Instituto Superior de Ciências Policiais e Segurança Interna

A SEGURANÇA ENERGÉTICA EM PORTUGAL:

REFLEXÕES SOBRE AS CONSEQUÊNCIAS POTENCIAIS DA SUA CONDUÇÃO NA SEGURANÇA NACIONAL

Autor:
Carlos Manuel Catalão Antunes
Comissário M/151449

Tipo de artigo: Estudo Teórico

Trabalho Individual Final
V Curso de Comando e Direção Policial

Lisboa, 25 de julho de 2022

Resumo

Numa sociedade altamente tecnologizada e necessitada de um fluxo constante e ininterrupto de energia, um bloco económico como a União Europeia, que integra Portugal, um grande consumidor mas onde rareiam as fontes energéticas primárias, encontra-se numa posição de enorme vulnerabilidade. Esta fragilidade, que tem vindo a ser equilibrada com o estabelecimento de uma diplomacia energética baseada na diversificação de fontes e fornecedores, comporta também riscos securitários evidentes. Num mundo onde cidadãos, empresas e Estados se interconectam como nunca, um conjunto de novas ameaças, mais perigosas e com maior potencial destrutivo aparente que as anteriores, resultantes da operação universal no ciberespaço, emergem no horizonte. Como as consequências antecipáveis resultantes de um ciberataque a uma infraestrutura crítica energética seriam potencialmente devastadoras, refletiu-se sobre a necessidade de Portugal adaptar a sua arquitetura de segurança às novas exigências. Considerando, simultaneamente, a urgência em dar resposta aos novos desafios do ciberespaço, a escassez de recursos e a necessidade de formular uma definição clara, global e holística dos interesses vitais do país; examinou-se uma proposta de reforma baseada na criação de um conceito estratégico de segurança nacional que, coerentemente, alinhasse, reunindo ao invés de segregar, segurança, defesa, economia/finanças, proteção civil, informações, diplomacia e cultura.

Palavras-chave: Ciberespaço; Infraestruturas Críticas; Segurança Energética; Segurança Interna; Segurança Nacional.

Abstract

In a highly technological society that needs a constant and uninterrupted flow of energy, an economic bloc such as the European Union, which includes Portugal, a major consumer but where primary energy sources are rare, is in a position of enormous vulnerability. This fragility, which has been balanced by the establishment of an energy diplomacy based on the diversification of sources and suppliers, also entails obvious security risks. In a world where citizens, companies and States are interconnected as never before, a set of new threats, more dangerous and with greater apparent destructive potential than the previous ones, resulting from the universal operation in cyberspace, emerge on the horizon. As the anticipated consequences resulting from a cyber-attack to a critical energy infrastructure would be potentially devastating, the need for Portugal to adapt its security architecture to the new demands was reflected upon. Considering, simultaneously, the urgency to respond to the new challenges of cyberspace, the scarcity of resources and the need to formulate a clear, global and holistic definition of the country's vital interests; a reform proposal based on the creation of a strategic concept of national security that coherently aligns, bringing together rather than segregating, security, defence, economy/finance, civil protection, intelligence, diplomacy and culture was examined.

Keywords: Critical Infrastructure; Cyberspace; Energy Security; Internal Security; National Security.

Introdução

A revolução industrial, que abriu caminho ao mais intenso período de crescimento económico continuado jamais visto, se encolheu e homogeneizou o mundo, também criou, tecnológica e energeticamente falando, perdedores e ganhadores (Landes, 2005), iniciando a chamada *grande divergência*. Como afirmou o almirante Rickover (1972), numa sociedade altamente tecnologizada em que a qualidade de vida e as possibilidades de crescimento económico dependem da disponibilização constante e ininterrupta de energia que "alimenta máquinas que fazem de cada um de nós senhores de um exército de escravos mecânicos" (p. 678) que nos servem, e num mundo em que "o alto consumo de energia foi sempre um requisito para o poder político" e no qual a potência dominante tenderá a ser aquela que controlar os recursos energéticos (p. 684); o aprovisionamento e o fornecimento de energia continuam a ser uma questão fundamental de segurança nacional, sem os quais a sociedade pode colapsar (Yergin, 2011).

A condução de políticas de segurança energética por parte dos Estados-Membros, e concretamente por Portugal, que continuará a representar uma prioridade governativa de primeira ordem nas próximas décadas (Campos, 2017; Comissão Europeia [CE], 2015; Silva, 2007), deverá continuar a merecer uma abordagem multidimensional e plurissectorial e ser operada através de uma diplomacia energética capaz de diversificar fontes e fornecedores (Fernandes, 2015; Leal, 2015; Santos, 2021; Silva & Rodrigues, 2015; Viana et al., 2014; Yergin, 2006, 2011) alinhando-se com a política da União Europeia (UE). Tendo em conta que Portugal, parte integrante de um enorme espaço económico, a UE, mas, como os demais Estados-Membros, importador líquido de energia, está numa posição de enorme vulnerabilidade geopolítica/securitária, importa perceber se a atual arquitetura de segurança nacional está à altura dos desafios imediatos e futuros (Barros, 1984; Campos, 2017; Duarte & Fernandes, 2011; Eiras, 2011; Rodrigues & Campos, 2017; Santos, 2021).

Uma moderna avaliação conceptual de segurança energética não deve esgotar, contudo, o tema à pura avaliação da gestão e condução político-estratégica entre Estados. As alterações à ordem pública verificadas na sequência do movimento dos coletes amarelos de 2018, motivações políticas à parte (Sousa, 2019), e que eclodiram na sequência do aumento do custo dos combustíveis em França, juntamente com a greve dos motoristas de matérias perigosas que ameaçou paralisar Portugal em 2019,

justificam, *per se*, julga-se, uma reflexão aprofundada considerando o potencial disruptivo imanente.

Às ameaças clássicas, e tão ou mais preocupantes, juntam-se agora os desafios representados pela anarquia do ciberespaço e, especialmente, pela possibilidade de realização de ciberataques a infraestruturas críticas (IC) do setor energético, sem o funcionamento das quais as sociedades paralisariam (Fernandes, 2012; Natário, 2014; Nye, 2022). Importa aferir, urgentemente, qual a capacidade dos atuais sistemas de segurança e defesa, construídos para operar de forma independente noutros teatros operacionais, para responderem às novas ciberameaças, antecipando-se, por isso, a necessidade de convergência, complementaridade e coerência estratégica e sinergética entre eles (Santos, 2018; Moniz, 2018).

Para responder eficientemente a estes novos desafios, os edifícios de segurança e defesa, bem como os de outras dimensões do Estado, poderão adotar um conceito compreensivo e amplo de segurança nacional, agregador e convergente, capaz de adaptar as instituições aos novos tempos e aos desafios do ciberespaço (Lourenço et al., 2015; Lourenço & Costa, 2018), contrariando a tradição portuguesa de fuga para a frente em que, frequentemente, "a eficácia e eficiência são prejudicadas por razões políticas, históricas e corporativas" (Oliveira, 2006, p. 313).

Se, no meio académico policial, os temas ligados ao ciberespaço vêm merecendo recentemente, entre outros, a atenção de Maia (2019), Moreira (2019) e Silva (2019), no que diz respeito aos estudos relativos à segurança energética e às infraestruturas críticas, Santos (2021) e Pestana (2016), sucessivamente, assinam reflexões únicas nesses domínios tão importantes para o futuro da Polícia de Segurança Pública (PSP) num mundo em mudança acelerada. A triangulação destas três importantes áreas, sucedidas pelo corolário reformatório do sistema, constituem justamente o objeto deste trabalho.

Suportado na análise de legislação e de documentos julgados relevantes para a investigação, como livros, artigos e trabalhos científicos, são então objetivos conjuntos deste estudo teórico: i) a definição do conceito de segurança energética; ii) a caracterização breve da insegurança e dependência energéticas europeia e portuguesa; iii) a análise das ameaças às IC no ciberespaço; iv) a reflexão sobre a necessidade de adotar um conceito estratégico de segurança nacional capaz de responder aos desafios do ciberespaço.

Segurança energética: anatomia de um conceito em constante evolução

Quando, nas vésperas da grande guerra, o então primeiro-lorde do almirantado Winston Churchill tomou a ousada decisão de substituir o carvão galês pelo mais eficiente petróleo persa como novo sistema motriz da *Royal Navy*, os equilíbrios estratégicos alteraram-se profundamente, obrigando a política externa britânica a gerir as vulnerabilidades emergentes (Roberts, 2018). Churchill terá então declarado que "a segurança e a certeza no petróleo residem na variedade e na variedade apenas" (Yergin, 2006, p. 69).

