idn nação e defesa

SEGURANÇA EM TEMPO DE CRISE

idn Instituto da Defesa Nacional

Agosto 2020 n.º 156

idn nação e defesa

SEGURANÇA EM TEMPO DE CRISE

idn Instituto da Defesa Nacional

Agosto
2020
n.º 156

NAÇÃO E DEFESA
Revista Quadrimestral – P.V.P. 8,50 €

Propriedade e Edição

Instituto da Defesa Nacional
Calçada das Necessidades, 5, 1399-017 Lisboa
Tel.: 21 392 46 00 Fax.: 21 392 46 58 E-mail: idn.publicacoes@defesa.pt www.idn.gov.pt

Pré-Impressão, Impressão e Acabamento

Editorial do Ministério da Educação e Ciência
Estrada de Mem Martins, 4, São Carlos — Apartado 113 – 2726-901 Mem Martins
Tel.: 219 266 600 Fax: 219 202 765 E-mail: geral@emec.gov.pt

ISSN 0870-757X Publicação Eletrónica ISSN 2183-9662
Depósito Legal 54 801/92
Tiragem 400 exemplares

Anotado na ERC Registada na Latindex – Sistema Regional de Informação em Linha para Revistas Cientícas da América Latina, Caraíbas, Espanha e Portugal; MIAR, RedAlyC e JSTOR.
Disponível no RCAAP – Repositório Cientíco de Acesso Aberto de Portugal

Na última década têm-se prefigurado várias crises no plano internacional e regional com consequências quer sobre a tipologia das respostas, quer sobre o perfil dos atores nacionais e internacionais envolvidos na sua prevenção, mitigação e resolução. Este número dedicado à "Segurança em Tempo de Crise", analisa várias destas dimensões resultantes da presença de novos atores na prevenção e resolução de crises, no plano internacional e no da feitura da paz; do recurso à tecnologia no apoio à tomada de decisão; da ação de atores privados no combate às novas ameaças e das alterações decorrentes de novos equilíbrios geopolíticos, que se configuram no Indo-Pacífico e na Europa Oriental, com implicações securitárias sobre o espaço euro-atlântico.

Luís Elias examina os efeitos decorrentes das medidas adotadas na mitigação da crise provocada pela disseminação do Covid-19 e o seu impacto em Portugal no que respeita ao enquadramento político-institucional da gestão de crises, gerador de oportunidades de cooperação interministerial, indutora de uma maior resiliência das instituições e da sociedade e de uma melhor interação entre o Estado e os cidadãos.

Luís Lapão reflete sobre a complexidade da gestão das designadas novas crises, cuja natureza ultrapassa o plano estrito da segurança e da defesa, mas cujas consequências colocam desafios diretos à segurança nacional. Neste contexto os apoios de novas tecnologias, como a inteligência artificial, poderão constituir importantes instrumentos de apoio à tomada de decisão.

Rui Florêncio analisa o recurso a atores privados na deteção de vulnerabilidades nos sistemas informáticos e no fomento da ciber-resiliência com o apoio de incentivos, como os *bug bounties*, concedidos pelos governos com o objetivo de incrementar a cooperação no quadro da segurança no espaço cibernético.

Domingos Rodrigues e José Pedro Teixeira Fernandes analisam a evolução do posicionamento interno e internacional da Turquia, desde a chegada de Recep Erdoğan ao poder e em que medida essa evolução permite retirar ilações sobre a sua consequência no sistema de segurança euro-atlântico.

Fernando Bessa e Luís Malheiro, assinalando o vigésimo aniversário sobre a adoção da Resolução do Conselho de Segurança das Nações Unidas 1325, examinam a participação das mulheres na feitura da paz e na resolução das crises e conflitos com base num trabalho aplicado, sustentado na condução de um inquérito sobre o papel das mulheres nas forças de segurança na dupla dimensão da feitura da paz e do garante da segurança internacional.

Bruno Cardoso Reis examina as implicações das alterações ocorridas na política, economia e segurança global sobre a centralidade das potências do Atlântico Norte com dois objetivos. Em primeiro lugar, debater a ideia de um certo declínio dos Estados e das organizações, que constituem aquela região, face à ascensão da China e das potências asiáticas. Em segundo, avalia as consequências para os interesses de Portugal e Brasil desta eventual alteração geopolítica e o seu impacto no quadro das relações bilaterais entre ambos.

Isabel Ferreira Nunes

Segurança em Tempo de Crise

Gestão de Crises e a Pandemia de COVID-19

Luís Elias
Superintendente da PSP. Investigador do Centro de Investigação (ICPOL) do Instituto Superior de Ciências Policiais e Segurança Interna (ISCPSI).

Resumo

Face à situação de emergência global provocada pela disseminação do vírus COVID-19, declarada pela Organização Mundial de Saúde, é patente que as organizações internacionais, os Estados, as instituições públicas e privadas e os cidadãos foram surpreendidos pelos seus efeitos nas diferentes sociedades.
Os anos de 2020 e 2021 têm sido caraterizados pela adoção de sucessivas medidas em termos globais e nacionais, visando mitigar os efeitos da pandemia, as quais, têm provocado efeitos profundos em termos socioeconómicos e políticos. Refletimos sobre o enquadramento político-institucional da gestão de crises em Portugal e sobre o edifício jurídico que resultou de um processo evolutivo, o qual, criou algumas áreas de complementaridade, mas muitas também de sobreposição e de atomização. Nesse sentido, refletimos sobre a necessidade de consolidar uma abordagem transversal, transdisciplinar, multi-institucional e coordenada entre o MNE, MDN, MAI, MJ, Ministério da Saúde, Ministério da Educação e Ministério das Finanças. A gestão de crises cada vez mais complexas e marcadas pela incerteza implica abordagens holísticas que confiram maior resiliência e preparação às sociedades, assim como aproveitem o conhecimento e experiência acumulados em termos institucionais e pessoais. Aspetos igualmente fundamentais são a necessidade de criação de mecanismos de direção estratégica e de comando e controlo mais coerentes que ultrapassem entropias, prestando assim um melhor serviço à comunidade e aos cidadãos.

Palavras-chave: Pandemia; Crise; Segurança; Proteção; Saúde; Gestão de Crises.

Abstract
Crisis Management and the COVID-19 Pandemic

In view of the global emergency situation caused by the spread of the COVID-19 virus, declared by the World Health Organization, it is clear that International Organizations, States, public and private institutions and citizens were surprised by its effects on different societies.
The years 2020 and 2021 have been characterized by the adoption of successive measures in global and national terms, aiming to mitigate the effects of the pandemic, which, have provoked profound effects in socioeconomic and political terms. We reflected on the political-institutional framework of crisis management in Portugal and on the legal building that resulted from an evolutionary process, which created some areas of complementarity, but many also of overlap and fragmentation. In this sense, we reflect on the need to consolidate a transversal, transdisciplinary, multi-institutional and coordinated approach between the Foreign Affairs, National Defense, Internal Security, Justice, Health, Education and Finance. Crisis management that is increasingly complex and marked by uncertainty implies holistic approaches that provide greater resilience and preparation for societies, as well as taking advantage of the accumulated institutional and personal knowledge and experience. Equally fundamental aspects are the need to create more coherent strategic direction and command and control mechanisms that go beyond entropy, thus providing a better service to the community and citizens.

Keywords: Pandemic; Crisis; Security; Protection; Health; Crisis Management.

Artigo recebido: 15.06.2020
Aprovado: 30.06.2020
https://doi.org/10.47906/ND2020.156.01

Introdução

O mundo globalizado e em rede do século XXI é marcado pela interconexão. As crises são mais frequentes, variando de intensidade e duração, de acordo com o contexto geográfico, político, social e económico.

A pandemia de COVID-19 veio colocar a segurança sanitária no centro da agenda política dos Estados e das Organizações Internacionais (Carreiras, 2020). Nos próximos meses (talvez nos próximos anos) a atenção das organizações supranacionais, dos governos, das empresas multinacionais, da academia e dos cidadãos será centrada em aspetos como a procura de uma vacina, o controlo da transmissão da doença, a sustentabilidade dos sistemas de saúde pública, a crise económico-financeira, o desemprego, a segurança interna e a segurança transnacional.

Face à situação de emergência global de saúde pública provocada pela disseminação do vírus COVID-19, declarada pela Organização Mundial de Saúde a 30 de janeiro de 2020 e de pandemia a 11 de março de 2020, em Portugal, o Ministro da Administração Interna e a Ministra da Saúde, assinaram o despacho de Declaração de Situação de Alerta que abrangia todo o território nacional a 13 de março de 2020.

O contágio galopante em vários países da União Europeia, especialmente no Reino Unido, em Itália e em Espanha, determinaram em 18 de março de 2020 a Declaração do estado de emergência por S. Exa. o Presidente da República, nos termos dos Artigos 19.º, 134.º, alínea d), e 138.º da Constituição e da Lei n.º 44/86, de 30 de setembro, a primeira vez, desde 1975 que, no nosso país, foi decretado um estado de exceção (o estado de emergência), o qual, foi renovado por Decreto Presidencial por duas vezes: em 2 de abril e em 17 de abril, tendo vigorado até ao dia 2 de maio de 2020.

Com o fim do estado de emergência, a partir do dia 3 de maio, o Governo decretou a Situação de Calamidade nos termos da Lei de Bases de Proteção Civil (LBPC).

Entretanto, depois de sucessivas renovações da situação de calamidade em 29 de junho de 2020 entra em vigor a situação de calamidade, contingência ou de alerta em diferentes concelhos do país.

De 12 a 23 de agosto de 2020 decorre a fase final da Liga dos Campeões em Lisboa com a realização sucessiva de quartos de final, meias finais e final, num total de sete jogos sem público.

Em 14 de agosto de 2020 é declarada a situação de contingência e de alerta. Em 11 de setembro é declarada a situação de contingência.

Em 14 de outubro a declaração de calamidade.

Em 6 de novembro de 2020 o estado de emergência volta a ser decretado pelo Presidente da República, sendo renovado sucessivamente.

1. Problemática, Objetivos e Metodologia

Formulamos o seguinte problema de partida: os sistemas de gestão de crises encontram-se preparados para as prevenir e enfrentar?
Os objetivos da nossa investigação serão: 1) refletir sobre as implicações das crises na segurança e qualidade de vida das nossas sociedades; 2) abordar os diferentes conceitos e tipologias de crises; 3) apresentar alguns modelos de evolução das mesmas; 4) refletir sobre a direção político-estratégica, sobre o comando operacional e tático em situações de crise, abordando a pandemia gerada pelo COVID-19; 5) propor medidas de âmbito estratégico, no sentido de melhorar a abordagem sistémica a esta problemática.
Um conjunto de questões chave orienta a nossa análise, designadamente: as crises podem ter um efeito de tal forma negativo ao ponto de perturbarem gravemente a estabilidade política, social, económica e segurança internacionais? O estudo da tipologia crises e da sua evolução pode ajudar na adoção de estratégias preventivas e reativas? Deverá ser criado no nosso país um órgão de direção político-estratégica para gerir e coordenar a intervenção em situação de crise?
Formulamos as seguintes hipóteses de estudo que tentaremos confirmar ou não no final:

1. as ameaças, riscos e as crises contemporâneas são mais complexas, menos previsíveis e difíceis de catalogar;
2. o(s) sistema(s) nacional(is) de prevenção e resposta a crises revela(m) um excesso de departamentalização e alguma atomização;
3. em Portugal será essencial uma maior coerência política e legislativa e a criação de um órgão de coordenação estratégica e de gestão de crises de grande magnitude.

2. Crises e Segurança

O conceito de segurança abarca nos nossos dias a atuação e o empenhamento de instituições públicas e privadas, da sociedade local e da sociedade civil, bem como de organizações internacionais (Elias, 2011, p. 27). Abordaremos as ameaças e riscos, os diferentes conceitos de crise, tipologias de crise e modelos de evolução das crises e impactos na segurança.

2.1. Ameaças e Riscos Contemporâneos

Na atualidade, as ameaças são mais diversificadas, menos visíveis e menos previsíveis. A maioria das estratégias e relatórios internacionais debruçam-se sobre

as ameaças transnacionais que têm maior impacto nas nossas sociedades, sendo identificadas invariavelmente ameaças de origem humana como o terrorismo, a criminalidade organizada, a criminalidade violenta e grave, as ciberameaças, os acidentes de origem dolosa ou negligente. Quanto às ameaças naturais são referidos: sismos, incêndios florestais, cheias, poluição, entre outras. Podemos ainda acrescentar as crises económico-financeiras e crises bolsistas, as pandemias, os problemas ambientais e os problemas na segurança alimentar.

Diversos relatórios internacionais identificam as principais ameaças e riscos transnacionais potencialmente geradoras de crises pontuais ou sistémicas. A "Estratégia Europeia em matéria de Segurança – uma Europa segura num mundo melhor" de 12 de dezembro de 2003, "Estratégia de Segurança Interna da UE – rumo a um modelo Europeu de segurança", de março de 2010 e a Agenda Europeia para a Segurança apresentada em 28 de abril de 2015 apontam invariavelmente o terrorismo, a criminalidade organizada e a cibercriminalidade como ameaças à segurança interna dos Estados e à segurança global.

O Conceito Estratégico de Defesa Nacional (CEDN), aprovado pela Resolução do Conselho de Ministros (RCM) n.º 19/2013 de 5 de abril elenca no ambiente de segurança global e à segurança nacional, entre outras: o terrorismo, a criminalidade transnacional organizada, a cibercriminalidade, a pirataria, alterações climáticas, riscos ambientais e sísmicos, ondas de calor e de frio, atentados ao ecossistema, terrestre e marítimo, pandemias e outros riscos sanitários.

Entretanto, a Estratégia da UE para a União da Segurança para o período de 2020 a 2025[1] sublinha a necessidade de garantir a proteção e resiliência das infraestruturas críticas, garantir a cibersegurança, assegurar a proteção dos espaços públicos, prevenir e reprimir a cibercriminalidade, consolidar a justiça e forças policiais enquanto serviços modernos e com acesso às novas tecnologias (inteligência artificial, acesso a metadados, acesso a elementos de prova digitais, 5G, interoperabilidade entre os sistemas de informação da UE), combate aos conteúdos ilegais em linha, deteção e prevenção de ameaças híbridas, prevenção e combate ao terrorismo e radicalização, prevenção e combate à criminalidade organizada, cooperação e intercâmbio de informações, garantia de fronteiras externas sólidas, reforço da investigação e da inovação em matéria de segurança.

As ameaças e riscos atrás elencados poderão, de forma individual ou combinada, ser causadores de crises pontuais, de crises sistémicas ou de crises em cadeia.

1 Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões (COM (2020) 605 final de 24-07-2020).

2.2. Conceitos de Crise

O termo "crise" provém do grego, *krisis*. Significava conflito, disputa, separação, decisão, juízo, sentença. Podemos referir que, "do ponto de vista social e sobretudo de política interna ou internacional, o conceito mais abstrato é o que identifica a crise como o ponto crucial de um processo que marca a eventual passagem da paz para a guerra ou da guerra para a paz, do diálogo para o combate, da vida para a morte" (Moreira, 2010, p. 17).

Crise significa "algo em perigo, sob ataque, em transformação (...), indica situações em que agentes ou estruturas políticas passam por mudanças radicais" (Thaler e Sustein, 2008, p. 68). Para Coombs (2007) e Coombs e Holladay (2010), um incidente é uma desordem localizada e de menor dimensão. O conceito de crise – sistémica ou pontual – deve ficar reservado para os eventos de maior dimensão, ou seja, para aqueles que requerem atenção especial por parte dos dirigentes políticos, dos gestores, dos comandantes militares e policiais e que têm potencial para causar sérios impactos na sociedade, na atividade organizacional e nos seus *stakeholders*. De acordo com Sellnow e Seeger (2013, p. 7), uma crise tanto se pode consubstanciar em um evento único, como pode derivar de uma "série de eventos interativos e em cascata", isto é, pode ter origem num acontecimento específico, inesperado e não-rotineiro ou numa série de eventos. Tanto uma situação como a outra criam altos níveis de incerteza e representam uma ameaça significativa para os Estados ou as organizações.

Em momentos de crise geram-se situações delicadas onde se revela necessário, por um lado, salvaguardar a ordem e a paz social, e por outro, não cair em excessos resultantes de quem detém o poder, sendo fundamental manter-se o equilíbrio necessário para a estabilidade do Estado e da sua sociedade (Faria, 2011).

De um modo geral, uma crise corresponde a uma mudança ou alteração, de um cenário, que anteriormente estava em equilíbrio, e que passa a estar numa situação problemática, instável, causada por um ou mais fatores, "designa uma fase ou uma situação perigosa, da qual pode resultar algo benéfico ou algo nocivo para o indivíduo ou para a comunidade que passa por essa situação" (Morujão, 1989).

O conceito de crise é poliédrico, podendo integrar-se em mais do que um quadro teórico ou conceitual, conforme o fim e o domínio em que se desenvolve. Consoante o objeto de análise, pode-se falar em crise humanitária, sanitária, diplomática, económico-financeira, social, política, securitária, ambiental, militar, energética, do sistema de justiça, do quadro de valores. Em muitos casos, as crises são multidimensionais e transversais, não podendo ser caraterizadas como tendo uma vertente meramente política, social ou económica e, numa outra perspetiva, são difíceis de catalogar enquanto crises internas ou externas ou como crises nas áreas militar, *security* ou *safety*. Na "realidade líquida" (Bauman, 2000), num mundo globalizado

e em rede, as crises podem mais facilmente propagar os seus efeitos para diversas latitudes e de forma quase imediata.

Diegues (2011) considera pertinente dividir as crises em situações imprevisíveis e previsíveis, referindo que as imprevisíveis são aquelas, tais como catástrofes naturais, acidentes ou sabotagem, que provocam mais danos decorrentes da sua imponderabilidade, ao passo que as previsíveis decorrem de ações que à partida já existe conhecimento, podendo de certa forma existir uma preparação prévia para enfrentar a crise que surgirá, como é o caso de algumas crises económicas que atingem países ou instituições.

Oficialmente a OTAN considera que podem existir "crises políticas, militares ou humanitárias, podendo ser causadas por conflitos armados ou políticos, incidentes tecnológicos ou desastres naturais", no entanto, para se lidar com uma crise, é necessária uma "avaliação sobre a natureza, dimensão e gravidade da mesma" (Saraiva, 2011).

A Cláusula de Solidariedade, prevista no Título VII, Art.º 222.º, do Tratado sobre o Funcionamento da União Europeia poderá ser invocada aquando de crises graves na UE, em vários Estados-membros ou apenas num Estado. A Cláusula menciona que a UE e os seus Estados-membros atuarão em conjunto, num espírito de solidariedade, se um Estado-membro for alvo de um ataque terrorista ou vítima de uma catástrofe. Nestes casos, a mesma Cláusula refere que a UE mobilizará todos os meios ao seu dispor, incluindo os militares, disponibilizados pelos Estados-membros, para prevenir a ameaça terrorista noutros Estados-membros bem como para proteger as instituições democráticas e a população de um eventual ataque, prestar assistência, a pedido das autoridades políticas, em caso de ataque terrorista e ainda prestar assistência a um Estados-membros, também a pedido das autoridades políticas, caso ocorra uma catástrofe. Para que, a pedido de uma autoridade política, ocorra esta assistência de um Estado-membro para outro Estado, os mesmos devem coordenar-se no Conselho Europeu.

A UE não aprovou ainda uma definição política de crise para orientar os seus esforços e dos seus membros na gestão de crises que afetem a segurança internacional e os interesses da União. Ainda assim, a Decisão Quadro 2008/617/JAI de 23 de junho de 2008 do Conselho, relativa à melhoria da cooperação entre as unidades especiais de intervenção dos Estados-membros da UE perante crises, define "situação de crise" como: "qualquer situação em que as autoridades competentes de um Estado-membro tenham motivos razoáveis para crer que existe uma infração penal que apresenta uma ameaça física grave e direta para as pessoas, bens patrimoniais, infraestruturas ou instituições nesse Estado-membro, em particular as situações (...), relativa à luta contra o terrorismo". Esta Decisão, também designada por Decisão ATLAS, estabelece as regras e condições gerais que permitem às unidades especiais de intervenção de um Estado-membro prestar assistência e/ou atuar

no território de outro Estado-membro, a pedido deste último para fazer face a uma situação de crise.

Em Portugal não existe também um conceito político ou jurídico consolidado sobre crises. As referências legais a esta questão encontram-se dispersas por diversos diplomas e, sem se pretender ser exaustivo e esgotar o assunto, temos por objetivo ajudar à reflexão sobre a prevenção e resposta às crises.

O Decreto-Lei n.º 173/2004, de 21 de julho que criava um sistema nacional de gestão de crises - destinado a apoiar o Primeiro-Ministro no processo da tomada de decisão e na sua execução em situações de crise – foi revogado pela Lei n.º 53/2008 de 29 de agosto, Lei de Segurança Interna (LSI). Há que referir que este mecanismo não chegou verdadeiramente a ser implementado, dado o curto período de vigência deste diploma legal. Este, definia as crises como situando-se "entre a normalidade e a guerra, a urgência de decisões e de ações imediatas e a aplicação de meios adequados de resposta, no sentido do restabelecimento da situação anterior, ou da salvaguarda dos interesses postos em causa". Criava um gabinete de crise[2] presidido pelo Primeiro-Ministro e um gabinete de apoio, os quais, na prática nunca chegaram a ser constituídos.

2.3. Tipologias de Crises

Decorrente da abordagem em diversos relatórios internacionais e nacionais as tipologias de crises que consideramos mais relevantes e que, por isso, vamos abordar para enquadrar os diversos Sistemas e Subsistemas de Gestão de Crises em Portugal são: os acontecimentos que possam levar a que seja decretado o estado de sítio ou o estado de emergência, os Incidentes Tático-Policiais, os Acidentes Graves e as Catástrofes e as Crises no Ciberespaço.

2 O Gabinete de Crise era composto por Ministro das Finanças; Ministro da Defesa Nacional; Ministro dos Negócios Estrangeiros; Ministro da Administração Interna; Ministro da Justiça; outros membros do Governo, por determinação do Primeiro-Ministro; o membro do Governo que coordena o Grupo de Apoio; Ministros da República para as Regiões Autónomas dos Açores e da Madeira, sempre que a situação de crise envolva ou possa envolver, as respetivas Regiões Autónomas; Chefe do Estado-Maior-General das Forças Armadas; os Presidentes dos Governos Regionais dos Açores e da Madeira, sempre que a situação de crise envolva, ou possa envolver, as respetivas Regiões Autónomas; os diretores dos serviços de informações que integram o Sistema de Informações da República Portuguesa; o diretor nacional da Polícia Judiciária; outras entidades ou personalidades, designadas pelo Primeiro-Ministro, quando a situação o aconselhe.

2.3.1. Estado de Sítio e Estado de Emergência

A tipologia mais grave de crises prevista no ordenamento jurídico português está estatuída no Art.º 19.º da Constituição da República Portuguesa (CRP), implicando a suspensão do exercício de direitos, liberdades e garantias dos cidadãos. Referimo-nos aos estados de exceção: estado de sítio e estado de emergência.

O Art.º 19.º n.º 2 da CRP prevê que "o estado de sítio ou o estado de emergência só podem ser declarados, no todo ou em parte do território nacional, nos casos de agressão efetiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou de calamidade pública". Poderemos considerar, neste âmbito, ameaças como: um ataque militar convencional ou não convencional de um Estado ou de um poder errático contra o Estado português, uma catástrofe natural – sismos, cheias e inundações, incêndios florestais, ou outros – ou um acidente grave de origem humana e/ou tecnológica – acidentes rodoviários, ferroviários e marítimos, acidentes industriais, acidentes com substâncias perigosas ou semelhantes.

Nos termos do Art.º 8.º n.º 1 da Lei n.º 44/86 de 30 de setembro, alterada pela Lei Orgânica n.º 1/2012, de 11 de maio, Regime do estado de sítio e do estado de emergência (RESEE), "o estado de sítio é declarado quando se verifiquem ou estejam iminentes atos de força ou insurreição que ponham em causa a soberania, a independência, a integridade territorial ou a ordem constitucional democrática e não possam ser eliminados pelos meios normais previstos na Constituição e na lei". A declaração deste estado de exceção implica a subordinação das autoridades civis às autoridades militares ou a sua substituição por estas (Art.º 8.º n.º 2). As Forças de Segurança, durante o estado de sítio, ficarão colocadas, para efeitos operacionais, sob o comando do Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), por intermédio dos respetivos Comandantes-Gerais (Art.º 8.º n.º 3).

Segundo o Art.º 9.º n.º 1 do RESEE, "o estado de emergência é declarado quando se verifiquem situações de menor gravidade, nomeadamente quando se verifiquem ou ameacem verificar-se casos de calamidade pública". Neste âmbito, está previsto, se necessário, o reforço dos poderes das autoridades administrativas civis e o apoio às mesmas pelas Forças Armadas.

No Art.º 1.º do RESEE, bem como no n.º 2 do Art.º 19.º da CRP, consta que ambos os estados de exceção "só podem ser declarados, no todo ou em parte do território nacional, no caso de agressão efetiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou ainda em caso de calamidade pública", podendo ser decretados da "forma prevista na CRP, regendo-se pelas normas constitucionais, e pelo regulamentado no RESEE", ressalvando-se que, especificamente, no caso do estado de emergência, este apenas é declarado quando as agressões, ameaças, perturbações ou as calamidades em causa, são de

menor gravidade, e apenas poderá "determinar a suspensão parcial de alguns Direitos, Liberdades e Garantias (DLG) suscetíveis de serem suspensos, prevendo-se, se necessário, o reforço dos poderes das Autoridades Administrativas Civis e o apoio às mesmas por parte das Forças Armadas" (Art.º 19.º, n.º 3, CRP e Art.º 9.º do RESEE), o que aconteceu aliás com a presente crise pandémica.

O estado de sítio é declarado "quando se verifiquem ou estejam iminentes atos de força ou insurreição, que ponham em causa a soberania, a independência, a integridade territorial ou a ordem constitucional democrática, e não possam ser eliminados pelos meios normais previstos na Constituição e na lei" (Art.º 8.º, n.º1), podendo o mesmo estado de exceção "suspender ou restringir, parcial ou totalmente, o exercício de DLG, sendo possível estabelecer a subordinação das Autoridades Civis às Autoridades Militares ou a sua substituição por estas" (Art.º 8.º, n.º 2). No Art.º 4.º do RESEE, verificamos ainda que cada um dos estados de exceção possam ser declarados "em relação a todo ou a parte do território nacional, consoante o âmbito geográfico das suas causas determinantes, só podendo sê-lo relativamente à área em que a sua aplicação se mostre necessária para manter ou restabelecer a normalidade". Segundo o Art.º 3.º, n.º 1 do RESEE, bem como o Art.º 19.º, n.º 4 da CRP, constatamos que a declaração e execução de ambos os estados de exceção "devem respeitar o princípio da proporcionalidade, e adequação das medidas, e limitar-se, nomeadamente quanto à sua extensão, duração e meios utilizados, ao estritamente necessário ao pronto restabelecimento da normalidade constitucional".

No que concerne às Forças de Segurança, no decorrer do estado de sítio, as mesmas "ficam colocadas, para efeitos operacionais, sob o comando do CEMGFA, por intermédio dos respetivos Comandantes-Gerais" (Art.º 8.º, n.º 3 do RESEE), ao passo que as Autoridades Administrativas Civis "continuarão no exercício das competências que, nos termos da lei e da declaração do estado de sítio, não tenham sido afetadas pelos poderes conferidos às autoridades militares, mas deverão em qualquer caso facultar a estas os elementos de informação que lhes forem solicitados" (Art.º 8.º, n.º 4).

O estado de emergência, nos termos do Art.º 9.º é declarado quando se verifiquem situações de menor gravidade, nomeadamente quando se verifiquem ou ameacem verificar-se casos de calamidade pública. Na declaração do estado de emergência apenas pode ser determinada a suspensão parcial do exercício de direitos, liberdades e garantias (como aconteceu na fase mais grave da pandemia de COVID-19), prevendo-se, se necessário, o reforço dos poderes das autoridades administrativas civis e o apoio por parte das Forças Armadas.

No Art.º 13.º prevê-se a cessação dos mesmos estados de exceção, quando as circunstâncias que os fizeram ser declarados também cessam, ou então quando termina o prazo fixado na respetiva declaração ou pela recusa da sua ratificação pelo Plenário.

Os cenários de crise, em alguns casos, podem levar à perturbação do exercício pacífico e integral, no todo ou em parte, dos DLG dos cidadãos, existindo a possibilidade de se proceder à suspensão ou limitação dos mesmos (Faria, 2011). A aplicação destes dois estados de exceção, limita e condiciona de certa forma alguns direitos, porém, no que concerne aos DLG dos cidadãos, "a declaração do estado de sítio ou do estado de emergência é adequadamente fundamentada e contém a especificação dos DLG cujo exercício fica suspenso, não podendo o estado declarado ter duração superior a quinze dias, ou duração superior à fixada por lei quando em consequência de declaração de guerra, sem prejuízo de eventuais renovações, com salvaguarda dos mesmos limites" (Art.º 19.º, n.º 5, CRP e Art.º 5.º do RESEE), como aliás tem acontecido durante a pandemia de COVID-19. A declaração destes mesmos estados não pode, em caso algum, colocar em causa alguns DLG, nomeadamente o direito à vida, à integridade pessoal, o direito à identidade pessoal, à capacidade civil e à cidadania, à não retroatividade da lei criminal, direito à defesa dos arguidos e os direitos à liberdade de consciência e de religião (Art.º 19.º, n.º 6, CRP e Art.º 2.º, n.º 1 do RESEE). Nos casos em que possa ocorrer a suspensão dos DLG dos cidadãos terá sempre de ser respeitado o princípio da igualdade e da não discriminação assim como os limites expostos nas alíneas do n.º 2 do Art.º 2.º do RESEE.

Nos termos do Art.º 27.º, os atos de processo previstos nos Artigos respeitantes à declaração e vigência dos dois estados de exceção, revestem natureza urgentíssima e têm prioridade sobre quaisquer outros.

A declaração do estado de sítio ou de emergência deverá conter, de forma clara e expressa, a caraterização e fundamentação do estado declarado, o âmbito territorial, a duração, deverá conter a especificação dos DLG cujo exercício fica suspenso ou restringido. No estado de sítio deverão ser expressamente definidos os poderes conferidos às autoridades militares, nos termos do n.º 2 do Art.º 8.º do mesmo diploma legal, e no estado de emergência, deverá ser determinado o grau de reforço dos poderes das autoridades administrativas civis e o tipo de apoio às mesmas pelas Forças Armadas, sendo caso disso, conforme verificável no Art.º 14.º do RESEE.

A execução da declaração de ambos estados de exceção compete ao Governo, que deverá, por sua vez, manter informados o Presidente da República e a Assembleia da República (Art.º 17.º do RESEE). O emprego das Forças Armadas para execução da declaração do estado de sítio nas regiões autónomas é assegurado pelo respetivo comandante-chefe, verificando-se igualmente que a execução da declaração do estado de emergência nas regiões autónomas é assegurada pelo Representante da República, em cooperação com o governo regional (Art.º 20.º do RESEE). No que concerne aos poderes conferidos às autoridades militares, nos termos do disposto no n.º 2 do Art.º 8.º, do RESEE, a execução da declaração do estado de sítio no território continental, a nível local, é assegurada pelos comandantes militares, na área do respetivo comando. Compete ainda ao Governo da República, nomear as

autoridades que coordenam a execução da declaração do estado de emergência no território continental, a nível local, sem embargo de, em situações de calamidade pública, a coordenação mencionada ser assegurada pelos comandantes operacionais distritais de operações de socorro, na área da respetiva jurisdição (Art.º 20.º do RESEE).

No que respeita ao funcionamento dos órgãos de direção e fiscalização, conforme o Art.º 18.º do RESEE, declarado um dos referidos estados de exceção, que abranja todo o território nacional, o Conselho Superior de Defesa Nacional, bem como a Procuradoria-Geral da República e o Serviço do Provedor de Justiça, mantêm-se em sessão permanente.

A modificação da declaração do estado de sítio ou do estado de emergência no sentido da redução das respetivas providências ou medidas, bem como a sua revogação, operam-se por decreto do Presidente da República, referendado pelo Governo, independentemente de prévia audição deste e de autorização da Assembleia da República (n.º 2, Art.º 26.º do RESEE).

Quem violar o legalmente disposto quanto ao estado de sítio e estado de emergência, incorre no crime de desobediência (Art.º 7.º RESEE), como aliás tem acontecido durante os períodos de estado de emergência decretados pelo Presidente da República durante a presente pandemia de COVID-19. É importante referir que, mesmo declarado um destes estados de exceção, as medidas de polícia estão sempre sujeitas ao princípio da proporcionalidade (Faria, 2011).

Como consta no Art.º 59.º, da Lei n.º 80/2015, de 3 de agosto, em estado de guerra, de sítio ou de emergência, verifica-se ainda que as atividades de proteção civil subordinam-se ao disposto na LDN e no RESEE.

A formação e os exercícios conjuntos entre as Forças Armadas e as Forças e Serviços de Segurança têm sido praticamente inexistentes para preparar a atuação conjunta, as relações de comando e controlo, as comunicações entre os diferentes atores num cenário de extrema gravidade.

2.3.2. Incidentes Tático-Policiais

No domínio da segurança interna, os incidentes tático-policiais são tipificados na lei como ocorrências resultantes de ameaças como o terrorismo, a criminalidade organizada e a criminalidade violenta e grave. Segundo o Art.º 18.º n.º 3 da LSI, "consideram-se incidentes tático-policiais graves, além dos que venham a ser classificados como tal pelos MAI e MJ, os que requeiram a intervenção conjunta e combinada de mais de uma Força e Serviço de Segurança e que envolvam:

a) ataques a órgãos de soberania, estabelecimentos hospitalares, prisionais ou de ensino, infraestruturas destinadas ao abastecimento e satisfação de

necessidades vitais da população, meios e vias de comunicação ou meios de transporte coletivo de passageiros e infraestruturas classificadas como infraestruturas nacionais críticas;
b) o emprego de armas de fogo em circunstâncias em que se ponha em perigo a vida ou a integridade física de uma pluralidade de pessoas;
c) a utilização de substâncias explosivas, incendiárias, nucleares, radiológicas, biológicas ou químicas;
d) sequestro ou tomada de reféns".

O Secretário-Geral do Sistema de Segurança Interna (SGSSI) tem competências de direção, coordenação, controlo e comando operacional das Forças e Serviços de Segurança. De acordo com o Art.º 19.º n.º 1 da LSI, "em situações extraordinárias, determinadas pelo Primeiro-Ministro após comunicação fundamentada ao Presidente da República, de ataques terroristas ou de acidentes graves ou catástrofes que requeiram a intervenção conjunta e combinada de diferentes Forças e Serviços de Segurança e, eventualmente, do Sistema Integrado de Operações de Proteção e Socorro (SIOPS), estes são colocados na dependência operacional do SGSSI, através dos seus dirigentes máximos". O Art.º 19.º n.º 2 estipula que no âmbito destas competências extraordinárias, o SGSSI tem poderes de planeamento e atribuição de missões ou tarefas que requeiram a intervenção conjugada de diferentes forças e serviços de segurança e de controlo da respetiva execução, de acordo com o plano de coordenação, controlo e comando operacional das forças e dos serviços de segurança.
Refira-se ainda que o SGSSI, nos termos do Art.º 17.º n.º 2 alínea e) da LSI é "o ponto nacional de contacto permanente para situações de alerta e resposta rápidas às ameaças à segurança interna, no âmbito dos mecanismos da União Europeia", sendo o ponto de entrada de alertas de outros Estados-membros e também o canal de difusão de pedidos de apoio no quadro da cooperação internacional.
No Art.º 35.º da LSI estipula-se que "as Forças Armadas colaboram em matéria de segurança interna nos termos da Constituição e da lei, competindo ao SGSSI e ao CEMGFA assegurarem entre si a articulação operacional", a qual terá que ser delineada através de um plano que ainda não foi aprovado.

2.3.3. Acidentes Graves e Catástrofes

Nos termos do Art.º 3.º n.º 1 e 2 da Lei n.º 27/2006, de 3 de julho (LBPC), alterada e republicada pela Lei n.º 80/2015 de 03 agosto, "acidente grave é um acontecimento inusitado com efeitos relativamente limitados no tempo e no espaço, suscetível de atingir as pessoas e outros seres vivos, os bens ou o ambiente" e "catástrofe é o acidente grave ou a série de acidentes graves suscetíveis de provocarem elevados

prejuízos materiais e, eventualmente, vítimas, afetando intensamente as condições de vida e o tecido socioeconómico em áreas ou na totalidade do território nacional". Paralelamente à ocorrência de um acidente grave ou de uma catástrofe, pode ser declarada a situação de alerta, de contingência ou de calamidade. Assim, face à ocorrência ou iminência da ocorrência de um acidente grave ou de uma catástrofe, estaremos perante uma situação de alerta quando é reconhecida a necessidade de adotar medidas preventivas ou de medidas especiais de reação (Art.º 9.º n.º 1 da LBPC); perante uma situação de contingência quando é reconhecida a necessidade de adotar medidas preventivas e ou medidas especiais de reação não mobilizáveis no âmbito municipal (Art.º 9.º n.º 2 da mesma Lei); e perante uma situação de calamidade (Art.º 9.º n.º 3 da LBPC) quando é reconhecida a necessidade de adotar medidas de carácter excecional destinadas a prevenir, reagir ou repor a normalidade das condições de vida nas áreas atingidas pelos seus efeitos.

Os Artigos 19.º e 20.º da LBPC preveem que a declaração da situação de calamidade é da competência do Governo e reveste a forma de RCM, a qual pode ser precedida de despacho do Primeiro-Ministro e do MAI reconhecendo a necessidade de declarar a situação de calamidade.

O Decreto-Lei n.º 73/2012, de 26 de março, transferiu para a ANEPC as atribuições do Conselho Nacional de Planeamento Civil de Emergência, nomeadamente: a missão de assegurar o planeamento e coordenação das necessidades nacionais na área do planeamento civil de emergência, com vista a fazer face a situações de crise ou de guerra.

Tratou-se de um reforço substancial da ação da ANEPC, a qual passou a englobar as situações de crise e de guerra para além dos acidentes graves e catástrofes. A promoção e coordenação das atividades em matéria de planeamento civil de emergência, em estreita ligação com os serviços públicos competentes em cada setor, deverá ser empreendida pela ANEPC, sem prejuízo da necessária coordenação com o MDN.

2.3.4. Crises no Ciberespaço

De acordo com a Estratégia Nacional de Segurança do Ciberespaço (RCM n.º 36/2015, de 12 de junho), cabe ao Centro Nacional de Cibersegurança (CNCS) "consolidar o papel de coordenação operacional e de autoridade nacional em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas". O CNCS deve desenvolver e aplicar medidas que visem a capacitação humana e tecnológica das infraestruturas públicas e das infraestruturas críticas, com vista à prevenção e à reação de e a incidentes de cibersegurança. Com vista à eficácia operacional e a uma melhor avaliação situacional, devem ser criados mecanismos de reporte

de incidentes de cibersegurança para entidades públicas e para os operadores de infraestruturas críticas. A desejada avaliação situacional resulta na criação de condições para a identificação de um nível de alerta nacional em matéria de segurança do ciberespaço, partilhado entre todas as entidades envolvidas.

Em articulação com as autoridades competentes e a comunidade nacional de segurança do ciberespaço, o CNCS deve: criar uma base de conhecimento que reúna informação sobre ameaças e vulnerabilidades conhecidas, para servir as entidades públicas e os operadores de infraestruturas críticas e produzir e apresentar um quadro integral e atual dos incidentes, ameaças e vulnerabilidades que pendem sobre o ciberespaço nacional.

Esta missão do CNCS deverá ser desenvolvida em cooperação com diversas entidades públicas e privadas e designadamente com o Centro de Ciberdefesa.

Nos termos da Estratégia Nacional de Segurança do Ciberespaço e do respetivo Eixo 1 (Estrutura de segurança do ciberespaço), encontram-se previstas várias medidas.

Uma das primeiras medidas é a de consolidar o papel de coordenação operacional e de autoridade nacional do CNCS em matéria de cibersegurança, relativamente às entidades públicas e às infraestruturas críticas.

Outra das medidas previstas consiste em estabelecer um gabinete para gestão de crises no ciberespaço que se insira numa abordagem integrada na resposta às ameaças e riscos num efetivo sistema nacional de gestão de crises e que integre atores relevantes neste domínio; organizar e realizar exercícios nacionais de gestão de crises no ciberespaço, que permitam avaliar o grau de preparação e a maturidade das diversas entidades para lidar com incidentes de grande dimensão, potenciando as sinergias decorrentes da integração, sempre que possível, com outros exercícios neste âmbito, organizados e conduzidos a nível nacional.

