financiamento externo – europeu, mas também de outras fontes – será condição necessária para o sucesso das iniciativas propostas.

O financiamento sustentável representa desafio adicional. A criação de estruturas permanentes como o Centro de Cibersegurança Lusófono ou a Academia de Ciberdefesa exige compromissos financeiros de longo prazo que colidem com as restrições orçamentárias da maioria dos Estados-membros. Modelos de financiamento inovadores, que combinem contribuições estatais, financiamento europeu e parcerias com o setor privado, deverão ser explorados.

As questões de soberania também não podem ser negligenciadas. O compartilhamento de informações sensíveis sobre vulnerabilidades e incidentes de segurança suscita reservas legítimas por parte de Estados que zelam por sua autonomia.

33 Conselho da Europa (2001) *Convenção sobre o Cibercrime (Convenção de Budapeste)*, CETS n.º 185, Budapeste, 23 de novembro.

34 Regulamento (UE) 2016/679 (Regulamento Geral sobre a Proteção de Dados – RGPD).

A construção de confiança entre parceiros – pré-requisito para uma cooperação eficaz – é um processo necessariamente gradual que não pode ser acelerado por decretos ou tratados. A experiência da cooperação técnico-militar lusófona, construída ao longo de décadas, oferece lições valiosas sobre a gestão de expectativas e a consolidação progressiva de relações de confiança.

5.2. Competição de potências externas

O espaço lusófono não é imune às dinâmicas de competição geopolítica que caracterizam o sistema internacional contemporâneo. A presença crescente de potências externas, nomeadamente a China, mas também a Rússia e, em menor escala, a Turquia, nos países lusófonos africanos e na Guiné Equatorial, suscita desafios específicos para a cooperação em cibersegurança. A China tem desenvolvido uma estratégia de investimento em infraestruturas de telecomunicações na África que inclui a construção de redes, centros de dados e sistemas de cidades inteligentes. Empresas chinesas detêm posições dominantes em vários mercados africanos, incluindo nos PALOP e na Guiné Equatorial.[35] Essa presença suscita preocupações quanto à segurança das cadeias de fornecimento e à eventual existência de vulnerabilidades em equipamentos críticos.

A Rússia, embora com presença econômica mais limitada, desenvolve parcerias em matéria de segurança com vários Estados africanos, incluindo capacidades de operações no ciberespaço. Campanhas de desinformação em língua portuguesa, algumas com ligações documentadas a atores russos, afetam o espaço lusófono, particularmente o Brasil.

Face a essa competição, a cooperação lusófona em cibersegurança não deve ser conceituada como jogo de soma zero contra potências terceiras. Uma abordagem mais inteligente passa por oferecer aos Estados-membros opções credíveis que diversifiquem as suas dependências e reforcem a sua autonomia estratégica. A proposta de "CPLP 3.0" inscreve-se nessa lógica: não se trata de substituir a presença chinesa ou a russa, mas de complementá-las com capacidades próprias que confiram aos Estados lusófonos maior margem de manobra e resiliência.

35 União Europeia, Comissão Europeia (2019) *Recomendação da UE 2019/534 da Comissão, de 26 de março, sobre a cibersegurança das redes 5G*. Jornal da União Europeia. Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019H0534&from=PT [Acesso em: 01 de janeiro de 2026].

Conclusões

O presente artigo procurou demonstrar que a cooperação em cibersegurança e inteligência artificial constitui um domínio promissor, mas amplamente inexplorado, para o aprofundamento das relações entre os países de língua portuguesa. A partilha linguística, tradicionalmente valorizada sobretudo por suas dimensões culturais e diplomáticas, revela-se um ativo estratégico operacional num contexto no qual a velocidade de comunicação, a confiança entre parceiros e a capacidade de desenvolvimento tecnológico conjunto assumem relevância crítica.

O diagnóstico apresentado evidencia um conjunto de lacunas estruturais na cooperação lusófona no ciberespaço: fragmentação institucional, assimetrias de capacidade, ausência de doutrina comum e défice de recursos humanos qualificados. Essas lacunas comprometem a capacidade de resposta coletiva às ciberameaças transnacionais que afetam o espaço lusófono e impedem a exploração das sinergias potenciais entre Estados que compartilham um idioma comum.