Inaugurada para Yergin (2006, 2011) a origem simbólica do conceito de segurança energética, centrada então apenas na diversificação das fontes de abastecimento numa parte do mundo até meados do século XX controlada, como avança Roberts (2018), pelos impérios europeus, e num tempo de retração pós-colonial destes em que, como afirma Kissinger (1996), a França estava aniquilada, a Grã-Bretanha exaurida e a Alemanha dividida, e em que "os grandes problemas do planeta [deixavam] de se confundir com os da Europa" (Vaïsse, 2004, p. 9); importava ao conceito poliedrizar-se e alargar o seu perímetro explicativo, complexificando-se e densificando-se. Como apontam Silva (2007), Silva e Rodrigues (2015) e Yergin (2006), cujas apreciações e variáveis foram combinadas, o conceito passou a integrar, para além da variedade de fornecedores, componentes como a proteção face ao terrorismo e à pirataria, a proteção ambiental e a necessidade de descarbonização, a garantia de acessibilidade ininterrupta, a estabilidade e competitividade dos preços, a necessidade de manter uma capacidade produtiva excedentária para acomodar a volatilidade, os conflitos internos e as derivas nacionalistas/disruptivas dos países produtores, a liberdade de navegação, a segurança das redes, a estreiteza dos mercados de oferta e a necessidade de manter operacional apenas um grande mercado — mais eficiente e competitivo — ou, como notado em 2021 e 2022, as rivalidades geopolíticas. Mais recentemente, sobretudo depois dos furacões Katrina e Rita terem destruído infraestruturas energéticas de produção e transporte no golfo do México, também os fenómenos naturais e as alterações climáticas passaram a ser fatores-chave desta avaliação conceptual (Eiras, 2011; Silva, 2007; Yergin, 2011). Finalmente, também a segurança IC no ciberespaço vem sendo considerada uma componente fundamental, encorajando-se até a tomada de "medidas para reduzir o risco e mitigar potenciais impactos" (Agência Internacional de Energia [IEA], 2021, p. 16).

Para Yergin (2006, 2011) as variáveis que constituem o núcleo duro operacionalizável do conceito são as que resultam do mandato da IEA, agência criada na sequência da guerra do *Yom Kippur*. Conforme refere Vaïsse (2004), com o duplo objetivo de punir aqueles que apoiavam diplomaticamente Israel e de maximizar as suas receitas, alguns países árabes da Organização dos Países Exportadores de Petróleo quadruplicaram o preço desta fonte nos primeiros meses de 1974. Em 1981 o preço disparou novamente quando o Iraque invadiu o Irão. Foram os dois choques petrolíferos (IEA, 1994). Desejosos de evitar a repetição destas disrupções que ameaçavam a estabilidade das suas economias e faziam perigar a paz social e a ordem pública, como descrevem Yergin (2006) e a IEA (1994), os países industrializados decidiram precaver-se contra o uso dos recursos como arma por parte dos fornecedores, criando então reservas estratégicas de petróleo, desenvolvendo instrumentos de coordenação emergencial, que permitiriam a gestão conjunta dessas reservas, e gerindo mecanismos de monitorização e análise dos mercados de energia.

Mais recentemente, eficiência energética e energias renováveis têm ganho importância crescente e até lugar especial no planeamento estratégico dos Estados e da UE. Com efeito, conforme avançam Yergin (2006) e Silva (2007), com a substituição da indústria pelos serviços, e mercê de desenvolvimentos tecnológicos, grandes ganhos de eficiência energética foram conseguidos. Por seu turno, as renováveis, para além de diminuírem a dependência do exterior, contribuem para o *mix* energético, aumentando a capacitação endógena, descarbonizando a economia e protegendo o ambiente (Campos, 2017; Comissão Europeia [CE], 2015; Observatório da Energia [OE] et al., 2021).

A forma como os documentos estratégicos priorizam e recombinam, em função das respetivas necessidades, as variáveis supramencionadas, aumentam a compreensão prática do conceito. O Pacote União de Energia (CE, 2015) e a Estratégia de Longo Prazo da UE de Alcançar a Neutralidade Carbónica (Parlamento Europeu & Conselho da União Europeia [CUE], 2018), são modelos europeus. Se o primeiro elege a segurança, a diversificação e o custo do abastecimento de petróleo e da eletricidade, mas sobretudo do gás — fonte primária de transição entre os combustíveis fósseis e as energias renováveis, ambientalmente orientado e mais eficiente na produção elétrica (Eiras, 2011) — como preocupações cimeiras, embora não exclusivas, o segundo foca-se numa estratégia holística/multidisciplinar destinada a atingir a neutralidade carbónica da UE em 2050. Como exemplos de documentos estratégicos portugueses,

temos a Estratégia Nacional para o Hidrogénio, aprovado pela Resolução do Conselho de Ministros (RCM) n.º 63/2020, de 14 de agosto, em que a IEA (2021) recomenda que se aposte para diminuir o peso dos combustíveis na fatura energética, focada sobretudo na neutralidade carbónica e na garantia da independência energética nacional, e o Roteiro para a Neutralidade Carbónica 2050, aprovado pela RCM nº. 107/2019, de 1 de julho, destinado a materializar o assumido no Acordo de Paris e a garantir o cumprimento local, na qualidade de Estado-Membro, da supracitada Estratégia de Longo Prazo da UE.

Pese embora Campos (2017, 2018) argumente que não existe consenso para uma definição plena, importa contudo refletir sobre tentativas conceptuais estabilizadoras. Assim, o conceito de segurança energética, que foi definido por Kalicki & Goldwyn (2005, como citado em Silva & Rodrigues, 2015, p. 46) como "a capacidade de aceder aos recursos que são necessários para o desenvolvimento contínuo do poder nacional", pela IEA (2022) como a "disponibilidade ininterrupta de fontes energéticas a um preço acessível", que viu alargado o seu perímetro conceptual aos quatro "As" — availability/acessibility/affordability/acceptability —, que remetem, sucessivamente, para uma análise geológica/geopolítica/económica/ambiental (Asia Pacific Energy Research Centre, 2007) ou, entre muitos outros esforços definidores, pela percepção que a política de segurança energética "deve procurar assegurar que os produtos energéticos estejam fisicamente disponíveis no mercado de forma contínua e a um preço acessível (tanto para os consumidores privados como para a indústria)" (CE, 2000, p. 9); tem natureza policêntrica. Qualquer que seja a enunciação apresentada, cuja recombinação de fatores dependerá sempre das particulares necessidades do formulante, sendo necessariamente diferente para compradores ou vendedores, parece ser seguro afirmar que a condução de uma política de segurança energética tem como finalidade a redução da incerteza através do balanceamento eficiente de necessidades e recursos com o objetivo último de garantir o bem-estar, o crescimento económico e a segurança nacional (Barros, 1984; Campos, 2017, 2018; Eiras, 2011; Nunes, 2015; Rodrigues & Campos, 2017; Silva & Rodrigues, 2015). Importa, agora, perceber quais as fragilidades europeias e portuguesas neste domínio.

Da (in)segurança energética europeia à (in)dependência portuguesa: a espada de Dâmocles em suspensão

A UE a 27, para além de, provavelmente, o mais bem-sucedido projeto de integração supranacional e intergovernamental da história, continua a ser, com os Estados Unidos e a China, um dos três grandes blocos económicos, sendo o maior importador de energia do mundo (CE, 2015). Com um passado turbulento, os Estados-Membros souberam compreender "(…) a importância histórica do fim da divisão do continente europeu e a necessidade da criação de bases sólidas para a construção da futura Europa" (Tratado da União Europeia, 2016, p. 3). Depois de séculos de confrontos ininterruptos no continente e nos respetivos impérios, em 1945 os países europeus estava à beira do colapso, esmagados entre o capitalismo americano e do comunismo soviético (Vaïsse, 2004). Cientes da sua nova fraqueza e da estreiteza dos seus recursos, nomeadamente de fontes energéticas primárias, sobretudo comparados com os dos novos blocos, decidem que a única forma de a Europa se manter relevante no mundo é unindo-se (Kissinger, 1996). Federica Mogherini, antiga Alta Representante para os Negócios Estrangeiros e Política de Segurança da UE, sumarizou tudo quando afirmou que "a [UE] é composta por dois tipos de Estados: os pequenos e os que ainda não perceberam que são pequenos" (Mogherini, 2017). Foi a forma como as suas diferenças foram geridas e a sua fragmentação, razão do seu poder e força desde o século XV, como assinalou Diamond (2015), ultrapassada, que fazem deste união voluntária de Estados um exemplo. Assim, e não surpreendentemente, dois dos primeiros três tratados constitutivos das então Comunidades Europeias — Comunidade Europeia do Carvão e do Aço, de 1951, e Comunidade Europeia da Energia Atómica, de 1957 — tiveram exatamente a questão energética como seu eixo fundacional (CE, 2000; Silva, 2007).