A Lei n.º 46/2018, de 13 de agosto, estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Esta lei aplica-se: à Administração Pública; aos operadores de infraestruturas críticas; aos operadores de serviços essenciais; aos prestadores de serviços digitais; a quaisquer outras entidades que utilizem redes e sistemas de informação.

O Art.º 7.º da Lei n.º 46/2018, de 13 de agosto prevê que o CNCS funciona no âmbito do Gabinete Nacional de Segurança (GNS) e é a Autoridade Nacional de Cibersegurança. O CNCS tem por missão garantir que o País usa o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da definição e implementação das medidas e instrumentos

necessários à antecipação, deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes, ponham em causa o interesse nacional, o funcionamento da Administração Pública, dos operadores de infraestruturas críticas, dos operadores de serviços essenciais e dos prestadores de serviços digitais.
O desenvolvimento da capacidade de Ciberdefesa foi aprovado pelo Despacho n.º 13692/2013, de 11 de outubro, publicado no *Diário da República* n.º 208, 2.ª série, de 28 de outubro. Esta Orientação Política para a Ciberdefesa, edifica a estrutura de ciberdefesa nacional; visa estabelecer e consolidar uma estrutura de comando e controlo da ciberdefesa nacional, recaindo as atribuições de orientação estratégica-militar da ciberdefesa sobre o Conselho de Chefes de Estado-Maior e o planeamento e resposta imediata e efetiva a uma crise no ciberespaço ao Centro de Ciberdefesa e às capacidades dos ramos das Forças Armadas; visa implementar, desenvolver e consolidar a capacidade de ciberdefesa, com vista a assegurar a condução de operações militares no ciberespaço, assegurando a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração proactiva do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse nacional; tem por objetivo que a ciberdefesa promova sinergias e potencie o emprego dual das suas capacidades, no âmbito das operações militares e da cibersegurança nacional, desenvolvendo e consolidando um sistema de partilha de informação aos vários níveis e patamares de decisão.

3. Gestão de Crises

A gestão de crises não deve ser apenas a resposta à(s) crise(s). É um processo integrado que engloba a atividade contínua de avaliação das ameaças e de gestão de riscos concretos e potenciais, o desenvolvimento de capacidades institucionais e de competências das lideranças, dos diversos setores da sociedade e grupos profissionais para fazer face a essas ameaças, para gerir os riscos, reduzir as vulnerabilidades, procurando assim diminuir as oportunidades para que as ameaças se concretizem. Deverá prever a análise de riscos e de vulnerabilidades, estudos de impacto de crises potenciais, sistemas de deteção de sinais, barómetros/sensores dos sinais de desordem ou de crise e planos de contingência.
O diagnóstico das crises preconiza a identificação e categorização dos fenómenos despoletados por um evento por uma sucessão de eventos críticos, a identificação e caraterização de parceiros, *stakeholders*, adversários e públicos, a seleção e preparação da estratégia de resposta à crise e das diferentes variáveis operacionais e táticas e a ativação do sistema de resposta.
A gestão de crises deverá contemplar também a resposta aos fenómenos que perturbem o equilíbrio das sociedades e das organizações, auditorias pós-crise, a

recuperação bem como a aprendizagem, com vista a sedimentar a aprendizagem e a memória institucional e a memória no seio da comunidade, realimentando assim o sistema.
Para Coombs (2007), a gestão de crises é um processo que pode ser dividido nas fases pré-crise, crise e pós-crise. A fase pré-crise consiste na prevenção e na preparação; a fase da resposta à crise é quando se verifica uma reação, uma resposta às manifestações da crise; e, por último, na fase de pós-crise procura-se tirar ilações para situações futuras (lições aprendidas) e estabelecer mecanismos de acompanhamento/monitorização para que o Estado, as instituições e a sociedade civil se restabeleça, de forma a prevenir futuras ocorrências (Coombs, 2007; Heath, 2010).

3.1. Mecanismos Nacionais de Gestão de Crises

Os cinco mecanismos nacionais de gestão de crises que consideramos fundamentais são os seguintes: diplomacia/negócios estrangeiros, defesa nacional, segurança interna, proteção civil e segurança do ciberespaço.

3.1.1. A Diplomacia

A diplomacia tem um caráter oficial, de onde lhe advém a legitimidade, nacional e internacional e a sua capacidade funcional. Tem ainda um conjunto de regras, rituais, vocabulário específico e um corpo de funcionários especializados – a sua natureza generalista, evolutiva e universalista – e, à *la limite*, dispõe de um certo grau de autonomia, sobretudo, em cenários espácio-temporais mais complexos que requerem urgência/imediatismo na ação e na decisão. Reunindo estes pressupostos, a Diplomacia teve sempre um caráter preventivo e de gestão de crises. Quando falha, pode desencadear-se a guerra. Contudo, mesmo em cenário de guerra, a Diplomacia atua, direta ou indiretamente, através de intermediários, para negociar a paz (Mongiardim, 2007: 25-45). Atua também durante as crises e no pós-crise, procurando criar condições para a resolução de problemas e para consolidação da normalidade.
O Ministério dos Negócios Estrangeiros (MNE) é o departamento governamental que tem por missão formular, coordenar e executar a política externa de Portugal. Neste âmbito coordena, nomeadamente com o MDN, a participação das Forças Armadas em operações de apoio à paz da ONU, operações da OTAN, missões de gestão de crises da UE, missões de cooperação técnico-militar, entre outras. Coordena também com o MAI a participação das Forças e Serviços de Segurança em operações de apoio à paz da ONU (na respetiva componente policial), em missões de gestão civil de crises no quadro da UE, em operações desenvolvidas pela agência FRONTEX – na

atual crise migratória para a Europa –, a cooperação policial europeia no âmbito da EUROPOL e do Acervo Schengen – ao nível do combate ao terrorismo e criminalidade organizada –, entre outras.

O Plano Nacional de Regresso, aprovado pela Deliberação do Conselho de Ministros n.º 254/2016 de 28 de julho, é uma das referências importantes neste enquadramento. Tem por objetivo responder com eficácia às necessidades de apoio a cidadãos portugueses residentes ou localizados no estrangeiro, que por motivo de situações de crise nos países onde residem ou se localizam, tenham de regressar a Portugal num curto espaço de tempo ou tenham de ser evacuados desses países devido a crises de segurança, catástrofes naturais, pandemias ou outras. O Plano tem três fases de abordagem, que podem ocorrer de forma sucessiva ou em simultâneo, englobando as seguintes ações:

1.ª Fase – a efetuar no país de proveniência e as relativas ao transporte para local seguro ou para Portugal – coordenada pelo MNE, com a colaboração do MDN;
2.ª Fase – relativas ao acolhimento inicial e de emergência, à chegada a Portugal – coordenada pelo MAI, com a colaboração dos Ministérios das Finanças, do MDN e do Ministério da Segurança Social; e
3.ª Fase – relativas ao acolhimento até à integração definitiva – coordenada pelo Ministério da Segurança Social, em articulação com os membros do Governo responsáveis pelas áreas do Trabalho e da Educação.

3.1.2. A Defesa Nacional

De acordo com o Art.º 273.º n.º 1 da CRP é obrigação do Estado assegurar a defesa nacional. O n.º 2 do mesmo artigo prevê que a defesa nacional tem por objetivos garantir, no respeito da ordem constitucional, das instituições democráticas e das convenções internacionais, a independência nacional, a integridade do território e a liberdade e a segurança das populações contra qualquer agressão ou ameaça externas.

O Art.º 1.º n.º 1 da Lei n.º 31-A/2009 de 7 de julho (Lei da Defesa Nacional) reitera o previsto na Constituição prevendo que a defesa nacional tem por objetivos garantir a soberania do Estado, a independência nacional e a integridade territorial de Portugal, bem como assegurar a liberdade e a segurança das populações e a proteção dos valores fundamentais da ordem constitucional contra qualquer agressão ou ameaça externas.

O Art.º 10.º da LDN prevê que os ramos das Forças Armadas – Marinha, Exército e Força Aérea – têm por missão principal participar, de forma integrada, na defesa militar da República, nos termos da Constituição e da lei, sendo fundamentalmente

vocacionados para a geração, preparação e sustentação das forças da componente operacional do sistema de forças, assegurando também o cumprimento das missões reguladas por legislação própria e das missões de natureza operacional que lhes sejam atribuídas pelo CEMGFA.

3.1.3. Sistema de Segurança Interna

Nos termos do Art.º 1.º n.º 1 da LSI a segurança interna é a atividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática. Segundo o n.º 2 do mesmo artigo a atividade de segurança interna exerce-se nos termos da Constituição e da Lei, designadamente da lei penal e processual penal, da lei-quadro da política criminal, das leis sobre política criminal e das leis orgânicas das forças e dos serviços de segurança. O n.º 3 refere que as medidas previstas na presente lei destinam-se, em especial, a proteger a vida e a integridade das pessoas, a paz pública e a ordem democrática, designadamente contra o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem, a prevenir e reagir a acidentes graves ou catástrofes, a defender o ambiente e a preservar a saúde pública.

O Sistema de Segurança Interna tem um conjunto de órgãos relevantes: o já mencionado Secretário-Geral do SSI (SGSSI), o Conselho Superior de Segurança Interna, o Gabinete Coordenador de Segurança (GCS), a Unidade de Coordenação Antiterrorismo (UCAT) e o Ponto Único de Contacto para a Cooperação Policial Internacional (PUC-CPI).

O SGSSI funciona na direta dependência do Primeiro-Ministro ou, por sua delegação, do Ministro da Administração Interna. Tem competências de coordenação, direção, controlo e comando operacional.

De acordo com o Art.º 16.º da LSI no âmbito das suas competências de coordenação, o SGSSI tem os poderes necessários à concertação de medidas, planos ou operações entre as diversas forças e serviços de segurança, à articulação entre estas e outros serviços ou entidades públicas ou privadas e à cooperação com os organismos congéneres internacionais ou estrangeiros, de acordo com o plano de coordenação, controlo e comando operacional das forças e dos serviços de segurança.

O SGSSI tem competências de comando operacional (Art.º 19.º da LSI) em caso de incidentes tático-policiais graves, coordenando com o Diretor Nacional da PSP e/ou com o Comandante-Geral da GNR a gestão dos mesmos, de acordo com o princípio da competência territorial. A LSI prevê, em situações extraordinárias

perante incidentes graves no quadro da segurança interna e da proteção civil, determinadas pelo Primeiro-Ministro após comunicação fundamentada ao Presidente da República, a possibilidade de serem colocados sob o comando operacional do SGSSI. Estão abrangidos atentados terroristas, acidentes graves ou catástrofes, situações de criminalidade violenta ou grave (sequestro ou tomada de reféns), ataques a órgãos de soberania, estabelecimentos hospitalares, prisionais ou de ensino, infraestruturas destinadas ao abastecimento e satisfação de necessidades vitais da população, meios e vias de comunicação ou meios de transporte coletivo de passageiros e infraestruturas classificadas como infraestruturas nacionais críticas, o emprego de armas de fogo em circunstâncias em que se ponha em perigo a vida ou a integridade física de uma pluralidade de pessoas, utilização de substâncias explosivas, incendiárias, nucleares, radiológicas, biológicas ou químicas.
Exercem funções de segurança interna a Guarda Nacional Republicana, a Polícia de Segurança Pública, a Polícia Judiciária, o Serviço de Estrangeiros e Fronteiras, os órgãos da Autoridade Marítima Nacional e os órgãos do Sistema da Autoridade Aeronáutica (Art.º 25.º n.º 2 da LSI).

3.1.4. O Sistema Integrado de Operações de Socorro

A proteção civil é a atividade desenvolvida pelo Estado, regiões autónomas e autarquias locais, pelos cidadãos e por todas as entidades públicas e privadas com a finalidade de prevenir riscos coletivos inerentes a situações de acidente grave ou catástrofe, de atenuar os seus efeitos e proteger e socorrer as pessoas e bens em perigo quando aquelas situações ocorram. A atividade de proteção civil tem caráter permanente, multidisciplinar e plurissectorial, cabendo a todos os órgãos e departamentos da Administração Pública promover as condições indispensáveis à sua execução, de forma descentralizada, sem prejuízo do apoio mutuo entre organismos e entidades do mesmo nível ou proveniente de níveis superiores (Art.º 1.º da LBPC).
Nos termos do Art.º 37.º do mesmo diploma, a Comissão Nacional de Proteção Civil é presidida pelo MAI.. Segundo o Art.º 48.º da LBPC, o Sistema Integrado de Operações de Proteção e Socorro (SIOPS) é o conjunto de estruturas, de normas e procedimentos que asseguram que todos os agentes de proteção civil atuam, no plano operacional, articuladamente sob um comando único, sem prejuízo da respetiva dependência hierárquica e funcional.
A lei em referência prevê que são agentes de proteção civil, de acordo com as suas atribuições próprias, os seguintes: os corpos de bombeiros, as forças de segurança, as Forças Armadas. os órgãos da Autoridade Marítima Nacional, a Autoridade Nacional da Aviação Civil, o INEM e demais entidades públicas prestadoras de

cuidados de saúde, os sapadores florestais. A Cruz Vermelha Portuguesa exerce, em cooperação com os demais agentes e de harmonia com o seu estatuto próprio, funções de proteção civil nos domínios da intervenção, apoio, socorro e assistência sanitária e social (Art.º 46.º da LBPC).

A ANEPC, de acordo com o Decreto-Lei n.º 398/2019 tem atribuições de planeamento civil de emergência, de previsão e gestão de riscos e planeamento de emergência de proteção civil e de proteção e socorro, no âmbito dos recursos de proteção civil e da atuação dos bombeiros (Art.º 4.º). A nova organização da proteção civil prevê: um Comando Nacional de Emergência e Proteção Civil, Comandos Regionais de Emergência e Proteção Civil (Norte, Centro, Lisboa e Vale do Tejo, Alentejo e Algarve) e Comandos Sub-regionais de Emergência e Proteção Civil – circunscrição territorial correspondente ao território de cada entidade intermunicipal existe um comando sub-regional de emergência e proteção civil.

No Comando Nacional de Emergência e Proteção Civil, nos comandos regionais de emergência e proteção civil e nos comandos sub-regionais de emergência e proteção civil funcionam salas de operações e comunicações dotadas de operadores de telecomunicações de emergência.

O Decreto-Lei n.º 2/2019 de 11 de janeiro institui o Sistema Nacional de Monitorização e Comunicação de Risco, de Alerta Especial e de Aviso à População, estabelecendo orientações para o fluxo da informação entre as autoridades de proteção civil, agentes de proteção civil, entidades técnico-científicas e demais entidades envolvidas nos domínios da monitorização e comunicação de riscos, do alerta ao sistema de proteção civil e do aviso às populações, face à iminência ou ocorrência de acidente grave ou catástrofe.

No relatório de dezembro de 2018 do sistema nacional de proteção civil no âmbito dos incêndios rurais elaborado pelo Observatório Técnico Independente no quadro da Assembleia da República, é mencionado que "apesar de as áreas de atuação estarem por vezes bem definidas, há muitas vezes repetições (embora nem sempre prejudiciais), mas por vezes contradições, quase sempre ineficiências e, mais ou menos explicitamente, até competição entre organismos públicos que teriam por obrigação primeira a cooperação (...). O sistema é apelidado de "excessivamente complexo" (...). "A complexidade do sistema é fruto da complexidade do problema mas também de um histórico de acumulação de entidades e estruturas que se vão criando ao longo do tempo, sendo muito mais fácil e politicamente atraente criar novas entidades ou estruturas do que extingui-las ou fundi-las de modo a torná-lo mais operacional" (OTI, 2018, p. 18).

3.1.5. A Segurança do Ciberespaço

O CNCS tem por missão contribuir para que o país use o ciberespaço de uma forma livre, confiável e segura, através da promoção da melhoria contínua da cibersegurança nacional e da cooperação internacional, em articulação com todas as autoridades competentes, bem como da implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais.
Neste sentido, o CNCS atua junto dos operadores de serviços essenciais, dos prestadores de serviços digitais e das entidades do Estado na medida em que estes são cruciais para o bom funcionamento da sociedade portuguesa. O CNCS atua também em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa e cibercrime e ciberterrorismo, devendo comunicar à Polícia Judiciária, os factos de que tenha conhecimento relativos à preparação e execução de crimes.

4. Comando Estratégico e Operacional

Todo o edifício jurídico atrás exposto é marcado pela complexidade, por sistemas com competências complementares em alguns cenários e concorrentes ou sobrepostos noutros, o que não facilita a prevenção e resposta às crises.
A formulação de políticas públicas em Portugal não se tem caraterizado pela racionalidade e continuidade, mas em grande medida por estas políticas serem casuísticas, reativas e descontínuas. Em face de um problema, a opção adotada é legislar, criar novas estruturas e novos sistemas e, muito poucas vezes, se envereda pela fusão ou redução das redundâncias e estruturas duplicadas.
De acordo com Dye (2010) a maioria das políticas públicas é uma combinação de: planeamento racional, incrementalismo, competição entre grupos, preferências das elites, escolhas públicas, processos políticos e influências institucionais que contribuem para criar, alterar, ajustar interesses e ideias antes, durante e após cada uma das fases da geração da política. Temos, assim, um processo complexo de adoção de políticas e estratégias para garantir a defesa nacional, a segurança interna, a proteção civil, a cibersegurança com estruturas próprias e com poucos vasos comunicantes.
Abordámos cinco sistemas paralelos e em alguns vetores sobrepostos para fazer face a crises: diplomacia, defesa, segurança interna, proteção civil e cibersegurança, verificando-se que muitas forças/entidades empenhadas têm uma atuação multimodal ou transversal, de acordo com o tipo de cenário.

A estratégia, para Abel Cabral Couto, é "a ciência e a arte de desenvolver e utilizar forças morais e materiais de uma unidade política ou coligação, a fim de se atingirem objetivos políticos que suscitam ou podem suscitar, a hostilidade de uma outra vontade política" (Couto, 1987: 209). Segundo o mesmo autor, "a sua finalidade é a consecução de objetivos políticos, através do desenvolvimento e utilização da força. É da competência das mais altas hierarquias civis e militares. A sua execução estende-se a todos os setores de uma unidade política ou coligação. É simultaneamente uma ciência e uma arte" (Couto: 1987: 209). O nível estratégico coincide com a tutela política e com as direções nacionais, direções gerais ou comandos gerais.

Ao comando estratégico cabe: manter a ligação com a tutela política; definir de forma clara os objetivos estratégicos orientadores de cada operação, devendo ser evitados os demasiado genéricos – ex.: garantir a segurança pública, em vez de especificar como se pretende garantir a segurança pública na operação em concreto; manter a ligação com o nível operacional de comando e assegurar o seu alinhamento com a estratégia definida; acionar recursos necessários ao comando operacional; assegurar o alinhamento das ações policiais com as linhas estratégicas orientadoras definidas; apesar do comandante estratégico não tomar decisões táticas, é responsável por garantir que aquelas são genericamente adequadas e proporcionais aos riscos identificados, são legais e estão alinhadas aos objetivos estratégicos; assegurar o registo do racional e dos pressupostos das decisões estratégicas e das ordens emitidas; definir os pressupostos genéricos que justificam uma intervenção de emergência em ITP; aprovar a política e orientações da comunicação institucional para o evento que originou o acionamento da cadeia de comando e controlo dedicada; assegurar a realização de um *debriefing* sobre o incidente/operação com os comandantes dos diversos níveis de comando.

De acordo com o Art.º 19.º n.º 2 do RESEE, o estado de sítio ou o estado de emergência só podem ser declarados, no todo ou em parte do território nacional, nos casos de agressão efetiva ou iminente por forças estrangeiras, de grave ameaça ou perturbação da ordem constitucional democrática ou de calamidade pública. O n.º 3 prevê que o estado de emergência é declarado quando os pressupostos referidos no número anterior se revistam de menor gravidade e apenas pode determinar a suspensão de alguns dos direitos, liberdades e garantias suscetíveis de serem suspensos. O n.º 4 estipula que a opção pelo estado de sítio ou pelo estado de emergência, bem como as respetivas declaração e execução, devem respeitar o princípio da proporcionalidade e limitar-se, nomeadamente quanto à sua extensão e duração e aos meios utilizados, ao estritamente necessário ao pronto restabelecimento da normalidade constitucional. Nos termos do n.º 8 do mesmo artigo, a declaração do estado de sítio ou do estado de emergência confere às autoridades competência para tomarem as providências necessárias e adequadas ao pronto restabelecimento da normalidade constitucional.

Segundo o Art.º 10.º do RESEE, a declaração do estado de sítio ou do estado de emergência compete ao Presidente da República e depende da audição do Governo e da autorização da Assembleia da República ou, quando esta não estiver reunida nem for possível a sua reunião imediata, da respetiva Comissão Permanente, sendo que, quando autorizada pela Comissão Permanente da Assembleia da República, a declaração do estado de sítio ou do estado de emergência terá de ser ratificada pelo Plenário logo que seja possível reuni-lo. No Art.º 11.º do RESEE apura-se ainda que a declaração do estado de sítio ou do estado de emergência reveste a forma de Decreto do Presidente da República e carece da Referenda do Governo. Em contraponto, verificamos no n.º 2 do Art.º 26.º do RESEE, que a modificação da declaração do estado de sítio ou do estado de emergência no sentido da redução das respetivas providências ou medidas, bem como a sua revogação, operam-se por Decreto do Presidente da República, referendado pelo Governo, independentemente de prévia audição deste e de autorização da Assembleia da República.

Ao nível da segurança interna os órgãos estratégicos com competências genéricas ou específicas são o Presidente da República, a Assembleia da República, o Primeiro-Ministro, o MAI, o MJ, o SG/SSI, o Conselho Superior de Segurança Interna, o CGS, o PUC-CPI, a UCAT, o Comando-Geral da GNR, as Direções Nacionais da PSP, PJ e SEF, o Comando Geral da Polícia Marítima e a Direção do SIS.

O MAI tem por missão formular, conduzir, executar e avaliar as políticas de segurança interna, do controlo de fronteiras, de proteção e socorro, de segurança rodoviária, de administração eleitoral, bem como uma política global e coordenada na área das autarquias locais (Art.º 15.º n.º 1 do Decreto-Lei n.º 251-A/2015 de 17 de dezembro). O SG/SSI, no plano estratégico constitui-se como a pedra angular do sistema, detendo competências de direção, coordenação e controlo.

No que tange à proteção civil, os órgãos estratégicos são o Presidente da República, a Assembleia da República, o Primeiro-Ministro, MAI, a Comissão Nacional de Proteção Civil, o SGSSI, a ANEPC, o ICNF, a AGIF, os supracitados agentes de proteção civil: os corpos de bombeiros; as Forças de Segurança; as Forças Armadas; os órgãos da Autoridade Marítima Nacional; a ANAC; o INEM, e demais entidades públicas prestadoras de cuidados de saúde; os sapadores florestais e a Cruz Vermelha Portuguesa.

No quadro da segurança do ciberespaço os principais órgãos estratégicos são o Presidente da República, a Assembleia da República, o Primeiro-Ministro, o Ministro da Presidência, o Diretor Geral do GNS, o coordenador do CNC, e o Conselho Superior de Segurança do Ciberespaço. Ao nível da Ciberdefesa destacam-se do ponto de vista estratégico, o Presidente da República, o Ministro da Defesa, o CEMGFA, os comandantes dos três ramos.

Neste contexto, podemos salientar a existência em Portugal de cinco estruturas ou órgãos de comando e controlo, e coordenação, suscetíveis de serem acionados em

situações de crise e, neste sentido, permitirem a gestão da mesma no plano político-estratégico e, nos casos previstos na lei, também no plano operacional e tático, assim como recursos e meios interinstitucionais e abordagens transdisciplinares.

No que concerne à Defesa Nacional e em concreto na dependência do Estado-Maior-General das Forças Armadas (EMGFA), encontra-se a funcionar o Comando Conjunto para as Operações Militares (CCOM). Está previsto no Art.º 9.º n.º 1 alínea a) da Lei Orgânica n.º 1-A/2009 de 7 de julho que aprova a Lei Orgânica de Bases da Organização das Forças Armadas (LOBOFA). O CCOM assegura o exercício do comando operacional das forças e meios da componente operacional do sistema de forças, pelo CEMGFA, em todo o tipo de situações e para as missões das Forças Armadas, com exceção das reguladas por legislação própria e atribuídas aos ramos, bem como a ligação com as forças e serviços de segurança e outros organismos do Estado relacionados com a segurança e defesa e a proteção civil, no âmbito das suas atribuições.

Na dependência do GCS, existe a Sala de Situação para "acompanhar situações de grave ameaça à segurança interna", conforme estabelecido no Art.º 21.º n.º 6 da LSI.

Ao nível do SIOPS, encontra-se o Centro de Coordenação Operacional Nacional (CCON). Este está previsto no Art.º 3.º do Decreto-Lei n.º 134/2006, de 25 de julho, alterado pelos Decreto-Lei n.º 114/2011, de 30 de novembro e Decreto-Lei n.º 72/2013, de 31 de maio, assegurando que todas as entidades e instituições de âmbito nacional imprescindíveis às operações de proteção e socorro, emergência e assistência previsíveis ou decorrentes de acidente grave ou catástrofe se articulam entre si, garantindo os meios considerados adequados à gestão da ocorrência em cada caso concreto. O CCON integra representantes da ANEPC, das Forças Armadas, da GNR, da PSP, do INEM, do Instituto Português do Mar e da Atmosfera, I.P., e do Instituto de Conservação da Natureza e das Florestas, I.P., e de outras entidades que cada ocorrência em concreto venha a justificar. O CCON é coordenado pelo presidente da ANEPC, podendo este fazer-se substituir pelo comandante operacional nacional da ANEPC. O CCON tem como atribuições: integrar, monitorizar e avaliar toda a atividade operacional quando em situação de acidente grave ou catástrofe. O CCON é coordenado pelo presidente da ANPC, podendo este fazer-se substituir pelo comandante operacional nacional da ANEPC. Ao CCON compete, entre outras: integrar, monitorizar e avaliar toda a atividade operacional quando em situação de acidente grave ou catástrofe.

No quadro da Segurança do Ciberespaço, na dependência do Gabinete Nacional de Segurança, está sedeado o CNC e sob tutela do Estado-Maior-General das Forças Armadas, o Centro de Ciberdefesa.

O Centro de Ciberdefesa, de acordo com o Despacho n.º 13692/2013, de 11 de outubro de 2013 do Ministro da Defesa Nacional, constitui o órgão, na dependência do CEMGFA, responsável pela condução de operações no ciberespaço e pela resposta

a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas. A Escola de Comunicações e Sistemas de Informação da Aliança – NATO Communications and Information Academy, a NCI Academy – em construção em Oeiras será um polo fundamental em termos internacionais e nacionais na criação de conhecimento sobre a segurança e defesa do ciberespaço.

Merece ainda referência o Sistema de Busca e Salvamento que no âmbito marítimo funciona com um Centro de Coordenação para a Busca e Salvamento Marítimo, sediado no Comando Naval, no Alfeite e, no âmbito aéreo, é de salientar a existência do Centro de Coordenação para a Busca e Salvamento Aéreo, sediado no Comando Aéreo, em Monsanto.

As estratégias em vigor são diversificadas e cobrem um vasto leque de áreas, mas raramente estão relacionadas entre si. Têm vindo a ser aprovadas ao longo dos anos em função dos ciclos políticos e, por vezes, não recorrem à memória institucional sobre as temáticas que abordam e nem sempre têm uma perspetiva holística. Apresentamos apenas alguns exemplos: o Conceito Estratégico de Defesa Nacional, a Estratégia Nacional sobre Segurança e Desenvolvimento, a Estratégia Nacional de Combate ao Terrorismo, a Estratégia Nacional para uma Proteção Civil Preventiva, a Estratégia Nacional de Segurança do Ciberespaço, a Estratégia Nacional para a Igualdade e a Não Discriminação 2018-2030, a Estratégia Nacional de Segurança Rodoviária.

Para além dos órgãos nacionais de natureza mais transversal, existem centros de comando e controlo/salas de situação nos três ramos das Forças Armadas (Marinha, Exército e Força Aérea) e nas Forças e Serviços de Segurança (GNR, PSP, Polícia Marítima e PJ).

No caso dos centros de comando e controlo operacionais das Forças de Segurança é de referir que têm ligação via SIRESP, por videoconferência e através dos respetivos sistemas de informação (SIOP da GNR e SEI da PSP) aos Comandos Regionais e Distritais em todo o país, o que se constitui como uma mais-valia para as situações de crise e emergência no quadro da segurança interna.

No âmbito do SIOPS existem os centros de coordenação operacional distrital (CCOD)[3] que asseguram que todas as entidades e instituições de âmbito distrital imprescindíveis às operações de proteção e socorro, emergência e assistência previsíveis ou decorrentes de acidente grave ou catástrofe se articulam entre si, garantindo os meios considerados adequados à gestão da ocorrência em cada caso concreto.

3 Os CCOD integram, obrigatoriamente, representantes da ANPC, das Forças Armadas, da GNR, da PSP, do INEM, I.P. e do Instituto de Conservação da Natureza e das Florestas, I.P., e das demais entidades que cada ocorrência em concreto venha a justificar.

5. A Pandemia de COVID-19

Uma das lições aprendidas com a crise decorrente da disseminação do vírus COVID-19 consiste na necessidade de planear de forma prospetiva, delinear cenários e avaliar potenciais ameaças e riscos. Esta pandemia surpreendeu as Organizações Internacionais, os Governos, as instituições públicas e privadas e os cidadãos.

Em termos estratégicos, a criação das estruturas interministeriais de monitorização do estado de emergência e de acompanhamento da situação de calamidade, funcionando em formato de reuniões regulares e não como estruturas permanentes, as reuniões com presença do Presidente da República, Primeiro-Ministro, Ministros e diversos membros da comunidade cientifica, assim como o trabalho da Comissão Nacional de Proteção Civil e dos Centros de Coordenação Operacional Distrital revelaram-se muito importantes. As reuniões ao nível da Subcomissão de Proteção Civil, assim como as realizadas ao nível do Sistema de Segurança Interna e com a Procuradoria-Geral da República contribuíram para a coordenação entre entidades de diversos quadrantes, a troca de informações e o estabelecimento de procedimentos.

A Direção-Geral de Saúde (DGS) enquanto Autoridade Nacional de Saúde (Art.º 3.º n.º 3 do Decreto-Lei n.º 82/2009, de 2 de abril), os delegados de saúde aos níveis regional e local, assim como todo o sistema nacional de saúde têm desempenhado um papel incontornável. Revelaram-se fundamentais os *briefings* e relatórios diários da evolução pandémica por parte da DGS, o parecer sobre a miríade de diplomas legais que foram sendo publicados durante o estado de emergência e situação de calamidade regulando o exercício de diversos setores económicos e atividades laborais, o decretar de medidas de confinamento a cidadãos infetados pelos delegados de saúde, assim como o trabalho de todos os profissionais de saúde.

Durante os 45 dias de estado de emergência, entre 18 de março e 2 de maio de 2020, a Polícia de Segurança Pública (PSP) efetuou 266 detenções por crime de desobediência, das quais, 87 detenções por violação do dever de confinamento obrigatório a cidadãos infetados, uma média de 6 detenções por dia, realizou 19.244 operações policiais, fiscalizou 359.373 viaturas, encerrou 490 estabelecimentos, sensibilizou 225.957 cidadãos, contactou e sinalizou 98.100 cidadãos idosos, protegeu mais de 8.000 vítimas de violência doméstica, efetuou 120 escoltas a material sanitário, transporte de análises clínicas, escoltas sanitárias de cidadãos estrangeiros, segurança das cidades, dos aeroportos, dos transportes públicos, de infraestruturas críticas, entre muitas outras missões. Efetuou igualmente 81 detenções por violência doméstica, a maioria em flagrante delito, 160 por tráfico de estupefacientes e 87 por crimes contra a propriedade.

Após a declaração de situação de calamidade e até ao dia 1 de junho de 2020, a PSP deteve 15 pessoas por crime de desobediência, das quais, 13 em situação de

confinamento obrigatório, 129 por tráfico de estupefacientes e 84 por crimes contra a propriedade. Neste período a PSP realizou 12.428 operações, fiscalizou 89.820 viaturas, encerrou 140 estabelecimentos comerciais, sensibilizou 90.683 cidadãos, contactou e sinalizou 23.200 idosos, protegeu 4.111 vítimas de violência doméstica. Desde março de 2020, a PSP efetuou 476 detenções por crimes relacionados com a prevenção da pandemia, detetou 4.604 contraordenações e encerrou 1.075 estabelecimentos comerciais, dados que retratam o trabalho realizado por esta Força de Segurança.

Sublinha-se sobretudo a cooperação registada entre municípios, agentes de proteção civil, forças e serviços de segurança, Forças Armadas, entidades públicas e privadas que muito contribuiu para a prevenção e para respostas multidisciplinares para fazer face à pandemia.

Considerações Finais e Propostas

A segurança e as crises tornaram-se conceitos de banda larga (Guedes e Elias, 2010, p. 30). Já não são matérias exclusivas da atenção dos Estados. Por um lado, a segurança perdeu a sua dimensão quase exclusivamente pública, nacional e militar. Por outro, as crises podem ser políticas, económicas, sociais, de segurança, sanitárias, ambientais.

Refletimos sobre as crises nos planos diplomático, de defesa, de segurança interna, de proteção civil e de segurança no ciberespaço. Estamos conscientes da existência de outras tipologias de crises e de dimensões de prevenção e resposta a crises, por exemplo: no âmbito bancário e do sistema financeiro; de segurança das matérias-classificadas e de segurança industrial para prevenir atos de espionagem e sabotagem. Pareceu-nos relevante circunscrever este breve estudo sobre a gestão de crises às áreas que poderão ter um imediato impacto disruptor do Estado de direito e respetivas instituições, daí termos considerado as áreas que estudámos mais detalhadamente, como prioritárias na gestão de crises.

Os acontecimentos críticos podem ser transversais ou podem começar num determinado setor e ter um efeito catalisador de outros eventos que impliquem a adoção de procedimentos excecionais de prevenção de consequências mais gravosas ou de reação a incidentes em curso. Daí pensarmos que as políticas públicas de segurança e estratégias preventivas e de ação têm que ser transversais, multi-institucionais, flexíveis, apostando sobretudo, no comando e controlo, na interoperabilidade de comunicações e de equipamentos.

No debate público e em alguns meios académicos é referido que em Portugal não existe uma estrutura consolidada de resposta a crises. Muitas vezes, é apontada a extinção do Sistema Nacional de Gestão de Crises como uma opção política que

amputou as nossas estruturas de segurança, de defesa e de proteção na reação a emergências e na resolução de incidentes críticos ou catástrofes de diversa natureza. Mas esse sistema não passou efetivamente do papel e, quer as Forças e Serviços de Segurança quer as Forças Armadas, quer a Proteção Civil evoluíram, modernizaram-se e adaptaram-se aos novos desafios.

A questão fulcral consiste no aperfeiçoamento do trabalho conjunto e na definição clara do comando e controlo e de coordenação estratégica, operacional e tática perante crises inesperadas, voláteis, em constante evolução e difíceis de catalogar. Face a crises sistémicas ou transversais será importante estabelecer pontes entre as diversas áreas da resposta, sendo o exemplo da crise gerada pela pandemia de COVID-19 significativo em relação a este aspeto. A nossa perceção é que perante eventos críticos inesperados e de grande intensidade as estruturas de resposta nacionais podem colapsar por falta de articulação sistémica.

Não existe um Sistema Nacional de Prevenção e Resposta a Crises. Existem diversos sistemas que cumprem esta missão nas suas áreas de competência, embora de forma paralela, por vezes coordenada, outros de modo sobreposto ou em competição. Não é, todavia, verdade que não tenhamos dispositivos legais, estruturas e órgãos para a prevenção e reação a crises de diversa natureza. Eles existem em grande quantidade e em permanente atualização, numa dinâmica legislativa profícua.

Em resultado da nossa investigação, tendo em vista confirmar ou refutar as hipóteses colocadas na abertura, colocamos em evidência o seguinte:

1. confirmámos que as ameaças, riscos e as crises contemporâneas são mais complexas, menos previsíveis e difíceis de catalogar, na medida em que se interpenetram, são flexíveis e interrelacionadas. Uma crise pode começar por ser económica e rapidamente tornar-se uma crise política e uma crise de segurança. Na sequência de uma catástrofe pode verificar-se uma crise social, sanitária e de segurança. Assim como, perante uma crise sanitária, como a que vivemos, surgirá uma crise económico-financeira com muito prováveis efeitos políticos;
2. concluímos que o sistema nacional de prevenção e resposta a crises revela um excesso de departamentalização e uma marcada atomização, patente nos diversos documentos estratégicos aprovados para um conjunto de matérias que são, na maioria das vezes, relacionadas entre si, assim como na multiplicidade de estruturas de coordenação e de comando e controlo criadas;
3. comprovámos que em Portugal será essencial uma maior coerência política e legislativa bem como a criação de um órgão de coordenação estratégica e de gestão de crises de grande magnitude.

No nosso ponto de vista, fará sentido refletir sobre a resiliência destas estruturas, a interoperabilidade de recursos, de comunicações e de sistemas de informação.

Os diversos Ministérios – e em concreto, o MNE, MDN, MAI, MJ, Ministério da Saúde, Ministério da Educação, Ministério das Finanças – deverão adotar uma abordagem transversal, transdisciplinar, multi-institucional e atuarem de forma mais coordenada nas suas áreas de sobreposição.

Na sociedade do risco (Beck, 1992), a passagem do estado de normalidade ao estado de crise pode, em muitas circunstâncias, ser instantâneo e ter efeitos em cadeia, pelo que será avisado estudar causas previsíveis e apostar na prevenção a médio e longo prazo, no fortalecimento das estruturas de gestão de crises, no planeamento conjunto entre diversas entidades e na sensibilização e formação da sociedade civil.

Em termos internacionais a pandemia tem provocado um crescimento dos índices de corrupção e de crime organizado, fomentando, por exemplo, o açambarcamento e a especulação de preços de medicamentos e de vacinas em muitos países. Outra tendência contemporânea tem consistido no incremento da desinformação, de teorias da conspiração e de outro tipo de ameaças híbridas em ambiente virtual, as quais, aludem à adoção de um "estado de exceção permanente" violador de direitos fundamentais e têm gerado manifestações de protesto e desordens públicas orquestradas por movimentos (oriundos de um vasto espectro ideológico) contestatários das medidas de prevenção, profiláticas e de confinamento adotadas pelos Estados.

A COVID-19 não se resume a um mero problema de saúde pública, mas tem consequências sociopolíticas, económicas e de segurança. Em Portugal o serviço nacional de saúde tem revelado uma capacidade de resposta extraordinária. A segurança interna e, em particular a PSP, por desempenhar a sua missão nos principais centros urbanos em Portugal, tem demonstrado um papel insubstituível, uma grande capacidade de adaptação, resiliência e competência para fazer face à miríade de desafios resultantes desta crise, salientando-se o seguinte: fiscalização do cumprimento dos normativos aprovados em contexto de pandemia, gestão de segurança durante reuniões e manifestações de protesto em relação às restrições legais impostas, gestão da segurança de grandes eventos desportivos (Final da Liga dos Campeões em agosto de 2020, por exemplo), segurança da campanha eleitoral e as eleições para a Presidência da República em janeiro de 2021, os eventos relacionados com a Presidência Portuguesa do Conselho da UE desde janeiro de 2021.

Os profissionais de saúde, as Forças de Segurança, as Forças Armadas, a proteção civil, mas também a sociedade civil no seu todo, têm conseguido num trabalho titânico fazer face a uma pandemia inesperada.

Permanece, todavia, a necessidade de criar estruturas que reúnam os diferentes atores relevantes, com vista a garantir uma visão holística, assim como maior robustez, sustentabilidade, conhecimento, experiência, capacidade de planeamento e de execução, em respeito pelos diretos liberdades e garantias dos cidadãos. Um vírus que surpreendeu o mundo, bem como o país e as suas instituições, confirma

a tendência de incerteza e de interconexão das ameaças e riscos, multiformes e difusas, que impendem sobre uma sociedade globalizada e em rede. Antecipa-se também que estes fenómenos tenham um caráter cada vez mais cíclico e impactante na sociedade contemporânea, pelo que a geração de cenários e o planeamento estratégico serão cruciais.

Neste contexto, o desafio que se coloca aos Estados e em concreto a Portugal, será a consolidação de uma cultura de trabalho mais cooperativa e cada vez menos corporativa, a criação de estruturas e de mecanismos interinstitucionais de comando, controlo e coordenação.