Portugal, por sua inserção em estruturas europeias e atlânticas, pelas capacidades técnicas desenvolvidas na última década e pelo capital relacional acumulado junto aos parceiros lusófonos, surge como catalisador natural de estratégia integrada de cooperação no ciberespaço. O modelo proposto – designado "CPLP 3.0" – assenta em quatro pilares complementares: um Centro de Cibersegurança Lusófono, uma Academia de Ciberdefesa comum, um laboratório de IA em Português e um quadro normativo harmonizado.

O caso particular da Guiné Equatorial ilustra simultaneamente as oportunidades e os desafios dessa estratégia. A integração desse membro mais recente da CPLP na arquitetura de cooperação no ciberespaço exigirá abordagens diferenciadas que reconheçam as suas especificidades – a ausência de tradição linguística portuguesa, a disponibilidade de recursos financeiros, a posição geopolítica estratégica no Golfo da Guiné – sem comprometer os requisitos de confiança e a convergência de valores que a cooperação em matéria de segurança necessariamente pressupõe.

A materialização dessa visão enfrentará obstáculos significativos, desde as assimetrias de desenvolvimento entre Estados-membros até às dinâmicas de competição geopolítica que atravessam o espaço lusófono. Contudo, os custos da inação afiguram-se superiores aos custos da ação. Num mundo no qual o ciberespaço se tornou arena de conflito e a inteligência artificial emerge como tecnologia transformadora, os países que não desenvolverem capacidades próprias ficarão inexoravelmente dependentes de terceiros – frequentemente de potências cujos valores e interesses divergem dos seus (Black et al., 2024).

A língua portuguesa, falada por mais de 250 milhões de pessoas em quatro continentes, constitui um ativo singular que nenhuma outra comunidade linguística comparável pode reivindicar na mesma medida. Cabe aos Estados lusófonos – e,

em particular, a Portugal, pelas razões expostas – mobilizar esse ativo para a construção de um espaço mais seguro, mais autônomo e mais próspero no ciberespaço. O tempo para agir é agora.

Bibliografia

Black, J. et al. (2024) *Strategic competition in the age of AI: emerging risks and opportunities from military use of artificial intelligence*. Disponível em: https://www.rand.org/pubs/research_reports/RRA3295-1.html (Acedido em: 1 de janeiro de 2026).

Brasil (2012) *Portaria normativa n.º 3389/MD, de 21 de dezembro*. Diário Oficial da União, 26 de dezembro de 2012.

Brasil (2019) Linha do tempo: do eletrónico ao digital, *Gov.br*. Disponível em: https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital (Acedido em: 1 de janeiro de 2026).

Brasil (2020) *Decreto n.º 10222, de 5 de fevereiro*. Diário Oficial da União, 6 de fevereiro de 2020.

Calandro, E. e Berglund, N. (2019) Cybersecurity in Africa: an assessment, *Research ICT Africa Policy Brief*, n.º 2, pp. 1-12.

Comissão do Golfo da Guiné (2001) *Tratado da Comissão do Golfo da Guiné*. Libreville, 3 de julho de 2001.

Commonwealth Secretariat (2020) *Commonwealth cyber declaration: implementation plan 2018--2020*. Londres: Commonwealth Secretariat.

Conselho da Europa (2001) *Convenção sobre o cibercrime (Convenção de Budapeste)*. CETS n.º 185. Budapeste, 23 de novembro de 2001.

CPLP (1996) *Declaração constitutiva da Comunidade dos Países de Língua Portuguesa*. Lisboa, 17 de julho de 1996.

CPLP (2002) *Declaração de Brasília sobre a sociedade da informação*. Brasília, 1 de agosto de 2002.

CPLP (2006) *Protocolo de cooperação da CPLP no domínio da defesa*. Bissau, 17 de julho de 2006.

CPLP (2014) *Resolução sobre a adesão da República da Guiné Equatorial à Comunidade dos Países de Língua Portuguesa*. Díli, 23 de julho de 2014.

CPLP (2018) *Plano de ação de Lisboa para a promoção, difusão e projeção da língua portuguesa*. Lisboa, 17 de julho de 2018.

ENISA (2022) *European cybersecurity skills framework*. Atenas: European Union Agency for Cybersecurity.