As fraquezas europeias no domínio energético são assim imensas, como se uma espada de Dâmocles, como referem Rodrigues e Silva (2015), sobre ela pendesse. Na realidade, a UE, sendo um gigante económico e uma potência industrial, e de acordo com o Eurostat (2022), importava em 2020 mais de 57% de toda a energia primária, compreendida como "toda a energia utilizada diretamente ou a que é sujeita a transformação para outras formas de energia" (OE et al., 2021, p. 130), que consumia. Ainda de acordo com a estatística explicada do Eurostat (2022), pese embora se tenham registado, nos anos anteriores, sistemáticas diminuições do consumo de fontes primárias de energia, como carvão, petróleo e gás natural, fruto da descarbonização e da melhoria na eficiência energética, ainda assim a vulnerabilidade era evidente, e nem o considerável crescimento das renováveis atenuou esta dependência do exterior,

tendo em conta que todos os Estados-Membros eram, e são, importadores líquidos de energia, sendo a Rússia, entre 2010 e 2020, responsável pelo fornecimento de entre 25 e 50% do carvão, entre 25 e 35% do petróleo e 30 e 38% do gás natural. A atitude revisionista da Rússia, que foi merecendo uma resposta europeia fragmentada, incapaz de moderar os apetites do vizinho, constitui uma vulnerabilidade gritante que afeta fortemente a sua segurança energética, especialmente no tocante ao gás, transportado sobretudo em gasodutos e não facilmente substituível (Eiras, 2011; Franco, 2017; Marques, 2020). Pelo menos desde a invasão da Geórgia em 2008 e da anexação de Crimeia, em 2014, dos ciberataques dirigidos à Estónia e Geórgia em 2007/2008, e do *bullying* contínuo aos países bálticos e à Ucrânia, este último consumado com a invasão de fevereiro de 2022, que ficou claro que a utilizações destes recursos naturais, especialmente do gás, constituiriam uma arma geopolítica que exigiria alternativas (Friedman, 2009; Instituto de Defesa Nacional [IDN], 2013; Lima, 2016; Marshall, 2016; Milhazes, 2016). Note-se que a tensão política russo-europeia causada pela invasão aumentou exponencialmente a atividade maliciosa russa no ciberespaço contra interesses da UE, que se viu forçada a robustecer a proteção de IC (CUE, 2022).

Para além disso, ao longo dessa década, quase 60% do fornecimento de gás provinha de apenas três fornecedores — Rússia, Noruega e Argélia —, o que corresponde a uma ameaça séria à segurança do aprovisionamento, sobretudo se tivermos em conta a instabilidade e elevado risco de incumprimento contratual de muitos dos países comercializadores de fontes primárias (Coface, 2020). Idêntica ameaça, embora mitigada, é identificável no campo do petróleo, com outros *players*. Na década em análise, a taxa de dependência energética, cujo inquietante aumento, com raízes no pretérito, tinha já dado origem à Estratégia Europeia de Segurança do Aprovisionamento Energético (CE, 2000), compreendida como a proporção de energia que uma economia tem de importar, manteve-se sempre perto dos 60%, sendo cerca de 95% devidos ao petróleo, 80% ao gás natural e 40% aos combustíveis líquidos (Eurostat, 2022).

Como afirmam Silva e Rodrigues (2015), Rodrigues e Silva (2015) e Lima (2016), a fragilidade europeia neste domínio é evidente. Para além de uma união energética, de um mercado único de energia e de interconexões transfronteiriças cuja concretização tarda, e que tem como pano de fundo o choque de interesses dos Estados-Membros, a Europa, que até terá interessantes reservas, incluindo a bacia lusitana em Portugal (Oil Industry Insight, 2018), entendeu não enveredar pela

revolução tecnológica que, recentemente, independentizou energeticamente os Estados Unidos, o designado *fracking*, perdendo assim uma oportunidade de se capacitar endogenamente, de aumentar a sua soberania energética e de se defender contra ameaças geopolíticas num momento no qual a doutrina *might-makes-right* parece renascer (Fix & Kimmage, 2022), não tendo demonstrado também vontade de diversificar o abastecimento, por exemplo, para a bacia atlântica e América Latina (Silva, 2007), para o ocidente e norte de África (Leal, 2015) ou à Ásia central via Grécia e Turquia (Fernandes, 2015).

Portugal, tal como os seus parceiros europeus (Rodrigues & Silva, 2015), tem também uma fortíssima dependência energética face ao exterior, que em 2019 se cifrava em 74,2%. Para piorar a situação, dois terços da energia primária consumida, por forma de energia, provem do petróleo e do gás natural, importados. Da energia final consumida, 46,2% é-o na forma de petróleo, 10,6% de gás natural e 24,7% na forma de eletricidade, sendo as renováveis responsáveis por apenas 10,8% do consumo (OE et al., 2021). Como o saldo importador continua a ser elevado, e não se espera que diminua com a velocidade que seria desejável já que quase 40% da energia consumida o é no setor dos transportes (OE et al., 2021), cuja mudança de perfil energético, que tenderá à eletrificação da sociedade através de sistemas inteligentes, abandonando os combustíveis fósseis, fundamental na descarbonização e no esforço de aproveitamento das renováveis, será demorada (IEA, 2021; Silva, 2015); o crescimento e a competitividade das economias nacional e europeia (CE, 2015) ficam dependentes do preço destas matérias-primas nos mercados, o que constitui, para além de um garrote ao desenvolvimento, uma fragilidade evidente, pelo potencial de chantagem de terceiros, e.g. da Rússia, com consequências potenciais graves na segurança nacional (Campos, 2017; Leal, 2015; Silva, 2007), como justamente agora se vê.

Pese embora a dimensão marítima de Portugal, por onde entra 70% da energia que consome, represente uma oportunidade, aumentando a resiliência do País (Brito, 2017), que assim pode manobrar politicamente, desde que em alinhamento com a potência marítima dominante, os Estados Unidos da América, naqueles que têm representado, desde o 25 de Abril, os três eixos da política externa portuguesa — o Europeu, o Atlântico e o Lusófono (Sá, 2015) — importará, como refere (Lima, 2016), que se possam aproveitar as vantagens que o Atlântico, enquanto centro de revolução energética, apresentará no futuro, desde que Portugal tenha capacidade para exercer

soberania sobre ele e de garantir a segurança, em terra e no ciberespaço, da IC energéticas essenciais ao País.

As ameaças às infraestruturas críticas no ciberespaço

Conforme sumarizou Friedman (2020), muitos dos bens de consumo de que hoje disfrutamos, como o microship, o telemóvel, as baterias de lítio ou o GPS foram, originalmente, criações militares.

Contudo, talvez nenhuma tenha impactado tão profundamente a nossa vida como a internet, criada nos anos 60 para partilha rápida de informação militar. Neste particular, e conforme sustenta a atual Estratégia Nacional de Segurança no Ciberespaço (ENSC), aprovada pela RCM 92/2019, de 5 de junho, se o uso maciço, e crescente, das tecnologias, com especial ênfase futuro na *internet-of-things*, vem permitindo um desenvolvimento social sem paralelo, criando o que Giddens (1990, p. 177) chamou de "modernidade inerentemente globalizante", é também verdade que as oportunidades de comprometimento das redes e sistemas de informação é imenso, sobretudo num tempo de exponencial crescimento das profundas interligações e conexões entre instituições e infraestruturas, incluindo críticas, onde como afirma Natário (2014), a sociedade prefere o risco da interligação à segurança dos processos. Novos problemas securitários exigem abordagens renovadas, sobretudo neste admirável mundo novo onde Castells (2010) afirma que "o virtual se torna uma dimensão essencial da nossa realidade" (p. XVIII), a internet "o tecido de comunicação das nossas vidas" (p. XXVI) e o ciberespaço aparece como novo palco de uma velha "disputa global pelo conhecimento e poder" (Poiares, 2019, p. 20). Ciente dos constrangimentos, a ENSC entendeu definir, lado a lado, cibersegurança e ciberdefesa, sendo também de notar a referência, em quatro momentos distintos, e de forma conjunta, à necessidade de alinhamento com a Estratégia da União Europeia para a Cibersegurança de 2013 (CE, 2013) e à política de ciberdefesa da Organização do Tratado do Atlântico Norte (NATO) que, no seu novo conceito estratégico, para além de eleger a UE como "parceiro único e essencial" (NATO, 2022, p. 10) priorizou a defesa do ciberespaço e a proteção de IC. A Estratégia da União Europeia para a Cibersegurança, que presta uma especial atenção às IC, globalmente consideradas, e que prescreve expressamente a necessidade de reforçar a resiliência "dos sistemas de controlo industriais e das infraestruturas de transporte e de energia no ciberespaço" (CE, 2013, p. 8); entendia também já então a NATO como parceiro decisivo, importando pois não desperdiçar esse potencial sinergético. Se Santos (2018, p. 30) reflete na necessidade "de criar uma estrutura de

coordenação político-estratégica para a cibersegurança" que dê coerência às políticas parcelarmente prosseguidas, para Moniz (2018) essa convergência sinergética parece inevitável, não apenas considerando a natureza difusa da ameaça ciberespacial, mas sobretudo quando se questiona se um ataque a uma IC energética deverá ser considerada cibercrime ou um ato de ciberguerra.