A comunidade científica e em particular as universidades e as instituições das áreas da defesa, da segurança interna, da proteção civil, da cibersegurança, da saúde, entre outras, podem dar um contributo muito relevante quanto à reflexão e investigação científica sobre o planeamento, execução e avaliação da intervenção conjunta e combinada nos planos estratégico, operacional e tático, entre as vertentes *security* e *safety*, entre os setores público e privado, entre as instituições e a sociedade civil, entre a prevenção e a reação.

Defendemos a aprovação de uma Estratégia Nacional de Gestão de Crises e a constituição formal de um Gabinete Nacional de Gestão de Crises na dependência do Primeiro-Ministro, sem que se faça tábua rasa das estruturas e legislação já existentes, às quais, fizemos referência com algum detalhe. Este Gabinete deveria ter uma componente interministerial e multissectorial, devendo ser composto pelos Ministros dos Negócios Estrangeiros, Presidência do Conselho de Ministros, Finanças, Defesa Nacional, Administração Interna, Justiça, Saúde, Planeamento e Infraestruturas, Ambiente, podendo incluir caso necessário, o Procurador-Geral da República, o CEMGFA, o SG/SSI e o SG/SIRP e faria a ligação com o CCOM, com a Sala de Situação do Sistema de Segurança Interna, com o CCON, com o Centro de Ciberdefesa e com CNCS, na condução político-estratégica das crises. Poderia desempenhar também um papel relevante na coordenação de eventuais pedidos de apoio internacional, assim como das operações de recuperação, de restabelecimento e de regresso à normalidade. O Gabinete teria que ter condições de segurança e ligação permanente através de redes seguras e redundância (por exemplo analógica) com os Centros de Comando Estratégico da defesa, da segurança interna, da proteção civil e da segurança do ciberespaço.

Esta Estratégia Nacional de Gestão de Crises tem que ter em conta a definição das infraestruturas críticas nacionais, de modo a estabelecer prioridades e ativar os planos de segurança necessários.

A formação e exercícios conjuntos regulares entre Forças Armadas, Forças e Serviços de Segurança, Proteção Civil, Emergência Médica, CNCS e de muitos outros atores, ações de sensibilização junto da sociedade civil, das universidades, escolas do ensino básico e secundário, autarquias, aeroportos internacionais, empresas de

transportes públicos, serviços públicos, empresas privadas de setores estratégicos, a realização de exercícios conjuntos, seriam fundamentais com vista à supressão dos ruídos e competição institucionais que resultam em desconfianças, competição e desperdício de energias e de recursos.

A interoperabilidade de meios de comunicação, de recursos informáticos, de equipamento e de infraestruturas parece-nos algo essencial e evidente num país com recursos financeiros limitados.

A comunicação pública em situação de crise deverá ser privilegiada e coordenada, porquanto, contribuirá para informar os cidadãos. Antes das crises, será crucial a sensibilização e formação sobre procedimentos em situação de catástrofe, acidentes graves ou outros. Durante as crises é primordial o aconselhamento sobre comportamentos preventivos, ações recomendadas, a informação sobre o evoluir da situação.

Apesar de, até ao momento, a cooperação interinstitucional ser globalmente positiva na presente pandemia, a lógica de abordagem corporativa, setorial e pouco coordenada para responder a emergências e incidentes críticos poderá revelar-se desastrosa em crises de grande dimensão. Torna-se crucial aproveitar o conhecimento e experiência acumulados em termos institucionais e pessoais e criar mecanismos de direção estratégica mais coerente e de comando e controlo eficazes e eficientes que ultrapassem as entropias existentes, prestando assim um melhor serviço à sociedade e aos cidadãos.

A segunda, terceira e eventuais vagas subsequentes apresentam-se como desafios ainda maiores para Portugal, tendo em conta o aumento do número de óbitos e de infeções e os impactos avassaladores em termos sociais, económicos e em outras vertentes ainda difíceis de apurar. Será crucial que, em conjunto, o Governo e restantes órgãos de soberania, instituições públicas, privadas, a sociedade civil, encarem de frente este desafio e ajam de forma planeada e coerente, sendo o processo de vacinação em curso fulcral, de modo a derrotarmos este inimigo invisível e conseguirmos regressar a uma vida normal.

Bibliografia

Barrento, António (2010). *Da Estratégia.* Parede: Tribuna da História.

Bauman, Zygmunt (2008). *Liquid Times,* 2nd ed. Cambridge: Polity Press.

Beck, Ulrich (2009). *World at Risk.* Cambridge: Polity Press.

Beck, Ulrich (1992). *Risk Society. Towards a New Modernity.* London: Sage Publications.

Bigo, Didier (2001). Internal and External Security(ies): The Möbius Ribbon. In Mathias Albert, David Jacobson e Yosef Lapid, eds., *Identities, Borders and Orders: Rethinking International Relations Theory.* Minneapolis: Minnesota University Press, pp. 91-136.

Buzan, Barry (1991). *People, States and Fear.* Boulder: Lynne Rienner.

Buzan, Barry; Waever, Ole e de Wilde, Jaap (1998). *Security. A New Framework For Analysis.* Boulder, London: Lynne Rienner Publishers.

Carreiras, Helena (2020). Covid-19 e a gestão de crises: um novo paradigma? *IDN Brief,* 13 de maio. Disponível em https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2020/idnbrief_13maio2020.pdf

Chiles, J. R. (2001). *Inviting Disaster: Lessons from the Edge of Technology.* New York: Harper Business.

Cochran, Clark E., *et al.* (2009). *American Public Policy: An Introduction.* Boston: Wadsworth Cengage Learning.

Coombs, Timothy (2007). *Crisis Management and Communications* [em linha], October 30. Institute for Public Relations. Disponível em: http: //www.instituteforpr.org/crisis-management-and-communications/ [consultado em: 2 de outubro de 2017].

Coombs, Timothy e Holladay, Sherry (2010). *The Handbook of Crisis Communication.* UK: Wiley-Blackwell.

Couto, Abel Cabral (1987). *Elementos da Estratégia.* Lisboa: Instituto de Altos Estudos Militares.

Diegues, Silvia (2011). *A Comunicação da Crise e a Web 2.0: um Retrato das Empresas Portuguesas.* Dissertação de Mestrado. Covilhã: Universidade da Beira Interior.

Dye, Thomas R. (2010). *Understanding Public Policy.* Boston: Longman.

Elias, Luís (2011). Estratégia Portuguesa na Gestão Civil de Crises. *Nação e Defesa,* n.º 129, pp. 145-184.

Elias, Luís (2011). *Segurança na Contemporaneidade. Comunitarização e Internacionalização.* Dissertação de Doutoramento. Lisboa: Faculdade de Ciências Sociais e Humanas

Elias, Luís e Guedes, Armando Marques (2010). *Controlos Remotos. As Dimensões Externas da Segurança Interna.* Coimbra: Almedina.

Faria, M. J. (2001). *Direitos Fundamentais e Direitos do Homem,* Vol. I. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

Heath, Robert L. e O'Hair, H. Dan (2010). *Handbook of risk and crisis communication.* New York. Routledge.

Mongiardim, Maria Regina (2007). *Diplomacia.* Coimbra: Edições Almedina.

Moreira, Adriano (2010). *A Crise, a Segurança, a Mudança.* Lisboa: Academia de Ciências de Lisboa.

Morujão, Carlos (2013). *Crise e Responsabilidade. Husserl, Heidegger e a Fenomenologia.* Lisboa: Editorial Aster.

Roberts, Jonathan C. (2005). Exploratory visualization with multiple linked views. In Alan MacEachren, Menno-Jan Kraak, e Jason Dykes, eds., *Exploring Geovisualization.* Amsterdam: Elseviers.

Seeger, Matthew W., *et al.,* (2009). Crisis and Emergency Risk Communication in Health Contexts: Applying the CDC Model to Pandemic Influenza. In Heath, Robert L., O'Hair, H. Dan, eds., *Handbook of Risk and Crisis Communication.* New York, Routledge.

Sellnow, T. e Seeger, M. (2013). *Theorizing Crisis Communication.* Oxford, UK: Wiley-Blackwell.

Snyder, M.; Decker Tanke, E. e Berscheid, E. (1977). Social perception and interpersonal behavior: on the self-fulfilling nature of social stereotypes. *Journal of Personality and Social Psychology,* 35, pp. 656-666.

Thaler, Richard e Sustein, Cass (2008). *Nudge. Improving Decisions About Health, Wealth and Happiness.* New Haven & London: Yale University Press

Legislação Nacional e Internacional

Decisão 2008/617/JAI do Conselho de 23 de Junho de 2008 relativa à melhoria da cooperação entre as unidades especiais de intervenção dos Estados-Membros da União Europeia em situações de crise. *Jornal Oficial da União Europeia,* L 210, 6.8.2008, pp. 73-75. Conselho da União Europeia. Disponível em EUR-Lex [website] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008D0617&from=HU

Declaração n.º 344/2008, Comissão Nacional de Protecção Civil. Regulamento de Funcionamento dos Centros de Coordenação Operacional. *Diário da República*, 2.ª série, n.º 202, 17 de outubro de 2008. Disponível em http://www.prociv.pt/bk/LEGISLACAO/Documents/declaracao_344_2008_CCO.pdf

Decreto Legislativo Regional n.º 16/2009/M, de 30 de junho. Aprova o regime jurídico do Sistema de Protecção Civil da Região Autónoma da Madeira. *Diário da República* n.º 124/2009, Série I de 2009-06-30. Região Autónoma da Madeira - Assembleia Legislativa.

Decreto Legislativo Regional n.º 17/2009/M, de 30 de junho. Cria o Serviço Regional de Protecção Civil, IP-RAM e aprova a respetiva orgânica. *Diário da República,* n.º 124/2009, Série I de 2009-06-30. Região Autónoma da Madeira - Assembleia Legislativa.

Decreto Legislativo Regional n.º 7/99/A, de 19 de março. Estabelece a orgânica do Serviço Regional de Protecção Civil e de Bombeiros dos Açores. Revoga o Decreto Legislativo Regional n.º 8/87/A, de 22 de junho. *Diário da República,* n.º 66/1999, Série I-A de 1999-03-19. Região Autónoma dos Açores - Assembleia Legislativa Regional (Alterado pelo Decreto Legislativo Regional n.º 39/2006/A, de 31 de outubro e pelo Decreto Legislativo Regional n.º 11/2007-A, de 23 de abril).

Decreto-Lei n.º 12/2018, de 16 de fevereiro. Aprova a orgânica da Agência para a Gestão Integrada de Fogos Rurais, I. P. *Diário da República,* n.º 34/2018, Série I de 2018-02-16.

Decreto-Lei n.º 126-B/2011, de 29 de dezembro. Aprova a Lei Orgânica do Ministério da Administração Interna. *Diário da República,* n.º 249/2011, 1.º Suplemento, Série I de 2011-12-29. Ministério da Administração Interna (alterado pelo Decreto-Lei n.º 163/2014, de 31 de outubro, pelo Decreto-Lei n.º 161-A/2013, de 2 de dezembro, e pelo Decreto-Lei n.º 112/2014, de 11 de julho).

Decreto-Lei n.º 163/2014, de 31 de outubro. Procede à terceira alteração ao Decreto-Lei n.º 126-B/2011, de 29 de dezembro, que aprova a Lei Orgânica do Ministério da Administração Interna, e à primeira alteração ao Decreto-Lei n.º 73/2013, de 31 de maio, que aprova a orgânica da Autoridade Nacional de Proteção Civil. *Diário da República,* n.º 211/2014, Série I de 2014-10-31. Ministério da Administração Interna.

Decreto-Lei n.º 173/2004, de 21 de julho. Cria o Sistema Nacional de Gestão de Crises. *Diário da República,* n.º 170/2004, Série I-A de 2004-07-21. Ministério da Defesa Nacional.

Decreto-Lei n.º 2/2019, de 11 de janeiro. Institui o Sistema Nacional de Monitorização e Comunicação de Risco, de Alerta Especial e de Aviso à População. *Diário da República,* n.º 8/2019, Série I de 2019-01-11. Presidência do Conselho de Ministros.

Decreto-Lei n.º 251-A/2015, de 17 de dezembro. Aprova a Lei Orgânica do XXI Governo Constitucional. *Diário da República,* n.º 246/2015, 1.º Suplemento, Série I de 2015-12-17. Presidência do Conselho de Ministros.

Decreto-Lei n.º 49/2017, de 24 de maio. Cria o Ponto Único de Contacto para a Cooperação Policial Internacional. *Diário da República,* n.º 100/2017, Série I de 2017-05-24. Presidência do Conselho de Ministros (conclusões do Conselho sobre a Estratégia Renovada de Segurança Interna da UE para 2015-2020, Doc. 9798/15, de 10 de junho de 2015, JAI 442 COSI 67).

Decreto-Lei n.º 72/2013, de 31 de maio. Procede à segunda alteração ao Decreto-Lei n.º 134/2006, de 25 de julho, que cria o Sistema Integrado de Operações de Proteção e Socorro. *Diário da República,* n.º 105/2013, Série I de 2013-05-31. Ministério da Administração Interna (Sistema criado pelo Decreto-Lei n.º 134/2006, de 25 de julho, e alterado pelo Decreto-Lei n.º 114/2011, de 30 de novembro).

Deliberação do Conselho de Ministros 254/2016, de 28 de julho. Aprova o Plano de Regresso.

Despacho n.º 13692/2013, de 11 de outubro. Orientação para a política de Ciberdefesa. *Diário da República,* n.º 208/2013, Série II de 2013-10-28. Ministério da Defesa Nacional – Gabinete do Ministro (Cria o Centro de Ciberdefesa).

Despacho n.º 14688/2014, de 25 de novembro. Unidades orgânicas flexíveis da Autoridade Nacional de Proteção Civil. *Diário da República,* n.º 235/2014, Série II de 2014-12-04. Ministério da Administração Interna – Autoridade Nacional de Proteção Civil. Retificado pela Declaração de Retificação n.º 85/2015 de 13 de janeiro (Retificação do Despacho n.º 14688/2014, de 25 de novembro) *Diário da República,* n.º 21/2015, Série II de 2015-01-30, Ministério da Administração Interna - Autoridade Nacional de Proteção Civil; e alterado pelo Despacho n.º 1553/2015 de 13 de janeiro (Alteração ao Despacho n.º 14688/2014, de 25 de novembro), *Diário da República,* n.º 31/2015, Série II de 2015-02-13, Ministério da Administração Interna – Autoridade Nacional de Proteção Civil.

Lei Constitucional n.º 1/2005, de 12 de agosto. Sétima revisão constitucional. *Diário da República,* n.º 155/2005, Série I-A de 2005-08-12. Assembleia da República.

Lei n.º 27/2006, de 3 de julho. Aprova a Lei de Bases da Proteção Civil. *Diário da República,* n.º 126/2006, Série I de 2006-07-03. Assembleia da República (Alterada pela Lei Orgânica n.º 1/2011, de 30 de novembro e pela Lei n.º 80/2015, de 3 de agosto, que republica o diploma).

Lei n.º 31-A/2009, de 7 de julho. Aprova a Lei da Defesa Nacional. Esta Lei é rectificada pela Declaração de Rectificação n.º 52/2009, de 20 de Julho, na qual se publica a Lei Orgânica n.º 1-B/2009, de 7 de Julho. *Diário da República,* n.º 129/2009, 1.º Suplemento, Série I de 2009-07-07. Assembleia da República

Lei n.º 44/86, de 30 de setembro. Regime do estado de sítio e do estado de emergência. *Diário da República,* n.º 225/1986, Série I de 1986-09-30. Assembleia da República.

Lei n.º 46/2018, de 13 de agosto. Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. *Diário da República,* n.º 155/2018, Série I de 2018-08-13. Assembleia da República.

Lei n.º 65/2007, de 12 de novembro. Define o enquadramento institucional e operacional da protecção civil no âmbito municipal, estabelece a organização dos serviços municipais de protecção civil e determina as competências do comandante operacional municipal. *Diário da República,* n.º 217/2007, Série I de 2007-11-12. Assembleia da República.

Lei n.º 53/2008, de 29 de agosto. Aprova a Lei de Segurança Interna. *Diário da República,* n.º 167/2008, Série I de 2008-08-29. Assembleia da República.

Lei Orgânica n.º 1-A/2009, de 7 de julho. Aprova a Lei Orgânica de Bases da Organização das Forças Armadas. *Diário da República,* n.º 129/2009, 1.º Suplemento, Série I de 2009-07-07. Assembleia da República.

Portaria n.º 224-A/2014, de 4 de novembro. Fixa a Estrutura nuclear da Autoridade Nacional de Proteção Civil. *Diário da República,* n.º 213/2014, 1.º Suplemento, Série I de 2014-11-04. Ministérios das Finanças e da Administração Interna

Portaria n.º 302/2008, de 18 de abril. Estabelece as normas de funcionamento da Comissão Nacional de Protecção Civil. *Diário da República,* n.º 77/2008, Série I de 2008-04-18. Ministério da Administração Interna.

Resolução do Conselho de Ministros (RCM) n.º 134/2017 de 27 de setembro. Aprova a Estratégia para o Turismo 2027. *Diário da República,* n.º 187/2017, Série I de 2017-09-27. Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros (RCM) n.º 157-A/2017, de 27 de outubro. Aprova alterações estruturais na prevenção e combate a incêndios florestais. *Diário da República,* n.º 208/2017, 1.º Suplemento, Série I de 2017-10-27 Presidência do Conselho de Ministros (determina a criação da Agência para a Gestão Integrada de Fogos Rurais).

Resolução do Conselho de Ministros (RCM) n.º 157-B/2017, de 27 de outubro de 2017. Cria uma Estrutura de Missão para a instalação do Sistema de Gestão Integrada de Fogos Rurais (SGIF). *Diário da República,* n.º 208/2017, 1.º Suplemento, Série I de 2017-10-27. Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros (RCM) n.º 19/2013, de 5 de abril. Aprova o Conceito Estratégico de Defesa Nacional. *Diário da República,* n.º 67/2013, Série I de 2013-04-05. Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros (RCM) n.º 26/2013, de 19 de abril. Aprova as linhas de orientação para a execução da reforma estrutural da defesa nacional e das Forças Armadas, designada por Reforma "Defesa 2020". *Diário da República,* n.º 77/2013, Série I de 2013-04-19. Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros (RCM) n.º 36/2015, de 12 de junho. Aprova a Estratégia Nacional de Segurança do Ciberespaço. *Diário da República,* n.º 113/2015, Série I de 2015-06-12. Presidência do Conselho de Ministros.

Resolução n.º 25/2008, de 18 de julho. Diretiva relativa aos critérios e normas técnicas para a elaboração e operacionalização de planos de emergência de proteção civil. *Diário da República,* n.º 138, 2.ª série, 18 de julho de 2008. Comissão Nacional de Proteção Civil. Disponível em http://www.prociv.pt/bk/LEGISLACAO/Documents/Res.%20CNPC%20n%C2%BA%2025-2008.pdf

Relatórios Nacionais e Internacionais

Agenda Europeia para a Segurança. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. COM(2015) 185 final. Estrasburgo, 28 de abril de 2015. Disponível em EUR-Lex [website] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0185&from=EN

Observatório Técnico Independente (OTI): Castro Rego, F., Fernandes, P., Sande Silva, J., Azevedo, J., Moura, J. M., Oliveira, E., Cortes, R., Viegas, D. X., Caldeira, D., e Duarte Santos, F., coords., 2018. *Avaliação do sistema nacional de proteção civil no âmbito dos incêndios rurais.* Relatório Final. Observatório Técnico Independente, Assembleia da República, Lisboa, pp. 116. Disponível em Observatório Técnico Independente, Assembleia da República [website] https://www.parlamento.pt/Documents/2019/janeiro/RelatorioFinal_OTI_GABPAR.pdf

Estratégia Global para a Política Externa e de Segurança (PES) da UE de 2016

Secretariado-Geral do Conselho, 2010. *Estratégia de segurança interna da União Europeia – Rumo a um modelo europeu de segurança,* março de 2010. Luxemburgo: Serviço das Publicações da União Europeia. Disponível em Conselho Europeu [website] https://www.consilium.europa.eu/media/30754/qc3010313ptc.pdf

Conselho da União Europeia, 2003. *Estratégia Europeia em matéria de Segurança: uma Europa segura num mundo melhor,* 12 de dezembro. Luxemburgo: Serviço das Publicações da União Europeia. Disponível em Conselho Europeu [website] https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf

Sistema de Segurança Interna, Gabinete do Secretário-Geral. *Relatório Anual de Segurança Interna* (RASI) 2017. Disponível em Portal do Governo [website] https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABAAzMTE2AgAWydNBBAAAAA%3d%3d

Preparação para a Resposta a Situações de Crise: A Resiliência Assente na Capacitação com Sistemas Inteligentes de Apoio à Decisão

Luís Velez Lapão

Resumo

Com o aumento da complexidade das sociedades humanas, o impacto resultante de situações de crise pode ser muito significativo, sobretudo tendo em conta a história de situações passadas. Como se viu com a Pandemia do COVID-19, muitas destas situações transformaram-se em situações de risco à segurança nacional. O planeamento, a comunicação e a preparação são cruciais, bem como o uso adequado das tecnologias de informação e apoio à decisão. Perante o risco de ameaças, sobretudo aquelas às quais Portugal é vulnerável, é necessária uma maior articulação entre as autoridades nacionais e as comunidades de especialistas. Neste artigo explorar-se-á como se podem criar lideranças capacitadas para a ação ágil e concertada no terreno, e como é que o papel das novas tecnologias, pode apoiar o desenvolvimento de cenários de tomada de decisão. O artigo examina como é que as novas tecnologias, nomeadamente os "drones" e Inteligência Artificial, poderão ser instrumentos importantes no apoio aos decisores, e argumenta que a resiliência do sistema e a articulação entre equipas de decisores e especialistas poderá produzir um impacto positivo sobre a tomada de decisão.

Palavras-chave: crise; resiliência; tecnologias; pandemia.

Abstract

Preparing to Respond to Crisis Situations: Resilience Based on Empowerment Supported by Intelligent Decision Support Systems

With the increased complexity of human societies, the impact resulting from crisis situations can be very significant, especially considering the history of past situations. As seen with the COVID-19 Pandemic, many of these situations have turned into risks to national security. Planning, communication, and preparation are crucial, as well as the appropriate use of information and decision support technologies. Given the risk of threats, especially those to which Portugal is vulnerable, greater coordination is necessary between national authorities and communities of experts. This article will explore how to create leadership capable of agile and concerted action in the field, and how the role of new technologies can support the development of decision-making scenarios. The article examines how new technologies, namely drones and Artificial Intelligence, can be important instruments in supporting decision-makers, and argues that the system's resilience and the articulation between teams of decision-makers and experts can have a positive impact on decision making.

Keywords: crisis; resilience; technologies; pandemic.

Artigo recebido: 01.06.2020
Aprovado: 16.06.2020
https://doi.org/10.47906/ND2020.156.02

1. Introdução

Pandemias, catástrofes, muitas delas alterações climáticas são um processo complexo resultante de várias transformações nas dinâmicas do planeta muitas deles provocadas pela atividade humana – e.g., aumento do CO_2 na atmosfera e nos mares, redução das florestas e da biodiversidade, com surgimento frequente de novos vírus –, e que começam a ter um impacto relevante em áreas como a produção e segurança alimentar, na saúde das pessoas – e.g., questões de Saúde Pública, como poluição do ar – e nos conflitos entre Estados – e.g., pelo aumento da dificuldade de acesso a recursos fundamentais, como água ou alimentos – sobretudo num contexto de maior complexidade resultante da globalização.
Neste contexto, podem-se identificar cinco fatores principais que determinam o sucesso, ou o fracasso, das sociedades humanas (Diamond, 2005):

1) A degradação ambiental, que ocorre quando um ecossistema se deteriora à medida que seus recursos se esgotam;
2) As alterações climáticas, naturais ou provocadas pelo homem, como no exemplo da Ilha da Páscoa;
3) Existência de países vizinhos hostis;
4) Principais parceiros comerciais enfraquecidos; e
5) A falta de acesso a recursos que permitam à sociedade adaptar-se.

Todos estes aspetos constituem ameaça significativa para a segurança nacional, pelo que é preciso desenvolver, quer a capacidade de compreender as variáveis que geram aumento de risco, quer a capacidade de tomada de decisão em situação de crise, envolvendo vários atores, que agilizem as respostas a estas ameaças, potenciando a inovação e o uso das novas tecnologias – e.g., sensores ou *drones*.
O uso de sistemas de informação e do treino de cenários são instrumentos fundamentais para ajudar a preparar os decisores para eventuais situações futuras, preferencialmente precavendo a ocorrência de situações de risco, mitigando o risco ou reduzindo erros humanos evitáveis. Por exemplo, identificando quais os indicadores de segurança – i.e., potenciados pelo uso de sensores –, que, uma vez ultrapassados possam despoletar a tomada de determinadas medidas, como investimentos estratégicos em infraestruturas ou formação de recursos humanos. O que se pretende explorar neste texto é "como podemos melhor preparar decisores para que possam responder agilmente em situação de crise, e que ameace a segurança nacional".

Complexidade das Dinâmicas Societais Contemporâneas

A complexidade resulta do aumento do número de atores intervenientes e do aumento do número de interações entre atores (Plsek e Wilson, 2001; Lapão *et al.*, 2015).

A globalização fez crescer esta complexidade, sobretudo nas interações entre países, de uma forma dramática criando interdependência entre países e organizações. Com o aumento da complexidade, aumenta o fluxo de interações, e aumenta a necessidade de gestão para lidar com o aumento do risco. Um dos resultados recentes destas dinâmicas foram as crises financeiras de 2008 e a pandemia que acontece neste momento, com origem na China e que rapidamente se espalhou pelos quatro cantos do Mundo, e que afetou a vida das pessoas e perturbou de forma surpreendente a economia. A gestão do risco tem um propósito bem definido de contribuir para mitigar os riscos de uma qualquer ameaça, quer pela maior eficiência e eficácia – utilizando os recursos onde eles têm maior impacto –, isto é, contribuir para um uso dos recursos mais "inteligente".

A aplicação da teoria da complexidade pode conduzir a que a resposta a "ameaças climáticas" seja de facto um "sistema complexo adaptativo" (SCA), do inglês *complex adaptive system*. Pode caracterizar-se um SCA, no ambiente de gestão de crise climática, com as seguintes propriedades (Plsek *e* Wilson, 2001):

- Os profissionais que trabalham na mitigação da crise (ou interagindo entre eles) sabem lidar com o paradoxo (i.e., tiveram treino), ou seja sabem aceitar várias perspetivas sobre a mesma realidade – e.g., em contexto de COVID-19, que medicamentos se devem usar?
- A equipa de resposta mostra-se "auto-organizada", com controlo interno distribuído – nas suas diversas equipas de diferentes especialidades – de que resultam regras instituídas – protocolos de atuação, devidamente validados e praticados;
- O fenómeno da "emergência" provém com frequência na relação não-linear entre "atores", quer seja entre profissional e vítima da situação de crise, ou na interação entre profissionais no campo de intervenção, etc.

Na resposta à situação de crise, a cultura existente nas equipas é determinante para o sucesso. Esta cultura de resposta "surge" do *making sense* – da procura de sentido das coisas perante o caos –, resultante das múltiplas interações entre atores heterogéneos, das conversas, das práticas de diálogo e das regras de comunicações, etc. (Weick, 2010). Há determinados eventos que são componentes importantes na aprendizagem em equipa, porque a aprendizagem surge da identificação de alternativas a partir da tentativa e erro da atividade quotidiana. Dai a importância do simulacro ou de exercícios de cenários. A natureza complexa da resposta a crises obriga a identificar e a desenvolver as capacidades necessárias para a organização responder à incerteza (Plsek e Wilson, 2001).

Os profissionais da proteção civil, da saúde, militares, etc., devem (têm de!) saber lidar com a incerteza. Como afirmava, a páginas-tantas, o chefe da escuderia da Ferrari, quando lhe perguntaram sobre como lidava com as situações numa corrida de Fórmula 1, que todas as situações devem ser consideradas previamente, e definidos

os protocolos de atuação. E terminava dizendo, que não é possível decidir "a quente" determinadas situações. O responsável pela organização da resposta à crise deve saber orientar os seus colaboradores para que aprendam a lidar com a surpresa num contexto de trabalho em equipa. Nestas condições, os profissionais vão perceber que a "ação" é chave, qualquer que seja a circunstância, o que leva ao desenvolvimento de uma consciência para se ser exigente e rigoroso, relutante em simplificar, e disponível para lidar com o desconhecido.

O conhecimento é, neste ambiente, continuamente reproduzido e é potencialmente transformado durante os processos de interação das pessoas. Em cada crise, em cada resposta a uma crise existe um processo de aprendizagem. Cada crise é diferente, cada crise envolve diferentes atores, cada crise deve ser vivida com rigor e profissionalismo. A inovação, importante num contexto de complexidade, surge assim da mistura de experiências e da vontade – procura de benefícios em função de um risco –, de potenciar o conhecimento para criar valor, que "no final do dia", pode salvar vidas. Para que exista uma "auto-organização" são necessárias algumas condições. Kauffman (1995) sugere as seguintes três condições:

a) Diversidade de competências e de experiências nas equipas;
b) Liderança focada na qualidade dos procedimentos – i.e., com base na preparação e planeamento;
c) Profissionais muito qualificados que saibam viver no *edge of chaos*, isto é, sob condições de incerteza e paradoxais.

Por exemplo, a "auto-organização" numa Unidade de Saúde Familiar – USF, envolvendo médicos, enfermeiros, técnicos e outros especialistas – incluindo médicos especialistas hospitalares –, pode ajudar a encontrar os padrões "emergentes" nos doentes – e.g., sazonalidade da procura –, ou a reorganizar o serviço para que dê respostas mais ajustadas à procura. Tal deve acontecer também entre profissionais das equipas de resposta a crises, sobretudo quando perante situações de alta complexidade. A partilha de experiências entre elementos das equipas faz aumentar o conhecimento disponível e as alternativas estratégicas e comunicacionais para tratar os doentes de forma mais ajustada. A complexidade da Saúde e o facto de muitas vezes as equipas de gestão não conseguirem criar a sua "auto-organização" pode explicar o menos bom desempenho destas.

A "auto-organização" – resultante do somatório das várias interações pontuais, interação contextualizada durante a preparação para resposta a crises, ou nas reuniões periódicas de acompanhamento semanal – em ambiente de proteção civil permite aumentar o portfolio de soluções disponíveis e aumentar assim a qualidade da resposta, porque aumenta a probabilidade de se dispor da solução que melhor se enquadra no caso que enfrenta. Da mesma forma, o responsável de um centro de saúde ou de um serviço hospitalar deve procurar promover as condições da

"auto-organização", por forma a aumentar a capacidade de resposta aos problemas novos e complexos resultantes das interações quotidianas.
De igual modo, o responsável da coordenação de crises deve procurar ter uma equipa de bons profissionais, de promover debates "abertos" e que a comunicação entre todos seja livre – e.g. aprender com outras situações de crise –, de garantir que a comunicação é feita corretamente entre todos os profissionais. Deve promover-se espaço para refletir, tolerância e valores, por exemplo através de simulações e desenvolvimento de cenários. O coordenador de situações de crise deve manter os seus colaboradores motivados para que a liderança se espelhe na ação deles, quotidianamente. Sem ela não é possível a qualidade, nem a garantia de boa gestão da crise.

Apoio à Decisão

Os sistemas de vigilância e apoio à decisão – segurança, meteorológica, tráfego aéreo, epidemiológica, clínica, etc. – têm a potencial para melhorar a qualidade da decisão, pois aumentam a informação disponível para profissionais, permitindo uma revisão mais eficiente de dados e facilitar a avaliação do risco (Forrest *et al.*, 2014). Além disso, os sistemas de apoio à decisão têm sido descritos como eficazes em muitos intervenções: redução do risco direto, redução do consumo de recursos, otimização de aplicação de procedimentos e protocolos implementando em conformidade com recomendações e reduzindo resistência às intervenções (Pestotnik, 2005). O maior desafio de um sistema de vigilância e de apoio à decisão é que este deve ser eficiente e eficaz no acesso à informação crítica e ser aceite pelos profissionais como ferramenta útil. Isso requer uma arquitetura apropriada – i.e., que informação, que atores, que decisões, etc. – e o relato claro dos resultados com foco direto na resposta à crise (Rawson *et al.*, 2017). O desenvolvimento de sistemas de apoio à decisão pode ser feito usando métodos de *Design Science* (Hevner e Chatterjee, 2010; Lapão *et al.*, 2017).
Além disso, os sistemas de apoio à decisão geralmente são mais eficazes quando se verifica o seguinte: a informação é gerada automaticamente; baseiam-se num sistema amigável desenhado com o apoio dos profissionais; são incorporados os fluxos de trabalho operacionais – e.g., da resposta a uma situação de evento extremo ou seca prolongada; os dados estão disponíveis de forma agregada (Chow *et al.*, 2016). O processo de implementação de um sistema de informação é comummente desafiador, já que limitações como a complexidade de dados de mobilidade, meteorologia, qualidade do ar, segurança e confidencialidade e falta de interesse dos profissionais estão presentes na maioria das vezes (Grimson *et al.*, 2000). Para ser eficaz, o processo de implementação deve ser feito em estreita colaboração com os profissionais e adaptado às questões sociais, económicas, educacionais e culturais

onde será usado (Boonstra, Versluis e Vos, 2014). As principais limitações para a implementação de sistemas de apoio à decisão para gestão de risco de crise são:

(i) Falta de integração no âmbito da formação;
(ii) O preço excessivo da disponibilidade software no mercado, e muitas vezes não se enquadra na cultura do local;
(iii) Software que não esteja alinhado ao utilizador, com processos de trabalho pouco fáceis de usar; e
(iv) A maioria não responde aos requisitos dos profissionais.

O objetivo deste texto é propor, em colaboração com profissionais da resposta a crises, uma arquitetura de sistema de vigilância em tempo real e de apoio à decisão de risco de crise com impacto na saúde e segurança nacional. Este sistema pode ainda apoiar a implementação (monitorizando a evolução da crise e os processos de implementação dos procedimentos) e o desenvolvimento de simulacros ou cenarização, vinculado à estratégia de resposta local, e adaptado ao contexto sociocultural.

Implicações para a Segurança e Defesa

As alterações climáticas e o aumento da atividade humana têm causado o aumento da frequência e da energia associada a eventos climatéricos extremos, i.e., tempestades, secas, bem como casos de pandemia. Por este motivo, as provisões apontam para que nos próximos anos aumente a probabilidade de períodos de seca com consequências significativas no acesso a recursos como a água e o aumento de incêndios (Miranda *et al.*, 2000; Ribeiro e Pires, 2016), bem como de mais pandemias (Whiting, 2020). A preparação dos atores – responsáveis por investimentos em infraestruturas ou ações no terreno, ou pela implementação de novas tecnologias, especialistas em segurança, militares, etc. –, para situações complexas, como seja a iminência de situações de catástrofe ou de ameaça Pandémica é fundamental para que as respostas sejam ágeis para mitigar o impacto na segurança nacional.

A preparação destes atores, em contexto de simulacro de crise, com base em cenários pré-estabelecidos, suportados por sistemas de informação de apoio à decisão, deve permitir que os atores compreendam melhor o seu papel perante determinadas ameaças e desenvolver planos ação ágeis – considerando as capacidades existentes em Portugal – e resilientes – e.g., no contexto de mecanismos de ação Europeia –, bem como estabelecer mecanismos de resposta adaptada à complexidade das situações.

A sociedade atual não é apenas bem organizada, as organizações confiam em pessoas com competências altamente especializadas que utilizam sistemas e máquinas altamente especializados para atingir altos níveis de produtividade.

Pesquisas feitas por Tainter (2018) indicam que, com níveis crescentes de especialização, o custo de gestão numa sociedade complexa aumenta. Segundo Tainter, o crescente consumo de recursos causado por altos níveis de especialização levou ao colapso das sociedades avançadas ao longo da história, como é caso dos habitantes da ilha da Páscoa. Esse é um especto do desafio que a humanidade enfrenta, pois, as pessoas tentam transformar os fluxos de produção e distribuição em larga escala – que dominam a economia hoje, mas com uma pegada ecológica significativa – para uma economia circular mais sustentável, e sobretudo mais resiliente. Os avanços têm sido, todavia, bastante frágeis, sobretudo por falta de estratégia e de incentivos adequados. De acordo com os especialistas, é, no entanto, importante começar a agir, procurando soluções o quanto antes, pois os riscos são demasiado elevados.

2. Impacto da Atividade Humana

Os dados são claríssimos, o aumento do CO_2 na atmosfera, resultante da atividade humana, está a fazer aumentar a temperatura média na Terra. Deste processo resultam também o decréscimo dos gelos no Ártico e na Antártida, o que implica o aumento do nível do mar, e o aumento dos eventos atmosféricos extremos – chuvas, furacões, secas, etc. O aumento da temperatura e da ocupação dos solos pelo homem, tem tido também impacto na redução da biodiversidade, ameaçando a sustentabilidade dos ecossistemas e o surgimento de epidemias. Em conjunto, estas alterações implicam um aumento do risco para o homem. Um dos aspetos mais evidentes é o impacto sobre as infraestruturas fundamentais – barragens, centrais termonucleares, rede elétrica, portos, etc. – que podem colocar em risco a vida das populações. E Portugal é dos países mais ameaçados (Santos e Miranda, 2006).

Por isto é claro que a atividade humana conducente às alterações climáticas constitui uma ameaça à segurança dos países, e um risco que deve ser avaliado com seriedade. Vários países já assinalaram a sua preocupação com a definição de "emergência climática", e outro exemplo relevante é o *Statement Testimony* do Comité dos Serviços das Forças Armadas Americanas apresentado à House of Representatives em 2010, que aponta já a ameaças significativas das alterações climáticas para os portos militares americanos, tal como a ameaça dos cibersegurança.

Perante uma tal ameaça, de grande complexidade e contendo bastantes incertezas, será necessário ter uma abordagem estratégica, que inclua planeamento, preparação e capacidade de intervenção aos vários níveis das forças de segurança e intervenção.

Uma agenda estratégica, multidimensional, que defina como abordar do ponto de vista organizacional do impacto de eventos extremos deve ser discutida. Por

exemplo, que deve incluir a criação necessária de uma unidade de resposta às mudanças climáticas ou a situações de pandemia. Esta unidade deve ser técnica e "separada", mas integrante do aparato do governo, por exemplo dentro da proteção civil, devidamente apoiada por especialistas da área do clima, da saúde pública e da resposta a emergências. Essa unidade deve concentrar-se na execução de medidas de preparação de situações de crise associadas à mudança climática, envolvendo o governo, o sector privado, os especialistas e investigadores. A capacidade de resposta depende da capacidade de planeamento e de preparação para mitigar o impacto dos eventos extremos.

A colaboração com instituições – proteção civil, INEM, IPMA, etc. – e entidades regionais – Câmaras Municipais, Bombeiros, Associações Civis, etc. –, centros de investigação e internacionais – ECDC, Proteção Civil Europeia, etc. – é essencial para a unidade de resposta aos eventos extremos associados com as mudanças climáticas. O combate às mudanças climáticas requer ações tangíveis, como o aumento dos investimentos para melhorar a resiliência em energia e infraestruturas, bem como capacitação de lideranças locais, que temos visto serem tão importantes na presente pandemia COVID-19. Por isto, uma abordagem planeada à mudança climática implica a combinação da área da proteção civil, da saúde, das novas tecnologias, do ambiente, da energia, da logística, bem como da Defesa, para situações mais dramáticas, que podem ter impacto regional ao nível da NATO. Tendo em conta os possíveis (e prováveis) impactos, um governo deve definir em lei um enquadramento que permita garantir financiamento a partir de uma combinação eficaz de seguros de risco, financiamento para capacitação de primeira resposta e facilidade regional de gestão de risco de emergências.

A ilha de Sint Maarten possui reconhecidamente uma grande suscetibilidade ao impacto global das mudanças climáticas, sendo por isso um grande "desafio de governação" para o país ameaçado de perder parte do seu território. O país que pouco contribuiu para o impacto negativo no clima da Terra, mas que se encontra entre os mais vulneráveis. De facto, este país já enfrenta sérias dificuldades, como a seca de 2019, a devastação de dois furacões sem precedentes, o Irma e Maria, em setembro de 2017 e a previsão de aumento do nível do mar. A Nature Foundation (2018) coloca a capital do país, Philipsburg, em risco de ficar debaixo de água nas próximas duas décadas.