Espanha e Portugal (1778) *Tratado preliminar de límites en América Meridional (Tratado de El Pardo)*. El Pardo, 11 de março de 1778.

Grant, R. (2008) *Rise of cyber war*. Mitchell Institute Special Report, novembro de 2008.

Guiné Equatorial (1991) *Ley fundamental de Guinea Ecuatorial (Constitución)*. Malabo.

Hoffman, F. G. (2007) *Conflict in the 21st century: the rise of hybrid wars*. Arlington: Potomac Institute for Policy Studies.

Kello, L. (2017) *The virtual weapon and international order*. New Haven: Yale University Press.

Klimburg, A. (2012) *National cyber security framework manual*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Krepinevich, A. F. (2012) *Cyber warfare: a "nuclear option"?* Washington, DC: Center for Strategic and Budgetary Assessments.

Libicki, M. (2009) *Cyberdeterrence and cyberwar*. Santa Mónica: RAND Corporation.

Moreira, A. (2020) A CPLP e os desafios da segurança no espaço lusófono, *Nação e Defesa*, n.º 156, pp. 45-67.

NATO (2016) *Warsaw Summit communiqué*. Varsóvia, 8-9 de julho de 2016.

NATO Cooperative Cyber Defence Centre of Excellence (2017) *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press.

Nye, J. S. (2004) *Soft power: the means to success in world politics*. Nova Iorque: Public Affairs.

Nye, J. S. (2011) *The future of power*. Nova Iorque: Public Affairs.

OIF (2022) *Stratégie de la Francophonie numérique 2022-2026*. Paris: Organisation internationale de la Francophonie.

Pires, T. *et al.* (2019) "How multilingual is multilingual BERT?", *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, pp. 4996-5001.

Portugal (1996) *Decreto-Lei n.º 238/96, de 13 de dezembro*. Diário da República, 13 de dezembro de 1996.

Portugal (2009a) *Decreto-Lei n.º 231/2009, de 15 de setembro*. Diário da República, 15 de setembro de 2009.

Portugal (2009b) *Decreto do Presidente da República n.º 91/2009, de 15 de setembro*. Diário da República, 15 de setembro de 2009.

Portugal (2009c) *Lei n.º 109/2009, de 15 de setembro*. Diário da República, 15 de setembro de 2009.

Portugal (2012) *Decreto-Lei n.º 21/2012, de 30 de janeiro*. Diário da República, 30 de janeiro de 2012.

Portugal (2014) *Decreto-Lei n.º 69/2014, de 9 de maio*. Diário da República, 9 de maio de 2014.

Portugal (2019a) *Decreto-Lei n.º 88/2019, de 3 de julho*. Diário da República, 3 de julho de 2019.

Portugal (2019b) *Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho*. Disponível em: https://www.incode2030.gov.pt/estrategia-nacional-de-seguranca-do-ciberespaco/ (Acedido em: 1 de janeiro de 2026).

Portugal (2021) *Decreto-Lei n.º 65/2021, de 30 de julho*. Diário da República, 30 de julho de 2021.

Portugal e Guiné Equatorial (2015) *Memorando de entendimento no domínio do ensino da língua portuguesa*. Lisboa.

Štrucl, D. (2021) *Comparative study on the cyber defence of NATO member states*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

União Africana (2014) *Convenção sobre cibersegurança e proteção de dados pessoais (Convenção de Malabo)*. Malabo, 27 de junho de 2014.

União Europeia (2016a) *Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*, L 194, pp. 1-30.

União Europeia (2016b) *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*, L 119, pp. 1-88.

União Europeia (2019a) *Recomendação (UE) 2019/534 da Comissão*. *Jornal Oficial da União Europeia*, L 88, pp. 42-47.

União Europeia (2019b) *Regulamento (UE) 2019/452 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*, L 79 I, pp. 1-14.

União Europeia (2019c) *Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*, L 151, pp. 15-69.

União Europeia (2021) *Regulamento (UE) 2021/887 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*, L 202, pp. 1-31.

União Europeia (2022) *Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*, L 333, pp. 80-152.

União Europeia (2024) *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho*. *Jornal Oficial da União Europeia*.

United Nations Human Rights Council (2017) *Report of the Special Rapporteur on the situation of human rights defenders on his mission to Equatorial Guinea*. Geneva: United Nations.