Quer se tratem de organizações criminosas ou de Estados, o ciberespaço oferece a possibilidade de provocar elevados danos a um cada vez maior leque de alvos potenciais de forma rápida e frequentemente anónima com apenas um custo reduzido (Santos et al., 2018). Como aponta Nye (2022), se ataques de ransomware, interferência eleitoral, espionagem empresarial ou ataques a redes elétricas dão uma ideia da anarquia do ciberespaço, terá de ser, para já, a diplomacia, na ausência de tratados internacionais reguladores, apoiada pela capacidade de retaliar, a via negocial principal. Com a emergência da inteligência artificial, — cuja superinteligência poderá criar, a prazo, perigo existencial para a humanidade, e que deverá merecer crescentemente a nossa atenção (Oliveira, 2019) —, e com o impacto expectável desta na ordem e segurança mundiais, Kissinger et. al (2021) defendem que só tratados limitativos semelhantes àqueles assinados na guerra fria para o controlo de armamento estratégico, poderão, no interesse de todos, evitar o caos. Na mesma linha, afirma Alperovitch (2022), utilizando como exemplo a ciberespionagem feita pela China, que tem sido especialmente agressiva com os Estados Unidos no ataque a universidades e empresas *hi-tech*, que os ciberataques parecem ser um sintoma e não a doença, afirmando que as tensões geopolíticas exigem respostas geopolíticas e não meras soluções técnicas.

Como a segurança do ciberespaço depende de entidades públicas, de empresas privadas e de cidadãos particulares, uma política coerente neste domínio, que trate a ameaça como global (Natário, 2014), é difícil de conseguir. Tendo em conta que a poupança em matéria de cibersegurança de uma empresa pode comprometer o delicado sistema de interdependências onde opera e ter efeitos comprometedores sistémicos, pondo em causa a segurança nacional (Nye, 2022), o Regime Jurídico da Segurança do Ciberespaço (RJSC), aprovado pela Lei 46/2018, de 13 de agosto, impõe às empresas mais expostas que não só se protejam adequadamente como comuniquem os ataques de que forem alvo ao CERT.PT, um serviço do Centro Nacional de Cibersegurança (CNCS) — o órgão a quem compete garantir o que o ciberespaço é usado de forma livre e segura — que coordena a resposta a ciberincidentes, punindo com um quadro contraordenacional a desobediência a estes princípios. Como seria de esperar, o setor energético é, a par dos

transportes, o mais exposto à regulação, o que atesta da sua criticidade, o mesmo acontecendo no Decreto-Lei 20/2022, de 28 de janeiro, que aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das IC nacionais e europeias. Não obstante, o RJSC vai mais longe, prevendo expressamente, no nº 7 do art. 7º, que o CNCS atua em estreita colaboração com as estruturas da ciberespionagem, cibercrime, ciberterrorismo e ciberdefesa, deixando entender que "a articulação e estreita cooperação" de entidades tuteladas por diferentes órgãos e ministérios positivada na lei é uma realidade.

Achar que instrumentos de uso comum que foram, e são, armas de guerra, não representam uma ameaça é tão perigoso quanto ingénuo, sobretudo num tempo em que, crescentemente, a segurança e a soberania do Estado também se jogam no ciberespaço (IDN, 2013). Ainda que, até agora, os receios do Secretário da Defesa de Barack Obama, Leon Panetta, de um "cyber-Pearl Harbor" que tirasse vidas, destruísse IC, paralisasse o país e criasse um sentido de vulnerabilidade irrecordável não se tenham concretizado (Gordon & Rosenbach, 2022; Schneider, 2022; Nye, 2022), importará reformar as instituições existentes adequando-as às novas e mais demandantes exigências.

Em Portugal, a criação do Centro de Ciberdefesa (CC), dependente do Chefe de Estado-Maior-General das Forças Armadas (CEMGFA), foi talvez uma das respostas a esta necessidade emergente, competindo-lhe, nos termos do Despacho n.º 13692/2013, de 11 de outubro, "a deteção precoce de ataques e a resposta aos mesmos, envolvendo para esse efeito, sempre que necessário, a condução de operações no ciberespaço". Também aqui a necessidade de proteger IC é uma preocupação notada.

Do ponto de vista da proteção física das IC, cuja competência para a identificação e designação, nos termos do Decreto-Lei 20/2022, é de um órgão da Autoridade Nacional de Emergência e Proteção Civil (ANEPC), partilhando a competência da proteção e resiliência com o Secretário-Geral do Sistema de Segurança Interna (SGSSI) (Ferreira, 2016), as Forças e Serviços de Segurança (FSS) têm um papel fundamental na prevenção — nomeadamente mantendo os seus Planos de Proteção e Intervenção ativos, conjugáveis com os Planos de Segurança, alvo de parecer das FSS na vertente security, obrigatoriamente elaborados pelos operadores e aprovados pelo SGSSI, nos termos do arts. 13 e 16 do Decreto-Lei supra, e realizando simulacros periódicos e contactos frequentes com os operadores —, mas também no tempo da aquisição e tratamento de informações policiais sobre ameaças às IC e na vertente reativo-responsiva, mitigando efeitos de ataques cinéticos ou ciberataques e/ou gerindo outros incidentes. Neste domínio, o cadastro

está por fazer e o Plano Nacional de Proteção de IC por elaborar (Ministério da Administração Interna [MAI], 2022b; Pestana, 2016).

Às IC, que o RJSC define como as componentes/sistemas essenciais para a manutenção da vida em sociedade e cuja perturbação ou destruição poriam em causa a prestação dos serviços vitais por eles assegurados, a ENSC dedica o seu Eixo 3, proteção do ciberespaço e das infraestruturas, prevendo a possibilidade de um Estado agressor procurar provocar, no ciberespaço, a disrupção dos serviços do País através de operações de cibersabotagem contra elas. Tendo em conta que a Lei Orgânica da PSP, aprovada pela Lei 53/2007, de 31 de agosto, estabelece, na alínea j) do nº 2 do art. 3º que compete à PSP proteger pontos sensíveis e outras instalações críticas — sobre a indefinição conceptual relativa à matéria de IC e à sua dispersão legislativa, que em nada parece ter mudado desde 2016, ver (Pestana, 2016, pp. 9-10) —, a definição clara de quantas e quais são essas IC, bem como qual o modelo protetivo a respeitar e qual a coordenação possível entre as Forças Armadas (FA) e as FSS também no ciberespaço, num exercício já tentado por Martinho (2017), é fundamental.

A indissociabilidade entre as componentes interna e externa da segurança neste novo domínio operacional representado pelo ciberespaço, o quinto depois da terra, mar, ar e espaço (IDN, 2013; NATO, 2022), é bastante evidente no Conceito Estratégico de Defesa Nacional (CEDN), aprovado pela RCM 19/2013, de 21 de março, em processo de revisão, que expressamente consagra como uma das vulnerabilidades do País precisamente a dimensão energética. Interessante é também verificar a aproximação ao fenómeno da cibercriminalidade — cuja transnacionalidade da ameaça cibernética é reconhecida, estimulando-se a criação de uma estratégia integrada de respostas civis e militares — cujos ataques são classificadas como potencialmente devastadores porque suscetíveis de poderem fazer colapsar "uma organização social moderna", especialmente se se tratarem de IC.

Pese embora, por agora, as IC energéticas, como refinarias e centrais elétricas ou sistemas de transporte de gás, petróleo ou eletricidade, utilizem sistemas de controlo industrial — com especial ênfase os sistemas SCADA, mas também DCS — para apoio aos processos de gestão e operação, autónomos, frequentemente offline, localizados em lugares remotos onde são raramente acedidos por técnicos; espera-se que num futuro próximo possamos ter arquiteturas abertas e interligadas com sistemas corporativos online, o que representará uma enorme vulnerabilidade (IDN, 2013; Natário, 2014; Pestana, 2016). O precedente aberto pelo vírus Stuxnet, que atacou com sucesso precisamente sistemas

SCADA no Irão, prejudicando o respetivo programa nuclear (Carvalho, 2019; Kushner, 2013; Yergin, 2011), deve servir de alerta. Como acontece frequentemente na bruma do ciberespaço, não se percebeu, embora se desconfie, se se tratou de um crime ou de um quase-ato de guerra (Fernandes, 2012), uma vez que ninguém o assumiu (Kissinger et al., 2021).

Finalmente, importa destacar o ataque de ramsomware que em 2021 paralisou, durante uma semana, o *Colonial Pipeline*, um oleoduto que abastece a costa leste dos Estados Unidos com quase metade do combustível. Não obstante o impacto limitado do ciberataque, este criou um tal pânico que a população, num ápice, esgotou artificialmente as reservas existentes (Schneider, 2022; Bansemer, 2021). Se o incidente simulou os efeitos nefastos produzíveis na ordem pública pela escassez de energia, provou sobretudo que a defesa destas infraestruturas no ciberespaço será muito mais difícil de conseguir do que historicamente foi sendo com sistemas analógicos (Jaffe, 2021).