Para além da preparação necessária das equipas para a resposta a emergências associadas a crises climáticas, vai necessitar de ter capacidade de recolha e análise de dados. Uma rede de sensores e estações meteorológicas, e informação via satélite, são essenciais para permitir avaliar os riscos e alimentar os sistemas de alerta precoce.

Impacto na Segurança Nacional

As alterações climáticas têm causado o aumento da frequência e da energia associada a eventos extremos. Sabemos também que está associado a eventos como pandemias. As alterações climáticas estão a causar perturbações sobre populações e com grande impacto económico-social, ameaçando já destabilizar alguns países em África. Só a atual pandemia, espera ter um impacto económico entre 10 e 20% do PIB mundial (UN, 2020).

A preparação dos atores, responsáveis por investimentos em infraestruturas ou ações no terreno, ou pela implementação de novas tecnologias, especialistas em segurança, militares, etc., para situações complexas, como seja a iminência de situações de catástrofe, de pandemia ou de ameaça climática é fundamental para que as respostas sejam ágeis para mitigar o impacto na segurança nacional. Como ficou claro, nos últimos meses, a capacidade de produção industrial de equipamentos de segurança pessoal revela-se crítica em situação de Pandemia.

Hoje a resposta a eventos extremos deve ser multidisciplinar, colaborativa e dinâmica (Guo e Kapucu, 2015). A preparação destes atores com base em cenários, suportados por sistemas de informação de apoio à decisão, deve permitir que os atores compreendam melhor o seu papel perante determinadas ameaças e desenvolver planos de ação ágeis – considerando as capacidades existentes em Portugal – e resilientes – e.g., no contexto de mecanismos de ação europeia –, bem como estabelecer mecanismos de resposta adaptada à complexidade das situações. Que depende da existência de organização preparada especialmente para este tipo de resposta (Smith, 2005).

É preciso interpretar o significado por trás das evidências disponíveis que descrevem as sociedades que sobreviveram e as que eventualmente murcharam e desapareceram (Maggio, 2017). Porque que razão os nórdicos que colonizaram a Groenlândia no início do século X não sobreviveram, enquanto os habitantes das terras altas da Nova Guiné sobreviveram? Com as evidências disponíveis, pode observar-se que o colapso de uma sociedade tende a ser precedido por uma severa redução na população e consideráveis reduções na complexidade política (e.g., ditaduras), económica e social. Foram identificados cinco fatores principais que determinam o sucesso ou o fracasso das sociedades humanas em todos os períodos da história (Diamond, 2005): degradação ambiental, que ocorre quando um ecossistema se deteriora à medida que seus recursos se esgotam – tal como está a acontecer hoje, um pouco por todo o Mundo; mudanças climáticas, naturais ou provocadas pelo homem; países vizinhos hostis – aparentemente, há quem considere que o COVID-19 aumentou a hostilidade entre países; principais parceiros comerciais enfraquecidos – devemos estar atentos ao enfraquecimento da Europa comunitária e às mudanças políticas nos Estados Unidos?; e dificuldade de acesso

a outros recursos que permitem à sociedade adaptar seus desafios – e.g., a biodiversidade na natureza e a busca por uma vacina para o COVID-19.

Reconhece-se hoje que as alterações climáticas são uma ameaça às populações e às economias. O Reino Unido acaba de impedir a construção de uma nova pista em Heathrow (Guardian, 2020), como forma de mitigar os efeitos das alterações climáticas.

A migração e o deslocamento de populações foram mencionados repetidamente entre os maiores desafios de segurança colocados pelas mudanças climáticas (Ministério da Defesa da França, 14 de outubro de 2015). A conferência "As implicações das mudanças climáticas na defesa", reuniu ministros da Defesa e outros oficiais de alto nível e representantes do sector militar de vários países do Sul e do Norte para discutir as implicações de segurança das mudanças climáticas antes da 21.ª Conferência das Partes da UNFCCC. A conferência foi aberta pelo ministro das Relações Exteriores da França, Laurent Fabius, pelo ministro do Meio Ambiente, Ségolène Royal e pelo enviado especial francês para a Proteção do Planeta, Nicolas Hulot, que destacou os principais desafios sociais, económicos e políticos associados à mudança climática, incluindo deslocamento de populações (Mokhnacheva, 2019). Neste momento a Europa discute o pacto Europeu para a Sustentabilidade e os objetivos para 2030, sob os efeitos da crise resultante da Pandemia.

3. Meios de Mitigação

A resposta a crises com potencial impacto na segurança e defesa nacional dependem de vários fatores:

– Organização, planeamento e sistemas de comunicação;
– Preparação, liderança, e sistemas de monitorização;
– Estabelecimento de sistemas de resposta resilientes.

A organização da resposta é fundamental. As equipas e as responsabilidades bem definidas são críticas para se responder com eficácia e eficiência. No campo da resposta a emergências, a comunicação deve ser aprimorada, pois costuma ser um elo frágil, donde resultam situações graves, e.g., incêndios em Portugal em 2017. Por isso as tecnologias de informação (TI) e as conexões em rede de parceiros podem melhorar as interações na cadeia de comando, para ajudar os tomadores de decisão, fornecendo a tempo a informação necessária. O valor da informação depende da relevância e da acessibilidade (Ben-Haim, 2006). A interoperabilidade entre os diferentes dispositivos de comunicação usados por diferentes organizações envolvidas numa situação de emergência sempre foi um problema. Sem interoperabilidade, e em situações de emergência normalmente "caóticas", é muito difícil comunicar-se com eficácia (Morentz, 1994). Portanto, é preciso garantir que as várias entidades

envolvidas na gestão de crise utilizam equipamentos de comunicação compatíveis. Durante o atentado de 11 de setembro de 2001, um dos helicópteros da polícia que pairava perto do que restava da primeira torre, e minutos após o colapso, tendo um dos pilotos sugerido a evacuação de todas as pessoas do segundo edifício (Klapwijk e Rothkrantz, 2006). Contudo, os bombeiros não chegaram a receber este aviso.

Isto acontece por dois motivos. Primeiro, porque a rede de comunicações falha, e não estando disponível durante algum tempo, ou, segundo, se os diferentes dispositivos foram incapazes de trabalhar juntos e, de apoiarem uma resposta coordenada. A simulação de situações de crise ajuda a identificar este tipo de fragilidades, pelo que lideranças responsáveis devem promover a prática de exercícios de simulação ou mesmo simulacros. A importância de existir uma infraestrutura de comunicação confiável e robusta que permita partilhar informações e dados críticos de forma oportuna no local da crise, leva a um conjunto diferente de ações que aproximam o esforço do sucesso. Falhar na comunicação e na interação, por outro lado, reduz consideravelmente a hipótese de sucesso (Dilmaghani e Rao, 2009).

A preparação e liderança surgem com o trabalho e esforço de alinhar a resposta entre os vários elementos das equipas responsáveis. A liderança é comumente definida por lei, mas quem a assume deve estar à altura do desafio, reconhecendo que é apenas o topo de uma cadeia de comando. Esta liderança deve promover a preparação das equipas, quer através de formalização de processos, quer através de simulacros.

O estabelecimento de sistemas resilientes é fundamental para a eventualidade de se necessitar de escalar a resposta à situação de crise, de acordo com a dimensão da ameaça ou do risco. Exemplo da resposta ao Ébola em que falhou por problemas de coordenação e por falta de resiliência (Lapão *et al*., 2015). A OMS África não esteve à altura do desafio. Por isso, as organizações de proteção civil, com o apoio das equipas de saúde, devem planear a resposta a uma potencial epidemia de ébola, sobretudo antes de existirem casos confirmados.

Um ponto chave é garantir a preparação das equipas de coordenação (Lancet, 2014), e estabelecer capacidade de resiliência através de acordos nacionais e internacionais. Uma estratégia de resposta a crises, envolvendo várias organizações, deve privilegiar a formação dos profissionais a todos os níveis de serviços; prepará-los seriamente através de exercícios e formalização da cooperação entre entidades, para permitir preencher possíveis lacunas. Deve-se aproveitar a oportunidade destes exercícios para validar a existência de definições claras e a sua adequada implementação, de acordo com as diretrizes estabelecidas. Esses processos de validação precisam ser levados a sério e com toda a atenção. Repetidos com periodicidade.

Outro aspeto crítico para a liderança, e para que tudo funcione corretamente, é promover medidas que possam garantir o profissionalismo da coordenação e de todos os

procedimentos. Os riscos são demasiado sérios para serem tomados com leviandade. Por exemplo, no caso de situações de epidemia, a comissão de controle de infeção, deve colaborar com a gestão das unidades de saúde, a todos os níveis, e com a coordenação das entidades centrais. No caso do COVID-19, e em Portugal houve alguma fragilidade na gestão da resposta, sobretudo a nível hospitalar, e sobretudo por falta de coordenação. O fluxo de doentes num hospital é um problema de gestão, que deve ter em conta as especificidades epidemiológicas, mas é um problema de gestão. Para tal deve considerar utilizar na cooperação mecanismos de flexibilidade e aprendizagem.

Questões para Auditoria Interna

Aplicável em qualquer tipo de resposta a crises, as seguintes perguntas devem ser estritamente consideradas como diretriz de organização para validar a sua capacidade de resposta, neste caso exemplificado com o COVID-19 (Lapão *et al.*, 2015):

- Existe um "Plano Nacional de Contingência" para o COVID-19? em caso afirmativo, onde pode ser encontrado esse plano?
- Este plano trata adequadamente dos problemas relacionados à comunicação dos cidadãos com os serviços de saúde (ou quaisquer outros serviços relevantes), e dos serviços de saúde com os *media*? Estão definidos porta-vozes institucionais?
- Está bem definido, para o exemplo da ação de resposta a uma epidemia tipo COVID-19, o "papel que cada serviço" de saúde deve representar dentro do Sistema de Saúde (público e privado); e como articulá-los em conjunto?
- A rede nacional de serviços públicos (neste caso de saúde) já está preparada para realizar vigilância epidemiológica e atuar em conformidade? Que tipo de resiliência existe?
- Estão identificados os atores que deverão proceder à investigação epidemiológica dos casos relatados e seus contactos? Existe um "plano para proteger os profissionais" e dar-lhes condições de trabalho adequadas?
- Qual é o papel dos laboratórios e como eles são preparados e integrados dentro do "Plano Nacional de Contingência"? O laboratório nacional de referência para situações de epidemia está preparado para lidar com esta questão? E, particularmente com aspetos de segurança biológica e com o que isso implica? Existe um plano concreto para proteger os profissionais envolvidos no processo?
- Estão disponíveis no hospital, ou em outros serviços relevantes, o tratamento atualmente considerado de referência para tratar a doença ou os seus sintomas? Em caso afirmativo, quantas pessoas podem ser tratadas em cada unidade? Que opções de tratamento estão atualmente disponíveis no país ou na região? Existe capacidade logística de mobilizar viaturas preparadas, helicópteros, etc. e os doentes para os locais adequados?

– Foi disponibilizado treino, em momento oportuno, para os profissionais que irão eventualmente lidar diretamente com as vítimas? Nesse caso, há profissionais qualificados em número suficientes e disponíveis para enfrentar os riscos apresentados por um vírus de alta transmissibilidade e de alta letalidade?
– As autoridades responsáveis pela coordenação da resposta à crise forneceram os mecanismos para a regulamentação e controle do uso de protocolos e procedimentos de segurança para as instituições de referência? Estas instituições de referência (e.g., hospitais e outras unidades de saúde) foram devidamente identificadas?
– Foi adequadamente definida a relação entre o Ministério da Saúde e os Serviços de Estrangeiros e Fronteiras (SEF)? e serão fornecidas atualizações sobre as pessoas que entram no país provenientes de países de alto risco? Os profissionais do SEF receberam o treino adequado para lidar com esses casos? Foi fornecido com precisão as informações sobre pessoas que entram no país? Existe sistema de informação que garante a comunicação correta e atempada? Existem mecanismos definidos para detetar o potencial de risco de infeção nos pontos de entrada (aeroportos e portos)?
– Está bem estabelecida a coordenação? E os diversos níveis de risco e o envolvimento de outras instituições caso se atinjam esses níveis? Por exemplo, em que altura deve o Exército entrar para aumentar a capacidade de resposta, dado que a ameaça começa a ter repercussões do foro da defesa nacional?

Ao nível, por exemplo da organização de serviços de saúde, são as comissões de controle de infeção (CCI), que geralmente são os responsáveis pela coordenação dos esforços de resposta a crises do foro da saúde, em particular para o desenvolvimento, implementação e monitorização de protocolos de ação. Em outras situações de crise, outras instituições podem ser designadas para esse fim.

Deverão ser feitos esforços para criar condições de apoio e orientação de casos potencialmente infetados, de manutenção de higiene e da limpeza, e para garantir que os serviços essenciais sejam mantidos operacionais (Simões *et al.*, 2018). Neste caso, é essencial manter os serviços de saúde em funcionamento, pelo que devem ser munidos de todas as condições para se manterem operacionais, como sejam: maternidade; emergência; pediatria; Medicina Interna; cirurgia essencial; e trauma; coordenação, a nível institucional, deve garantir a organização adequada dos profissionais de saúde trabalham para evitar excesso de trabalho, o que muitas vezes levar a erros que podem ter sérias consequências.

Um aspeto importante passa pelo processo de racionalizar o acesso ao hospital ou a instituições críticas para pacientes crónicos – incluindo casos de tuberculose e HIV. Para tal é aconselhável que seja feito tratamento domiciliar de pacientes. Essa abordagem ajuda se você tiver o apoio dos cuidados primários – ou de bombeiros

ou outras instituições locais, em outras situações. Devem adotar-se todos os procedimentos – que foram devidamente testados e treinados previamente – para evitar a disseminação do vírus – Ébola ou Coronavírus, etc. – nos serviços de saúde e para minimizar as perturbações do funcionamento normal das unidades de saúde.

Coordenação e Integração de Serviços

A coordenação e a integração de serviços, no caso da Saúde, são frequentemente prestadas pelas Direções Nacionais de Saúde (como acontece em Portugal), que devem garantir um fluxo claro e o registo de todas as informações necessárias, bem como a sua partilha de forma oportuna. Por exemplo, em muitos países africanos, os hospitais (ou outras entidades locais) acabam tendo um papel importante no processo de classificação e, às vezes, diagnóstico, pelo que devem estar preparados para essa função (Lapão *et al.*, 2015). A prática de simulacros pode contribuir para esta capacitação.

A primeira medida deve incluir a criação de uma "linha verde" para facilitar a comunicação com a população, no caso de existir uma linha como a Saúde24, é importante garantir reforço da capacidade para que outros casos não sejam afetados. Em situações de crise, é comum a saturação das redes de telecomunicações. A coordenação nacional também desempenha um papel importante na gestão de recursos humanos. Primeiro para promover a agilidade na resposta, neste caso para evitar o alastrar da epidemia e para evitar interrupções dos serviços (resposta a acudir a vítimas, a incêndios, etc.), especialmente considerando o elevado número de equipas que possam eventualmente existir no terreno.

A exigência de uma coordenação efetiva entre os serviços é crítica: hospitais e conselhos clínicos devem estar envolvidos nos esforços gerais de planeamento. As CCI também devem incluir gestores para facilitar a mobilização de recursos; devem ainda monitorizar regularmente as atividades de planeamento e implementação; desenvolver um conjunto intervenções para melhorar o controle da infeção – supervisão, treino, triagem precoce e deteção de casos, desinfeção, transferência de suspeita de casos e medidas de melhoria da higiene. Todas estas funções devem ser devidamente treinadas em simulacro, ou similar.

Segurança e Logística em Gestão de Crises

Vários organismos internacionais promovem boas práticas ao nível da segurança e gestão de crises. No caso da Saúde e das epidemias, os Médicos-Sem Fronteiras (MSF, 2020) são uma excelente referência, sobretudo em zonas com limitações de

recursos. Os MSF sugerem uma lista abrangente de atividades que devem ser realizadas para avaliar a capacidade de resposta da logística em zonas potencialmente afetadas:

a) Avaliar recursos logísticos existentes na comunidade e desenvolver uma lista de itens em falta, incluindo transporte rodoviário e aquático, disponibilidade de combustível, etc.;
b) Verificar os *stocks* de equipamentos disponíveis – equipamento de proteção individual (EPI), desinfetantes, medicamentos, alimentos, etc. – e capacidade de esterilização dos equipamentos dentro da comunidade ou nas proximidades;
c) Avaliar capacidade de comunicações e registar localizações em GPS – estradas com referência geográfica, rádio, telefone, pistas de aterragem, material crítico, etc.;
d) Reunir mapas da área afetada, ou de locais críticos, como fontes disponíveis de água ou de agências governamentais relevantes;
e) Avaliar disponibilidade de água, eletricidade (energia) e alimentos para as equipas responsáveis pela resposta;
f) Avaliar a disponibilidade de recursos humanos locais com experiência profissional relevante, agentes comunitários de saúde, forças de segurança, voluntários da Cruz Vermelha, ONG e outros consultores técnicos que poderão operar na área afetada, etc.;
g) Visitar e avaliar os serviços disponíveis. No caso de uma epidemia, importa saber o número de camas, crematórios, capacidade da cadeia de abastecimento, acesso a água limpa, eletricidade, espaço para a criação de área de isolamento, espaço de armazenamento de materiais e alimentos, e identificar possíveis modificações logísticas que precisem ser executados.
h) Avaliar também o comportamento da procura de cuidados de saúde, como médicos, enfermeiros, curandeiros tradicionais (em África);
i) Identificar corretamente o contexto sociocultural, e as situações que possam complicar a operação;
j) Avaliar a situação de segurança na área. A situação de segurança deve ser reavaliada regularmente. Porventura poderá ser necessário a participação de forças de segurança.

Além disso, a MSF recomenda o estabelecimento de uma equipa de logística e segurança, a fim de fornecer suporte logístico nas operações e garantir a segurança para que as equipas possam trabalhar no terreno (WHO, 2014).

O Papel da Gestão de Informações

Um dos aspetos cruciais para a resposta a situações de crise, e que tem sido demonstrado como uma das fraquezas mais reiteradas e em várias circunstâncias, é a gestão da informação. Para uma boa gestão da informação é necessário transparência, e para tal que se estabeleça um fluxo claro de troca de informações para evitar o risco de decisões erradas. Igualmente, será preciso evitar os registos incompletos ou a contagem dupla de situações. A qualidade da gestão de informação deve garantir que as informações sejam partilhadas de maneira adequada e em tempo útil para permitir também uma rápida e correta resposta (WHO, 2014). Note-se que durante a crise do COVID-19 imensos relatos demonstraram que esta fragilidade afetou a gestão da crise.
A gestão de informação precisa ser levada a sério para garantir ainda questões de segurança dos dados, a privacidade e a proteção de doentes e vítimas, e de suas famílias, evitando o risco potencial de estigmatização social, bem como tendo em consideração a aspetos éticos. Outro ponto importante é organizar e estabelecer a capacidade de armazenar informação e apoiar o registo da mesma, de forma a libertar os profissionais no terreno dessa tarefa, pois eles estarão ocupados e com grandes limitações para o fazer convenientemente (Lapão *et al*., 2015).

Estratégia de Comunicação

As equipas de coordenação de crises devem procurar comunicar "a uma só voz", de forma clara e assertiva, por exemplo, através de um porta-voz respeitado e credível. Com o objetivo de potenciar os media como parceiros-chave, que devem ser tratados profissionalmente e com base na confiança para evitar a transmissão de informações que pudessem desestabilizar a capacidade de resposta no terreno. As redes de telecomunicações móveis podem ser utilizadas como acesso a mecanismos de informação, seja como comunicação entre pessoas e equipa de coordenação, ou comunicação entre as equipas (Lapão *et al.*, 2015).
Há que ter em conta a possibilidade de usar comunicações móveis para melhor entender a dinâmica da procura de serviços sociais, de saúde, e outros, associados a uma epidemia, ou a outra situação de crise. Hoje, as tecnologias de Big Data e Artificial Intelligence podem ajudar a compreender melhor os padrões de comportamento das populações. Esta informação pode ser muito útil para o planeamento de uma intervenção no terreno (The Economist, 2014). No entanto, deve haver sempre um coordenador comunicações, estabelecendo mecanismos para trocar rapidamente informações entre as várias equipas e os media, para evitar rumores e desinformação, e promover a partilha de informações que sejam facilmente compreendidas

pelas populações. Uma boa coordenação deve saber potenciar o papel ativo das populações, quando estas estão bem informadas.
Um mecanismo de comunicação assertivo também ajuda a demonstrar ao público que as autoridades locais estão a atuar, de forma a responder corretamente à situação, reduzindo a ansiedade e as preocupações das comunidades locais. Uma equipa de comunicação profissional deve desenvolver antecipadamente um Plano de Comunicação, juntamente com o Ministério tutelar e outros Ministérios, a fim de transmitir mensagens coerentes e abrangentes sobre a ação no terreno.

Cooperação com os Países Africanos de Língua Portuguesa

Pela primeira vez na história, as Nações Unidas adotaram uma resolução para o estabelecimento de uma missão de emergência em saúde pública (Nações Unidas Missão de Resposta de Emergência ao Ébola - UNMEER) para combater a epidemia de Ébola, cujo surto ocorreu na África Ocidental em março de 2014 (mas que se iniciara ainda em 2013) e se estenderá até 2016. Este tipo de resoluções é fundamental para aumentar a resiliência para enfrentar situações de crise.
Esta resolução juntou governos e parceiros internacionais procurando uma resposta global. As recomendações da OMS enfatizaram, na altura, que todos os países com fronteiras terrestres com os países afetados, deveriam:

a) Estabelecer acesso rápido e eficaz a diagnóstico laboratorial qualificado para a doença, vírus Ébola (como agora com o Coronavírus);
b) Garantir que os profissionais participantes na intervenção são adequadamente treinados em prevenção, segurança e controle de infeção;
c) Estabelecer equipas de resposta rápida, equipadas para estudar e gerir casos de vírus Ébola.

Outras estratégias incluíram o apoio da UNMEER aos esforços colaborativos dos países nos mecanismos de prevenção e resposta à doença, vírus Ébola (ou outro), com foco especial no treino de recursos humanos. Por exemplo, considerando a prevenção da propagação transfronteiriça do vírus, as autoridades portuguesas foram contactadas pela UNMEER para saber da disponibilidade de Portugal para participar da resposta à crise na Guiné-Bissau, país que possui fronteiras com a Guiné. Por interesse mútuo, e dentro da cooperação bilateral. Este tipo de ações, para além de apoio a situações de crise são também uma excelente oportunidade para aprender e desenvolver competências no terreno, em contexto real.
Neste contexto, Guiné-Bissau e Portugal assinaram o Plano de Ação (novembro 2014 a junho de 2015). Este plano visou apoiar a Guiné-Bissau no sector de saúde, e foi coordenado pelo Camões-Instituto de Cooperação e Língua. Com base nas estratégias definidas pela UNMEER, a iniciativa foi conduzida sob a Comissão

Interministerial de Coordenação Resposta ao Ébola, que incluiu também a Direção-Geral de Saúde (DGS), o Instituto Nacional de Emergência Médica (INEM) e o Instituto Nacional de Saúde Dr. Ricardo Jorge (INSA). Esta iniciativa, específica na Guiné-Bissau, incluiu o nível multilateral em parceria com a OMS.

A primeira etapa envolveu uma visita para avaliar as necessidades locais, seguida posteriormente de uma segunda visita de entidades portuguesas em conjunto com a OMS para avaliar as condições estruturais e de saúde existentes naquele país, como parte de prevenção e resposta à epidemia causada pelo vírus Ébola. Essas visitas descobriram que, apesar dos esforços e melhoria das condições da Guiné-Bissau nos últimos anos, permanecem muitas dificuldades locais na prevenção e resposta a epidemias, como resultado de várias restrições: falta de condições financeiras adequadas, falta de recursos e logística; falta de recursos humanos treinados para identificar e tratar esses pacientes; não existência um laboratório para detetar o vírus do tipo Ébola, entre outros. Este último aspeto foi classificado como crucial, dada a falta de instalações com os níveis necessários de biossegurança, além disso, uma vez que não seriam possíveis o manuseio e o envio de amostras viáveis para o laboratório de referência da OMS em Dakar.

Neste pacote de apoio bilateral à Guiné-Bissau, Portugal prestou apoio ao Município de Bissau nas atividades de conscientização à população no combater à propagação do vírus Ébola, com proposta de medidas preventivas. Isso incluiu, por exemplo, o envio de desinfetantes, EPI, medicamentos e bens alimentares. Também incluiu a capacitação de um técnico Guineense no transporte de substâncias infeciosas. Foi ainda disponibilizado um laboratório móvel e um laboratório multidisciplinar para ser utilizado pela equipa Portuguese, caso viesse a ser necessário. A missão de resposta portuguesa, enquadrou-se no âmbito da OMS, tendo começado a operar em março de 2015, e manteve-se no terreno até final de 2015. A colaboração entre OMS, Guiné-Bissau e Portugal é uma forma de dar resiliência a uma eventual situação de crise. Destinou-se a criar condições para uma deteção precoce, estabelecer condições de diagnóstico, com capacidade de resposta rápida através da implementação de um sistema de vigilância, e garantir o tratamento localmente de possíveis casos da doença provocada pelo vírus do Ébola, e assim evitar também a necessidade de evacuação de pacientes infetados. Essa intervenção teve um impacto positivo adicional, permitiu a retomada das ligações aéreas entre Portugal e Guiné-Bissau. Retomadas as ligações aéreas com a Guiné-Bissau a 14 de novembro de 2014, foi implementado um rastreio aos passageiros na saída do país – como está a ser feito atualmente por alguns países com a pandemia de COVID-19 –, consistindo na avaliação da temperatura corporal, atendendo aos critérios de triagem nos pontos de saída. Essa triagem foi realizada pelos técnicos do INEM para a deteção precoce de possíveis sinais e sintomas suspeitos do vírus Ébola.

O procedimento ocorreu em conjunto com as autoridades guineenses e o Serviço de Estrangeiros e Fronteiras de Portugal, regularmente em todos os voos realizados.

Manteve-se este procedimento enquanto o surto de Ébola foi considerado extinto na costa oeste de África. Esta atividade correu sem intercorrências, e não foram identificados pacientes potencialmente infetados. Na missão a Cabo Verde, que decorreu após solicitação do Hospital Central da Praia, uma equipa do IHMT – que incluiu um infeciologista e um especialista em saúde pública – visitou o hospital e, durante dois dias reviram os processos com a equipa responsável do hospital e com a autoridades nacionais de saúde pública. O plano de contingência foi igualmente revisto quanto à possibilidade de um surto de Ébola. A maior parte do trabalho foi a discussão de uma infinidade de detalhes operacionais. A simulação de uma situação realista foi importante. Os circuitos dos pacientes através do hospitalar, desde os diferentes pontos de entrada de potenciais pacientes infetados até ala de isolamento, também foram revisadas, assim como as instalações de isolamento e os circuitos dos diferentes materiais críticos. O uso de EPI era uma questão de grande preocupação. Além disso, no outono de 2014, a DGS enviou equipamentos de biossegurança nível de proteção 4. Portugal também trabalhou com outros países de língua portuguesa. Especialistas do INSA trabalharam com as autoridades de saúde de São Tomé e Príncipe, que envolveu informações sobre requisitos técnicos, equipamentos e de recursos humanos, para avaliar a capacidade de enviar amostras seguramente ao INSA, como um laboratório de referência para a análise do Ébola. O Ministério da Saúde de Portugal enviou também EPI de nível de biossegurança 4 para Moçambique.

4. Sistemas de Apoio à Decisão

Sem um sistema de informação que permita espelhar a realidade necessária à boa decisão, não será possível garantir que os profissionais de saúde possam melhorar a qualidade dos seus serviços. Para se intervir ao nível da qualidade há que compreender muito bem os processos organizacionais existentes e o fluxo de informação necessário à tomada de decisão ao longo de uma miríade de processos. Numa organização de saúde os fluxos de informação estão, por razões históricas, comummente organizados por silos – por serviços clínicos, por diferentes profissionais, por diferentes serviços suporte, etc. A rede social, que permite o acesso a comunicação e à resolução de problemas, de uma unidade de saúde mostra a dimensão da complexidade do sistema (Lapão, 2008).

A gestão lida frequentemente com aspetos não quantificáveis no processo de decisão – e.g. considerar e negociar as opiniões dos *stakeholders* –, contudo sem as ferramentas de gestão os processos negociais seriam muito mais difíceis e complexos. A descentralização da gestão, novas modalidades de prestação de serviços, de regulação, ou de formação dos prestadores são disso exemplo (Hamel e Breen, 2007).

Todavia, o sucesso dessas mudanças depende da existência de um ambiente institucional e organizacional que crie condições favoráveis para sua implementação (e liderança q.b.). A nível institucional, é fundamental um quadro jurídico-legal que elimine os maiores obstáculos ao processo de mudança e o facilite mesmo: isto pode implicar a adoção de legislação que redefina com clareza as responsabilidades e a tomada de decisão entre os diferentes níveis de governação; a revisão das definições legais das tarefas que podem ser executadas pelos diversos grupos ocupacionais, ou a criação de sistemas de incentivos financeiros e profissionais para estimular a cooperação dos prestadores. A nível organizacional, deve promover-se a existência de capacidades de gestão, tais como uma equipa de dirigentes preparada, o acesso a sistemas de informação seguros e confiáveis e a instrumentos de gestão adaptados para a alocação ágil de recursos. Neste contexto, reconhecendo a necessidade de evolução dos sistemas de informação, o DSRM pode desempenhar um papel importante.

Preparação para Crises

O planeamento é fundamental para a segurança da informação. Como nas forças armadas, onde mesmo uma missão de patrulha comum exige um planeamento significativo e detalhado, o planeamento da segurança é a chave para as operações bem-sucedidas. Não importa o quão detalhado e abrangente seja um plano de resposta a incidentes e quão extensa é a experiência e o treino da equipa de resposta, tudo muda quando se encontra numa situação real. Mesmo para equipas de resposta a incidentes altamente profissionais e bem treinadas, quando a situação muda num segundo e o sucesso depende de alguns recursos específicos, o coordenador não pode permitir que as equipas táticas no terreno estejam sem comando. Cabe ao coordenador alterar ou realinhar tarefas, atribuir recursos adicionais e solicitar suporte de outras equipas, que devem estar em alerta para o efeito. Se já é difícil de comunicar quando todos estão no mesmo edifício, mas, dada a natureza complexa das situações de resposta a incidentes, torna-se quase impossível.
Uma equipa global de resposta a incidentes precisa de uma sala de situação virtual (Poizner, 2017). Não se pode confiar numa teleconferência para gerir um incidente, é preciso ter informação direta do terreno e forma de ter contexto e compreender o que significam. Um auxílio visual bem organizado com a linha do tempo da comunicação e a lista de tarefas necessárias numa situação crítica é fundamental. Estas ferramentas são importantes para a coordenação orientar a tomada rápida de decisões e envolvendo os membros da equipa. Uma sala de situação virtual é uma "camada" que reúne todas as informações e as disponibiliza para um esforço de decisão colaborativo.

Desenvolvimento de Cenários

Para se construir os cenários para situações de crise, pode usar-se o método proposto por Lapão e Thore (1998), que condensa os 10 passos do procedimento descrito por Schoemaker (1995), em apenas 3 fases, nas quais o envolvimento de uma equipa especializada em cenarização é fundamental. Cada vez mais estes exercícios de cenarização podem ser apoiados por tecnologias de informação e salas de situação. As primeiras fases devem decorrer em modelo de *workshops* temáticos que devem decorreram em dias diferentes, com uma duração máxima de 3 horas cada:

a) O primeiro deve ser um *workshop* de contextualização da análise de cenários para o problema em estudo. Por exemplo o impacto das alterações climáticas na segurança nacional e estratégias de mitigação e a identificação dos cenários mais relevantes em termos de preparação.
b) O segundo *workshop* deve servir para a seleção (usualmente "3") e validação dos cenários identificados no primeiro *workshop*, para na terceira fase, os cenários finais sejam desenvolvidos e analisados pelos participantes.

Os critérios para a escolha dos participantes devem ser a experiência profissional e académica, devendo o painel ser composto por 5 a 12 pessoas. No caso de eventos relacionados com crises de alterações climáticas, sugerem-se os seguintes participantes (outros mais se podem juntar, por sugestão do coordenador da proteção civil):

1) Responsáveis da Proteção Civil (com o papel de coordenador da resposta);
2) Especialista em impacto das Alterações climáticas;
3) Membro de equipa do IPMA, contexto da evolução meteorológica;
4) Membro da equipa do INEM ou DGS ou Saúde Pública, coordenador de resposta às vítimas;
5) Membro da equipa das forças de segurança (e.g. PSP e GNR);
6) Membro da equipa de bombeiros;
7) Membro da equipa das forças militares;
8) Especialista em sistemas de comunicação;
9) Especialista em logística;
10) Especialista em comportamento da população; e
11) Especialista em Cenarização e Sala de Situação (que orienta o processo).

O procedimento de cenarização inicia-se com a definição de um período de tempo para o qual se querem imaginar os diversos cenários – digamos em 2022, para dar tempo a planear e a preparar as equipas –, e com a identificação das principais forças de mudança que afetam o mundo e o país que terão impacto na questão das alterações climáticas. A escolha do período de tempo mais adequado depende de diversos fatores, tais como a evolução tecnológica, a perceção de ameaças concretas ou o período político.

Escolheu-se para este trabalho um período de três anos porque permite pensar em mais alternativas para o planeamento de crises, sendo suficientemente curto para certos elementos predeterminados como os elementos demográficos, conferindo alguma previsibilidade neste fator, enquanto incertezas críticas como a evolução tecnológica ou o ambiente político tenderão a evoluir mais rápida e imprevisivelmente durante este período.

Para preparar as sessões de cenarização, deve ser feita previamente uma revisão das temáticas, com o objetivo de identificar as principais incertezas críticas e forças de mudança, que se relacione com o papel da resposta a situações de crise, bem como um olhar sobre as tendências futuras. Em face dos riscos percecionados – e.g., número de eventos extremos, ou dias de seca extrema –, será importante incluir, por exemplo, análises quantitativas do número de profissionais que devem participar nas diversas fases da resposta (do planeamento à operação no terreno), bem como de faseamento do nível de risco.

Todos estes fatores devem explorados em equipa no decorrer dos *workshops*, de modo que se possa determinar quais serão as "forças motrizes", ou seja, quais os fatores críticos que mais poderão moldar a capacidade de resposta a crises. São as diferentes combinações destas forças que originam diversas histórias de futuras situações de crise.

O primeiro *workshop* deve iniciar-se com uma pequena apresentação para a introduzir as ideias fundamentais, os princípios da análise prospetiva de cenários, tal como recomendado por Godet (2000), permitindo aos participantes dos *workshops* tornarem-se mais familiarizados com o conceito e as ferramentas deste tipo de análise.

Ambos os *workshops* podem ser gravados para permitir posterior análise de conteúdo, de modo a melhor detalhar os resultados obtidos. Aplicando este método, a primeira fase, pretende fazer um ponto da situação das situações mais relevantes provocadas pelas alterações climáticas e da capacidade de resposta ao risco e, identificando as principais tendências, os principais atores-chave (parceiros) e as principais incertezas, e fatores críticos com possível impacto na resposta a situações de crise climática. Em termos de alterações climáticas, potencialmente podem ser identificados os seguintes fatores e tendências:

- Aumento de dias de calor extremo (de 5 para 15 dias por ano);
- Aumento de eventos de chuvas fortes potencial causadoras de derrocadas e disrupção da circulação de pessoas ou mercadorias, e das telecomunicações;
- Redução de populações que vivem e trabalham em zonas de floresta, reduzindo a capacidade de limpeza das mesmas;
- Redução do número de efetivos treinados em situações de crise; etc.

De seguida, passa-se para a definição das principais incertezas e fatores críticos, que são condensados em duas incertezas críticas relacionadas com impacto na

resposta a situações de crise climática: as "forças motrizes" (ou *driving forces*) dos cenários (Heijden, 1996). Estas forças motrizes representam os fatores mais significativos que poderão influenciar, por exemplo, o impacto na resposta a situações de crise climática em Portugal, e é partir deles que se começam a desenhar os primeiros cenários. Por exemplo, podem-se identificar as seguintes duas forças motrizes:

– Aumento de situações de crise resultante de eventos extemos;
– Grau de preparação para responder às crises, com uso ou não de tecnologias.

Na segunda fase, concebeu-se o papel da resposta de acordo com o impacto das situações de crise climática em cada um dos cenários, construídos estrategicamente em torno das "forças motrizes", testando a consistência e a plausibilidade dos primeiros cenários. Numa terceira fase, em ambiente de sala de situação, com a participação dos membros das equipas de resposta, pode trabalhar-se o material recolhido previamente para se caracterizar cada um dos cenários com maior detalhe (e.g. com uma linha de tempo), fazendo-se evoluir os cenários encontrados nas fases anteriores para possíveis cenários de decisão, e identificando pontos-chave, mais sensíveis, que poderão influenciar a tomada de decisão dos diferentes atores-chave envolvidos.

Para tal, deve ser construída uma narrativa e definir-se indicadores (ou métricas) que permitam fazer a monitorização da situação de crise e da resposta e, se necessário, a atualização dos cenários. É nesta fase que se consegue determinar e identificar mais facilmente as necessidades de futura preparação para amenizar as incertezas encontradas.

Cenários em Sala de Situação

Uma sala de situação é um espaço onde se recolhe e trata a informação para garantir melhores decisões. Pode ser entendida como uma intervenção, não só por fazer parte dos componentes da política de segurança nacional, mas por também ser constituída por um conjunto de atividades, ou serviços coordenados, organizados segundo uma sequência temporal particular, empregando recursos e informação voltados ao alcance de um objetivo específico, em resposta a uma situação de crise que afete determinada população (OPAS, 2010). A situação de crise pode ser difícil de responder se houver insuficiência de organização das informações produzidas para auxiliar os decisores a planear as suas respostas e tomar decisões mais eficazes. A sala de situação disponibiliza ao coordenador de reposta a uma crise um conjunto bem determinado de informações e análises com possibilidades para as várias evoluções, que poderão ser discutidas em ambiente envolvendo vários atores permitindo assim a tomada de decisão informada e partilhada. A Sala de Situação é um espaço dinâmico, que envolve o processo de reunir continuamente informações,

analisá-las, caracterizar problemas e propor possíveis soluções. Hoje em dia um conjunto de aplicações informáticas pode ajudar na análise de risco e de cenários, ajudando a ponderar melhor as ações a desenvolver. Assim, a uma sala de situação deve estar associada um sistema de monitorização para a alimentar da informação necessária e no tempo correto.

Para dar resposta a situações de crise resultantes das alterações climáticas, a Sala de Situação deverá ser um local onde os dados estão disponíveis, analisados e interpretados para garantir ao coordenador de crises capacidade de formulação de estratégias que possam responder de forma mais adequada à crise. As salas de situação virtual são extremamente úteis durante exercícios de treino, nas quais é possível rever as ações da equipa para identificar deficiências que precisam de correção. O principal papel da Sala de Situação em crise de origem climática é dar suporte a processos transparentes e participativos de planeamento e resposta a situações concretas de crise, com uso intensivo de informações (muitas vezes a chegar de forma quase caótica) e conhecimento específico para cada situação. Melhor ainda, quando a Sala de Situação está inserida num contexto estratégico de mitigação das crises provocadas por alterações climáticas em que visa proteger as pessoas, ecossistemas e as infraestruturas.

Para garantir o sucesso das ações, com planeamento necessário, o gestor de risco precisa estar apoiado por informações, e é neste sentido que se deve propor a utilização de uma Sala de Situação. Pode-se desenvolver o processo de cenarização utilizando técnicas de "gamificação" (Marques *et al.*, 2017). A "gamificação" é uma abordagem recente, mas muito procurada, que pode ser definida como "o uso de elementos de jogo e design de jogos em contextos não relacionados a jogos", isto é, profissionais (Werbach e Hunter, 2012), para "envolver e motivar as pessoas a atingir seus objetivos" (Burka, 2014), proporcionando uma experiência totalmente diferente ao profissional. A ramificação pode criar incentivos sem incorrer em custos muito elevados. Apesar de estarem relacionados com os jogos, os sistemas "gamificados" não são completos; eles apenas usam componentes de jogos num processo que já existe (Hagglund, 2012). A gamificação também ajuda a compreender melhor o impacto de determinadas ações ou decisões. A utilização de "gamificação" em Salas de Situação no processo de aprendizagem de gestão e coordenação de crise é fundamental sobretudo tendo em consideração a necessidade de se desenvolver competências de decisão em grupo.