Perceber qual o melhor arranjo institucional possível para enfrentar este desafio e acomodar estas transformações é, pois, fundamental.

Reflexões sobre a necessidade de um conceito estratégico de segurança nacional

Para Elias (2011), o conceito de segurança é "cada vez mais polissémico, contestado, ambíguo e complexo" (p. 3), um conceito "banda larga" globalizante (p. 27). Se Jore (2019), numa perspetiva mais normativa, define *security* como a capacidade de prevenir e gerir os riscos, as crises e as ameaças causados maliciosamente como terrorismo, crime organizado e cibercrime — *hacking* —, construindo resiliência organizacional e humana manifestada, e.g., na necessidade de proteger IC, Oliveira (2006, pp. 15-16) observa que a "segurança é cada vez mais um bem público que deve ser coproduzido pelo conjunto dos atores sociais", incluindo novos "poderes supranacionais e infranacionais".

A segurança interna não é já uma atividade que se desenvolva apenas no território nacional pois, como afirma Elias (2013, 2019, 2011), se a necessidade de intervir policialmente no exterior, de forma a prevenir corolários negativos internos, externaliza a segurança interna, a admissibilidade da possibilidade de um reforço da atuação das FA em território nacional internaliza a segurança externa. O autor enfatiza, veementemente, a necessidade de coordenação e integração entre as políticas de relações internacionais, segurança interna e defesa, afirmando mesmo que, num país pequeno e de recursos limitados — em que, como atesta Pereira (2012), a falta de cooperação política para a

realização de reformas estruturais tem prejudicado todos e beneficiado ninguém, diminuído a soberania nacional — "as políticas públicas orientadas para a segurança têm-se caracterizado, desde sempre no nosso país, pela sua natureza gradualista, descontínua, fragmentada, casuística e sobretudo normativa, revelando uma perspetiva micro da realidade e falta de uma visão e de uma estratégia global" (Elias, 2013, p. 24). Também Tomé (2019) entende que a tradicional dicotomia entre segurança externa e interna deixou de fazer sentido. Argumentando que muitos dos perigos para a segurança interna vêm já do exterior — terrorismo e criminalidade organizada —, defende que o combate exigirá então não apenas respostas nacionais integradas como também cooperação transnacional, sobretudo no ciberespaço, "no qual é impossível traçar ou reclamar linhas de soberania estatal, [o que] obriga a rever todas as tradicionais conceções em torno das dimensões interna e externa da segurança" (p. 74). Com efeito, se a Estratégia Global para a Política Externa e de Segurança da União Europeia (UE, 2016) refere que "a segurança interna e externa estão cada vez mais interligadas: a nossa segurança interna depende da paz nas regiões para além das nossas fronteiras"(p. 5), acrescentando que essa ligação "abrange a resposta a desafios com uma dimensão interna e externa, como o terrorismo, as ameaças híbridas, a cibersegurança, a segurança energética, o crime organizado e a gestão das fronteiras externas"(p. 14), outros documentos europeus, como a Agenda Europeia para a Segurança, de 2015 ou a Estratégia Renovada de Segurança Interna da União Europeia para 2015-2020, de 2015, vão no mesmo sentido (Tomé, 2019).

O conceito de segurança interna constante na atual Lei de Segurança Interna (LSI) — Lei 53/2008, de 29 de agosto — está objetivamente datado, não obstante o Conselho Superior de Segurança Interna (CSSI), órgão de audição e consulta do Primeiro-Ministro, prever o assento do CEMGFA, do presidente da ANEPC e do coordenador do CNCS, o que permite à cibersegurança/ciberdefesa serem consideradas. Tendo-se perdido então a oportunidade para definir um Conceito Estratégico de Segurança Interna (CESI) nos termos preconizados na RCM nº 45/2007, de 19 de março, que marcou o início do processo legislativo da LSI e que já então recomendava a necessidade de uma mais estreita colaboração entre o SSI e o Sistema de Defesa Nacional e Proteção Civil, o tema volta à discussão pública na sequência das declarações proferidas pelo Ministro da Administração Interna que, numa audição parlamentar no âmbito da apreciação na especialidade do Orçamento do Estado de 2022, referiu ser sua intenção a definição de um CESI contando, para tanto, "com o contributo da Academia e dos demais centros de produção de conhecimento" (MAI, 2022a).

Oliveira (2006), numa obra seminal sobre a segurança interna que comparava os modelos policiais português, canadiano, francês e espanhol, concluiu que a complexidade do sistema policial português, sobretudo no que diz respeito ao número de organizações nacionais — cinco —, tipologia de tutela — com três ministérios, o mais elevado — e modelo — centralizado e plural —, não obstante a diferença considerável de escala territorial e populacional face aos comparantes; gerava fragmentação, descoordenação, desequilíbrios estatutários/remuneratórios — que inibiam, como agora se vê, fusões ou comandos conjuntos — e estanqueidade. Não obstante refletir criticamente sobre a adoção de um modelo dual puro, com uma Polícia Nacional civil e uma Gendarme, militarizada, como acontece em França e quase em Espanha — na linha do cenário Z, a mais disruptiva das três propostas avançadas pelo estudo encomendado pelo MAI em 2006 (Instituto Português de Relações Internacionais [IPRI], 2006) —; a reforma de 2007 acabou por ditar a manutenção do sistema dual mitigado/multitutelado (Guedes & Elias, 2010), que constituía, para alguns, um sistema original, atípico e próximo da ingovernabilidade (Elias, 2011; IPRI, 2006) e a emergência do SGSSI, o *diretor de segurança interna* previsto numa das opções de reforma avançadas por Oliveira (2006, p. 268).

Considerando a dimensão das mudanças sociais, tecnológicas, económicas e culturais que vivemos e os desafios que uma sociedade permanentemente interligada imporá às instituições (Castells, 2010), importa considerar duas propostas de reforma destinadas a acomodar, entre outros, os desafios ciberespaciais.

O primeiro, designado S*egurança Horizonte 2025. Um Conceito de Segurança Interna* (Lourenço et al., 2015), defendia a criação de um CESI que permitisse desenvolver um quadro doutrinal/estratégico, equivalente ao já existente na Defesa, destinado a melhorar a capacidade de enfrentamento de novas ameaças vindas do exterior, como a criminalidade organizada transfronteiriça e a cibercriminalidade — mas também a segurança energética — e que pudessem afetar as IC e os sistemas informáticos. Aliás, quando refletem sobre a eficiência do SSI, são perentórios a afirmar que o quadro de ameaças obriga à intervenção em todos os domínios operacionais, o que implica a existência de capacidades próprias de prevenção e repressão no ciberespaço, novo teatro agora gerador do seu próprio sentimento virtual de insegurança, propondo a centralização destas capacidades sob uma mesma dependência funcional. Nesse cenário, a utilização dual de meios e capacidades da segurança interna seria uma realidade (Costa, 2017). O CESI suportar-se-ia numa Estratégia de Segurança Interna, revista periodicamente

(Lourenço et al., 2015). Este modelo, representando uma evolução clara, é no entanto menos ousada, e multidisciplinar, que a proposta seguinte.

Considerada como uma evolução natural do primeiro modelo, e tendo por base os exemplos de Espanha, Reino Unido ou Estados Unidos, a *Estratégia de Segurança Nacional (ESN): Portugal Horizonte 2030* (Lourenço & Costa, 2018) é audaz. Reconhecendo as mudanças brutais, mais intensas e profundas que as anteriores, que a quarta revolução industrial (Schwab, 2016) trará no domínio das ameaças estratégicas e/ou híbridas, estatais ou inorgânicas/criminais, como a cibercriminalidade ou guerra tecnologizada, que não se compadecem com a linearidade e territorialidade das ameaças clássicas, e percebendo a interligação entre todos os setores societais, particularmente os de segurança — safety/security —; prevê uma inovadora abordagem conjunta suportada na defesa dos interesses vitais assim definidos pelo Estado onde os parcos recursos nacionais pudessem ser eficiente/racionalmente alocados, criando um conceito compreensivo de segurança que abarcaria não apenas defesa, segurança interna e proteção civil mas também a diplomacia, informações, economia/finanças, cultura e comunicação (Lourenço & Costa, 2018).

Concretamente no que diz respeito ao SSI, os proponentes, que não põem em causa a eficácia da atuação das FSS, atentos os números, questionam contudo a eficiência de um SSI com uma multiplicidade de polícias, com competências conflituantes e entropiadoras, tutelas políticas diferenciadas e com desejos autárquicos onde a competição/rivalidade e a luta por recursos prevalecem sobre a cooperação/colaboração. Como medida corretiva, entendem que o MAI deveria passar a tutelar diretamente, sem eventual delegação, o SGSSI e todas as FSS e ainda o Serviço de Informações de Segurança (SIS), impondo-se assim coerência a um sistema atomizado, propondo ainda o reforço dos poderes o SGSSI junto das polícias e a integração da ANEPC sob a sua direção operacional.