A preparação para Situações de Crise não é apenas uma forma de construir equipas com experiência e capacidade de decisão, mas também fornece treino de resiliência inovador, envolvente e pedagógico. Quer para treinar situações de incêndio, fazer simulações de evacuação ou treinar de protocolos de reposta de urgência. A existência de uma "Sala de Situação para Crises" do foro das Alterações Climáticas é cada vez mais premente para capacitar decisores e prepará-los para determinadas situações de crise complexas, que são dependentes da evolução das situações externas e de situações resultantes da organização da resposta.

Seria importante que a equipa de coordenação de crises resultantes das alterações climáticas pudesse desenvolver simulacros sobre situações que eventualmente tivesse impacto na segurança nacional e quiçá na defesa nacional. Eis alguns exemplos dessas situações, que podem ser simuladas utilizando o CRISETooL (Lapão, 2020):

– Seca prolongada por mais de dois anos no Alentejo leva à falta de água generalizada, que nem o Alqueva consegue superar. Esta situação apresenta risco de perdas de produção alimentar, risco de migração de populações e de conflito, eventualmente também com o a Espanha. O que é preciso fazer? Devemos ter várias fases de abordagem do problema?
– Furação de nível IV – com ventos da ordem dos 209-251 km/h e expectativa de chuvas torrenciais –, que devido ao aquecimento global circulou o Atlântico, e cuja trajetória se aproxima da região de Lisboa, podendo afetar mais de 2 milhões de habitantes. Como identificar as populações com maior risco? Como desenvolver a resposta?
– O rápido degelo do Antártico das últimas semanas provocado por um recorde de dias seguidos de máximas de temperatura no hemisfério Sul, está a fazer aumentar o nível do mar cerca de 30 centímetros. Acontece que neste momento Portugal está a ser afetado por um ciclone (com ventos fortes e chuvas) e com o aproximar da maré cheia há zonas da costa portuguesa cujo o risco aumentou severamente. Quais são essas zonas da costa? Que meios existem para responder?
– As temperaturas altas das últimas semanas e algumas chuvas do tipo tropical criaram as condições para que o COVID-22 (Coronavírus que surgiu no Irão em 2022) se tornasse uma pandemia, que acabou de chegar a Portugal. Vários infetados, sobretudo crianças, estão localizados em Lisboa, Porto, Faro, Braga, Viseu e Santarém, e os números parecem não parar. Os hospitais de referência estão lotados e é preciso outras soluções. Que alternativas para os infetados? Se a cadeia de abastecimento de alimentos falha o que se pode fazer? Está o exército português disponível para atuar?
– Várias tempestades localizadas no Atlântico Norte, resultantes da fragilidade do *Jet Stream*, estão a impedir o abastecimento da ilha da Madeira de barco e de avião há mais de 15 dias. Os seus *stocks* estão no limite. O que podemos fazer? Como racionar os alimentos na ilha da Madeira? Como lidar com os doentes e outras vítimas?

5. Discussão

As crises vão continuar a acontecer. Estaremos prontos? Como vamos treinar os nossos decisores? Como vamos preparar-nos para esse tipo de situações?

Conscientes deste risco acrescido, e do seu impacto, é preciso organização e planeamento para lidar com esses eventos extremos. Assim, a preparação da resposta a crises e a comunicação em situação de crise são críticas (Lapão *et al.*, 2015). A Proteção Civil Portuguesa tem um papel crucial, mas é preciso trabalhar mais aspetos como eventos extremos e capacidade de decisão multidisciplinar. Por exemplo, o caso do furacão Leslei foi uma oportunidade perdida para testar os meios de resposta em Lisboa. Ainda houve a situação caricata dos SMS, que acabaram sendo enviados no dia a seguir. É preciso aprender com estes casos que correram menos bem. Os eventos climáticos extremos colidem de forma "violenta" com o quotidiano "caótico" das grandes cidades. As grandes cidades vivem dependentes dos bombeiros, que por vezes mostram pouca capacidade de resiliência. Por isso, no contexto da complexidade do quotidiano moderno, a melhor resposta são equipas bem preparadas e coesas. Estas equipas precisam de funcionar de forma muito bem articulada, para tal é preciso propiciar formação avançada para estes profissionais. Um exemplo deste tipo de equipa são os GOE (Grupo Operações Especiais) da Polícia de Segurança Pública (PSP), que treina regularmente, e com afinco para a eventualidade de ser necessário intervir. A complexidade e diversidade das situações de crise requer muita especialização, que pode ser obtida, num primeiro nível, por treino em simulacro ou simulação em Sala de Situação virtual. A preparação visa que as equipas de resposta vivam diferentes situações para ganharem conhecimento e flexibilidade. Muitas vezes as situações obrigam à inovação, como o exemplo no caso do Ébola, onde se percebeu a importância dos antropólogos para lidar com aspetos culturais que estavam a ser prejudiciais. No caso da epidemia de 2018-19 surgiram robots a ajudar nas enfermarias de infetados.

O treino periódico é muito importante, com ele se ganha "músculo" para melhores respostas. Fazer simulacros no terreno são muito dispendiosos, pelo a discussão de cenários em Sala de Situação é mais fácil e económica, com a vantagem de se poder desenvolver novas situações. O treino periódico também ajuda a perceber onde estão as fragilidades e que outras entidades poderiam contribuir. Muitos clubes locais tiveram um papel importante durante os incêndios de 2017 em Portugal. Assim se ganha resiliência, tendo consciência onde existem recursos que podem ser úteis em determinadas circunstâncias. A simulação permite ter uma perspetiva mais alargada.

Outro aspeto relevante é a colaboração entre forças e proteção civil. Do ponto de vista da mobilidade, os atores de segurança e defesa podem desempenhar um papel fundamental tanto na proteção da população aquando da gestão de crises, bem como na contribuição para os esforços de redução do risco. Por exemplo, usando a tecnologia existentes nas forças de defesa para estabelecer sistemas de alerta (e.g., situações no mar) e partilha de informações. Ou apoiando projetos de adaptação e reabilitação de terrenos, para proteger os meios de subsistência, reduzir a vul-

nerabilidade e, assim, impedir a migração forçada. Todas estas dinâmicas podem ser testadas numa Sala de Situação. Sabemos que responder aos desafios impostos pelas mudanças climáticas exigirá a mobilização e o envolvimento de todas as entidades, e os esforços para lidar com as mudanças climáticas e garantir a segurança das populações beneficiaria da experiência de atores, com a experiência do sector de defesa. O aumento da cooperação internacional e o intercâmbio de boas práticas e conhecimentos entre os países seria também um imenso passo adiante (e.g. reuniões do C4, entre Portugal, Espanha, Itália e França).

Hoje as tecnologias de informação são essenciais para uma resposta mais efetiva e rápida. A comunicação é central num processo de resposta a crises (Lapão *et al.*, 2015). Os sistemas de informação devem recolher informação em tempo real e contextualizada, e o uso de aplicações que permitam a sua análise quase imediata. O potencial uso da IA para trabalhar os dados por forma a fazer chegar ao decisor informação sobre padrões que podem ajudar a tomar decisões mais inteligentes (Schwartz, 2018). Compreender a mobilidade das pessoas, dos rios (e das cheias) e dos fumos conforme o vento pode ser feito com recurso a AI. Será preciso saber como potenciar os "drones" para obter informação crítica em situação de crise.

Por fim, considero que se deve ter agentes bem preparados na comunidade. Agentes, quais "Auditores de Defesa Nacional", ou com experiência militar ou de forças de segurança, que possam ajudar a desenvolver os primeiros passos de uma resposta, antes da chegada dos agentes da proteção civil. É importante ter as comunidades com maior capacidade de resiliência, onde a capacitação por Sala de Situação pode ser relevante. A luta para mitigar as o impacto de situações de crise, é uma luta das comunidades, e também é delas a responsabilidade para evitar males maiores. É conhecida o grau de "preparação" das populações do vale do Tejo, aperfeiçoadas ao longo dos séculos.

6. Conclusão

Como revela o "2014 Climate Change Adaptation Roadmap" (DOD, 2014): "Among the future trends that will impact our national security is climate change. Rising global temperatures, changing precipitation patterns, climbing sea levels, and more extreme weather events will intensify the challenges of global instability, hunger, poverty, and conflict. By taking a proactive, flexible approach to assessment, analysis, and adaptation, the Defense Department will keep pace with a changing climate, minimize its impacts on our missions, and continue to protect our national security". Perante o risco de ameaças, como as alterações climáticas, à segurança nacional, e havendo a consciência de que Portugal é dos países mais ameaçados, como se costuma dizer, não há tempo a perder!

É preciso que as entidades nacionais de segurança e defesa nacional se articulem, cada vez mais. É necessário que se criem lideranças capacitadas para a ação concertada no terreno. É preciso capacitar bem os decisores para situações de crise de origem climática, que sendo mais extremas e inopinadas merecem uma atenção especial. As Universidades e os centros especializados são atores muito importantes que não podem ficar de fora. As novas tecnologias, como Salas de Situação, onde se podem desenvolver cenários são um instrumento fundamental. Outras tecnologias como "drones" e AI serão instrumentos que poderão funcionar para apoiar os decisores, mas serão as pessoas bem preparadas que farão a diferença.

Referências

Ben-Haim, Y., 2006. *Info-gap decision theory: decisions under severe uncertainty*, 2nd Edition. Elsevier.

Boonstra, A., Versluis, A. e Vos, J.F.J., 2014. Implementing electronic health records in hospitals: a systematic literature review. *BMC Health Serv Res*, 14(370).

Burke, B., 2014. Gamify: How Gamification motivates people to do extraordinary things. Bibliomotion, Inc.

Chow, A.L., Ang, A., Chow, C.Z., Ng, T.M., Teng, C., Ling. L.M., Ang, B.S. e Lye, D.C., 2016. Implementation hurdles of an interactive, integrated, point-ofcare computerised decision support system for hospital antibiotic prescription. *International Journal of Antimicrobial Agents*, 47(2), pp. 132-139.

Diamond, J., 2005. Collapse: How societies choose to fail or succeed. Penguin.

Dilmaghani, R.B., e Rao, R.R., 2009. A systematic approach to improve communication for emergency response. In 42nd Hawaii International Conference on System Sciences (pp. 1-8). IEEE.

DOD, 2014. 2014 Climate Change Adaptation Roadmap. DoD Releases, Oct. 13, 2014. Disponível em http://www.acq.osd.mil/ie/download/CCARprint.pdf.

Forrest, G.N., Van Schooneveld, T.C., Kullar, R., Schulz, L.T., Duong P. e Postelnick, M., 2014. Use of electronic health records and clinical decision support systems for antimicrobial stewardship. *Clin Infect Dis*., 59 (Suppl 3): S122-33. Disponível em doi: 10.1093/cid/ciu565

Godet, M., 2000. The art of scenarios and strategic planning: tools and pitfalls. *Technol Forecast Soc Change*, 65(1), pp. 3-22.

Grimson, J., Grimson, W. e Hasselbring, W., 2000. The SI challenge in health care. Commun ACM, 43:48e55.

Guardian, 2020. www.guardian.co.uk (página central, acedida a 27 de fevereiro de 2020).

Guo, X. e Kapucu, N., 2015. Examining collaborative disaster response in China: network perspectives. *Natural Hazards*, 79(3), pp.1773-1789.

Hagglund, P., 2012. Taking gamification to the next level. Umeå University.

Hamel, G. e Breen, B., 2007. The future of management, *Harvard Business Review*.

Heijden, K., 1996. Scenarios: the art of strategic conversation. 2nd ed. Chicester: John Wiley & Sons.

Hevner, A. e Chatterjee, S., 2010. Design science research in information systems. In: Design research in information systems: theory and practice. New York: Springer, pp. 9-22.

Holland, J., 1998. *Emergence, from chaos to order*. Oxford: Oxford University Press.

Kauffman, S. A., 1995. *At home in the universe: the search for the laws of self-organization and complexity*. Oxford: Oxford University Press.

Klapwijk, P. e Rothkrantz, L., 2006. Topology based infrastructure for crisis situations, Proceedings of 3rd International Conference on Information Systems for Crisis Response and Management (ISCRAM) Conference.

Lapão, L. V., 2008. The Role of Complexity Dynamics in the Innovation Process within the new Primary-Care Governance Model in Portugal. *The Innovation Journal: The Public Sector Innovation Journal*, 13(3), 8.

Lapão, L.V. e Thore, S., 1998. Prioritizing R&D projects in the face of technological and market uncertainty: Scenario planning in the telecommunication business. In: 18th International Symposium on Forecasting, Edinburgh, 1998 – Proceedings. Edinburgh: Napier University.

Lapão, L.V., Silva, M.M. e Gregório, J., 2017. Implementing an online pharmaceutical service using design science research. *BMC medical informatics and decision making*, 17(1), pp. 31.

Lapão, L.V., Silva, A., Pereira, N., Vasconcelos, P. e Conceição, C., 2015. Ebola impact on African health systems entails a quest for more international and local resilience: the case of African Portuguese speaking countries. *The Pan African Medical Journal*, 22(Suppl 1).

Maggio, R., 2017. Collapse: How Societies Choose to Fail Or Survive. Macat Library.

Marques, R., Gregório, J., Pinheiro, F., Póvoa, P., da Silva, M.M. e Lapão, L.V., 2017. How can information systems provide support to nurses' hand hygiene performance? Using gamification and indoor location to improve hand hygiene awareness and reduce hospital infections. *BMC medical informatics and decision making*, 17(1), pp.15.

Miranda, P., Coelho, F.E.S., Tomé, A.R., Valente, M.A., Carvalho, A., Pires, C., Pires, H.O., Pires, V.C. e Ramalho, C., 2002. 20th century Portuguese climate and climate scenarios. Climate Change in Portugal. Scenarios, Impacts and Adaptation Measures – SIAM Project (Santos, F.D., Forbes, K., Moita. R., eds.). Lisbon: Gradiva Publishers, pp. 23-83.

Mokhnacheva, D., 2019. Conference on The Implications of Climate Change for Defence.

Morentz, J.W., 1994. Can We talk? Proceedings, Rockville, Maryland.

MSF, 2020. Médecins sans frontiers: Ebola. Disponível em http://www.msf-azg. be/fr/theme/ebola

Nature Foundation, 2018. Response Plan for the Effects of Climate Change on the Marine and Coastal Zones of St. Maarten.

OPAS, 2010. Sala de Situação em Saúde: compartilhando as experiências do Brasil. Organização Pan-Americana da Saúde, Brasília-DF.

Pestotnik, S.L., 2005. Expert clinical decision support systems to enhance antimicrobial stewardship programs: insights from the Society of Infectious Diseases Pharmacists. *Pharmacotherapy*, 25(8), pp. 1116-1125.

Plsek, P. e Wilson, T., 2001. Complexity, leadership, and management in healthcare organisations. *BMJ*, 323(7315), pp. 746-749.

Rawson, T.M., Moore, L.S.P., Hernandez, B., Charani, E., Castro-Sanchez, E., Herrero, P., Hayhoe, B., Hope, W., Georgiou, P., e Holmes, A.H., 2017. A systematic review of clinical decision support systems for antimicrobial management: are we failing to investigate these interventions appropriately? *Clin Microbiol Infect*, 23(8), pp. 524-532.

Ribeiro, A.F.S. e Pires, C.A.L., 2016. Seasonal drought predictability in Portugal using statistical–dynamical techniques. Physics and Chemistry of the Earth, Parts A/B/C, 94, pp.155-166.

Santos, F.D. e Miranda, P., 2006. Alterações climáticas em Portugal. Cenários, Impactos e Medidas de Adaptação-Projecto SIAM II.

Schoemaker, P.J.H., 1995. Scenario planning: a tool for strategic thinking. *Sloan Manag Review*, 36(2), pp. 25-40.

Schwartz, J., 2018. How can AI help to prepare for Floods in a Climate-Changed World? Scientific American.

Simões, A.S., Maia, M.R., Gregório, J., Couto, I., Asfeldt, A.M., Simonsen, G.S., Póvoa, P., Viveiros, M. e Lapão, L.V., 2018. Participatory implementation of an antibiotic stewardship programme supported by an innovative surveillance and clinical decision-support system. *Journal of Hospital Infection*, 100(3), pp.257-264.

Smith, D.C., 2005. Organizing for disaster preparedness. *Journal of Community Practice*, 13(4), pp.131-141.

Tainter, J.A., 2018. Introduction: prehistoric societies as evolving complex systems. In *Evolving complexity and environmental risk in the prehistoric Southwest*. CRC Press, pp. 1-24.

The Economist, 2014. Ebola and big data: Call for help. Mobile-phone records are an invaluable tool to combat. Ebola They should be made available to researchers. Canadian Engineer. Oct 25th 2014; 16:51.

The Lancet, 2014. (Editorial) The silver bullet of resilience. *The Lancet*, 384(9947), pp. 930.

United Nations, 2020. Estimates of the impact of COVID-19 on global poverty. WIDER Working Paper 2020/43, April. Helsinki: UNU-WIDER. Disponível em https://www.wider.unu.edu/sites/default/files/Publications/Working-paper/PDF/wp2020-43.pdf

Weik, K.E., 2010. *Making Sense of the Organization*. Blackwell Publishing.

Werbach, K. e Hunter, D., 2012. For the Win: How Game Thinking Can Revolutionize Your Business. Wharton Digital Press.

Whiting, K., 2020. Coronavirus isn't an outlier, it's part of our interconnected viral age. World Economic Forum, May.

World Health Organization (WHO), 2014. Interim Version 1.1. Ebola and Marburg virus disease epidemics: preparedness, alert, control, and evaluation. World Health Organization, June.

Permissão para Atacar: Como Melhorar a Cibersegurança de Portugal através de Um Programa de *Bug Bounty* Governamental

Rui Florêncio
Frequenta o Mestrado em Ciência Política e Relações Internacionais na Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa. Possui uma Pós-Graduação em Gestão de Informações e Segurança pela NOVA Information Management School, Universidade Nova de Lisboa, em parceria com o SIRP e o IDN.

Resumo

Nos últimos anos, o número de ciberataques tem vindo a aumentar. Tais ciberataques são frequentemente tornados possíveis pela existência de vulnerabilidades no software. O artigo identifica quais as melhores políticas para assegurar que as vulnerabilidades são detetadas, divulgadas aos fabricantes de software e corrigidas. Neste contexto,os programas de *bug bounty* aparentam estar a emergir como uma estratégia viável para a correção de vulnerabilidades. Estes programas permitem aproveitar as competências de um grande número de investigadores para testar a segurança de um sistema. A nível governamental, os Estados Unidos, Singapura e Suíça melhoraram significativamente a sua cibersegurança recorrendo a esta abordagem. Considerando o sucesso destes programas, o propósito do presente artigo é avaliar de que forma Portugal poderia beneficiar de um programa de *bug bounty* governamental.

Palavras-chave: Cibersegurança; Vulnerabilidades; Programas de *Bug Bounty*; Portugal.

Abstract
Permission to attack: How to improve Portugal's cybersecurity through a government Bug Bounty Program

In recent years, the number of cyber attacks has been increasing. Such cyber attacks are often made possible by the existence of vulnerabilities in software. The article identifies the best policies to ensure that vulnerabilities are detected, disclosed to software manufacturers, and corrected. In this context, bug bounty programs appear to be emerging as a viable strategy for correcting vulnerabilities. These programs draw on the skills of a large number of researchers to test the security of a system. At the governmental level, the United States, Singapore and Switzerland have significantly improved their cybersecurity using this approach. Considering the success of these programs, the purpose of this article is to assess how Portugal could benefit from a governmental bug bounty program.

Keywords: *Cybersecurity; Vulnerabilities; Bug Bounty Programs; Portugal.*

Artigo recebido: 28.07.2020
Aprovado: 05.08.2020
https://doi.org/10.47906/ND2020.156.03

Introdução

Nos últimos anos, o número de ciberataques, tanto no setor público como no privado, tem vindo a aumentar. Tais ciberataques são frequentemente tornados possíveis pela existência de vulnerabilidades no *software*. Falhas como esta são tão comuns que há quem diga que existem dois tipos de organizações: as que sabem que foram alvo de *hacking*, e as que ainda não o descobriram. Isto porque a existência de vulnerabilidades é inevitável. O *software* é complexo e os humanos são falíveis, pelo que as vulnerabilidades estão destinadas a ocorrer (Wilson, Schulman, Bankston & Herr, 2016, p. 4).

Desde há muito tempo, existe um mercado negro de vulnerabilidades de *software*. Durante um longo período, os hackers estavam satisfeitos ao trocar ou vender as vulnerabilidades entre si, sobretudo por prestígio. Os investigadores faziam normalmente uma divulgação "responsável" das vulnerabilidades, que consistia em contactar o fabricante e geralmente em receber reconhecimento pela sua descoberta quando a vulnerabilidade fosse anunciada e a respetiva correção disponibilizada. No entanto, nos últimos anos, o mercado de vulnerabilidades começou a migrar para o espaço comercial (Miller, 2007, p. 2). A informação sobre vulnerabilidades de *software* tornou-se uma *commodity*: indivíduos que anteriormente partilhavam esta informação de forma a construírem a sua reputação enquanto especialistas em cibersegurança vendem agora este conhecimento no mercado de vulnerabilidades para aumentar o seu rendimento (Kuehn, 2014, p. 64).

Face à concorrência dos compradores no mercado de vulnerabilidades, os fabricantes de *software* começaram a criar programas de atribuição de recompensas pela descoberta de vulnerabilidades, também conhecidos por programas de *bug bounty* (Wilson, Schulman, Bankston & Herr, 2016, p. 18). Subjacente à escolha de pagar por vulnerabilidades está o facto de as vulnerabilidades poderem ser descobertas por outros investigadores. Como uma vulnerabilidade é algo que está embutido num *software*, um investigador que descubra independentemente uma vulnerabilidade não tem nenhuma garantia de ser a única pessoa que sabe da sua existência. A cada dia que passa, existe uma maior probabilidade de outro investigador que procura vulnerabilidades no mesmo *software* encontrar essa vulnerabilidade (Herr, Schneier & Morris, 2017, p. 4). Por exemplo, a vulnerabilidade Heartbleed existia desde 2011 no OpenSSL e, em 2014, foi, na mesma altura, descoberta independentemente por investigadores da empresa Codenomicon e por um investigador da Google Security (Synopsys, 2017).

Recentemente, alguns governos criaram programas de *bug bounty*. Por exemplo, o governo norte-americano lançou programas de *bug bounty* que incidiram sobre os sistemas do Pentágono, do Exército, da Força Área, do Defense Travel System (DTS), do Corpo de Fuzileiros Navais e do Technology Transformation Services (TTS). O governo de Singapura lançou programas de *bug bounty* que incidiram so-

bre os seus sistemas. O governo suíço lançou um programa de *bug bounty* que incidiu sobre o sistema de voto eletrónico da Suíça.
Portugal poderia também beneficiar de um programa deste género. Mesmo que o governo de Portugal restrinja a participação nos seus programas de *bug bounty* a cidadãos nacionais, como os governos dos Estados Unidos e de Singapura fizeram inicialmente, existe em Portugal muito talento nesta área. Por exemplo, num *ranking* que posiciona 17.577 equipas de todo o mundo que participam em concursos de cibersegurança, a equipa STT, constituída por alunos do Instituto Superior Técnico, encontra-se em 41.º lugar. A equipa xSTF, constituída por alunos do Departamento de Ciência de Computadores da Faculdade de Ciências da Universidade do Porto, encontra-se em 166.º lugar. A equipa TeamRocketIST, também constituída por alunos do Instituto Superior Técnico, encontra-se em 170.º lugar (CTFTime, 2020). E, no European Cyber Security Challenge 2019, um evento anual que reúne jovens talentos de toda a Europa para uma competição de cibersegurança, a equipa portuguesa ficou no top 10 (Centro Nacional de Cibersegurança, 2019).
O propósito do presente artigo é avaliar de que forma é que Portugal poderia beneficiar de um programa de *bug bounty* que incidisse sobre os sistemas governamentais do país. A questão orientadora desta análise é: "De que forma é que Portugal poderia beneficiar de um programa de *bug bounty* governamental?". Para dar resposta a esta questão, ir-se-á: (1) abordar o conceito de vulnerabilidade e descrever os mercados em que estas são transacionadas; (2) abordar o conceito de política de divulgação responsável; (3) abordar o conceito de programa de *bug bounty*; (4) apresentar casos da utilização de programas de *bug bounty* por governos; (5) analisar os desafios legais representados pelos programas de *bug bounty*; e, com base nos supramencionados pontos, (6) avaliar de que forma Portugal poderia beneficiar de um programa de *bug bounty* governamental.

Vulnerabilidades

Vulnerabilidades são debilidades num *software* que permitem a um atacante comprometer a integridade, disponibilidade ou confidencialidade de um *software*, colocando os utilizadores e as redes em risco. Uma grande parte da cibersegurança pode ser reduzida a uma corrida constante entre desenvolvedores de *software* e especialistas em segurança a tentarem descobrir e corrigir vulnerabilidades, e os atacantes – criminosos, Estados, *hacktivistas* e outros – que tentam encontrar e tirar partido dessas vulnerabilidades (Wilson, Schulman, Bankston & Herr, 2016. p. 5).
Todo o *software* está suscetível a vulnerabilidades, e é pouco provável que algum dia as vulnerabilidades sejam completamente erradicadas. Mesmo que um sistema seja suficientemente seguro quando é lançado, não existe garantia de que irá

continuar assim para sempre. A sua utilização num novo contexto, interações com novos sistemas ou o desenvolvimento de novos métodos de ataque podem revelar vulnerabilidades anteriormente desconhecidas (ENISA, 2018, p. 9).

As vulnerabilidades podem ser introduzidas num *software* de diversas formas. A maior parte das vulnerabilidades resulta de erros honestos: são causadas por simples gralhas no código do *software*, interações imprevistas entre subcomponentes complexos de um sistema maior, ou por não proteger um programa de uma utilização indevida imprevista. Outras vulnerabilidades são introduzidas deliberadamente pelos desenvolvedores do *software* para que posteriormente possam tirar partido destas (Wilson, Schulman, Bankston & Herr, 2016, p. 5).

Numa rede interconectada, a existência de vulnerabilidades em *software* popular pode representar um risco considerável para os sistemas e para a sociedade, requerendo uma eficiente identificação e correção das vulnerabilidades. As vulnerabilidades que passam despercebidas durante um período prolongado ou que são divulgadas inapropriadamente podem exacerbar ainda mais estes riscos, o que demonstra a necessidade da existência de processos eficazes de divulgação de vulnerabilidades (ENISA, 2018, p. 9).

Quando um investigador descobre uma vulnerabilidade, tem três formas para a divulgar (ENISA, 2018, p. 12):

- Divulgação total: o investigador divulga publicamente toda a informação sobre a vulnerabilidade que identificou, sem coordenar com um coordenador[1] ou com o fabricante.
- Divulgação limitada: o investigador trabalha com um coordenador ou com o fabricante para minimizar o risco da vulnerabilidade que identificou. Após a correção ter sido desenvolvida, o coordenador ou o fabricante irão publicar informação sobre a vulnerabilidade juntamente com as medidas de remediação.
- Não-divulgação: o investigador pode optar por não divulgar a vulnerabilidade ao fabricante por diversas razões. Por exemplo, o investigador poderá optar por vender a vulnerabilidade no mercado negro, onde conseguirá obter um pagamento maior. Outra área emergente da não-divulgação está relacionada com iniciativas governamentais para analisar, avaliar e selecionar vulnerabilidades para serem mantidas em segredo para fins de segurança

1 Coordenadores são organizações de confiança que funcionam como intermediários entre os investigadores e os fabricantes para garantir que as vulnerabilidades descobertas são divulgadas e mitigadas de forma responsável. Os coordenadores incluem Equipas de Resposta a Incidentes de Segurança Informática (European Agency for Network and Information Security, 2018, p. 10), como, por exemplo, o US-Cert (Estados Unidos), o CERT-FR (França), o CERT-UK (Reino Unido), o CERT.EE (Estónia), o SingCERT (Singapura), o AusCERT (Austrália), o JPCERT (Japão), o DKCERT (Dinamarca), o CERT-Bund (Alemanha), o CERT.at (Áustria), o CERT.SE (Suécia), o CERT NZ (Nova Zelândia), o GovCERT.ch (Suíça), o NorCERT (Noruega), e o CERT.PT (Portugal).

nacional. Os governos poderão não divulgar informação sobre determinadas vulnerabilidades para que possam tirar partido das mesmas para a recolha de *intelligence* e para outras ciberoperações ofensivas.

A divulgação limitada ou a não-divulgação pode ocorrer através de mercados de vulnerabilidades. As vulnerabilidades não divulgadas são *commodities*, que são vendidas pelos seus produtores (os investigadores que as descobrem) a consumidores (fabricantes, governos ou atores maliciosos). Um mercado de vulnerabilidades pode ser não regulado ou regulado. Num mercado não regulado, existem poucas regras ou limitações e, tipicamente, as vendas são feitas pela oferta mais alta. Por outro lado, os mercados regulados têm geralmente regras e processos definidos, que têm que ser cumpridos pelos vendedores, e que podem restringir vendas a determinados grupos de clientes, como, por exemplo, governos (ENISA, 2018, pp. 13-14).
Os mercados regulados incluem (ENISA, 2018, p. 14):

- Mercados de divulgação coordenada: as vulnerabilidades são divulgadas publicamente através do fabricante ou de um coordenador (como um CERT). O investigador poderá ou não receber recompensas financeiras ou não-financeiras pela divulgação da vulnerabilidade.
- Mercados cativos: o investigador divulga a vulnerabilidade ao fabricante ou à organização em que/para quem trabalha e a vulnerabilidade não é divulgada publicamente. Inclui investigadores que trabalham dentro ou sob contrato para uma determinada organização, assim como investigadores que trabalham para agências governamentais em serviços de defesa ou de *intelligence*.
- Mercados de recompensas por vulnerabilidades: o investigador divulga a vulnerabilidade através do fabricante ou de um terceiro de confiança em troca de recompensas financeiras ou não-financeiras, através de um programa de *bug bounty*. Tipicamente, as recompensas dependem da gravidade da vulnerabilidade e das suas potenciais implicações de segurança. Os programas de *bug bounty* incluem programas específicos do fabricante – como os da Mozilla, da Google e da Facebook –, plataformas de *bug bounty* – como a BugCrowd, a HackerOne e a Intigriti – ou programas coordenados de recompensas por vulnerabilidades – como a Zero Day Initiative.

Relativamente aos mercados não regulados, estes incluem (ENISA, 2018, p. 14):

- Mercados parcialmente regulados: mediadores de vulnerabilidades servem de elo de ligação entre compradores e vendedores e, tipicamente, cobram uma comissão quando a venda é finalizada. Trata-se de organizações ou indivíduos que recebem informação sobre uma vulnerabilidade de um investigador e que encontram um comprador para essa vulnerabilidade. Os mediadores de vulnerabilidades podem ter certas regras de conduta ou limitações, mas, tipicamente, vendem as vulnerabilidades pela oferta mais alta.

Os mediadores tendem a focar-se em vulnerabilidades *zero-day* e na venda de vulnerabilidades a agências governamentais.

- Mercados negros de vulnerabilidades: mercados não regulados com determinadas características como compradores desconhecidos, não-exclusividade das vulnerabilidades no mercado – o vendedor poderá vender a mesma vulnerabilidade a outro consumidor –, dependência de ligações pessoais para negociar e ausência de garantias para manter a vulnerabilidade em segredo. As vendas podem ser feitas em diversos locais como salas de *chat*, mercados online ou na *dark web*.

O caminho que cada investigador irá seguir para divulgar uma vulnerabilidade irá depender do seu resultado desejado. Um investigador que é motivado pelo desejo de construir a sua reputação e contribuir para a segurança poderá optar pela divulgação total ou pela divulgação limitada. O investigador poderá até receber uma recompensa financeira, diretamente do fabricante ou indiretamente, através de um terceiro. No entanto, um investigador que procure principalmente uma compensação financeira poderá ter menos incentivos para divulgar a vulnerabilidade ao fabricante, quando a pode vender por um preço muito mais elevado no mercado aberto. Frequentemente, Estados e criminosos estão dispostos a pagar muito mais por vulnerabilidades do que o fabricante está disposto ou é capaz de pagar (Wilson, Schulman, Bankston & Herr, 2016, p. 11).

Políticas de Divulgação Responsável: Úteis, mas Insuficientes

O modelo primário que as organizações podem implementar para que investigadores divulguem vulnerabilidades descobertas nos seus sistemas é uma política de divulgação responsável, que consiste num canal dedicado e estruturado para a divulgação de vulnerabilidades (ENISA, 2018, p. 15). As políticas de divulgação responsável baseiam-se no princípio "se vir algo, diga algo", na medida em que, se um investigador descobrir uma vulnerabilidade num sistema de uma organização, é convidado a divulgá-la à organização, mas a organização não encoraja necessariamente a investigação, nem atribui necessariamente recompensas pelas vulnerabilidades divulgadas (HackerOne, 2017a). Como tal, as políticas de divulgação responsável têm como vantagem o facto de não implicarem custos (por cada vulnerabilidade descoberta) para a organização. Em contrapartida, as desvantagens são que: (1) os investigadores descobrem vulnerabilidades de forma passiva; e que, por essa razão, (2) o número de vulnerabilidades descobertas tenderá a ser inferior às vulnerabilidades que poderiam ser descobertas através de uma investigação mais ativa.

Essencialmente, uma política de divulgação responsável estabelece diretrizes claras para os investigadores divulgarem vulnerabilidades às organizações, enquanto per-

mite que as organizações efetuem a gestão das vulnerabilidades divulgadas de forma simples (Bugcrowd, s.d.a). Tal é importante porque, por vezes, os investigadores receiam poder vir a ser alvo de acusações legais por divulgarem vulnerabilidades. Noutras situações, os investigadores não conseguem entrar em contacto com as organizações e, mesmo quando conseguem, as vulnerabilidades divulgadas podem ser ignoradas, ou podem demorar demasiado tempo a serem corrigidas (Bugcrowd, s.d.b). Veja-se o caso de Miguel de Moura, que descobriu várias vulnerabilidades no Portal das Finanças, a mais grave das quais permitia a alteração da password de qualquer contribuinte conhecendo apenas o seu Número de Identificação Fiscal. Não havendo um canal próprio para divulgar vulnerabilidades à Autoridade Tributária, Moura começou por divulgar estas vulnerabilidades ligando múltiplas vezes para a linha de suporte do Portal das Finanças e, seguidamente, para a Comissão Nacional de Proteção de Dados (CNPD) em janeiro de 2018. Como não obteve uma resposta positiva, Moura apresentou queixa à CNPD em março e voltou a contactar a linha de suporte em abril. Em maio, Moura contactou novamente a linha de suporte, tendo finalmente conseguido falar com alguém em posição para resolver os problemas, após uma chamada de 36 minutos em que foi transferido sucessivamente entre múltiplos departamentos. Apenas em junho de 2018 as vulnerabilidades foram corrigidas (Matos, 2018).

A situação descrita acima poderia ter sido evitada caso a Autoridade Tributária tivesse implementado uma política de divulgação responsável. Não obstante, a Autoridade Tributária continua a não dispor de uma política de divulgação responsável. Este cenário é transversal a todo o setor público em Portugal (Centre for European Policy Studies, 2018, p. 18).

A Holanda é um dos únicos países que possui orientações oficiais para a divulgação responsável. Em 2013, o Centro Nacional de Cibersegurança holandês publicou um documento que estabelece diretrizes, tanto do ponto de vista dos investigadores como da organização, para a divulgação de vulnerabilidades (Kranenbarg, Holt & Ham, 2018, p.2). Seguindo estas diretrizes, o governo central da Holanda implementou a sua própria política de divulgação responsável, segundo a qual vulnerabilidades descobertas nos seus sistemas devem ser comunicadas ao Centro Nacional de Cibersegurança holandês, através de *e-mail*. No que concerne a vulnerabilidades descobertas em sistemas de entidades governamentais fora do governo central, estas deverão ser divulgadas à própria entidade[2]. Caso o investigador não receba uma resposta, deverá contactar o Centro Nacional de Cibersegurança holandês, que irá funcionar como intermediário entre o investigador e a entidade (Government of the Netherlands, s.d.).

Outro país cuja abordagem à divulgação responsável importa analisar é o Reino Unido, na medida em que está a desenvolver um projeto-piloto que visa identificar

2 Algumas entidades possuem as suas próprias políticas de divulgação responsável.

"a melhor forma para orientar uma organização ao longo do processo de implementação de um processo de divulgação de vulnerabilidades". Este projeto integra o Centro Nacional de Cibersegurança britânico, a HackerOne enquanto fornecedora da plataforma e a empresa NCC Group enquanto parceira para a avaliação das vulnerabilidades divulgadas. A empresa Luta Security, especializada nesta área, está também envolvida para garantir que estão a ser seguidas as melhores práticas da indústria. No âmbito deste projeto, foi implementada uma política de divulgação responsável que estabelece diretrizes para a divulgação de vulnerabilidades nos serviços online do governo britânico (National Cyber Security Centre, 2018a). Segundo a referida política, os investigadores deverão primeiramente tentar contactar a entidade responsável pelos sistemas. Caso não consigam encontrar um ponto de contacto, ou se não obtiverem resposta, poderão comunicar as vulnerabilidades descobertas ao Centro Nacional de Cibersegurança britânico, através de um formulário disponível na plataforma HackerOne (National Cyber Security Centre, 2018b).
Em suma, as políticas de divulgação responsável são um modelo útil para identificar vulnerabilidades em sistemas governamentais. Semelhantemente à Holanda e ao Reino Unido, Portugal poderia beneficiar de uma política de divulgação responsável. No entanto, estas políticas pecam por o seu sucesso depender de investigadores descobrirem vulnerabilidades de forma passiva. Considerando a importância da cibersegurança para a segurança nacional, seria, portanto, preferível a implementação de um modelo que encorajasse a procura de vulnerabilidades de forma ativa.

Programas de *Bug Bounty*

Através de um programa de *bug bounty*, as organizações podem definir um programa em que investigadores são autorizados a tentar identificar vulnerabilidades nos seus sistemas, em troca de recompensas financeiras ou não-financeiras por cada vulnerabilidade considerada válida (ENISA, 2018, p. 15). Assim, comparativamente às políticas de divulgação responsável, os programas de *bug bounty* têm como desvantagem o facto de implicarem custos (por cada vulnerabilidade descoberta) para a organização. Note-se, no entanto, que o custo de cada vulnerabilidade divulgada depende da sua gravidade: quanto mais grave for, maior será a recompensa a atribuir ao investigador. Mas, por outro lado, as vantagens são que: (1) os investigadores procuram vulnerabilidades de forma ativa; e que, por esse motivo, (2) o número de vulnerabilidades descobertas tenderá a ser superior às vulnerabilidades que poderiam ser descobertas através de uma política de divulgação responsável.
A lógica dos programas de *bug bounty* baseia-se num conceito que surgiu com a cultura do *software* aberto, segundo o qual "havendo olhos suficientes, todos os *bugs*

são triviais". Isto significa que, se todos os investigadores do mundo se tornassem co-desenvolvedores de um determinado *software*, os *bugs* existentes no mesmo seriam descobertos e corrigidos mais rapidamente. Os programas de *bug bounty* tiram partido desta lógica, que se revelou especialmente eficaz no contexto da cibersegurança, ao expandir o conjunto de investigadores envolvidos na procura de *bugs* de segurança (On, 2019, pp. 231-232).

Os programas de *bug bounty* têm diversos benefícios para os fabricantes de *software*. A atribuição de recompensas incentiva os investigadores a procurarem vulnerabilidades, e esta atenção acrescida aumenta a probabilidade de serem descobertas vulnerabilidades latentes. Em segundo lugar, a coordenação com os investigadores permite aos fabricantes gerir mais eficazmente a divulgação de vulnerabilidades, reduzindo a probabilidade da divulgação de vulnerabilidades *zero-day*. As recompensas monetárias constituem um incentivo para os investigadores não venderem as vulnerabilidades que descobrirem a atores maliciosos no mercado cinzento e no mercado negro. Em terceiro lugar, os programas de *bug bounty* podem tornar mais difícil que atores maliciosos descubram vulnerabilidades para tirarem partido das mesmas. A correção de vulnerabilidades descobertas através de um programa de *bug bounty* aumenta a dificuldade e, consequentemente, o custo de atores maliciosos descobrirem vulnerabilidades *zero-day*, dado que o total de vulnerabilidades latentes foi diminuído. Para além disso, a experiência adquirida através de programas de *bug bounty* pode contribuir para a melhoria das técnicas de mitigação e ajudar a identificar outras vulnerabilidades relacionadas e fontes de *bugs*. Por último, os programas de *bug bounty* geram frequentemente boa vontade entre a comunidade de investigadores. No seu conjunto, estas vantagens fazem dos programas de *bug bounty* uma ferramenta interessante para melhorar a segurança dos produtos e proteger os consumidores (Finifter, Akhawe & Wagner, 2013, p. 273). Para além disso, os programas de *bug bounty* podem ser utilizados para identificar potenciais contratações para os departamentos de cibersegurança das organizações. Por exemplo, a Facebook contratou pelo menos dois investigadores que participaram no seu programa de *bug bounty* para trabalharem a tempo inteiro na equipa de segurança da rede social (Facebook, 2013). Também a Google e a Mozilla contrataram investigadores que participaram nos seus respetivos programas de *bug bounty*, tendo cada uma destas organizações contratado pelo menos três investigadores (Finifter, Akhawe & Wagner, 2013, p. 282). O investigador que descobriu mais vulnerabilidades no programa de *bug bounty* "Hack the Air Force" foi contratado pelo Defense Digital Service (DDS), a agência do Departamento de Defesa dos Estados Unidos que conduz o programa "Hack the Pentagon" (HackerOne, 2018a).

Para alojarem os seus programas de *bug bounty*, as organizações podem recorrer a plataformas externas, como a HackerOne, a Bugcrowd ou a Intigriti, ou fazê-lo de forma independente.

Utilização de Programas de *Bug Bounty* por Governos

No presente capítulo, ir-se-ão apresentar casos de governos que utilizam programas de *bug bounty* para melhorar a sua cibersegurança.

Estados Unidos

O governo dos Estados Unidos já lançou vários programas de *bug bounty*, tendo recorrido à plataforma HackerOne para os alojar.

Pentágono

O programa "Hack the Pentagon" foi o primeiro programa de *bug bounty* do governo dos Estados Unidos. Este programa foi lançado no dia 18 de abril de 2016, estando apenas aberto para cidadãos norte-americanos. Durante 24 dias, mais de 1400 investigadores testaram a segurança dos sistemas do Pentágono, tendo sido descobertas 138 vulnerabilidades. Foram atribuídas recompensas a 58 dos investigadores participantes, sendo que a recompensa mais elevada foi de 3500 dólares. A recompensa média foi de 588 dólares, e o investigador que recebeu mais recompensas arrecadou 15 mil dólares. O investigador mais novo que recebeu uma recompensa tinha 14 anos e o mais velho tinha 54 anos (HackerOne, 2016).

Exército

O programa "Hack the Army" decorreu entre 30 de novembro e 21 de dezembro de 2016, estando também apenas aberto para cidadãos norte-americanos. Neste período, 371 investigadores, 25 dos quais eram funcionários públicos, incluindo 17 militares, testaram a segurança dos sistemas do Exército. Foram descobertas 118 vulnerabilidades e atribuídos 100 mil dólares em recompensas (HackerOne, 2017b).

Força Aérea

O programa "Hack the Air Force" já teve três edições. A primeira edição deste programa foi, à data, o maior programa de *bug bounty* do governo dos Estados Unidos, estando aberto não só para cidadãos norte-americanos, mas para cidadãos da Austrália, Canadá, Nova Zelândia e Reino Unido. Este programa decorreu entre 30 de maio e 23 de junho de 2017. Neste período, 272 investigadores, 33 dos quais eram estrangeiros, testaram a segurança dos sistemas da Força Aérea. Foram descobertas 207 vulnerabilidades e atribuídos 130 mil dólares em recompensas. Alguns dos participantes que mais vulnerabilidades descobriram tinham idade inferior a 20 anos, incluindo um jovem de 17 anos que recebeu a maior recompensa total por ter descoberto 30 vulnerabilidades, o que foi também a maior recompensa atribuída a um indivíduo nos programas de *bug bounty* até à data (HackerOne, 2017c). Foi este

investigador que acabou por ser contratado pelo Defense Digital Service (DDS), a agência do Departamento de Defesa dos Estados Unidos que conduz o programa "Hack the Pentagon". A segunda edição deste programa foi ainda mais inclusiva pois, para além de estar aberta para cidadãos norte-americanos, da Austrália, do Canadá, da Nova Zelândia e do Reino Unido, puderam participar cidadãos ou residentes permanentes legais da Albânia, Bélgica, Bulgária, Canadá, Croácia, Dinamarca, Estónia, França, Alemanha, Islândia, Itália, Letónia, Lituânia, Holanda, Noruega, Polónia, Portugal, Eslovénia, Espanha, Suécia e Turquia, tornando-se, à data, o maior programa de *bug bounty* do governo dos Estados Unidos (Hacker One, 2018b). Este programa de *bug bounty* decorreu entre 9 de dezembro de 2017 e 1 de janeiro de 2018. Durante 20 dias, 27 investigadores descobriram 106 vulnerabilidades, tendo sido atribuídos 103.883 dólares em recompensas. A recompensa individual mais elevada foi de 12.500 dólares, constituindo a maior recompensa individual atribuída em todos os programas de *bug bounty* do governo dos Estados Unidos até à data. Investigadores dos Estados Unidos, Canadá, Reino Unido, Suécia, Holanda, Bélgica e Letónia participaram nesta segunda edição do "Hack the Air Force" (HackerOne, 2018c). A terceira edição foi ainda mais inclusiva, estando a participação aberta a 191 países, tornando-se no maior programa de *bug bounty* do governo dos Estados Unidos até à data. Este programa de *bug bounty* decorreu entre 19 de outubro e 22 de novembro de 2018. Durante um mês, 30 investigadores descobriram mais de 120 vulnerabilidades, tendo sido atribuídos 130.000 dólares em recompensas (HackerOne, 2018d).

Defense Travel System (DTS)

O programa "Hack the DTS" decorreu entre 1 e 29 de abril de 2018, estando aberto para cidadãos norte-americanos e cidadãos e residentes legais da Austrália, Canadá, Nova Zelândia e Reino Unido (HackerOne, 2018e). Durante 29 dias, 19 investigadores testaram a segurança do DTS, tendo sido descobertas 65 vulnerabilidades, 28 das quais foram consideradas de gravidade alta ou crítica. Foram atribuídos 78.650 dólares em recompensas, sendo que os investigadores que foram recompensados eram principalmente dos Estados Unidos e do Reino Unido. A recompensa mais elevada foi de 5.000 dólares, e foi paga 8 vezes a investigadores individuais (HackerOne, 2018f).

Corpo de Fuzileiros Navais

O programa "Hack the Marine Corps" decorreu entre 12 e 26 de agosto de 2018. Durante 20 dias, mais de 100 investigadores foram convidados a testar a segurança dos sistemas do Corpo de Fuzileiros Navais dos Estados Unidos. Foram descobertas 150 vulnerabilidades e atribuídos mais de 150 mil dólares em recompensas (HackerOne, 2018g).

Technology Transformation Services (TTS)

A Administração de Serviços Gerais dos Estados Unidos lançou um programa de *bug bounty* que incide sobre os sistemas da TTS, tornando-se na primeira agência civil do governo dos Estados Unidos a lançar um programa deste género (HackerOne, 2018h).

Singapura

Tal como o governo dos Estados Unidos, o governo de Singapura já lançou diversos programas de *bug bounty*, tendo também recorrido à plataforma HackerOne para os alojar.

Ministério da Defesa de Singapura

O primeiro programa de *bug bounty* do governo de Singapura foi lançado pelo Ministério da Defesa. Entre 15 de janeiro e 4 de fevereiro de 2018, 300 investigadores foram convidados a testar a segurança dos sistemas do Ministério da Defesa. Durante três semanas, foram descobertas 35 vulnerabilidades, 23 das quais foram consideradas de baixa gravidade, 10 de média gravidade, 2 de alta gravidade e nenhuma de gravidade crítica. Foram atribuídos 14.750 dólares em recompensas a 17 dos investigadores participantes, sendo que a recompensa mais elevada foi de 2.000 dólares. Participaram nesta iniciativa investigadores de todo o mundo, incluindo dos Estados Unidos, Singapura, Índia, Roménia, Canadá, Rússia, Suécia, Irlanda, Egipto e Paquistão (HackerOne, 2018i).

O segundo programa de *bug bounty* lançado pelo Ministério da Defesa de Singapura decorreu entre 30 de setembro e 21 de outubro de 2019, envolvendo mais de 300 investigadores convidados – 134 dos quais eram de Singapura. Durante três semanas, foram descobertas 20 vulnerabilidades, tendo sido atribuídos 16 mil dólares em recompensas (HackerOne, 2019a).

Government Technology Agency e Cyber Security Agency de Singapura

O segundo programa de *bug bounty* do governo de Singapura foi lançado pela Government Technology Agency e pela Cyber Security Agency de Singapura. Entre 27 de dezembro de 2018 e 16 de janeiro de 2019, mais de 400 investigadores de todo o mundo foram convidados a testar a segurança dos sistemas do governo. Durante três semanas, foram descobertas 26 vulnerabilidades, 7 das quais foram consideradas de baixa gravidade, 18 de média gravidade e 1 de alta gravidade. Foram atribuídos 11.750 dólares em recompensas. Um quarto de todos os investigadores participantes e 7 dos investigadores no top 10 dos investigadores que receberam mais recompensas eram de Singapura (HackerOne, 2019b).

O segundo programa de *bug bounty* lançado por estas agências decorreu entre 8 e 28 de julho de 2019, envolvendo cerca de 300 investigadores de todo o mundo.

Neste programa de *bug bounty*, foram descobertas 31 vulnerabilidades, 4 das quais foram consideradas de alta gravidade e as restantes 27 de baixa ou média gravidade, tendo sido atribuídos 25.950 dólares em recompensas. Cerca de um quarto dos investigadores eram de Singapura, 30 dos quais tinham participado no primeiro programa de *bug bounty*, e 7 dos investigadores no top 10 dos investigadores que receberam mais recompensas eram de Singapura (HackerOne, 2019c).
O terceiro programa de *bug bounty* destas agências decorreu entre 18 de novembro e 8 de dezembro de 2019, e contou com a participação de cerca de 300 investigadores – 72 dos quais eram de Singapura. Foram descobertas 33 vulnerabilidades e atribuídos 30.800 dólares em recompensas (HackerOne, 2020).

Suíça

Desde 2004, a Suíça tem realizado experiências com o voto eletrónico. A Swiss Post acredita que conseguiu agora desenvolver um sistema de voto eletrónico que é totalmente verificável, o que significa que o voto eletrónico pode vir a ser disponibilizado a todos os eleitores no futuro. No entanto, para tal, a lei federal requer que o sistema de voto eletrónico seja certificado antes de ser utilizado pela primeira vez e que o seu código fonte seja divulgado. Para além disso, a Confederação Suíça e os cantões determinaram que os sistemas de voto eletrónico totalmente verificáveis têm de ser sujeitos a um teste de intrusão antes de serem utilizados pela primeira vez. Como tal, a Suíça, para além de sujeitar o seu sistema de voto eletrónico a um teste de intrusão por parte de um organismo acreditado, lançou um teste de intrusão público através de um programa de *bug bounty* (Swiss Federal Council, 2019a). Este programa de *bug bounty* decorreu entre 25 de fevereiro e 24 de março de 2019, estipulando recompensas entre 30.000 e 50.000 francos suíços por vulnerabilidades que permitissem a manipulação de votos não detetada pelo sistema; 20.000 francos suíços por vulnerabilidades que permitissem a manipulação de votos detetada pelo sistema; 10.000 francos suíços por vulnerabilidades que permitissem o comprometimento do segredo de voto nos servidores; 5.000 francos suíços por vulnerabilidades que permitissem o corrompimento de votos; 1.000 francos suíços por vulnerabilidades que permitissem a intrusão no sistema de voto eletrónico; e 100 francos suíços por possibilidades de otimização não críticas (Swiss Post, 2019a). Durante 4 semanas, cerca de 3.200 investigadores de 137 países testaram a segurança do sistema de voto eletrónico da Suíça, tendo sido descobertas 16 vulnerabilidades, nenhuma das quais foi considerada crítica. A maior parte dos participantes eram suíços (27%), 13% eram franceses, 7% eram americanos, 5% eram alemães, 4% eram indianos, 3% eram polacos, 3% eram canadianos, 3% eram britânicos e 35% eram de outras nacionalidades (SwissPost, 2019b).
No entanto, as vulnerabilidades mais críticas foram descobertas fora do âmbito deste programa de *bug bounty*. Isto porque, no âmbito do programa de *bug bounty*, a

Swiss Post disponibilizou o código fonte do sistema de voto eletrónico aos participantes. Para obterem acesso ao código fonte, os participantes tinham que aceitar as condições de utilização, que estipulavam que apenas poderiam publicar informações sobre as vulnerabilidades descobertas após um período de 45 dias (Swiss Post, 2019c). Contudo, alguém publicou livremente o código fonte do sistema de voto eletrónico e, a partir desse momento, qualquer pessoa passou a poder analisar o código fonte para descobrir vulnerabilidades sem ter que aceitar as condições de utilização. Foi o que fizeram os investigadores Lewis, Pereira & Teague, tendo descoberto duas vulnerabilidades, que divulgaram publicamente antes do período de 45 dias imposto pela Swiss Post aos participantes no programa de *bug bounty*. A primeira vulnerabilidade permite que alguém que tenha implementado, administre ou obtenha o controlo do sistema manipule votos sem ser detetado (2019a). A segunda vulnerabilidade permite nulificar votos válidos (2019b).

Segundo a Swiss Post, anteriormente à realização deste programa de *bug bounty*, o código-fonte do sistema de voto eletrónico tinha sido auditado pela KPMG, mas os resultados da auditoria não foram tornados públicos devido a disposições contratuais. Por sua vez, os protocolos criptográficos utilizados pelo sistema foram auditados pelo Instituto Federal de Tecnologia de Zurique (Gamma, 2019). Por seu lado, a Scytl (2019), líder mundial em serviços de voto eletrónico, que é o parceiro tecnológico da Swiss Post no desenvolvimento do seu sistema de voto eletrónico, afirmou que estes protocolos "são o resultado da investigação realizada desde a fundação da Scytl em 2001, que foi disponibilizada ao público através de contínuas publicações académicas", tendo "passado com êxito o escrutínio de especialistas criptográficos externos", o que permitiu alcançar a verificabilidade total "com a confiança de que nenhum ataque pode comprometer o sigilo da urna e a integridade dos resultados da eleição". No entanto, as supramencionadas vulnerabilidades provam o contrário. Lewis levantou, por isso, as seguintes questões: "Porque é que várias auditorias anteriores foram incapazes de descobrir [o que nós descobrimos]? Porque é que alguém acreditou que este sistema era suficiente para proteger eleições nacionais? E o que iria acontecer se nós não tivéssemos descoberto?" (Zetter, 2019).

Após a descoberta destas vulnerabilidades, a Swiss Post (2019b) suspendeu temporariamente o sistema de voto eletrónico, que iria ser utilizado no dia 19 de maio de 2019. Posteriormente, a Suíça adiou provisoriamente a introdução do voto eletrónico como canal de voto oficial (Swiss Federal Council, 2019b). Pouco tempo depois, a Swiss Post (2019d) anunciou que iria continuar a trabalhar no seu sistema, e que planeava disponibilizá-lo aos cantões para ensaios a partir de 2020. No entanto, em dezembro de 2019, 100 deputados da Câmara dos Deputados da Suíça votaram a favor de uma proposta para suspender completamente os ensaios do sistema de voto eletrónico até o governo elaborar um relatório que prove que as questões de segurança foram resolvidas e que o *software* responde a necessidades reais. Apenas

75 deputados votaram contra esta proposta, sendo que 7 deputados se abstiveram. Note-se, no entanto, que este resultado não é definitivo e que não se trata de um ato legislativo vinculativo (Swissinfo, 2019). Não obstante, a Swiss Post continua a desenvolver o sistema de voto eletrónico, tendo, no entanto, adiado para 2021 a data em que planeia disponibilizá-lo aos cantões para ensaios (Swissinfo, 2020).

Em suma, os programas de *bug bounty* lançados pelos governos dos Estados Unidos, de Singapura e da Suíça permitiram identificar e corrigir diversas vulnerabilidades que poderiam ter sido utilizadas para realizar um ciberataque contra os sistemas governamentais dos respetivos países, melhorando significativamente a sua cibersegurança. Tendo em conta o sucesso destes programas, o autor do presente artigo considera que Portugal deveria também criar um programa de *bug bounty* para melhorar a sua cibersegurança.

Desafios Legais dos Programas de *Bug Bounty*

Os programas de *bug bounty* são frequentemente percecionados como uma abordagem arriscada para melhorar a segurança, na medida em que envolvem pedir a investigadores em grande parte anónimos e independentes de todo o mundo para escrutinarem os sistemas de uma organização remotamente. As organizações receiam que um investigador danifique os seus sistemas ou que roube os seus dados quando está à procura de vulnerabilidades, ou que divulgue as vulnerabilidades descobertas a terceiros ou até mesmo ao público. Por outro lado, os investigadores receiam poder vir a ser alvo de acusações legais por procurarem e divulgarem vulnerabilidades (Zhao, Laszka & Grossklags, 2017, p. 375).
Para reduzir os riscos, os programas de *bug bounty* possuem regras, que especificam que partes dos sistemas podem ser acedidas e que tipo de ações são permitidas. Para além disso, as regras estipulam que, se os investigadores cumprirem as diretrizes do programa durante a procura de vulnerabilidades, a organização não irá agir judicialmente contra os mesmos (Zhao, Laszka & Grossklags, 2017, p. 376). As regras funcionam como um contrato entre o investigador e a organização, e são o ponto central para determinar a responsabilidade legal e os riscos dos investigadores que participam no programa de *bug bounty* (On, 2019, p. 232). No entanto, por vezes, as organizações e os investigadores discordam relativamente à interpretação dessas regras (Zhao, Laszka & Grossklags, 2017, p. 404). Veja-se o caso do investigador Kevin Finisterre, nos Estados Unidos. Em agosto de 2017, a fabricante de drones DJI lançou o seu programa de *bug bounty*. No âmbito desse programa, Finisterre descobriu uma vulnerabilidade relacionada com os servidores da DJI, que permitia aceder a informação sensível dos clientes da empresa. Como a DJI não especificou as regras

do programa, Finisterre contactou a empresa para confirmar se os seus servidores estavam incluídos no âmbito do programa, tendo a empresa respondido afirmativamente. Em seguida, Finisterre escreveu um relatório detalhado sobre a vulnerabilidade e enviou-o para a DJI, tendo a empresa validado a mesma, o que iria valer ao investigador 30 mil dólares, a recompensa mais elevada do programa. No entanto, para receber a recompensa, Finisterre teria que assinar um contrato que, basicamente, não lhe permitiria falar publicamente sobre o trabalho que fez, nem sequer dizer que tinha feito qualquer trabalho de segurança para a DJI. Finisterre não concordou com estes termos e tentou negociar. No decorrer das negociações, Finisterre recebeu uma carta que mencionava a *Computer Fraud and Abuse Act* (CFAA). O investigador interpretou esta carta como uma ameaça, tendo, por isso, decidido abdicar da recompensa e tornar a sua experiência pública (Popper, 2017). Apesar de a DJI ter a sua própria versão da história, este mal-entendido poderia ter sido evitado se a empresa tivesse lançado o seu programa de *bug bounty* com regras claras. Mais importante ainda, se as regras incluíssem autorização clara para aceder ao sistema e o compromisso em não agir judicialmente – ao invés do que aparenta ser um consentimento implícito do anúncio do lançamento do programa de *bug bounty*, e da confirmação dada a Finisterre por *e-mail* –, seria mais difícil para a DJI utilizar uma carta legal como técnica de negociação. Este caso ilustra a posição potencialmente perigosa em que os investigadores poderão vir a encontrar-se caso as regras de um determinado programa de *bug bounty* não sejam claras, e a disparidade de poder negocial entre as partes. Para além disso, este caso demonstra a magnitude dos riscos legais que são transferidos para os investigadores caso não seja adotada uma linguagem clara *ex ante*. A não-utilização de uma linguagem clara deixa os investigadores expostos a ameaças legais *ex post*, na medida em que gera ambiguidade relativamente aos seus limites de atuação, tanto a nível técnico como legal (On, 2019, p. 241).

De forma geral, os programas de *bug bounty* incluem uma linguagem que não se coaduna com a prática de investigação de segurança, que não concede explicitamente uma autorização contratual que minimize o risco do investigador, e que compromete o propósito do programa. Isto porque a linguagem legal requer que os investigadores cumpram "todas as leis aplicáveis" ou proíbe testes que "infrinjam qualquer lei" ao invés de conceder aos investigadores uma autorização clara para investigar sob as leis *anti-hacking*. De modo semelhante, as plataformas de *bug bounty* requerem que os investigadores garantam que as suas ações não infringem direitos de propriedade intelectual de terceiros, e que a sua conduta cumpre todas as leis aplicáveis, tanto a nível nacional como internacional. Esta prática transfere o risco legal para o investigador. Outros programas de *bug bounty* não incluem qualquer referência à conformidade com a lei, gerando incerteza (On, 2019, p. 238). Sob as regras de alguns programas, os investigadores poderão ser forçados a uma situação de incumprimento contratual e responsabilidade civil e penal. Nas suas regras,

estes programas referem-se a Acordos de Licença do Utilizador Final, que, por sua vez, proíbem a engenharia reversa e outras ferramentas de investigação fundamentais para a investigação de segurança, e por vezes até proíbem a mera tentativa de obter acesso não autorizado. Ao invés de concederem aos investigadores permissão para realizar essas ações, as regras proíbem-nos de o fazer sob contrato. As regras do programa de *bug bounty* da empresa de antivírus AVG são um exemplo flagrante desta prática, na medida em que declaram que a submissão de uma vulnerabilidade "constitui a aceitação do Acordo de Licença do Utilizador Final da AVG". Por sua vez, o Acordo de Licença do Utilizador Final da AVG estipula que os utilizadores "não podem (…) (iii) exceto se expressamente autorizados por lei, (A) fazer engenharia reversa, desmontar, descompilar, traduzir, reconstruir, transformar ou extrair qualquer [*software*] ou qualquer parte do [*software*] (…), ou (B) alterar, modificar ou mudar de outra forma qualquer [*software*]". Um outro exemplo são as regras do programa de *bug bounty* da Facebook, que incluem um compromisso em não processar os investigadores que sigam as regras, mas estipulam também que "[a] utilização dos serviços da Facebook (…), incluindo para efeitos deste programa [de *bug bounty*], está sujeito aos Termos e Políticas da Facebook e aos termos e políticas de qualquer membro da família de empresas da Facebook cujos serviços você utiliza". Por sua vez, os termos de serviço do WhatsApp declaram que os utilizadores: "não podem (ou auxiliar outros a) aceder, utilizar, copiar, adaptar, modificar, preparar (…) ou explorar de outra forma os nossos Serviços (…) diretamente ou através de meios automatizados: (a) fazer engenharia reversa, alterar, modificar, criar obras derivadas, descompilar, ou extrair código a partir dos nossos Serviços; (b) enviar, armazenar, ou transmitir vírus ou outro código de computador prejudicial através ou para [os seus] Serviços; (c) obter ou tentar obter acesso não autorizado aos [seus] Serviços ou sistemas (…)". Ainda mais problemáticos são os programas de *bug bounty* cujas regras negam explicitamente a autorização para aceder. Por exemplo, nas regras do programa de *bug bounty* da Alibaba, pode ler-se: "Nenhuma licença ou permissão é dada para qualquer penetração ou ataque contra qualquer sistema da Alibaba" (On, 2019, pp. 239-240).

Considerando a supramencionada realidade, não é surpreendente que as preocupações legais sejam uma das principais barreiras à participação de investigadores em programas de *bug bounty* (National Telecommunications and Information Administration, 2016, p. 6; ENISA, 2018, p. 30; Centre for European Policy Studies, 2018, p. 81). Isto porque a eficácia de um programa de *bug bounty* depende fortemente da forma como as suas regras legais foram redigidas, e do conjunto de incentivos e garantias legais dadas aos investigadores. Tais garantias incluem a comunicação com clareza do âmbito do programa e do tipo de recompensa a atribuir por cada vulnerabilidade, assim como o tipo de risco legal assumido pelo investigador e o âmbito da autorização dada ao mesmo para agir nos termos da lei. De forma a

garantir que os programas de *bug bounty* continuam a funcionar como um mercado legal de vulnerabilidades é, portanto, fundamental que as suas regras sejam claras. Se as regras forem mal redigidas, os investigadores poderão estar a infringir a lei meramente por participarem no programa (On, 2019, p. 232).
Em Portugal, a Lei n.º 109/2009 de 15 de setembro, também conhecida como *Lei do Cibercrime*, tipificou o crime de acesso ilegítimo no seu Artigo 6.º:

- "Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias" (n.º 1).
- "Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior" (n.º 2).

Atente-se que o acesso a um sistema sem permissão legal ou sem autorização do proprietário desse sistema constitui um crime de acesso ilegítimo. O proprietário do sistema poderia, portanto, autorizar o acesso a investigadores no âmbito de um programa de *bug bounty*, ultrapassando a criminalização pelo acesso ilegítimo da Lei do Cibercrime. No entanto, o crime de acesso ilegítimo é o crime básico que poderia ser invocado no âmbito da participação de um investigador num programa de *bug bounty*. A *Lei do Cibercrime* tipifica outros crimes que poderiam também ser invocados, como os crimes de falsidade informática (Artigo 3.º), dano relativo a programas ou outros dados informáticos (Artigo 4.º), sabotagem informática (Artigo 5.º) e interceção ilegítima (Artigo 7.º). Para a criação de um programa de *bug bounty* governamental em Portugal, recomenda-se, por isso, que o acordo, entre o governo e os investigadores, que será a base de tal programa inclua autorização específica, com um âmbito claramente definido, para efeitos da *Lei do Cibercrime*. Segundo Rogério Bravo, Inspetor-Chefe da Polícia Judiciária na Secção Central de Investigação Digital, "a lei reconhece a autorização; o que não pode acontecer é a investigação ir além do acordo, porque se isso acontece, depreende-se que se tratam de atos não autorizados. Desta forma preenchidos os quesitos do princípio da tipicidade e da legalidade, uma vez que numa interpretação a *contrario sensu*, o que não for proibido, é permitido". Bravo considera, portanto, que o acordo terá que "ser estudado para evitar normas abertas e imprecisas relativamente à possibilidade de atuação e às cláusulas penais, contendo referências mais específicas"[3]. A linguagem do acordo estará assim em conformidade com as melhores práticas para a realização de programas de *bug bounty*, contrariando uma tendência geral de regras com uma linguagem paradoxal, que co-

3 Entrevista realizada por email em 12 de agosto de 2020.

locam em risco os investigadores que seguem as regras. Já na perspetiva do governo, a clareza do acordo irá estabelecer uma base legal concreta para acusações caso um investigador infrinja intencionalmente as regras do programa (On, 2019, p. 241).

Considerações Finais

A existência de vulnerabilidades é inevitável. Coloca-se então a seguinte questão: quais são as melhores políticas para assegurar que as vulnerabilidades são descobertas, divulgadas ao fabricante do *software*, e corrigidas o mais rápido possível? (Wilson, Schulman, Bankston & Herr, 2016, p. 4).

Os programas de *bug bounty* aparentam estar a emergir como uma estratégia viável para a correção de vulnerabilidades (Finifter, Akhawe & Wagner, 2013, p. 274). Estes programas permitem aproveitar as competências de um grande número de investigadores para testar a segurança de um sistema, e recompensá-los pelas vulnerabilidades que descobrirem. Simultaneamente, os programas de *bug bounty* podem ser utilizados para identificar potenciais contratações para os departamentos de cibersegurança das organizações.

Países como os Estados Unidos, Singapura e a Suíça melhoraram significativamente a sua cibersegurança através de programas de *bug bounty*. Tendo em conta o sucesso destes programas, o autor do presente artigo considera que Portugal deveria também criar um programa de *bug bounty* para melhorar a sua cibersegurança.

Para além dos benefícios em termos de cibersegurança, a criação de um programa de *bug bounty* governamental em Portugal iria contribuir para o ciberpoder do país, na medida em que esta iniciativa iria sinalizar perante a comunidade internacional que Portugal está realmente empenhado na melhoria da sua cibersegurança, de tal forma que está disposto a convidar investigadores de todo o mundo (ou, pelo menos, de países aliados ou até mesmo apenas de Portugal) a escrutinarem a segurança dos seus sistemas.

Para que esta iniciativa seja bem-sucedida, recomenda-se que Portugal siga as medidas que foram propostas no presente artigo. Isto porque, apesar de, geralmente, os programas de *bug bounty* definirem claramente o âmbito técnico da autorização concedida ao investigador, o âmbito legal da autorização e do acesso é frequentemente ignorado, inexistente ou insuficiente. Em alguns casos, as regras legais entram diretamente em tensão com o propósito do programa, colocando investigadores que utilizam técnicas de investigação básicas em violação direta das regras, e expondo-os a responsabilidade legal. Em outros casos, as regras criam uma realidade em que os investigadores infringem as regras quase que por defeito, ao fazerem o que o programa lhes pede para fazer: descobrir vulnerabilidades (On, 2019, p. 233). Ao seguir as medidas propostas para contrariar essa tendência geral, Portugal irá seguir as melhores práticas para a realização de programas de *bug bounty*.

Referências Bibliográficas

Bugcrowd, s.d.a. *Vulnerability Disclosure Program (VDP)*. Disponível em: https://www.bugcrowd.com/resources/glossary/vulnerability-disclosure-program-vdp/ [acedido em 9 de agosto de 2020].

Bugcrowd, s.d.b. *What is Responsible Disclosure?* Disponível em: https://www.bugcrowd.com/resource/what-is-responsible-disclosure/ [acedido em 9 de agosto de 2020].

Centre for European Policy Studies, 2018. *Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges*. Disponível em: https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf [acedido em 15 de janeiro de 2020].

Centro Nacional de Cibersegurança, 2019. *Equipa portuguesa conquista 10.º lugar no European Cyber Security Challenge 2019*. Disponível em: https://www.cncs.gov.pt/recursos/noticias/equipa-portuguesa-conquista-10-lugar-no-european-cyber-security-challenge-2019/ [acedido em 20 de junho de 2020].

CTFTime, 2020. *CTF Teams*. Disponível em: https://ctftime.org/stats/2020/PT [acedido em 20 de junho de 2020].

ENISA, 2018. *Economics of vulnerability disclosure*. Disponível em: https://www.enisa.europa.eu/publications/economics-of-vulnerability-disclosure/at_download/fullReport [acedido em 8 de junho de 2019].

Facebook, 2013. *An update on our Bug Bounty Program*. Disponível em: https://www.facebook.com/notes/facebook-security/an-update-on-our-bug-bounty-program/10151508163265766 [acedido em 6 de julho de 2019].

Finifter, M., Akhawe, D. & Wagner, D., 2013. *An Empirical Study of Vulnerability Rewards Programs*. In: Proceedings of the 22nd USENIX Security Symposium. Berkeley: USENIX Association; pp.273-288. Disponível em: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_finifter.pdf [acedido em 22 de junho de 2019].

Gamma, M., 2019. E-Voting-PIT: Welche Security-Standards ein Hacker überwinden muss. *Inside IT*. Disponível em: https://www.inside-it.ch/de/post/e-voting-pit-welche-security-standards-ein-hacker-ueberwinden-muss-20190226 [acedido em 5 de agosto de 2019].

Government of the Netherlands, s.d. *Responsible disclosure*. Disponível em: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure [acedido em 10 de agosto de 2020].

HackerOne, 2016. *What Was It Like To Hack the Pentagon?* Disponível em: https://www.hackerone.com/blog/hack-the-pentagon-results [acedido em 13 de julho de 2019].

HackerOne, 2017a. *The best security initiative you can take in 2017*. Disponível em: https://www.hackerone.com/blog/The-best-security-initiative-you-can-take-in-2017 [acedido em 8 de agosto de 2020].

HackerOne, 2017b. *Hack The Army Results Are In*. Disponível em: https://www.hackerone.com/blog/Hack-The-Army-Results-Are-In [acedido em 13 de julho de 2019].

HackerOne, 2017c. *Aim High...Find, Fix, Win!* Disponível em: https://www.hackerone.com/blog/hack-the-air-force-results [acedido em 13 de julho de 2019].

HackerOne, 2018a. *U.S. Department of Defense Announces Hack the Marine Corps Bug Bounty Program With HackerOne*. Disponível em: https://www.hackerone.com/press-release/us-department-defense-announces-hack-marine-corps-bug-bounty-program-hackerone [acedido em 6 de julho de 2019].

HackerOne, 2018b. *Hacking the U.S. Air Force (again) from a New York City subway station*. Disponível em: https://www.hackerone.com/blog/Hacking-US-Air-Force-again-New-York-City-subway-station [acedido em 13 de julho de 2019].

HackerOne, 2018c. *U.S. Air Force Boosts Security With Second Bug Bounty Challenge on Hacker One*. Disponível em: https://www.hackerone.com/press-release/us-air-force-boosts-security-second-bug-bounty-challenge-hackerone [acedido em 13 de julho de 2019].

HackerOne, 2018d. *U.S. Department of Defense Concludes Third "Hack the Air Force" Bug Bounty Challenge with HackerOne to Improve Cybersecurity*. Disponível em: https://www.hackerone.com/press-release/us-department-defense-concludes-third-hack-air-force-bug-bounty-challenge-hackerone [acedido em 13 de julho de 2019].

HackerOne, 2018e. *U.S. Department of Defense Kicks Off Fifth Bug Bounty Challenge With Hacker One*. Disponível em: https://www.hackerone.com/press-release/us-department-defense-kicks-fifth-bug-bounty-challenge-hackerone [acedido em 14 de julho de 2019].

HackerOne, 2018f. *U.S. Department of Defense Secures the DTS With Help From Hackers on Hacker One*. Disponível em: https://www.hackerone.com/press-release/hackers-are-finding-more-severe-vulnerabilities-ever-total-number-high-or-critical [acedido em 14 de julho de 2019].

HackerOne, 2018g. *Hack the Marine Corps Bug Bounty Challenge Concludes, Nearly 150 Security Vulnerabilities Surfaced and $151,542 Awarded to Hackers*. Disponível em: https://www.hackerone.com/press-release/hack-marine-corps-bug-bounty-challenge-concludes-nearly-150-security-vulnerabilities [acedido em 13 de julho de 2019].

HackerOne, 2018h. *U.S. General Services Administration Selects HackerOne as TTS Bug Bounty Partner*. Disponível em: https://www.hackerone.com/press-release/us-general-services-administration-selects-hackerone-tts-bug-bounty-partner [acedido em 13 de julho de 2019].

HackerOne, 2018i. *Singapore Ministry of Defence Concludes Successful Ethical Hacking Program*. Disponível em: https://www.hackerone.com/press-release/singapore-ministry-defence-concludes-successful-ethical-hacking-program [acedido em 13 de julho de 2019].

HackerOne, 2019a. *Hacking the Singapore Government: A Q&A With A Top Hacker & MINDEF 2.0 Results*. Disponível em: https://www.hackerone.com/blog/hacking-singapore-government-qa-top-hacker-mindef-20-results [acedido em 13 de janeiro de 2020].

HackerOne, 2019b. *Singapore Government Enhances Cybersecurity Defenses With Second Hacker One Bug Bounty Programme*. Disponível em: https://www.hackerone.com/press-release/singapore-government-enhances-cybersecurity-defenses-second-hackerone-bug-bounty [acedido em 13 de julho de 2019].

HackerOne, 2019c. *Government Technology Agency Launches Vulnerability Disclosure Programme with HackerOne Following Successful Bug Bounty Programmes*. Disponível em: https://www.hackerone.com/press-release/government-technology-agency-launches-vulnerability--disclosure-programme-hackerone [acedido em 6 de outubro de 2019].

HackerOne, 2020. *Government Technology Agency of Singapore Concludes Third HackerOne Bug Bounty Programme, Enhancing Cybersecurity Defenses*. Disponível em: https://www.hackerone.com/press-release/government-technology-agency-singapore-concludes-third-hackerone-bug-bounty-programme [acedido em 14 de junho de 2020].

Herr, T., Schneier, B. & Morris, C., 2017. *Taking Stock: Estimating Vulnerability Rediscovery*. Cambridge: Harvard Kennedy School Belfer Center for Science and International Affairs. Disponível em: https://www.belfercenter.org/sites/default/files/files/publication/Rediscovery%20-%20final%206.pdf [acedido em 29 de junho de 2019].

Kranenbarg, M., Holt, T. & Ham, J., 2018. *Don't shoot the messenger! A criminological and computer science perspective on coordinated vulnerability disclosure*. Crime Science, Volume 7. Disponível em: https://link.springer.com/content/pdf/10.1186/s40163-018-0090-8.pdf [acedido em 10 de agosto de 2020].

Kuehn, A. & Mueller, M., 2014. *Shifts in the Cybersecurity Paradigm: Zero-Day Exploits, Discourse, and Emerging Institutions*. In: Proceedings of the 2014 New Security Paradigms Workshop. Victoria: ACM Press; pp. 63-68.

Lei n.º 109/2009, de 15 de setembro. Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, do Conselho, de 24 de Fevereiro, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho da Europa. *Diário da República*, n.º 179/2009, Série I, pp. 6319-6325, Assembleia da República. Disponível em: https://dre.pt/application/conteudo/489693 [acedido em 17 de fevereiro de 2020].

Lewis, S. J., Pereira, O. & Teague, V., 2019a. *The use of trapdoor commitments in Bayer-Groth proofs and the implications for the verifiabilty of the Scytl-SwissPost Internet voting system*. Disponível em: https://people.eng.unimelb.edu.au/vjteague/UniversalVerifiabilitySwissPost.pdf [acedido em 3 de agosto de 2019].

Lewis, S. J., Pereira, O. & Teague, V., 2019b. *The use of non-adaptive zero knowledge proofs in the Scytl-SwissPost Internet voting system, and its implications for decryption proof soundness*. Disponível em: https://people.eng.unimelb.edu.au/vjteague/HowNotToProveElectionOutcome.pdf [acedido em 3 de agosto de 2019].

Matos, P., 2018. Investigador descobriu como entrar em qualquer conta do Portal das Finanças em segundos. *Exame Informática*. Disponível em: https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-08-22-investigador-descobriu-como-entrar-em--qualquer-conta-do-portal-das-financas-em-segundos/ [acedido em 9 de agosto de 2020].

Miller, C., 2007. *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales*. Disponível em: https://www.econinfosec.org/archive/weis2007/papers/29.pdf [acedido em 16 de junho de 2019].

National Cyber Security Centre, 2018a. *NCSC vulnerability disclosure co-ordination*. Disponível em: https://www.ncsc.gov.uk/blog-post/ncsc-vulnerability-disclosure-co-ordination [acedido em 10 de agosto de 2020].

National Cyber Security Centre, 2018b. *Vulnerability Reporting*. Disponível em: https://www.ncsc.gov.uk/information/vulnerability-reporting [acedido em 10 de agosto de 2020].

National Telecommunications and Information Administration, 2016. *Vulnerability Disclosure Attitudes and Actions: A Research Report from the NTIA Awareness and Adoption Group*. Disponível em: https://www.ntia.doc.gov/files/ntia/publications/2016_ntia_a_a_vulnerability_disclosure_insights_report.pdf [acedido em 15 de janeiro de 2020].

On, A., 2019. *Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties*. In: Ellis, R. & Mohan, V. (2019). *Rewired: Cybersecurity Governance*: Wiley, pp. 231-314.

Popper, B., 2017. DJI's bug bounty program starts with a stumble. *The Verge*. Disponível em: https://www.theverge.com/2017/11/20/16669724/dji-bug-bounty-program-conflict--researcher [acedido em 14 de janeiro de 2020].

Scytl, 2019. *Statement on recent comments regarding the source code publication of the Swiss e-voting system*. Disponível em: https://www.scytl.com/en/news/statement-recent-comments--regarding-source-code-publication-swiss-e-voting-system/ [acedido em 5 de agosto de 2019].

Swiss Federal Council, 2019a. *Public intrusion test for e-voting to take place in February and March*. Disponível em: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-73898.html [acedido em 20 de julho de 2019].

Swiss Federal Council, 2019b. *e-Voting: Federal Council to reframe trial phase and delay introduction as a regular voting channel*. Disponível em: https://www.admin.ch/gov/en/start/documentation/media-releases.msg-id-75615.html [acedido em 4 de agosto de 2019].

Swiss Post, 2019a. *Public hacker test on Swiss Post's e-voting system*. Disponível em: https://www.evoting-blog.ch/en/pages/2019/public-hacker-test-on-swiss-post-s-e-voting-system [acedido em 20 de julho de 2019].

Swiss Post, 2019b. *Ballot box not hacked, errors in the source code – Swiss Post temporarily suspends its e-voting system*. Disponível em: https://www.post.ch/en/about-us/media/press-releases/2019/swiss-post-temporarily-suspends-its-e-voting-system [acedido em 20 de julho de 2019].