Contudo, o grande *insight* desta ESN seria a subordinação de estratégias setoriais a uma grande ESN que guiasse, para um mesmo destino, para além de outras estruturas do Estado, serviços de informações, defesa, segurança interna e ainda a área da agora designada segurança humana e proteção civil, e que emprestasse depois coerência e integralidade ao fragmentado e incompleto. No que diz respeito ao ciberespaço, a ESN aconselha ao desenvolvimento de uma capacidade defensiva/protetiva e ofensiva interligadas, algo muito difícil de realizar sem um instrumento estratégico agregador, pondo ênfase simultâneo no combate ao cibercrime, proteção de IC e reação a incidentes. Antecipando ciberataques a IC, públicas ou privadas, sobretudo telecomunicações e

energia, suscetíveis de porem em causa a segurança nacional, propõem a sua identificação e protecção adicional, aumentando-lhes a resiliência, fazendo-se a gestão do risco possível entre a vertente *safety* — ANEPC — e *security* — SSI —, se necessário criando um organismo autónomo como em Espanha e Reino Unido, cooperando-se internacionalmente, estimulando a atuação conjunta do CNCS e do CC, sugerindo-se mesmo que no ciberespaço polícias, militares e diplomatas cooperem para cumprir os fins de segurança nacional enquanto se define o modelo de soberania digital a adotar num tempo de desterritorialização da segurança e territorialização do ciberespaço. Para o conseguir, os autores propõem como caminho a formulação de uma Estratégia de Segurança Nacional que suporte uma Lei de Segurança Nacional, revista com a adequada frequência, criando-se depois um Conselho Superior de Segurança Nacional, órgão de aconselhamento estratégico, onde estivessem representados todos os órgãos supramencionados (Lourenço & Costa, 2018).

Discussão/Conclusão

A energia é o sangue que corre nas veias do corpo societal contemporâneo. Sem ela, não nos movimentaríamos, comunicaríamos, trabalharíamos ou viveríamos da mesma forma, não seríamos tão produtivos nem teríamos a mesma qualidade de vida. Garantir o seu fluxo constante e ininterrupto é, portanto, uma tarefa fundamental do Estado, que deverá usar os instrumentos político-diplomáticos necessários para o conseguir, sobretudo se, como é o caso de Portugal e da Europa, for um grande importador de energia e estiver dependente, para manter o crescimento das suas economias e o bem-estar das suas populações, do fornecimento de um pequeno número de países politicamente instáveis e frequentemente incapazes de cumprir acordos firmados, que podem usar a energia como arma geopolítica, não apenas, num primeiro momento, comprimindo ou dificultando os fornecimentos, mas também, tensionadas ou quebradas as ligações diplomáticas, usando o ciberespaço como novo teatro de confronto. Havendo disrupções no fornecimento ou no preço, ou ataques bem-sucedidos a IC, a ordem pública pode ver-se alterada.

Numa sociedade tão intensamente interligada como a nossa, em que a segurança, e até a privacidade, são conscientemente sacrificadas ao altar da necessidade conectiva, as fragilidades emergentes são imensas, e são-no especialmente no ciberespaço, um novo domínio operacional com fronteiras ténues entre o ato criminoso e o bélico, e onde, com poucos recursos e de forma anónima, se podem produzir danos consideráveis a IC

energéticas interconectadas na rede cujos efeitos sistémicos potencialmente devastadores no conjunto representam uma enorme vulnerabilidade.

Neste cenário de grandes mudanças e de enorme volatilidade, o conceito e a própria arquitetura de segurança interna, fragmentado, descoordenado, desequilibrado e estanque, criado para enfrentar as ameaças clássicas, territorializadas e segmentadas, deverá adaptar-se às novas necessidades, dando agora um salto maior do que aquele que se propôs dar em 2007 com a tentativa de definir então um CESI. Com efeito, a emergência do terrorismo, criminalidade organizada e cibercriminalidade, e até os desafios antecipados pela inteligência artificial, que não conhecem fronteiras nem fazem exercícios preditivos de especialização investigatória de polícias e/ou de militares, vieram pôr em causa a tradicional dicotomia entre segurança interna e externa e a atual arquitetura de segurança e defesa. Para a ultrapassar, Portugal, um país com capacidades limitadas e endividado, onde as instituições rivalizam e lutam por recursos, ambiciosamente, deverá elencar claramente o conjunto de interesses que entende serem vitais e definir, de forma holística, um conceito estratégico concertado e multidimensional de segurança nacional, emulando outros países, que congregue esforços, racionalize recursos e coordene o fragmentado, interconectando não apenas as estruturas da segurança e defesa, mas também aquelas da proteção civil, das informações, da economia/finanças, da diplomacia, da cultura e da comunicação.

Numa altura em que há uma maioria parlamentar estável recentemente legitimada, em que o MAI manifestou a intenção de criar um CESI, e portanto de rever o SSI, e que o CEDN está em fase de revisão, parecem estar reunidas as condições ideais para reformar a arquitetura de segurança em Portugal, criando um CESN que prepare o País para os desafios vindouros.

Tendo em conta as limitações deste estudo teórico e a importância decisiva dos temas tratados, determinantes para o futuro da PSP, do SSI e do País, espera-se que os mesmos possam merecer investigação futura conjunta.

Referências Bibliográficas

Alperovitch, D. (2022). The Case For Cyber-Realism: Geopolitical Problems Don't Have Technical Solutions. *Foreign Affairs, 101*(1), 44-50. https://www.foreignaffairs.com/articles/united-states/2021-12-14/case-cyber-realism

Asia Pacific Energy Research Centre. (2007). *A quest for energy security in the 21st century: resources and constraints.* APERC. https://aperc.or.jp/file/2010/9/26/APERC_2007_A_Quest_for_Energy_Security.pdf

Bansemer, J. (2021, December 10). Soon, the Hackers Won't Be Human: But AI Can Boost Cyber Defenses, Too. *Foreign Affairs*. https://www.foreignaffairs.com/articles/united-states/2021-12-10/soon-hackers-wont-be-human

Barros, R. (1984). Política energética/segurança nacional. *Nação e Defesa, 9*(31), 89-118. http://hdl.handle.net/10400.26/2794

Brito, A. M. R. (2017). *A dimensão marítima da segurança energética de Portugal* [Trabalho de Investigação Individual não publicado do Curso de Estado-Maior Conjunto – Instituto Universitário Militar]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/21396

Campos, A. C. F. S. (2017). Segurança Energética e Defesa Nacional: o caso de Portugal. In V. D. R. Viana (Coord.), *I Seminário IDN Jovem* (pp. 157-171). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/22826

Campos, A. C. F. S. (2018). Segurança Energética Europeia: o Corredor de Gás Meridional e o Projeto EastMed. In V. D. R. Viana (Coord.), *III Seminário IDN Jovem* (pp. 215-235). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/25256

Carvalho, A. A. R. (2019). Ciberespaço e os Novos Desafios à Soberania e à Segurança dos Estados. In M. H. C. Carreiras (Coord.), *V Seminário IDN Jovem* (pp. 219-235). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/32433

Castells, M. (2010). *The Rise of the Network Society* (2nd ed.). Wiley-Blackwell.

Coface. (2020*). Coface Country & Sector Risks Handbook: Analysis And Forecast for 162 Countries and 13 Sectors*. Coface.

Comissão Europeia. (2000). *Livro Verde: Para yma Estratégia Europeia de Segurança do Aprovisionamento Energético (COM (2000) 769 final).* União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52000DC0769&from=PT

Comissão Europeia. (2013). *Estratégia da União Europeia para a Cibersegurança: Um Ciberespaço Aberto, Seguro e Protegido (JOIN(2013) 1 final).* União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001&from=PT

Comissão Europeia. (2015). *Pacote União de Energia: Uma Estratégia-Quadro para uma União Da Energia Resiliente Dotada de uma Política em Matéria de Alterações*

Climáticas Virada para o Futuro (COM(2015) 80 final). União Europeia. https://eur-lex.europa.eu/resource.html?uri=cellar:1bd46c90-bdd4-11e4-bbe1-01aa75ed71a1.0020.01/DOC_1&format=PDF

Conselho da União Europeia. (2010). *Estratégia de Segurança Interna da União Europeia: Rumo a um Modelo Europeu de Segurança.* Serviço das Publicações da União Europeia. https://data.europa.eu/doi/10.2860/87810

Conselho da União Europeia (2022, 19 de julho). *Declaração do Alto Representante em nome da União Europeia sobre atividades cibernéticas maliciosas conduzidas por hackers e grupos de hackers no contexto da agressão da Rússia contra a Ucrânia* [Nota à imprensa]. União Europeia. https://www.consilium.europa.eu/pt/press/press-releases/

Costa, A. (2017). Utilização Dual de Meios e Capacidades da Segurança Interna. *Segurança e Defesa,* (36), 17-24. https://eurodefense.pt/wp-content/uploads/2021/03/201709_Revista-Seguran%C3%A7a-e-Defesa-n.%C2%BA-36_Edi%C3%A7%C3%A3o-Digital.pdf

Decreto-Lei n.º 20/2022, de 28 de janeiro. *Diário da República, Série I*(20). https://data.dre.pt/eli/dec-lei/20/2022/01/28/p/dre/pt/html

Despacho n.º 13692/2013, de 28 de outubro. *Diário da República, Série II*(208). https://dre.pt/dre/detalhe/despacho/13692-2013-3295679

Diamond, J. (2015). *Armas, Germes e Aço: os destinos das soeciedades humanas.* Círculo de Leitores.