Swiss Post, 2019c. *ELECTRONIC VOTING SOLUTION SOURCE CODE ACCESS AGREEMENT*. Disponível em: https://www.post.ch/-/media/post/evoting/dokumente/nutzungsbedingungen-quellcode.pdf?la=en&vs=3 [acedido em 21 de julho de 2019].

Swiss Post, 2019d. *Swiss Post to focus solely on new system with universal verifiability*. Disponível em: https://www.post.ch/en/about-us/media/press-releases/2019/swiss-post-to-focus-solely-on-new-system-with-universal-verifiability [acedido em 4 de agosto de 2019].

Swissinfo, 2019. *E-voting dealt another political blow*. Disponível em: https://www.swissinfo.ch/eng/parliament_e-voting-dealt-another-political-blow/45425298 [acedido em 26 de dezembro de 2019].

Swissinfo, 2020. *Swiss Post set to relaunch its e-voting system*. Disponível em: https://www.swissinfo.ch/eng/swiss-post-set-to-relaunch-its-e-voting-system/45820842 [acedido em 21 de junho de 2019].

Synopsys, 2017. *Heartbleed Bug*. Disponível em: https://heartbleed.com/ [acedido em 29 de junho de 2019].

Wilson, A., Schulman, R., Bankston, K. & Herr, T., 2016. *Bugs in the System: A Primer on the Software Vulnerability Ecosystem and its Policy Implications*. Disponível em: https://newamerica.org/documents/1659/Bugs-in-the-System-Final.pdf [acedido em 8 de junho de 2019].

Zetter, K., 2019. Researchers Find Critical Backdoor in Swiss Online Voting System. *Motherboard*. Disponível em: https://www.vice.com/en_us/article/zmakk3/researchers-find-critical-backdoor-in-swiss-online-voting-system [acedido em 5 de agosto de 2019].

Zhao, M., Laszka, A. & Grossklags, J., 2017. Devising Effective Policies for Bug-Bounty Platforms and Security Vulnerability Discovery. *Journal of Information Policy*, Volume 7, pp. 372-418.

A Transformação da Turquia na Era Erdoğan: Implicações sobre a Segurança Euro-Atlântica

José Pedro Teixeira Fernandes
Doutorado em Ciência Política e Relações Internacionais pela Universidade do Minho, Professor Coordenador do ISCET, Investigador do IPRI-Universidade Nova de Lisboa e Investigador Associado do Instituto da Defesa Nacional.

Domingos Rodrigues
Responsável pela Delegação do Porto do Instituto da Defesa Nacional.

Resumo

A Turquia está situada na zona de transição entre a *island of peace* (ilha de paz) europeia e o conturbado Médio Oriente, dilacerado por diversos conflitos. A sua localização no cruzamento do sudeste europeu com o Médio Oriente tem-lhe dado uma continuada importância geopolítica, quer para os norte-americanos, quer para os europeus. A posição pública entre vários Estados aliados, bem como a literatura especializada refletem que estas transformações têm levantado dúvidas sobre o seu comprometimento com a segurança euro-atlântica. O artigo tem por objetivo, em primeiro lugar analisar nos seus traços fundamentais a política externa da Turquia desde o período em que Erdoğan chegou ao poder. Em segundo avaliar em que medida a transformação da Turquia está a afetar o atual sistema de segurança euro-atlântico.

Palavras-chave: Turquia; Erdoğan; Segurança; NATO; União Europeia.

Abstract
Turkey's Transformation in the Erdoğan Era: Implications for Euro-Atlantic Security

Turkey is located in the transition zone between the European island of peace and the troubled Middle East, torn by several conflicts. Its location at the intersection of southeastern Europe with the Middle East has enabled its persisting geopolitical importance, both for the Americans and for the Europeans. The public position among the several allied States, as well as the specialized literature reveal that these transformations have raised doubts about Turkey's commitment to Euro-Atlantic security. The article aims, in the first place, to analyze in its fundamental features the foreign policy of Turkey since the period when Erdoğan came to power. Second, it aims to assess the extent to which Turkey's transformation is affecting the current Euro- Atlantic security system.

Keywords: *Turkey; Erdoğan; Security; NATO; European Union.*

Artigo recebido: 28.07.2020
Aprovado: 15.08.2020
https://doi.org/10.47906/ND2020.156.04

Introdução

A grande transformação do mundo ocorrida nas duas primeiras décadas do século XXI é hoje uma realidade demasiado evidente para qualquer observador das questões internacionais. As mudanças que se operaram, ao nível político, económico, tecnológico e outros, têm inevitáveis repercussões no domínio da segurança e da defesa. Se, a nível global, a ascensão da China a potência mundial de primeira grandeza é a transformação mais óbvia e mais profunda, a nível regional outras mudanças de relevo ocorreram. No contexto europeu, a transformação da Turquia ocorrida nos últimos 20 anos – um Estado que é parte do sistema de segurança euro-atlântico desde os seus primórdios nos anos 1950 – é um aspeto maior. Pela sua posição geográfica, a Turquia está na zona de transição entre a *island of peace* (ilha de paz) europeia e o conturbado Médio Oriente, dilacerado por diversos conflitos sangrentos. A sua localização no cruzamento do Sudeste europeu com o Médio Oriente tem-lhe dado uma continuada importância geopolítica, quer para os norte-americanos, quer para os europeus. Quanto a estes últimos, a Turquia está envolvida num interminável processo de negociações de adesão[1] à União Europeia, desde 2005, sendo improvável a sua adesão futura, pelo menos no horizonte temporal discernível. Ao mesmo tempo, na Turquia do século XXI um político – Recep Tayyip Erdoğan – tornou-se incontornável. Não só está no poder há mais tempo do que o mítico fundador da república, Mustafa Kemal Atatürk, como a Turquia, sob a sua ação política, a nível interno e externo, tem sofrido múltiplas transformações as quais chamam à atenção, mesmo aos não especialistas na área internacional. Em vários Estados aliados, bem como na literatura especializada, as transformações da Turquia têm levantado dúvidas sobre o seu comprometimento com a segurança euro-atlântica. Entre outros, isso é visível nas publicações do professor da Columbia University, em Nova Iorque, David L. Phillips, *An Uncertain Ally: Turkey under Erdoğan's Dictatorship* (2017)[2] e de Soner Cagaptay do The Washington Institute, *Erdoğan's Dictatorship: Turkey and Politics of the Middle East* (2020)[3]. Algumas interrogações naturalmente ocorrem, às quais é necessário dar resposta: que impacto estão a ter as transformações ocorridas na Turquia sobre a segurança euro-atlântica? Está mesmo em causa a sua continuidade como membro desse sistema, como as análises mais pessimistas sugerem? E qual a sua real importância geopolítica no atual contexto político e estratégico internacional?

1 Comissão Europeia (2019), "Relações UE-Turquia", disponível em https://ec.europa.eu/neighbourhood-enlargement/candidate-countries/turkey/relation/index_pt.html [acedido em 07 de junho de 2020].

2 Phillips, David L. (2017), *An Uncertain Ally: Turkey under Erdoğan's Dictatorship*, Routledge, Londres-Nova Iorque.

3 Cagaptay, Soner (2020), *Erdoğan's Dictatorship: Turkey and Politics of the Middle Easty*, I.B. Tauris, Londres-Nova Iorque.

Analisar, nos seus traços fundamentais, a política externa da Turquia desde o período em que Recep Tayyip Erdoğan chegou ao poder, é, assim, o primeiro grande objetivo deste artigo. Ao mesmo tempo, daí decorre um segundo importante objetivo que é avaliar em que medida a política externa turca – durante a já extensa permanência de Recep Tayyip Erdoğan no poder – está a afetar, e sob que formas específicas, o sistema de segurança euro-atlântico centrado na Organização do Tratado do Atlântico Norte (NATO, na sigla usual em língua inglesa). Tal como ocorre com outros assuntos internacionais, o estudo desta temática está condicionado por diferentes lentes teóricas – realismo; neorrealismo; liberalismo; neoliberalismo; construtivismo; estudos críticos; feminismo; ou outras –, as quais refletem visões específicas do mundo[4]. Em termos de enquadramento nas grandes correntes das Relações Internacionais, esta análise vai estar mais ou menos próxima da visão do mundo neorrealista, usando, sobretudo, as suas lentes teórico-concetuais. A escolha teve em conta a adequação à investigação que se pretendeu aqui efetuar, nomeadamente a dimensão estratégica e de segurança subjacente ao tema abordado, onde a perspetiva realista e neorrealista têm tido – e continuam a ter – um enraizamento e contributos relevantes dados[5]. Numa área científica marcada pelo pluralismo teórico e metodológico, isso não significa que a temática investigada não possa ser analisada sob outras perspetivas teóricas, assentes em diferentes conceções epistemológicas e ontológicas. Mas essa seria uma outra abordagem provavelmente também com outros objetivos que não aqueles que aqui foram traçados. Como já referido, serão então aqui analisadas as transformações da política externa de um Estado, a Turquia, o que implica olhar não só para o mundo exterior como também para as suas transformações internas, de forma a detetar possíveis correlações. Será ainda analisada a questão da cooperação/competição/rivalidade entre Estados soberanos no sistema internacional, em particular da Turquia, dentro de uma aliança político-militar (a NATO). Para além da opção teórica apontada, agora em termos metodológicos, a escolha passou pelo recurso a uma metodologia de tipo qualitativo[6] combinada com algumas das técnicas mais usuais adotadas nos estudos de

4 Dunne, T., Kurki, M. e Smith, Steve, eds., (2016), *International Relations Theories. Discipline and diversity*, 4th ed., Oxford, Oxford University; Burchill, Scott e Linklater, Andrew, eds., (2013), *Theories of International Relations*, 5.ª ed., Nova Iorque, Palgrave Macmillan; Moreira, Adriano (2016), *Teoria das Relações Internacionais*, 9.ª ed., Coimbra, Almedina; Fernandes, José Pedro Teixeira (2009), *Teorias das Relações Internacionais: da abordagem clássica ao debate pós-positivista*, 2.ª ed., Coimbra, Almedina.

5 Entre outros ver Mahnken, Thomas G. e Maiolo, Joseph, A., eds., *Strategic Studies: A Reader*, Routledge, Londres-Nova Iorque.

6 Sobre a metodologia qualitativa nas investigações em Relações Internacionais ver entre outros, Klotz, Audie e Prakash, Deepa, eds., (2008), *Qualitative Methods in International Relations: A Pluralist Guide*, Nova Iorque, Palgrave MacMillan.

caso[7] em Relações Internacionais. Envolveu assim uma recolha de dados assente numa pesquisa e análise documental sobre textos oficiais e declarações políticas relevantes para o caso investigado[8], bem como uma pesquisa bibliográfica, ainda que relativamente seletiva, na literatura sobre o tema. Para efeitos de resposta às interrogações formuladas e aos objetivos indicados, o trabalho de investigação foi estruturado da seguinte forma: num primeiro ponto será passada em revista a política externa e de segurança da Turquia durante a Guerra Fria e sua dependência da NATO e do Ocidente; em seguida, são analisadas as mutações da política externa turca face ao ambiente geopolítico do pós-Guerra Fria; num terceiro ponto é abordada a era Erdoğan e a ambição da Turquia se transformar numa grande potência (neo-otomana) do século XXI; por fim, num quarto ponto, são analisadas divergências da Turquia com a NATO e a União Europeia, as quais tornaram os tradicionais aliados em parceiros desavindos, em grande parte devido às transformações do Médio Oriente após a chamada "Primavera Árabe" e aos diferentes interesses estratégicos que daí emergiram em questões vistas como críticas. A investigação termina formulando algumas conclusões e deixando pistas para possíveis investigações futuras.

1. A Dependência da Turquia Face à NATO no Contexto da Guerra Fria

Para avaliar corretamente as transformações da Turquia sob o comando Recep Tayyip Erdoğan é necessário olhar primeiro – ainda que de forma necessariamente abreviada –, para o seu posicionamento político-estratégico anterior, recuando à altura da formação do atual sistema de segurança e defesa euro-atlântico. Como é bem conhecido, este teve origem na política dos Estados Unidos da América (EUA) de *containment* (contenção) da antiga União Soviética. E teve também na formação da NATO, pelo Tratado de Washington[9] de 4 de abril de 1949, uma peça fundamental. Quanto à Turquia, a sua adesão à NATO – tal como a da Grécia, ambas efetuadas no ano 1952 numa cimeira[10] em Lisboa – in-

7 Lamont, Christopher K., (2017), *Case Study Methods in International Relations,* Oxford Bibliographies, 29 November, disponível em https://www.oxfordbibliographies.com/view/document/obo-9780199743292/obo-9780199743292-0225.xml [acedido em 30 de outubro de 2020].

8 Importa aqui notar as limitações que inevitavelmente decorrem do não domínio da língua turca pelos autores desta investigação, apesar desta ser razoavelmente suprível pelo recurso à bibliografia e documentação publicada em língua inglesa e noutras línguas ocidentais.

9 NATO (2019), *The North Atlantic Treaty*, Washington, 4 April 1949, disponível em https://www.nato.int/cps/en/natolive/official_texts_17120.htm [acedido em 03 de junho de 2020].

10 Marcos, Daniel (2010), "Portugal e a evolução do sistema defensivo europeu. A Cimeira de Lisboa de 1952", *Relações Internacionais*, n.º 27, pp. 65-80, disponível em http://www.scielo.mec.pt/pdf/ri/n27/n27a07.pdf [acedido em 08 de junho de 2020].

sere-se nesse contexto. Durante a II Guerra Mundial e no pós-guerra uma disputa em torno da passagem nos estreitos do Bósforo e Dardanelos (re)emergiu entre a União Soviética e a Turquia. Várias tensões tinham ocorrido entre ambos os Estados durante a II Guerra Mundial devido à passagem de navios alemães e italianos nos estreitos.[11] Mas a pressão soviética não era apenas exercida em relação à navegação no Bósforo e Dardanelos – ou seja, sobre a passagem do Mar Negro para o Mediterrâneo e o inverso –, pois colocava ainda em causa o anteriormente estabelecido na Convenção de Montreux[12]. Estaline reivindicou parte do território do Leste da Anatólia, sobre o qual a República Soviética da Geórgia teria direitos históricos, argumentando que teriam sido usurpados pelo Império Otomano/Turquia.

A pressão soviética do pós-II Guerra Mundial trouxe muito más memórias à Turquia. Mais do que qualquer outra grande potência europeia, a Rússia teve um papel maior no retrocesso[13] do Império Otomano, especialmente nos territórios do Sudeste da Europa e do Cáucaso. A história desse período mostra inequivocamente que o Império Russo foi a principal ameaça militar ao Império Otomano – o "homem doente da Europa"[14] – na memorável frase atribuída ao czar Nicolau I nas vésperas da Guerra da Crimeia (1853-1856). Por sua vez, o maior aliado tradicional do Império Otomano/Turquia para conter a ambição expansionista russa, ainda que problemático, foi o Império Britânico. Tendo em conta esse passado, a ambição de entrada da Turquia na NATO representava uma vontade de reforçar a antiga garantia de segurança britânica com a da nova superpotência norte-americana. Assim, a Turquia do pós-II Guerra Mundial, primeiro sob o comando de İsmet İnönü que tinha sucedido a Mustafa Kemal Atatürk em finais de 1938, e depois de Celâl Bayar (presidente da república) e Adnan Menderes (primeiro-ministro), procurou aliados nos EUA e na NATO contra o poderio russo/soviético.

Para além do medo da expansão União Soviética sobre o seu território – e da óbvia dificuldade da Turquia para enfrentar sozinha essa ameaça –, existiam outras circunstâncias políticas que explicam a proximidade (e dependência) face à NATO e

11 Hasanli, Jamil (2009), "The 'Turkish crisis' of the Cold War Period and the South Caucasian Republics. Part II: The Rise of Pro-American Sentiments in Turkey", *Central Asia and the Caucasus* (English Edition), disponível em https://www.ca-c.org/c-g/2009/journal_eng/c-g-1/13.shtml [acedido em 13 de junho de 2020].

12 *Convention Concernant le Régime des Détroits* (1936), disponível em https://basedoc.diplomatie.gouv.fr/exl-php/cadcgp.php [acedido em 16 de junho de 2020].

13 Editors of Encyclopaedia Britannica (2014), "Russo-Turkish Wars", *Encyclopaedia Britannica*, April 28, disponível em https://www.britannica.com/topic/Russo-Turkish-wars [acedido em 02 de junho de 2020].

14 Editors of Encyclopaedia Britannica (2014), "Russo-Turkish Wars", *Encyclopaedia Britannica*, April 28, disponível em https://www.britannica.com/topic/Russo-Turkish-wars [acedido em 02 de junho de 2020].

ao Ocidente. Aqui destacam-se as más relações com os antigos súbditos imperiais/coloniais otomanos das províncias árabes do Império Otomano – Síria, Iraque, Líbano, Jordânia, Arábia Saudita, etc. – devido à "traição árabe" de 1916-1918[15]. Um outro aspeto relevante é que, mesmo nesse período de grande proximidade com a NATO e o Ocidente, a aliança político-militar nunca esteve totalmente isenta de tensões e de contradições. Os seu aliados ocidentais da NATO, sobretudo os europeus – França e Reino Unido –, são os mesmos que em 1919-1920 pretendiam retalhar o território do Império Otomano na costa Mediterrânica (que seria atribuído à Grécia) e no Centro e Leste da Anatólia (para dois novos Estados independentes, um arménio, o outro curdo). Essa pretensão política ficou consagrada no Tratado de Sèvres (1919)[16] que o Império Otomano/Turquia nunca ratificaram. O Estado fundado por Mustafa Kemal Atatürk em 1923 conseguiu afirmar o seu poder sobre a totalidade desse território após uma guerra vitoriosa sobre a Grécia – e uma deportação mútua de populações[17] entre ambos –, conflito que teve ainda uma dimensão de guerra civil. Ironias da história, na época, para a vitória dos nacionalistas turcos de Mustafa Kemal Atatürk, foi decisivo o apoio dos bolcheviques russos em processo de fundação da União Soviética[18] que viam no movimento nacionalista turco um aliado contra o imperialismo ocidental. Quanto à memória histórica do Tratado de Sèvres alimenta, ainda hoje, na Turquia, uma "fobia de Sèvres", na qual alguns dos seus inimigos são os aliados da NATO.

O problema curdo[19] da Turquia é talvez o exemplo mais revelador de todas essas contradições político-estratégicas. O conflito com a população curda que habita território turco esteve adormecido[20] nas décadas subsequentes ao final da II Guerra Mundial, mas (re)surgiu em 1984 com a revolta armada do Partiya Karkeran Kur-

15 Nessa altura o Império Otomano estava em guerra com a Entente franco-britânica e a Rússia na frente oriental da I Guerra Mundial, mas os súbditos árabes acabaram por aliar-se às tropas britânicas contra os exércitos otomanos.

16 *Traité de paix entre les Puissances alliées et associées et la Turquie* (1920), disponível em Digithèque de matériaux juridiques et politiques [website] https://mjp.univ-perp.fr/traites/1920sevres.htm [acedido em 12 de junho de 2020].

17 Fernandes, José Pedro Teixeira (2007), "O Fim do Império Otomano e a Troca de Populações entre a Grécia e a Turquia", *História*, n.º 97, maio, pp. 36-41, disponível em Realpolitik https://realpolitikmag.org/index.php/2015/06/05/o-fim-do-imperio-otomano-e-a-troca-de-populacoes-entre-a-grecia-e-a-turquia/ [acedido em 20 de junho de 2020].

18 Karaveli, Halil (2018), *Why Turkey is Authoritarian*, London, Pluto Press. Em especial o capítulo 1, "A Pattern of Violence".

19 Sobre os curdos e o problema curdo da Turquia ver, entre outros: Çiçek, Cuma (2016), *The Kurds of Turkey: National, Religious and Economic Identities,* London-New York, I. B. Tauris; e, McDowall, David (2004), *A Modern History of the Kurds*, ed. rev., London-New York, I. B. Tauris.

20 Durante o período de Mustafa Kemal Atatürk (1923-1938), das 18 revoltas armadas que ocorreram contra o regime, 17 tiveram lugar no Sudeste da Anatólia e em 16 estiveram envolvidos grupos curdos. Na altura as revoltas eram contra as transformações radicais feitas por Atatürk, especialmente pelo afastamento do Islão da vida pública.

distan (PKK)[21]. Mas se a questão curda ficou no centro das preocupações de segurança da Turquia valeu-lhe, também, muitas críticas, sobretudo devido às graves violações de Direitos Humanos. Nessas críticas, os seus aliados ocidentais – em especial a União Europeia – têm tido um papel importante o que desagrada à Turquia. Após um período de relativa acalmia, a questão agravou-se nos últimos anos com a Guerra da Síria, contribuindo também para esse agravamento as incursões militares turcas do outro lado da fronteira, na zona dos curdos da Síria. Este é um conflito que, pelo seu impacto nas relações com os seus aliados europeus e norte-americano, analisaremos mais à frente.

2. A Geopolítica do Pós-Guerra Fria e a Gradual Transformação da Política Externa Turca

Em finais de Outubro de 1989 Turgut Özal[22] – um político da direita conservadora-nacionalista do Anavatan Partisi – ANAP, Partido da Pátria – que tinha ocupado o cargo de primeiro-ministro –, foi eleito Presidente da República na Grande Assembleia Nacional da Turquia. Em termos de política externa, Turgut Özal manteve-se fundamentalmente alinhado com os EUA e a NATO. Exemplificativo desse alinhamento foi o apoio dado à grande coligação multinacional liderada pelos EUA contra o Iraque, durante a Guerra do Golfo de 1991, após Saddam Hussein ter anexado o Kuwait. Mas, em paralelo, durante esse mesmo período, emergiram outras facetas da política externa turca até aí praticamente inexistentes. No Sudeste europeu (Balcãs), no Cáucaso e na Ásia Central a Turquia tentou aproveitar a profunda transformação geopolítica em curso – e o enfraquecimento do seu inimigo histórico, a União Soviética/Rússia – para projetar novamente a sua influência nessas zonas. As ligações históricas e culturais associadas a uma certa nostalgia do passado otomano, tornaram-se, subitamente, numa mais-valia estratégica. No caso do Balcãs, essas ligações derivam da multisecular presença do Império Otomano no Sudeste europeu. A conexão mais óbvia são as diversas populações islamizadas pelos otomanos que existem um pouco por toda a região, especialmente na Bósnia-Herzegovina, Kosovo e Albânia. Quanto à outra área onde a Turquia ambicionou projetar a sua influência foi, como já notado, a dos antigos territórios da União Soviética, do Cáucaso à Ásia Central. Aí a alteração do mapa político levou ao aparecimento de novos Estados independentes "turcófonos" – Azerbaijão, Turquemenistão, Uzbequistão, Cazaquistão e Quirguistão. Juntamente com a Turquia formaram um grupo informal conhecido como T5. A alteração geopolítica fez despontar, ainda que

21 O início da guerrilha do PKK ocorreu em 1984, na sequência da proibição pelo governo da Turquia da celebração do ano novo curdo/iraniano (o *Nevroz*), a 21 de março.

22 Presidency of the Republic of Turkey (2020), *Turgut Özal*, disponível em https://www.tccb.gov.tr/turgut-ozal [acedido em 05 de junho de 2020].

de forma inicialmente contida e prudente, um misto de ambições de otomanismo – onde o Islão é um veículo privilegiado face a povos que foram governados pelos otomanos – e de panturquismo[23] – explorando conexões étnicas com povos fora do Império Otomano/Turquia.

Importa sublinhar que essa reconfiguração da política externa foi, nos seus primórdios, efetuada de forma bastante cautelosa e pragmática, procurando preservar, simultaneamente, a tradicional orientação estratégica anterior. Por outras palavras, manteve uma ligação forte à NATO e deu continuidade às relações estratégicas privilegiadas com os EUA (e também com Israel). Sinal desses tempos, em 1996 foi assinado um acordo político-militar com Israel[24] apesar de, pela primeira vez na história da República da Turquia, um partido conservador-islamista, o Refah Partisi – Partido da Prosperidade ou Partido do Bem-Estar – de Necmettin Erbakan, conhecido pelas suas posições antijudaicas, ter chegado ao governo. Nessa época o *establishment* secular da Turquia detinha os mecanismos institucionais de poder, algo que nas décadas subsequentes se alterou drasticamente no plano interno projetando-se na (re)configuração da política externa.

3. A Era Erdoğan e o Regresso da Ambição de Grande Potência (Neo-Otomana)

Sem qualquer dúvida, Recep Tayyip Erdoğan é o político mais importante da República da Turquia desde a sua fundação por Mustafa Kemal Atatürk, sendo já qualificado como o "novo pai da Turquia"[25]. Pelo menos em número de anos no poder – quer como primeiro-ministro, quer como presidente da república –, ultrapassou Atatürk. Desde a chegada ao poder em finais de 2002 que o seu partido, o Adalet ve Kalkınma Partisi – AKP, Partido da Justiça e do Desenvolvimento – marcou decisivamente a Turquia[26]. Até aos fortes protestos ocorridos no Parque

23 Estas germinavam sobretudo no início do século XX, na fase terminal do Império Otomano. Na época, Enver Paxá era o líder dos Jovens Turcos e também o principal rosto dessa ambição política de reconstituir o Império Otomano/Turquia para Oriente. Chefiou o triunvirato dos Jovens Turcos que governou o Império Otomano durante a I Guerra Mundial. Morreu em 1922 quando combatia o Exército Vermelho no Uzbequistão, tentando sublevar as populações turco-muçulmanas para constituir um império pan-turco.

24 Fernandes, José Pedro Teixeira (2010), "A Política Externa da Turquia Face a Israel: O Regresso da Ambição Otomana", *Nação e Defesa*, n.º 127, pp. 159-180, disponível em https://comum.rcaap.pt/bitstream/10400.26/4724/1/NeD127_Jos%C3%A9PedroTeixeiraFernandes.pdf [acedido em 02 de junho de 2020].

25 Cheviron, Nicolas e Pérouse, Jean-François (2016), *Erdoğan: Nouveau Père de la Turquie?* Paris, François Bourin Editions.

26 Fernandes, José Pedro Teixeira (2013), "A contestação na Turquia em perspetiva: a era Erdogan revisitada", *Público*, 12 de junho, disponível em https://www.publico.pt/2013/06/12/jornal/a-contestacao-na-turquia-em-perspectiva-a-era-erdogan-revisitada-26671186 [acedido em 22 de junho de 2020]. Ver também David, Isabel e Pinto, Gabriela (2017), "The Gezi Protests and the Europeanization of the Turkish Public Sphere", *Journal of Civil Society*, 13(3), pp. 307-322.

Gezi[27], em Istambul, durante o ano de 2013, Recep Tayyip Erdoğan e o AKP eram normalmente vistos de forma muito benigna. Na frente interna fez reformas vistas como aproximando a Turquia dos valores europeus da liberdade, da democracia e dos direitos humanos. Não menos importante, obteve uma vitória diplomática ao conseguir a abertura de negociações de adesão à União Europeia, iniciadas em finais de 2005. Os seus anos de governo como primeiro-ministro, de 2003 a 2014, foram marcados por um grande crescimento económico. No plano externo, aumentou a influência política turca, especialmente nos países árabes-islâmicos. Com a chamada Primavera Árabe[28], em 2011, a Turquia parecia emergir como um modelo para as populações que, um pouco por todo o Mediterrâneo Sul e Oriental, derrubavam governos autoritários e aspiravam à democracia e à prosperidade económica. A sua combinação entre Islão e democracia parecia irresistível[29].
Nessa mesma época, Ahmet Davutoğlu[30] era o influente ministro dos Negócios Estrangeiros da Turquia, que impressionava a maioria dos europeus e ocidentais[31]. As suas ideias sobre o que deveria ser a política externa e a estratégia de afirmação internacional do Estado turco tinham sido delineadas em *Stratejik Derinlik: Türkiye'nin Uluslararası Konumu*[32] – Profundidade Estratégica: a Posição Internacional da Turquia, 2001. Fundamentalmente, denotavam uma ambição de afirmação da Turquia como grande potência (regional). Levava mais longe mais longe as tendências já detetáveis em Turgut Özal, não só em termos geográficos – alargando-a a novas partes do mundo, como o Brasil e a África subsariana –, mas também em termos de diversificação (e distanciamento) face à política externa tradicional anterior. Emergiu, assim, uma nova ambição que é neo-

27 Amnesty International (2013), *Gezi Park Protests: Brutal Denial of The Right to Peaceful Assembly in Turkey*, 2 de outubro, disponível em https://www.amnesty.org/download/Documents/12000/eur440222013en.pdf [acedido em 08 de junho de 2020].

28 Para uma cronologia dos acontecimentos da chamada 'Primavera Árabe' ver: History.com Editors (2018), "Arab Spring", disponível em [website] https://www.history.com/topics/middle-east/arab-spring [acedido em 02 de junho de 2020]. Sobre as revoltas no Mediterrâneo Sul e Oriental vistas pelos *media* ocidentais como uma 'Primavera Árabe' e a sua apropriação pelos grupos e partidos islamistas ver: Bradley, John R. (2012), *After the Arab Spring: How Islamists Hijacked The Middle East Revolts*, New York, St. Martin's Press.

29 Fernandes, José Pedro Teixeira (2010), "A Política Externa da Turquia Face a Israel: O Regresso da Ambição Otomana", *Nação e Defesa*, n.º 127, pp. 159-180, disponível em https://comum.rcaap.pt/bitstream/10400.26/4724/1/NeD127_Jos%C3%A9PedroTeixeiraFernandes.pdf [acedido em 02 de junho de 2020].

30 Republic of Turkey/Ministry of Foreign Affairs (2020), *Prof. Dr. Mr. Ahmet Davutoğlu*, disponível em http://www.mfa.gov.tr/ahmet-davutoglu.en.mfa [acedido em 13 de junho de 2020].

31 Traub, James (2011), "Turkey's Rules", *The New York Times Magazine*, 20 de janeiro, disponível em https://www.nytimes.com/2011/01/23/magazine/23davutoglu-t.html?pagewanted=all [acedido em 21 de junho de 2020].

32 Davutoğlu, Ahmet (2001), *Stratejik Derinlik: Türkiye'nin Uluslararası Konumu*, İstanbul, Küre Yayınları.

otomana, mas também mais do que isso, por querer entrar em áreas fora da influência tradicional otomana/turca, deixando o país de ser um Estado periférico do Ocidente. Essa ambição passava por transformar a Turquia numa espécie de novo "centro do mundo" (islâmico) face ao Médio Oriente, aos Balcãs, ao Cáucaso e à Ásia Central, através de uma política de proximidade onde a economia, o comércio a influência cultural turca eram instrumentos privilegiados. Claro que se pode discutir se essa visão grandiosa de Ahmet Davutoğlu não era feita mais para consumo interno de um público turco nostálgico da grandiosidade do império perdido. Em qualquer caso, era uma visão que apontava essencialmente para a prossecução de uma abrangente estratégia de *soft power* (poder suave) no sentido que Joseph Nye Jr.[33] deu ao conceito.

A política externa turca dessa época, com o seu *slogan* de "zero problemas com os vizinhos"[34], impressionava bem a generalidade do mundo exterior. Todavia, essa imagem benigna passou, em relativamente pouco tempo, de "zero problemas a zero amigos"[35]. Foram especialmente os acontecimentos da Primavera Árabe que fizeram implodir a (superficial) imagem benigna de um irresistível *soft power* turco, evidenciado, também, cruamente, as ambições, as limitações e as contradições estratégicas da sua política externa[36]. Mas vários sinais estavam já presentes anteriormente. As situações de Israel, da Síria e do Irão mostravam já o problema. Vale a pena revê-los sucintamente. No caso de Israel, a Turquia cancelou em 2009 o usual convite dirigido a esse Estado para exercícios militares aéreos conjuntos, no qual participavam também os EUA e outros membros da NATO. Ao mesmo tempo, convidou a Síria de Bashar al-Assad para exercícios militares conjuntos, ainda que limitados, e anunciou a criação de um conselho de cooperação estratégica com esse país[37]. Em relação ao Irão, em maio de 2010, a Turquia e o Brasil – que eram nessa altura membros não permanentes do Conselho de Segurança das Nações Unidas –, patrocinaram um acordo sobre o programa nuclear iraniano. Segundo Ahmet Davutoğlu e Recep Tayyip Erdoğan tal permitiria resolver a questão sem necessidade

33 Nye Jr., Joseph S. (2005), "Soft Power: The Means to Success In World Politics", *PublicAffairs*, New York.

34 Republic of Turkey/Ministry of Foreign Affairs (2005), *Policy of Zero Problems with our Neighbors*, disponível em http://www.mfa.gov.tr/ahmet-davutoglu.en.mfa [acedido em 18 de junho de 2020].

35 Zalewski, Piotr (2013), "How Turkey Went From 'Zero Problems' to Zero Friends", *Foreign Policy*, 22 de agosto, disponível em https://foreignpolicy.com/2013/08/22/how-turkey-went-from--zero-problems-to-zero-friends/ [acedido em 22 de junho de 2020].

36 Sobre o que correu mal com a doutrina e política de "zero problemas" com os vizinhos ver também: Kibaroğlu, Mustafa (2012), "What Went Wrong With The 'Zero Problem With Neighbors' Doctrine?", *Turkish Policy Quarterly*, vol. 11, no. 3, pp. 85-93, disponível em http://turkishpolicy.com/files/articlepdf/what-went-wrong-with-the-zero-problem-with-neighbors-doctrine-fall-2012-en.pdf [acedido em 28 de junho de 2020].

37 Fernandes, José Pedro Teixeira (2010), "A Política Externa da Turquia Face a Israel: O Regresso da Ambição Otomana", *Nação e Defesa*, n.º 127, p. 170, disponível em https://comum.rcaap.pt/bitstream/10400.26/4724/1/NeD127_Jos%C3%A9PedroTeixeiraFernandes.pdf [acedido em 02 de junho de 2020].

de aplicação de mais sanções pelo Conselho de Segurança. Apesar de inconsequente, pois não foi validado pelo Conselho de Segurança, a atitude da Turquia foi reveladora da sua ambição e dos problemas estratégicos que daí resultavam. A iniciativa diplomática foi desenvolvida à margem dos seus aliados euro-atlânticos, para os quais essa era também uma questão de primeira grandeza[38]. Assim, o desencadear da Primavera Árabe – especialmente a guerra civil na Síria[39], iniciada em 2011 para tentar afastar Bashar al-Assad do poder; e a revolta no Egipto, que permitiu à Irmandade Muçulmana e a Mohamed Morsi chegarem ao poder governamental, sendo este último posteriormente deposto pelo exército em 2013, numa ação chefiada por Abdul Fatah al-Sisi –, obrigaram a Turquia a escolher campos. A Turquia posicionou-se ostensivamente no campo anti-Assad[40], na Síria, e pró-Irmandade Muçulmana/Mohammed Morsi[41], no Egipto. O resultado foi não apenas o colapso da política de "zero problemas com os vizinhos", como tornar demasiado evidente uma ambição neo-otomana de poder associada a uma nova dimensão ideológica da política externa, com simpatias pró-islamistas.

Em termos histórico-políticos levanta-se aqui uma possibilidade de leitura mais abrangente das transformações ocorridas na Turquia, no Médio Oriente e Mediterrâneo Oriental, a qual vai para além dos acontecimentos da Primavera Árabe – uma designação cunhada por analogia com a Primavera dos Povos, as revoluções de 1848[42] na Europa. Essa possível leitura é estarmos a assistir a um reemergir, ainda que sob outras formas, daquilo que na história diplomática europeia do século XIX e inícios do século XX se designava como a Questão do Oriente[43]. Na realidade, é

38 Fernandes, José Pedro Teixeira (2010), "A Política Externa da Turquia Face a Israel: O Regresso da Ambição Otomana", *Nação e Defesa*, n.º 127, pp. 170-171, disponível em https://comum.rcaap.pt/bitstream/10400.26/4724/1/NeD127_Jos%C3%A9PedroTeixeiraFernandes.pdf [acedido em 02 de junho de 2020].

39 Council on Foreign Relations/Global Conflict Tracker (2020), *Civil War in Syria*, disponível em https://www.cfr.org/global-conflict-tracker/conflict/civil-war-syria [acedido em 29 de junho de 2020].

40 Arsu, Sebnem (2011), "Turkish Premier Urges Assad to Quit in Syria", *The New York Times*, 22 de novembro, disponível em https://www.nytimes.com/2011/11/23/world/middleeast/turkish-leader-says-syrian-president-should-quit.html [acedido em 05 de junho de 2020].

41 Republic of Turkey/Ministry of Foreign Affairs (2013), *Press Statement by H.E. Mr. Ahmet Davutoglu, Minister of Foreign Affairs of the Republic of Turkey on the Latest Developments in Egypt, 4 July 2013, Istanbul*, disponível em http://www.mfa.gov.tr/press-statement-by-h_e_-mr_-ahmet-davutoglu_-minister-of-foreign-affairs-of-the-republic-of-turkey-on-the-latest-developments-in-egypt_-4-july-2013_-istanbul.en.mfa [acedido em 09 de junho de 2020].

42 Editors of Encyclopædia Britannica (2020), "Revolutions of 1848", *Encyclopædia Britannica*, May 12, disponível em https://www.britannica.com/event/Revolutions-of-1848 [acedido em 21 de junho de 2020].

43 Foi um longo período histórico cheio de conflitos sangrentos cujos marcos convencionais são o tratado entre a Rússia e o Império Otomano de 1774, após a derrota deste último – Tratado de Küçük-Kaijnardja, na atual Bulgária; e o Tratado de Lausana, na Suíça, em 1923, sobre a dissolução do Império Otomano e a emergência da Turquia moderna. Para uma panorâmica das sucessivas crises que marcaram a questão do Oriente ver: Macfie, A. L. (1996), *The Eastern Question 1774-1923*, 2 ed., London-New York, Routledge.

observável que hoje as áreas de maior turbulência geopolítica na proximidade Sul/Sudeste da União Europeia, ou até já no seu interior – caso dos Balcãs incluindo aí a Grécia e Chipre –, mas também a Síria, o Líbano, Iraque, Israel/Palestina e Líbia –, têm todas um ponto de contacto histórico-político comum: são territórios do antigo Império Otomano onde há sequelas significativas desse passado. A ser assim, estamos perante o que pode ser designado como uma nova Questão do Oriente[44]. Esta não é agora marcada pelos problemas de um império territorialmente em retrocesso – o "homem doente da Europa", como ocorreu no século XIX, mas de uma ambiciosa Turquia em ascensão em termos políticos, económicos e militares – e em processo de religação cultural e política ao seu passado islâmico-otomano.

Para além desta possível leitura histórico-política dos acontecimentos do presente, uma outra questão relevante que aqui se coloca é a de saber que influência concreta tiveram as transformações políticas internas da Turquia, ocorridas durante a era Erdoğan na (re)configuração da política externa[45]. O seu partido – o AKP – foi durante muito tempo visto na Europa e Ocidente como uma espécie de partido democrata-islâmico, ou seja, uma normal força política conservadora de centro-direita que participava no jogo democrático liberal-pluralista. Na realidade, há uma outra leitura[46] que emerge da complexa história política do país, menos benigna e menos tranquilizadora. Está relacionada com as marcas deixadas pela forma autoritária como a República da Turquia foi construída nos anos 1920 e 1930 por Mustafa Kemal Atatürk e o seu círculo próximo – incluindo a curiosa figura de Latife Hanım[47], uma feminista *avant la lettre* –, através de múltiplas transformações culturais e políticas radicais para a época. Ganhou raízes nos setores da sociedade ligados ao funcionamento do Estado – o exército, os tribunais, as universidades públicas, a máquina burocrática-

44 Fernandes, José Pedro Teixeira (2020), "A nova 'Questão do Oriente': refugiados, gás natural e imperialismo neo-otomano", *Público*, 8 de março, disponível em https://www.publico.pt/2020/03/08/mundo/opiniao/nova-questao-oriente-refugiados-gas-natural-imperialismo-neootomano-1906860 [acedido em 23 de junho de 2020].

45 Na comunidade académico-científica portuguesa das Relações Internacionais a questão das transformações da Turquia e do seu impacto na geopolítica do Médio Oriente tem também suscitado algum interesse. Entre outros trabalhos, ver os de: Arena, Maria do Céu Pinto (2019), "A reconfiguração dos equilíbrios do poder no Médio Oriente", em Pavia, José Francisco e Monteiro, Manuel, coord., *Estudos de Relações Internacionais*, Lisboa, Universidade Lusíada Editora; e o de Kumru F. Toktamis e Isabel David, eds., (2018), "Critical Crossroads: Erdoğan and the Transformation of Turkey", Special Issue *Mediterranean Quarterly*, 29(3).