Duarte, A. P. D. S. & Fernandes, C. I. P. (2011). O problema do Abastecimento de Espanha e Portugal: a Questão do Magrebe. In V. D. R. Viana (Coord.), *Segurança Nacional e Estratégias Energéticas de Portugal e de Espanha* (pp. 37-76). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/1780

Eiras, R. (2011). Os Desafios Estratégicos da Segurança Energética Europeia. In V. D. R. Viana (Coord.), *Segurança Nacional e Estratégias Energéticas de Portugal e de Espanha* (pp. 17-35). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/1780

Elias, L. M. A. (2011). *Segurança na Contemporaneidade - Internacionalização e Comunitarização* [Tese de Doutoramento em Ciência Política não publicada – Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa]. Repositório da Universidade Nova. http://hdl.handle.net/10362/14011

Elias, L. M. A. (2013). A Externalização da Segurança Interna: as Dimensões Global, Europeia e Lusófona. *Relações Internacionais*, (40), 9-29. http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri40/n40a02.pdf

Elias, L. M. A. (2019). A Dimensão Externa da Segurança Interna de Portugal. *JANUS 2018-19 Anuário de Relações Exteriores*, (19), 78-79. http://hdl.handle.net/11144/4863

Eurostat. (2022). *Energy production and imports.* European Comission. https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Energy_production_and_imports#The_EU_and_its_Member_States_are_all_net_importers_of_energy

Fernandes, C. I. P. (2015). Potencialidades e Desafios da Bacia do Cáspio para a Estratégia Europeia de Aprovisionamento: Oportunidades para Portugal. *Relações Internacionais*, (46), 83-99. http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri46/n46a06.pdf

Fernandes, J. (2012). Utopia, Liberdade e Soberania no Ciberespaço. *Nação e Defesa*, (133), 11-31. https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD133/NeD133.pdf

Ferreira, H. J. D. (2016). *Identificação e caracterização de Infraestruturas Críticas - Uma Metodologia* [Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto não publicado – Departamento de Estudos Pós-graduados do Instituto Universitário Militar]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/14615

Fix, L., & Kimmage, M. (2022, February 18). What If Russia Wins? A Kremlin-Controlled Ukraine Would Transform Europe. *Foreign Affairs*. https://www.foreignaffairs.com/articles/ukraine/2022-02-18/what-if-russia-wins

Franco, L. (2017). O Regresso da Geopolítica à Europa. In A. A. Alves (Coord.), *Teoria Política e Geoestrégia: Desafios contemporâneos* (pp. 272-284). Alêtheia.

Friedman, G. (2009). *Os próximos 100 anos: uma previsão para o século XXI* (5ª ed.). Dom Quixote.

Friedman, G. (2020). *The Storm Before the Calm: America's Discord, the Coming Crisis of the 2020s, and the Triumph Beyond*. Penguin Random House.

Giddens, A. (1990). *The Consequences of Modernity*. Polity Press.

Gordon, S., & Rosenbach, E. (2022). America's Cyber-Reckoning: How to Fix a Failing Strategy. *Foreign Affairs*, *101*(1), 10-20.

https://www.foreignaffairs.com/articles/united-states/2021-12-14/americas-cyber-reckoning

Guedes, A. M., & Elias, L. M. A. (2010). *Controlos Remotos: Dimensões Externas da Segurança Interna em Portugal.* Almedina.

Instituto de Defesa Nacional. (2013). *Cadernos IDN nº 12 - Estratégia da Informação e Segurança no Ciberespaço.* Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/7757

International Energy Agency. (1994). *The history of the International Energy Agency: Major Policies an Actions of the IEA* (Vol. 2). IEA. https://iea.blob.core.windows.net/assets/521c392f-dc53-4ab7-9970-b3ab8c29e82c/TheHistoryoftheInternationalEnergyAgency-vol2.pdf

International Energy Agency. (2021). *Portugal 2021: Energy Policy Review.* IEA. https://iea.blob.core.windows.net/assets/a58d6151-f75f-4cd7-891e-6b06540ce01f/Portugal2021EnergyPolicyReview.pdf

International Energy Agency. (2022, July 19). *Energy Security*. https://www.iea.org/topics/energy-security

Instituto Português de Relações Internacionais. (2006). *Estudo para a reforma do modelo de organização do Sistema de Segurança Interna: Relatório Final - Modelos e Cenários.* IPRI - Universidade Nova de Lisboa. http://dx.doi.org/10.13140/2.1.2761.0560

Jaffe, A. M. (2021, June 17). Electricity Is the New Oil: A U.S. Strategy for the Post-Hydrocarbon World. *Foreign Affairs.* https://www.foreignaffairs.com/articles/united-states/2021-06-17/electricity-new-oil

Jore, S. (2019). The conceptual and scientific demarcation of security in contrast to safety. *European Journal for Security Research, 4,* 157-174. https://doi.org/10.1007/s41125-017-0021-9

Kalicki, J. H., & Goldwyn, D. L. (Eds.). (2005). *Energy and Security: Toward a New Foreign Policy Strategy.* Woodrow Wilson Center Press and John Hopkins University Press.

Kissinger, H. A. (1996). *Diplomacia.* Gradiva.

Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021). *The Age of A.I. And Our Human Future.* Little, Brown.

Kushner, D. (2013). The real story of Stuxnet: How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program. *IEEE Spectrum, 50*(3), 48-53. https://doi.org/10.1109/MSPEC.2013.6471059

Landes, D. (2005). *A riqueza e a pobreza das Nações: Por que são algumas tão ricas e outras tão pobres* (7ª ed.). Gradiva.

Leal, C. M. (2015). Os Riscos e Oportunidade das Bacias do Norte de África e da África Ocidental no Abastecimento a Portugal. *Relações Internacionais,* (46), 45-60. http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri46/n46a04.pdf

Lei n.º 53/2007, de 31 de agosto. *Diário da República, Série I*(168). https://data.dre.pt/eli/lei/53/2007/08/31/p/dre/pt/html

Lei n.º 53/2008, de 29 de agosto. *Diário da República, Série I*(167). https://data.dre.pt/eli/lei/53/2008/08/29/p/dre/pt/html

Lei n.º 46/2018, de 13 de agosto. *Diário da República, Série I*(155). https://data.dre.pt/eli/lei/46/2018/08/13/p/dre/pt/html

Lima, B. P. (2016). *Portugal e o Atlântico.* Fundação Francisco Manuel dos Santos.

Lourenço, N., Lopes, A. F., Rodrigues, J. C., Costa, A., & Silvério, P. (Eds.). (2015). *Segurança Horizonte 2025. Um Conceito de Segurança Interna.* Colibri & Grupo de Reflexão Estratégica Sobre a Segurança Interna [GRESI]. https://drive.google.com/file/d/0B1EI2nLqkd-VdnpuSzY3VVdaaVU/view?resourcekey=0-thIT8OfI5X4eAnDj2eFM4g

Lourenço, N., & Costa, A. (Coords.). (2018). *Estratégia de Segurança Nacional: Portugal Horizonte 2030.* Almedina.

Ministério da Adiministração Interna. (2022a). *Orçamento de Estado 2022: Nota Explicativa*. Ministério da Administração Interna. https://www.parlamento.pt/sites/COM/XVLeg/5COF/Paginas/oe2022.aspx

Ministério da Adiministração Interna. (2022b, 8 de julho). *Ministro da Administração Interna empossa José António Gil Oliveira como vice-presidente do Conselho Nacional de Planeamento Civil de Emergência* [Nota à imprensa]. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBQAAAB%2bLCAAAAAAABAAzNDYwsQAAnZ%2b%2bDwUAAAA%3d

Maia, C. M. T. (2019). *O Ciberpoliciamento das Redes Sociais: o Contributo das Ciências Tecnológicas* [Trabalho Individual Final do III Curso de Comando e Direção Policial não publicado, Instituto Superior de Ciências Policiais e Segurança

Interna]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/34925

Marques, D. A. (2020). União Europeia da Defesa: a PESCO e a Participação Portuguesa. In M. H. C. Carreiras (Coord.), *V Seminário IDN Jovem* (pp. 95-116). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/32433

Marshall, T. (2016). *Prisioners of Geography.* Elliott and Thompson Limited.

Martinho, J. P. S. (2017). *As Infraestruturas Críticas em Portugal: um Modelo de Abordagem* [Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto não publicado – Departamento de Estudos Pós-graduados do Instituto Universitário Militar]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/21379

Milhazes, J. (2016). *Rússia e Europa: uma parte do todo.* Fundação Francisco Manuel dos Santos.

Mogherini, F. (2017, October 17). *Speech by High Representative/Vice-President Federica Mogherini* [Award cerimony]. Kaiser-Otto-Preis 2017, Magdeburg, Saxony-Anhalt, Germany. https://www.eeas.europa.eu/node/34107_en

Moniz, P. (2018). Impacto do Ciberespaço na Sociedade em Rede. In P. V. Nunes (Coord.), *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 17-24). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/23687

Moreira, F. (2019). *Cibercriminalidade e Cibersegurança* [Trabalho Individual Final do III Curso de Comando e Direção Policial não publicado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/34934

Natário, R. M. P. (2014). *O ciberespaço e a vulnerabilidade das infraestruturas críticas: contributos para um modelo nacional de análise e gestão do risco social* [Dissertação de Mestrado não publicada – Departamento de Estudos Pós-graduados da Academia Militar]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/8609

North Atlantic Organization Treaty. (2022). *NATO 2022 Strategic Concept.* https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

Nunes, C. M. C. (2015). *O Golfo da Guiné e a segurança energética dos EUA e da China* [Tese de Doutoramento não publicada – Faculdade de Ciências Sociais e Humanas

da Universidade Nova de Lisboa]. Repositório da Universidade Nova. http://hdl.handle.net/10362/16296

Nye, J. S. (2022). The end of Cyber-Anarchy? How to Build a New Digital Order. *Foreign Affairs, 101*(1), 32-42. https://www.foreignaffairs.com/articles/russian-federation/2021-12-14/end-cyber-anarchy

Observatório da Energia, Direção Geral da Energia e Geologia, & ADENE – Agência para a Energia. (2021). *Energia em Números - Edição 2021.* ADENE – Agência para a Energia. https://www.dgeg.gov.pt/media/32skj5iv/dgeg-aen-2021e.pdf

Oil Industry Insight. (2018, September 22). *Europe Shale Gas: An Overview*. https://oilindustryinsight.com/oil-gas/petroknowledge/europe-shale-gas-an-overview/

Oliveira, A. (2019). *Inteligência Artificial*. Fundação Francisco Manuel dos Santos.

Oliveira, J. F. (2006). *As políticas de segurança e os modelos de policiamento: A emergência do policiamento de proximidade.* Almedina.

Parlamento Europeu, & Conselho da União Europeia. (2018). *Regulamento (UE) 2018/1999 do Parlamento Europeu e do Conselho.* Jornal Oficial da União Europeia. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1999&from=PL

Pereira, P. T. (2012). *Portugal: Dívida Pública e Défice Democrático*. Fundação Francisco Manuel dos Santos.

Pestana, J. F. F. (2016). *A proteção de infraestruturas críticas: contributos para o desenvolvimento de um plano nacional de proteção de infraestruturas críticas* [Trabalho Individual Final do II Curso de Comando e Direção Policial não publicado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/34802

Poiares, N. C. L. B. (2019). A cibersegurança à luz da criminologia moderna. In N. T. Castro (Ed.), *Cyberlaw by CIJIC – Centro de Investigação Jurídica do Ciberespaço da Faculdade de Direito da Universidade de Lisboa* (7ª ed.). http://hdl.handle.net/10400.26/34692

Quivy, R., Campenhoudt, L. V. (2008). *Manual de Investigação em Ciências Sociais* (5ª ed.). Gradiva.

Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril. *Diário da República, Série I*(67). https://data.dre.pt/eli/resolconsmin/19/2013/04/05/p/dre/pt/html

Resolução do Conselho de Ministros n.º 45/2007, de 19 de março. *Diário da República, Série I*(55). https://data.dre.pt/eli/resolconsmin/45/2007/03/19/p/dre/pt/html

Resolução do Conselho de Ministros n.º 63/2020, de 14 de agosto. *Diário da República, Série I*(158). https://data.dre.pt/eli/resolconsmin/63/2020/08/14/p/dre/pt/html

Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. *Diário da República, Série I*(108). https://data.dre.pt/eli/resolconsmin/92/2019/06/05/p/dre/pt/html

Resolução do Conselho de Ministros n.º 107/2019, de 1 de julho. *Diário da República, Série I*(123). https://data.dre.pt/eli/resolconsmin/107/2019/07/01/p/dre/pt/html

Rickover, H. (1972). Energy Resources and Our Future. In *Fuel and energy resources, 1972. Part II. Hearings before the Committee on Interior and Insular Affairs, House of Representatives, Ninety-Second Congress, Second Session* (pp. 677-684). U.S. Government Printing Office.

Roberts, A. (2018). *Churchill: Walking with destiny*. Penguin Random House.

Rodrigues, T. M. F., & Campos, A. C. F. S. (2017). Portugal e a segurança energética. Retrato atual e cenários futuros possíveis [Working paper]. In GEO4GER, '*Projecto' A Geopolítica do Gás e o Futuro da relação Euro-Russa.* Fundação para a Ciência e Tecnologia, Instituto Português de Relações Internacionais e Instituto de Defesa Nacional. https://research.unl.pt/ws/portalfiles/portal/6598865/TFR_AC_Portugal_Seguranca Energetica_WP_1_2017.pdf

Rodrigues, T. M. F., & Silva, A. C. (2015). Nota introdutória: Que modelo de segurança energética? *Relações Internacionais*, (46), 05-10. http://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri46/n46a01.pdf

Sá, T. M. (2015). *Política Externa Portuguesa*. Fundação Francisco Manuel dos Santos.

Santos, J. M. M. P. (2021). Segurança energética e a relação Argélia-Portugal: reflexões na segurança. *Politeia, XVIII,* 161-180. http://hdl.handle.net/10400.26/39324

Santos, L. C. (2018). Segurança no Ciberespaço. In P. V. Nunes (Coord.), *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 25-32). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/23687

Santos, L. C., Nunes, P. V., Ralo, J., & Mendes, C. P. (2018). Defesa do Ciberespaço. In P. V. Nunes (Coord.), *Contributos para uma Estratégia Nacional de Ciberdefesa* (pp. 33-46). Instituto de Defesa Nacional. http://hdl.handle.net/10400.26/23687

Schneider, J. (2022). A World Without Trust: The Insidious Cyberthreat. *Foreign Affairs, 101*(1), 22-31. https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust

Schwab, K. (2016). *The Fourth Industrial Revolution*. Crown Business.

Silva, A. C. (2007). A segurança energética da Europa. *Nação e Defesa, 116*(3), 31-72. https://comum.rcaap.pt/bitstream/10400.26/1231/1/NeD116_AntonioCostaSilva.pdf

Silva, A. C., & Rodrigues, T. M. F. (2015). A segurança energética e um modelo para o futuro da Europa. *Relações Internacionais*, (46), 11-24. http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri46/n46a02.pdf

Silva, J. J. C. (2019). *Apontamentos sobre Cibersegurança e Cibercrime* [Trabalho Individual Final do III Curso de Comando e Direção Policial não publicado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Científico de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/34970

Silva, M. M. (2015). A Segurança nas Redes Energéticas e o Caso de Portugal. *Relações Internacionais*, (46), 101-124. http://www.ipri.pt/images/publicacoes/revista_ri/pdf/ri46/n46a07.pdf

Sousa, R. A. (2019). O 'Story Building' de uma Revolução: Perspetivas Pós-Marxistas e Neonacionalistas sobre o Movimento Coletes Amarelos. *Perspectivas - Journal of Political Science, 20*, 9-21. https://doi.org/10.21814/perspectivas.329

Tomé, L. (2019). Sobre a dimensão externa da segurança interna. *JANUS 2018-19 Anuário de Relações Exteriores*, (19), 74-75. http://hdl.handle.net/11144/4861

Tratado da União Europeia, 7 de junho de 2016, https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_2&format=PDF

União Europeia. (2016). *Visão Partilhada, Ação Comum: uma Europa Mais Forte. Estratégia Global para a Política Externa e de Segurança da União Europeia*. União Europeia. https://www.eeas.europa.eu/eeas/global-strategy-european-unions-foreign-and-security-policy_en

Vaïsse, M. (2004). *As relações internacionais desde 1945*. Edições 70.

Viana, V. D. R. (Coord.), Silva, A. C., Duarte, A. P., Fernandes, C., Fânzeres, J., Ribeiro, J. F., Eiras, R., Rodrigues, T. F. (2014). Portugal, a Geopolítica da Energia e a Segurança Energética Europeia. *Instituto de Defesa Nacional - Policy Paper 5/2014*, 1-12. http://hdl.handle.net/10400.26/34074

Yergin, D. (2006). Ensuring Energy Security. *Foreign Affairs, 85*(2), 69-82. https://www.foreignaffairs.com/articles/2006-03-01/ensuring-energy-security

Yergin, D. (2011). *The quest: energy, security, and the remaking of the modern world*. Penguin Books.