46 Naturalmente que há ainda outras leituras possíveis. Numa perspetiva fundamentalmente marxista, uma outra curiosa leitura da história da Turquia – e também sobre o papel de Mustafa Kemal Atatürk – é feita por Karaveli, Halil (2018), *Why Turkey is Authoritarian*, London, Pluto Press.

47 Sobre Latife Hanım, que foi casada com Mustafa Kemal Atatürk entre 1923-1925 e o influenciou em várias medidas de emancipação feminina, ver: Çalışlar, İpek (2013), *Madam Atatürk. A Biography*, trad. inglesa, London, Saqui Books.

-administrativa. Mas os seus valores nunca penetraram na massa populacional fora de grandes cidades, impregnada de valores islâmicos conservadores, sendo essa base mais sólida de apoio do AKP e a maioria da população. A roupagem democrática-liberal usada por Recep Tayyip Erdoğan nos seus primeiros tempos no poder foi-lhe muito útil. Tal como foi o processo de negociações de adesão à União Europeia, mas não exatamente da maneira que muitos europeus pensavam. Erdoğan atacou as formas de funcionamento instituídas no Estado turco por Atatürk e os seus continuadores, acusando-as de serem não democráticas. A crítica era certeira pelo autoritarismo[48] que impregna o Estado desde a sua fundação – que entronca, por sua vez, no autoritarismo do Império Otomano –, mas essa nunca foi a história toda[49]. É verdade que a aproximação à União Europeia permitiu a eliminação de disposições da Constituição de 1982[50] – e de legislação restritiva dos direitos políticos e religiosos – merecedoras de objeções democráticas. Mas esses dispositivos eram também alicerces do secularismo pelo que tais transformações teriam sempre um duplo resultado – democratização e dessecularização. Assim, as transformações internas terão sido mais uma democratização instrumental[51] com vista à dessecularização do Estado e a abrir a porta ao autoritarismo conservador-religioso e pró-islamista.

A ser assim, explica também, pelo menos em parte, a (re)configuração da política externa da Turquia no Médio Oriente, abertamente pró-Irmandade Muçulmana[52] e anti Abdul Fatah al-Sisi (Egipto)[53] e a vontade de afastamento de Bashar al-Assad (Síria) do poder. Quanto a este último caso, e para além das responsabilidades do

48 Sobre o autoritarismo que impregna o Estado turco e apresentando uma leitura interessante sobre as suas razões mais profundas, que entroncam também no passado otomano ver: Karaveli, Halil (2018), *Why Turkey is Authoritarian*, London, Pluto Press.

49 Cheviron, Nicolas e Pérouse, Jean-François (2016), *Erdoğan: Nouveau Père de la Turquie?* Paris, François Bourin Editions, em particular a 4.ª parte "Consolidation" e o capítulo 7 "Les oppositions neutralisées".

50 A Constituição de 1982 foi resultado do golpe militar de 1980, sendo feita sob tutela militar, ainda que aprovada posteriormente por referendo. Já foi emendada 17 vezes, a última das quais em 2017, permitindo, entre outras modificações, ao reconfigurar a função presidencial, a continuidade no poder como presidente da república de Recep Tayyip Erdoğan. Ver também: The Grand National Assembly of Turkey (2019), *Sources of Parliamentary Law*, disponível em https://global.tbmm.gov.tr/index.php/EN/yd/icerik/39 [acedido em 07 de junho de 2020].

51 Similar interpretação da ação política interna de Recep Tayyip Erdoğan foi efetuada em: Cheviron, Nicolas e Pérouse, Jean-François (2016), *Erdoğan: Nouveau Père de la Turquie?* Paris, François Bourin Editions.

52 Gurpinar, Bulut (2015), "Turkey and the Muslim Brotherhood: Crossing Roads in Syria". *Eurasian Journal of Social Sciences*, 3(4), pp. 22-36, disponível em DOI: 10.15604/ejss.2015.03.04.003 [acedido em 17 de junho de 2020].

53 Bozkurt, Abdullah (2020), "Erdoğan government believed Muslim Brotherhood would make a huge comeback in Egypt in few years", *Nordic Monitor*, 2 de abril, disponível em https://www.nordicmonitor.com/2020/04/erdogan-government-believed-muslim-brotherhood-would-make-a-huge-comeback-in-egypt-in-few-years/ [acedido em 12 de junho de 2020].

próprio Bashar al-Assad na deterioração das relações entre ambos os países, existiu um cálculo estratégico da Turquia de ganhos em derrubar o Governo sírio. A chegada ao poder da maioria árabe sunita da população – na qual a Irmandade Muçulmana, que Erdoğan apoia, dispõe de significativa influência – instalaria um Estado amistoso subordinado à influência religioso-política da Turquia. Não é o que ocorre com Bashar al-Assad, que é oriundo da minoria alauita, próxima do xiismo e aberta à influência do Irão.

4. Aliados Desavindos: as Divergências da Turquia com a NATO e a União Europeia

A tentativa de golpe de Estado ocorrida de 15 para 16 de julho de 2016 na Turquia, ainda hoje pouco clara nos seus contornos, acelerou as tendências anteriores. A ação terá tido origem em divergências entre Recep Tayyip Erdoğan e os seus antigos aliados, afetos a Fethullah Gülen, tendo estes últimos tentado afastá-lo do poder pela força. O Movimento Gülen, com milhões de seguidores dentro e fora da Turquia, ocupava importantes posições, não só no ensino – a sua base de influência tradicional –, como em diversas áreas do Estado – forças de segurança, magistraturas, etc. –, foi em seguida alvo de uma purga e inúmeras perseguições[54].
Na política externa ocorreu uma viragem face à Guerra da Síria, emergindo uma surpreendente *entente cordiale* entre Recep Tayyip Erdoğan e Vladimir Putin. Este reposicionamento estratégico da Turquia foi provavelmente para Erdoğan o resultado de uma dupla frustração. A primeira ligada ao falhanço do seu objetivo inicial de afastar Bashar al-Assad do poder e ganhar uma influência decisiva na Síria, com a Rússia a mostrar-se um obstáculo intransponível a partir da sua intervenção militar em finais de 2015, ao lado das forças de Bashar al-Assad (e do Irão). A segunda frustração ligada aos aliados euro-atlânticos e à sua falta de vontade de envolvimento na Guerra da Síria, acrescida da constatação, após a tentativa falhada de golpe de Estado de 2016, de que não se importariam muito se tivesse sido afastado do poder. A acrescer a isso, há ainda a recusa reiterada dos EUA de extraditarem[55] Fethullah Gülen, que vive em território norte-americano e que o governo da Turquia quer julgar nos seus tribunais.
Se a clivagem da Turquia com os seus aliados se tornou muito visível a partir de 2016, durante o ano de 2019 e inícios de 2020 os desentendimentos acentuaram-se, especialmente devido à questão curda, agora em território da Síria. Ainda em 2018 a Turquia

54 Sobre a tentativa de golpe de Estado de 2016 e suas consequências na política e sociedade turcas ver: Christofis, Nikos, ed., (2019), *Erdoğan's 'New' Turkey: Attempted Coup d'état and the Acceleration of Political Crisis*, London-New York, Routledge.

55 "America rejects plans to extradite Gülen for US preacher held in Turkey", *Middle East Eye*, 21 de julho de 2018, disponível em https://www.middleeasteye.net/news/america-rejects-plans-extradite-gulen-us-preacher-held-turkey [acedido em 07 de junho de 2020].

tinha já efetuado uma intervenção militar em Afrin[56] – a operação "ramo de oliveira" –, cujo objetivo seria expulsar dessa área, a noroeste de Alepo, as forças curdas das Yekîneyên Parastina Gel – YPG, Unidades de Proteção Popular – qualificadas como uma ramificação "terrorista" do PKK turco. Para além disso, o outro objetivo seria combater os membros do Daesh – acrónimo árabe de Estado Islâmico do Iraque e do Levante – nessa região próxima da fronteira da Turquia. Uma análise atenta mostra, todavia, que o Daesh e outros grupos islamistas-jihadistas não são o maior problema da Turquia na Guerra da Síria. Pelo contrário, foram vistos, pelo menos até certo ponto, como taticamente úteis para travar uma guerra por procuração contra os curdos e o governo de Bashar al-Assad. A calculista inércia turca na altura do cerco de Kobani[57], em 2014 e 2015, quando o Daesh estava em expansão no Iraque e na Síria e massacrava indiscriminadamente as populações civis, não deixa grandes dúvidas. Evidenciou uma divergência profunda da Turquia face aos seus aliados euro-atlânticos que viam com simpatia a causa curda – com a sua ambição maior autonomia ou mesmo independência –, e procuraram apoiar, ainda que de forma limitada, os curdos na sua resistência contra o Daesh.
Em outubro de 2019 ocorreu uma nova incursão militar das forças turcas e seus aliados no Norte da Síria, numa outra zona histórica de populações curdas. Esta nova operação militar, tal como a do ano anterior em Afrin, foi apresentada como uma operação de *peacekeeping* – a operação "fonte da paz" –, tendo como alvo a província síria de al-Raqqa, no Norte/Nordeste da Síria. A teórica operação de *peacekeeping* teve na realidade dois outros objetivos político-estratégicos[58]. Um primeiro foi impedir a formação de um Estado curdo autónomo *de facto* encostado à sua fronteira Sul, onde as YPG curdas teriam necessariamente um papel importante. O segundo objetivo foi procurar uma solução para os problemas levantados pelos refugiados sírios na Turquia. Essas operações militares mostram uma obsessão turca com os curdos, dentro e fora das suas fronteiras. Em parte, a explicação é de natureza geopolítica. Como já referido anteriormente, na Turquia existe uma substancial população de etnia curda, a qual historicamente habita o Leste e Sudeste do país. Ao mesmo tempo, as populações curdas[59] têm continuidade nas zonas fronteiriças da Síria, Iraque e Irão. Há ainda, como já anteriormente referido, o antecedente da sublevação armada do PKK nos anos 1980, à

56 "Turkish forces and Free Syrian Army capture Afrin city", *Al Jazeera*, 18 de março de 2018, disponível em https://www.aljazeera.com/news/2018/03/18/turkish-forces-and-free-syrian-army-capture-afrin-city/ [acedido em 09 de junho de 2020].

57 Cecire, Michael (2014), "Strategic Cynicism in Kobani", *Carnegie Moscow Center*, 10 de outubro, disponível em https://carnegie.ru/commentary/57075 [acedido em 02 de junho de 2020].

58 Erkmen, Serhat (2020), "Operation Peace Spring: Objectives, Current Situation and its Future", *Discussion Paper (2)*, April 2020. Syria Transition Challenges Project, The Geneva Centre for Security Policy (GCSP), disponível em https://dam.gcsp.ch/files/doc/discussion-paper-syria-transition-challenges-project-2 [acedido em 27 de junho de 2020].

59 Sobre os curdos da Síria ver: Allsopp, Harriet e Wilgenburg, Wladimir van (2019), *The Kurds of Northern Syria: Governance, Diversity and Conflicts*, London-New York, I. B. Tauris.

qual o exército turco respondeu com uma violenta repressão num conflito que provocou dezenas de milhares de vítimas e deixou muitas feridas sociais e políticas.

Mas Recep Tayyip Erdoğan faz mais do que ignorar as advertências dos seus aliados da NATO – em especial dos europeus – para não intervir militarmente. Num virulento discurso efetuado para os seus partidários ameaçou a União Europeia afirmando que "se tentarem descrever a nossa operação como uma invasão faremos o que é mais fácil para nós: abriremos as portas e enviaremos 3,6 milhões de refugiados"[60]. Para além da questão curda e do problema dos refugiados da Guerra da Síria, um dos pontos mais delicados é a já referida aproximação, ainda que efetuada num jogo de conveniências tático, da Turquia à Rússia. Essa aproximação teve um novo desenvolvimento crítico durante o ano de 2019. A Turquia decidiu adquirir material militar sofisticado à Rússia – os mísseis antiaéreos S-400[61] –, provavelmente mais do que para reforçar as suas defesas, como forma de manter a Rússia do seu lado no conflito da Síria, sinalizando que se poderia tornar um cliente da sua indústria de armamento. Também neste passo (muito) pouco compreensível para um membro da NATO, a Turquia ignorou as objeções dos EUA e dos seus aliados. Ao mesmo tempo, pretendia continuar a beneficiar do mais sofisticado material norte-americano, como os aviões Lockheed Martin F-35 Lightning II, acabando por ser afastada pelo Governo dos EUA desse programa militar-tecnológico[62].

Apesar do "jogo duplo" da Turquia, a relação com a Rússia não é fácil, desde logo porque os objetivos estratégicos dos dois países só (muito) superficialmente convergem. A Turquia quer ganhar, o mais possível, influência na Síria à custa dos curdos e do Governo de Bashar al-Assad. A Rússia tem condescendido com a Turquia em incursões limitadas nas zonas fronteiriças, à custa dos curdos, mas está empenhada – tal como Irão – em manter Bashar al-Assad no poder e em que este volte a ter um controlo total do território sírio. Com a província do Idblid a tornar-se o último bastião territorial dos combatentes que procuravam derrubar Bashar al-Assad, alguns atuando sob proteção *de facto* turca, os riscos de colisão aumentaram. Um confronto[63], ainda que

60 "Turkey's Erdogan threatens to send Syrian refugees to Europe", *Reuters*, 10 de outubro de 2019, disponível em https://www.reuters.com/article/us-syria-security-turkey-europe/turkeys-erdogan-threatens-to-send-syrian-refugees-to-europe-idUSKBN1WP1ED [acedido em 24 de junho de 2020].

61 Kasapoglu, Can (2020), "Turkey's Critical 'S-400 Moment' Has Arrived", *Eurasia Daily Monitor*, 17(61),The Jamestown Foundation, 4 de maio, disponível em https://jamestown.org/program/turkeys-critical-s-400-moment-has-arrived/ [acedido em 14 de junho de 2020].

62 Mehta, Aaron (2019), "Turkey officially kicked out of F-35 program, costing US half a billion dollars", *Defense News*, 17 de julho, disponível em https://www.defensenews.com/air/2019/07/17/turkey-officially-kicked-out-of-f-35-program/ [acedido em 08 de junho de 2020].

63 *Al Jazeera* (2020), "33 Turkish soldiers killed in Syrian air raid in Idlib", 28 de fevereiro, disponível em https://www.aljazeera.com/news/2018/03/free-syrian-army-group-captures-afrin-city-180318081430817.html [acedido em 24 de junho de 2020].

limitado, entre forças militares turcas e forças governamentais sírias, ocorreu em finais de fevereiro de 2020. A situação tornou-se perigosa pois, no pior cenário, há o risco de levar a um confronto militar direto entre a Turquia e a Rússia no território da Síria. Face a esse risco, a Turquia virou-se novamente para os seus aliados euro-atlânticos – pedindo uma reunião de emergência da NATO para analisar o assunto –, aparentemente reapreciando o valor da garantia[64] do artigo 5.º do Tratado do Atlântico Norte.

Para além da Síria, agora na Líbia, as tensões da Turquia com os seus aliados tiveram um novo episódio em junho de 2020. Neste caso, foi com um navio da marinha francesa[65] que participava numa missão da NATO – a Operação *Sea Guardian*[66] – que terá sido objeto de uma ação agressiva por parte de fragatas turcas quando procurava controlar um navio cargueiro (também turco) suspeito de violar o embargo de armas com destino à Líbia, versão negada pela Turquia. Como resultado, a França pediu um inquérito à NATO e suspendeu a sua participação nessa operação[67]. No cerne do conflito estão os apoios a fações opostas[68] da guerra na Líbia – o governo da unidade nacional de Fayez al-Sarraj, reconhecido pela ONU e apoiado política e militarmente pela Turquia, bem como pelo Qatar e pela Itália. No outro campo está o Exército Nacional da Líbia, nascido da fusão de várias tribos e grupos militares, chefiado pelo marechal Khalifa Haftar, apoiado pelo Egipto, Emirados Árabes Unidos, Rússia e também pela França.

Por último, a acrescer a toda esta complexidade geopolítica está agora o gás natural. Há importantes reservas descobertas no subsolo marítimo do Mediterrâneo Oriental, ao largo das costas de Israel/Palestina, Egipto, Líbano, Síria, Chipre e Turquia. A zona principal em exploração está entre Israel e Chipre e sua exploração está a ter impacto económico e geopolítico. Já provocou um realinhamento estratégico[69] entre Chipre, a Grécia e Israel, ao qual se junta ainda o Egipto. No outro campo está a Tur-

64 NATO (2019), *The North Atlantic Treaty*, Washington D.C., 4 April 1949, disponível em https://www.nato.int/cps/en/natolive/official_texts_17120.htm [acedido em 12 de junho de 2020].

65 Billion, Didier (2020), "Que révèlent les tensions franco-turques en Libye?", *Institut de Relations Internationales et Stratégiques*, 19 de junho, disponível em https://www.iris-france.org/147989-que-revelent-les-tensions-franco-turques-en-libye/ [acedido em 06 de junho de 2020].

66 NATO (2020), *Operation Sea Guardian*, disponível em https://mc.nato.int/missions/operation-sea-guardian [acedido em 24 de junho de 2020].

67 "La France suspend sa participation à une opération de l'OTAN en Méditerranée après des tensions avec la Turquie", *Le Monde*, 1 de julho de 2020, disponível em https://www.lemonde.fr/international/article/2020/07/01/la-france-suspend-sa-participation-a-une-operation-de-l-otan-en-mediterranee-apres-des-tensions-avec-la-turquie_6044849_3210.html [acedido em 07 de junho de 2020].

68 Robinson, Kali (2010), "Who's Who in Libya's War?", *Council on Foreign Relations*, 18 de junho, disponível em https://www.cfr.org/in-brief/whos-who-libyas-war [acedido em 02 de junho de 2020].

69 Aydıntaşbaş, Asli, *et al*. (2020), "Deep Sea rivals: Europe, Turkey and New Eastern Mediterranean conflict lines", *European Council on Foreign Relations*, maio, disponível em https://www.ecfr.eu/special/eastern_med [acedido em 03 de junho de 2020].

quia, em disputa territorial com Chipre – ocupa militarmente a parte Norte da ilha desde 1974[70] – e agora reclama também, através do Estado por si criado – a República Turca de Chipre do Norte, sem reconhecimento internacional –, uma zona económica exclusiva[71]. Com algum interesse convergente com a Turquia está a Rússia. Pretende, o mais possível, continuar com o seu monopólio de abastecimento à Europa de Leste e Central, não estando interessada em novos fornecedores, nem em gasodutos pelo Sul da Europa e Mediterrâneo. O problema projeta-se no interior da própria União Europeia. Há dois Estados-membros (a Grécia e Chipre), ao qual se junta um terceiro, a Itália, a explorarem esse gás natural. E um Estado candidato à adesão – a Turquia – a tentar impedi-la, incluindo com recurso à pressão militar.

Conclusões

A análise anteriormente efetuada sugere a possibilidade de estarmos a assistir a um reemergir, ainda que sob outras formas, daquilo que na história diplomática europeia do século XIX se designava como a "Questão do Oriente". Como anteriormente notado, hoje as áreas de maior turbulência geopolítica na proximidade do Sul/Sudeste da União Europeia têm um traço histórico-político comum: são territórios do antigo Império Otomano. A ser assim, estamos perante o que pode ser designado como uma nova Questão do Oriente. Agora não são os problemas de um império em retrocesso, como no século XIX, mas de uma ambiciosa Turquia em ascensão e em processo de religação cultural e política ao seu passado islâmico-otomano. As ambições neo-otomanas da Turquia atual, procurando reconstituir uma esfera de influência nos territórios perdidos do império, ligam-se de forma intrincada com a crise dos migrantes/refugiados da guerra na Síria e as descobertas de gás natural no Mediterrâneo Oriental. Mas esta leitura à luz do passado da Europa, nas suas relações com o Império Otomano/Turquia, necessita de aprofundamento pelo que fica aqui uma pista para investigação futura.

Uma outra faceta importante da transformação ocorrida na Turquia durante a era Erdoğan está ligada ao facto de as mudanças terem ocorrido em paralelo ao processo de adesão do país à União Europeia. Entre os vários efeitos que daí resultaram, as negociações de adesão levaram à eliminação de legislação restritiva dos direitos políticos e religiosos e outros direitos fundamentais na Turquia, o que trouxe uma melhoria democrática para o país. Por princípio, tais mudanças deveriam funcionar

70 Fernandes, José Pedro Teixeira (2008), *A Questão de Chipre: Implicações para a União Europeia e a Adesão da Turquia*, Coimbra, Almedina.

71 Sobre o conceito legal de Zona Económica Exclusiva (ZEE), ver: United Nations (2020), *United Nations Convention on the Law of the Sea,* disponível em https://www.un.org/Depts/los/convention_agreements/texts/unclos/part6.htm [acedido em 08 de junho de 2020].

como mais um fator de aproximação aos seus aliados euro-atlânticos. Mas a Turquia é mais complexa do que muitos no Ocidente imaginam e tais transformações tiveram um duplo resultado – democratização e dessecularização. Uma leitura possível é que as modificações internas efetuadas por Recep Tayyip Erdoğan não foram usadas para uma genuína democratização da Turquia, como era a expetativa europeia, mas para uma democratização instrumental, com vista à dessecularização do Estado e a abrir caminho a um autoritarismo conservador-religioso. Seja como for, acabaram, na prática, por ter um efeito quase contrário – em vez de aproximarem, originaram atritos sobretudo com a União Europeia – o que se projetou na área da política externa. Aí emergiu uma nova ambição na Turquia que é neo-otomana, mas também mais do que isso, ao ambicionar chegar a áreas do mundo fora da influência tradicional otomana/turca, deixando a Turquia de ser um Estado periférico do Ocidente e do seu sistema de segurança euro-atlântico. A ambição levou a dar nova centralidade ao Médio Oriente, aos Balcãs, ao Cáucaso e à Ásia Central, através de uma política de proximidade onde a economia, o comércio e a influência cultural-religiosa eram privilegiados.

Quanto à imagem benigna de uma política externa neo-otomana de "zero problemas com os vizinhos" ruiu gradualmente após os acontecimentos da Primavera Árabe em 2011. A partir dessa altura a Turquia começou a colidir, por vezes de maneira ostensiva, como os seus aliados euro-atlânticos. A Guerra da Síria e a questão curda formam os acontecimentos que mais projetaram divergências e tensões no sistema de segurança euro-atlântico. A atitude da Turquia em 2014 – quando os islamistas-jihadistas do Daesh massacravam indiscriminadamente populações civis na Síria e cercaram a cidade de Kobani junto à sua fronteira –, ficando o exército turco a ver o que se passava, teve um enorme impacto negativo no Ocidente. A clivagem com os aliados euro-atlânticos acentuou-se após falhada tentativa de golpe de Estado de 2016. Nesse contexto, Recep Tayyip Erdoğan aproximou-se da Rússia de Vladimir Putin, que lhe frustrara o objetivo inicial de afastar Bashar al-Assad do poder. Com este volte-face, vingava-se da falta de vontade dos aliados euro-atlânticos de envolvimento na Guerra da Síria.

O conflito de objetivos de política externa entre a Turquia e os seu aliados euro-atlânticos acentuou-se, ainda mais, durante o ano de 2019 e inícios de 2020. O caso dos mísseis antiaéreos russos S-400 é bem exemplificativo do mal-estar instalado. Todavia, aspeto relevante, o retardamento da ativação desse sistema de defesa antiaéreo em mais de um ano – feito em cima das eleições presidenciais norte-americanas –, sugere um jogo estratégico calculado com a Rússia e os EUA/NATO, provavelmente para a Turquia se mostrar mais independente em matéria de defesa e/ou obter concessões políticas destes últimos.

Este "jogo duplo" que a Turquia tem efetuado com a NATO/EUA (e União Europeia) e com a Rússia é, sem dúvida, problemático para a segurança e defesa euro-

-atlântica. No entanto, é necessário ter também em conta que o pôr em causa da segurança euro-atlântica tem limites para a própria Turquia. Estes decorrem, desde logo, da sua posição de inferioridade face à Rússia. Como já notado, os objetivos estratégicos dos dois países só superficialmente convergem. Na Síria, a Turquia quer ganhar, o mais possível, influência à custa dos curdos e do Governo de Bashar al-Assad. A Rússia condescende com a Turquia em incursões limitadas nas zonas fronteiriças, à custa dos curdos. Todavia, está empenhada, tal como Irão, em manter Bashar al-Assad no poder e em que este volte a ter controlo do território sírio. No limite, este conflito de objetivos coloca a Turquia em colisão com a Rússia, cenário que não é meramente teórico como se viu em fevereiro de 2020 no Idlib.

Por último, importa reconhecer que a conflitualidade e belicosidade da Turquia face a alguns dos seus aliados euro-atlânticos – não é apenas o caso clássico da Grécia, país com o qual tem um bem conhecido contencioso histórico, nem do já antigo conflito de Chipre que não sendo membro da NATO, é membro da União Europeia – levanta muitas incógnitas sobre o seu valor efetivo como aliado político-militar. Paradoxalmente, hoje a situação da Turquia dentro da NATO começa a assemelhar-se demasiado à sua relação de fora, com a União Europeia, cheia de desentendimentos e atritos nas negociações de adesão. Há quinze anos a Turquia parecia ser um membro confiável de grande valor estratégico da NATO e também um futuro membro e mais-valia da União Europeia. Hoje, a hipótese da sua adesão à União Europeia parece mais remota do que nunca e há cada vez mais dúvidas, em muitos dos seus parceiros, sobre o que vale efetivamente na NATO como aliado político-militar. Mas é preciso também não esquecer que há uma mais-valia intrínseca estratégica da Turquia, a qual decorre, mesmo sem ter um conta outras dimensões da questão, da sua própria localização geográfica encostada ao Sudeste europeu e na intersecção com o Médio Oriente e o flanco Sul da Rússia. Para além disso, a Turquia não é assim tão poderosa para se emancipar facilmente da NATO e da própria União Europeia, sem ficar na dependência estratégica de outros – desde logo da Rússia. Se o fosse, eventualmente já teria seguido esse caminho. Mas ficar na dependência da Rússia é certamente algo que a Turquia também não quer, pelo elevado preço político e de segurança que teria de suportar. Assim, uma rotura com sistema de segurança euro-atlântico – ou a ideia extrema da sua expulsão, a qual nem sequer está prevista na NATO – é improvável no horizonte temporal discernível. Todavia, isso não significa que os aliados euro-atlânticos não se devam preparar estrategicamente para um cenário que, por analogia com o passado, designamos como a nova Questão do Oriente, marcado por crises e tensões políticas ligadas à nova Turquia da era Erdoğan. Mas esse é um tema que precisará de aprofundamento em investigações futuras.

A Agenda Mulheres, Paz e Segurança: Um Olhar sobre as Forças de Segurança

Fernando Bessa
Coronel da Guarda Nacional Republicana. Licenciado em Sociologia e Planeamento, Mestre em Organização do Trabalho e da Empresa e Doutor em Sociologia pelo ISCTE- IUL. Investigador no Centro de Investigação e Estudos de Sociologia e no Centro de Investigação e Desenvolvimento do Instituto Universitário Militar. Desempenhou várias missões em operações de paz.

Luís Malheiro
Capitão da Guarda Nacional Republicana a desempenhar funções na Academia Militar. Doutorado em Políticas Públicas pelo ISCTE-IUL e Mestre pela Academia Militar. Investigador no Centro de Investigação e Desenvolvimento do Instituto Universitário Militar e no Centro de Investigação, Desenvolvimento e Inovação da Academia Militar.

Resumo

No vigésimo aniversário da agenda Mulheres, Paz e Segurança (Resolução 1325 (2000) do Conselho de Segurança das Nações Unidas), apesar do progresso registado, ainda persistem barreiras à sua total implementação. Portugal não sendo exceção, é recomendável, e oportuno, que reforce o desempenho para a participação integradora das mulheres na paz e segurança internacionais, especialmente no espetro de ação das forças de segurança.
O artigo, com base no conceito de política pública, recorre a um inquérito por questionário aplicado a um universo de 288 cadetes das duas forças de segurança (GNR e PSP). O artigo sugere que o resultado deste inquérito pode reforçar a noção da necessidade de implementação da agenda neste setor, fornecer recomendações para a próxima década sobre a vantagem integradora das mulheres no domínio da paz e da segurança e contribuir para o desenvolvimento de sociedades mais pacíficas, justas e inclusivas.

Palavras-chave: Mulheres; Paz; Segurança; Segurança; Resolução 1325; Nações Unidas; Portugal.

Abstract
The Women, Peace and Security Agenda: a Look at the Security Forces

On the twentieth anniversary of the Women, Peace and Security agenda (United Nations Security Council Resolution 1325 (2000)), barriers to its full implementation persist, despite the progress made. Portugal is no exception. It is recommended and opportune, that the country reinforces the inclusive participation of women in international peace and security, especially in the security forces' realm of action.
The article, based on the concept of public policy, uses a questionnaire survey applied to a universe of 288 cadets from the two security forces (GNR and PSP). The article suggests that the findings of this survey may reinforce the understanding of the need to implement the agenda in this sector, provide recommendations for the next decade on the integrative advantage of women in the field of peace and security, and contribute to the development of more peaceful, fair and inclusive societies.

Keywords: *Women; Peace; Security; Safety; Resolution 1325; United Nations; Portugal.*

Artigo recebido: 26.05.2020
Aprovado: 19.06.2020
https://doi.org/10.47906/ND2020.156.05

Introdução

É comummente aceite que, historicamente, os processos políticos de mediação da paz foram sempre conduzidos por elites políticas e militares exclusivamente masculinas. Somente na década de 90 é que as mulheres começaram a desempenhar papéis/funções transversais no seio das Nações Unidas e foi necessário esperar até ao final do milénio para que o Conselho de Segurança assumisse que são determinantes nos processos de prevenção de conflitos e na construção da paz (United Nations, 2000 e 2015a).

A Resolução n.º 1325/2000 de 31 de outubro, do Conselho de Segurança das Nações Unidas (CSNU) foi pioneira e teve o mérito de exortar os Estados-membros a promoverem o papel das mulheres em todos os esforços de promoção da paz e da segurança, com a criação da denominada agenda Mulheres, Paz e Segurança (MPS) (CSNU, 2000). No entanto, o vigésimo aniversário da agenda não deverá ser aproveitado unicamente para enfatizar os progressos registados! Esta janela de oportunidade, recentemente reconhecida pela Resolução 2493/2019 (CSNU, 2019), deverá assumir-se como uma plataforma de lançamento de novos esforços de implementação, de melhoria da sua monitorização e de coordenação/cooperação entre atores.

As avaliações internacionais de largo espetro sugerem que as principais limitações da agenda estão ligadas à falta de progressos consolidados, ao não comprometimento dos atores, à inexistência de recursos e a uma monitorização administrativo-burocrática dos planos de ação (United Nations, 2015). As avaliações nacionais, por seu lado, ainda identificam dificuldades na atomização dos objetivos estratégicos em táticas eficientes, ao que ainda acrescem limitações na mensuração da execução (Equipa de Avaliação Externa do II Plano, 2018).

Deste modo, se Portugal almejar uma plena implementação da agenda terá de alavancar o desempenho neste campo de elevada relevância para a participação integradora das mulheres na paz e segurança internacionais, especialmente em áreas cujo impacto é significativo, devido aos atrasos que subsistem ou pelo universo que abrange, este reforço de atenção é fundamental.

Estamos convictos de que o setor da segurança é merecedor desse cuidado redobrado e renovado. Os dados disponibilizados pela Direção-Geral da Administração e do Emprego Público (DGAEP, 2020) relevam que as forças de segurança – Guarda Nacional Republicana (GNR) e Polícia de Segurança Pública (PSP) – possuem uma das mais reduzidas taxas de feminização da Administração Pública, 7.1% e 8.2% respetivamente. Porém, os atores políticos não apontam a agenda como sendo uma prioridade para estas instituições. Por exemplo, o Programa de Governo e as Grandes Opções do Plano 2020-2023 remetem estes compromissos para a defesa (XXII Governo Constitucional, 2020). Outrossim, é o facto de que a magnitude resultante de uma maior aposta neste campo tenderia a produzir uma impacto superior ao

que poderá produzir nas forças armadas, por se estar perante um maior universo de colaboradores, 44.772 para as forças de segurança e 25.845 para as forças armadas (DGAEP, 2020).

Neste contexto, considerando que as explicações sobre as limitações da agenda no espetro de ação das forças de segurança são limitadas, surge a necessidade de se responder à seguinte pergunta: que elementos podem reforçar a implementação da agenda MPS nas forças de segurança em Portugal?

Tendo por base um quadro analítico ancorado no estudo da implementação das políticas públicas, bem como nos resultados das tendências da perceção de integração de género dos futuros líderes institucionais, pretende-se analisar os mesmos e obter elementos que nos transportem para além das avaliações próprias do senso comum. Ao mesmo tempo, indagar sobre os contextos e as variáveis com impacto no sucesso da implementação da agenda e sobre os fatores que podem impedir ou promover o seu futuro sucesso. Em síntese, procura-se disponibilizar ferramentas a que os decisores possam recorrer para consolidarem as transformaç**ões** necessárias nas organizações, tornando-as mais equitativas, resilientes e eficazes.

1. A Agenda Mulheres, Paz e Segurança

Em 1995 começaram a ser apresentados estudos que demonstravam uma correlação direta entre a existência de paz e a igualdade entre mulheres e homens, para além de dados estatísticos sobre o facto de as mulheres e crianças constituírem perto de 80% dos refugiados e de as mulheres ocuparem apenas 10% dos lugares parlamentares (United Nations, 1995).

Estes indícios, aliados ao conhecimento de dados concretos sobre os abusos contra as mulheres e crianças em situações de conflito – *e.g.* ex-Jugoslávia e Ruanda – consagraram um ímpeto redobrado às iniciativas preconizadas pelas Conferências Mundiais das Nações Unidas sobre as Mulheres – Nairobi (1985) e Pequim (1985) e as convenções existentes sobre o assunto – *e.g.* Convenção das Nações Unidas sobre os Direitos das Crianças.

Todos estes fenómenos tiveram a virtude de despertar consciências e de exigirem uma maior atenção à participação das mulheres na resolução de conflitos e para desempenharem um papel igualitário em todo o processo de paz. Foi neste contexto que, em 2000, surgiu o reconhecimento formal de que o conflito armado tem impactos mais destrutivos sobre mulheres, tornando-se fundamental uma abordagem mais sensível às questões de género. A RCSNU 1325 marcou o início da agenda que reconheceu o direito e a importância de as mulheres estarem presentes em todos os processos de construção da paz e da segurança, devendo a sua representação ser promovida em todos os níveis.

Este marco foi tão relevante que continua a ditar o contexto e o modo como o tema é discutido e analisado, em parte porque é, e tenderá a ser, uma obra inacabada. No entanto, já foi adaptada e melhorada pelas Nações Unidas e aplicada por outras organizações – *e.g.* União Europeia (UE) e Organização do Tratado do Atlântico Norte – e, passou a consubstanciar políticas públicas em diversos países, nomeadamente em Portugal.

1.1. Os Esforços de Portugal

Os esforços nacionais mais visíveis datam de 2007, durante a Presidência da UE, e dizem respeito ao empenho na construção de um compromisso e sinergias entre as políticas externas da UE e os desideratos da RCSNU 1325 (PCM, 2009). Porém, foram necessários mais dois anos para se desenhar e publicar um plano de ação nacional neste domínio da igualdade de género.

Em agosto de 2009 surgiu o I plano cuja justificação para o *agendamento*, patente no preâmbulo, estava alinhada com os argumentos internacionais. O Governo explicava a necessidade de intervir devido à reduzida taxa de feminização nas forças de segurança (5%), sendo avançado como argumento justificativo a eliminação tardia dos condicionalismos estruturais e funcionais à paridade (PCM, 2009).[1]

Até 2020, surgiram mais dois planos. No entanto, apesar de os indicadores não terem evoluído significativamente, a fundamentação para as novas medidas encontra-se mais ligada ao cumprimento de compromissos internacionais (PCM, 2014 e 2019).

Deste modo, a informação produzida, a pressão da comunidade científica, o efeito de *feedback* e o fenómeno de *spillover* têm sido decisivos para contagiar o nível interno com os instrumentos amplamente usados (planos de ação), por serem considerados como mecanismos eficazes para transpor a agenda, segundo a Comissão para a Cidadania e a Igualdade de Género (CIG, 2019). A agenda a nível doméstico é interpretada de forma mais ampla, estendendo-se à promoção das políticas nacionais de combate à violência de género e defesa dos direitos humanos, para além da abordagem aos conflitos armados e ajuda humanitária, ligando-se por isso a outros planos – *e.g.* plano para a igualdade de género, cidadania e não-discriminação.

As opções vertidas nos três planos de ação são o resultado de grupos de trabalho compostos por especialistas dos ministérios, mas incorporam conhecimento de outras áreas da sociedade como a academia, a CIG ou a Comissão para a igualdade entre mulheres e homens (2017). No caso específico do III plano, publicado em 2019,

1 O documento também frisava uma reduzida taxa de feminização nas forças armadas (14.5%). Por não ser o foco deste artigo, não se elenca, mas não se pode deixar de sublinhar que passados dez anos e três planos de ação, o valor tenha sofrido um decréscimo e se situe nos 11.8% (DGAEP, 2020).

não são detalhados os vários ministérios, contrariamente à opção de 2009 onde esse detalhe incluía representantes do Ministério da Administração Interna (MAI) (PCM, 2009; CIG, 2019). Ao nível da coordenação (III plano) foi criada uma Comissão Técnica de Acompanhamento composta por representantes das áreas governativas dos negócios estrangeiros, da cidadania e da igualdade e da defesa nacional, o MAI não é referido (PCM, 2019).

Este elemento permite enfatizar um argumento central, anteriormente avançado, sobre a falta de foco da agenda MPS nas forças de segurança. Não se contestando a existência de consenso nacional sobre a necessidade de continuar a avançar no quadro da igualdade em todos os campos,[2] apenas se pretende reconhecer a factualidade expressa no programa do XXII Governo Constitucional (2020a) com referência exclusiva à implementação da agenda nas forças armadas.

O estudo do Relatório Anual de Segurança Interna de 2018, também sugere um âmbito limitado da agenda MPS nas forças de segurança, atendendo a que refere que se prosseguiu o acompanhamento, mas não existem referências nas orientações estratégicas para 2019 (Gabinete do Secretário-Geral do Sistema de Segurança Interna, 2019).

Analisando vinte anos de Programas de Governo (tabela 1) é notória a evolução neste campo, pelo menos em alguns elementos. Em 2002, este documento estruturante apenas fazia cinco referências à palavra *mulher*, 19 à *igualdade* e zero à expressão igualdade de género. Por seu lado, em 2020, identificam-se 28 referências à palavra *mulher*, 93 à *igualdade* e 10 à expressão *igualdade de género*.

2 Caso existissem dúvidas, o estudo das propostas de programa de governo, dos partidos com maior representação que antecederam o III plano, esclarece que o tema não cria especiais clivagens (Coligação Portugal à Frente, 2015; Partido Socialista, 2015).

Tabela 1

Referências à agenda MPS nos Programas de Governo (2000-2020)

Governo	Partido(s)	Referência à agenda MPS
Programa do XXII Governo Constitucional (2019- …)	PS	Reforçar a participação de mulheres nas Forças Armadas, em linha com as melhores práticas internacionais, garantindo a aplicação e contínua monitorização do Plano Nacional de Ação para implementação da Resolução das Nações Unidas sobre Mulheres, Paz e Segurança nas instituições da Defesa.
Programa do XXI Governo Constitucional (2015-2019)	PS	Garantindo a aplicação, nas instituições da Defesa, do Plano Nacional de Ação para a implementação da resolução CSNU1325 sobre Mulheres, Paz e Segurança e promover a sua contínua monitorização.
Programa do XX Governo Constitucional (2015-2015)	PSD/CDS-PP	Sem referências expressas.
Programa do XIX Governo Constitucional (2011-2015)	PSD/CDS-PP	
Programa do XVIII Governo Constitucional (2009-2011)	PS	
Programa do XVII Governo Constitucional (2009-2011)	PS	
Programa do XVI Governo Constitucional (2004-2005)	PSD/CDS-PP	
Programa do XV Governo Constitucional (2002-2004)	PSD/CDS-PP	

Fonte: elaboração própria.

Apesar de existir o risco de a evolução ser mais simbólica do que efetiva e que é fruto de os programas resultarem de diferentes partidos, a realidade demonstra que existiu uma evolução real com as preocupações sobre este assunto. São várias as referências partidárias à necessidade de se aprofundar esforços para que se atinja a igualdade efetiva, e não apenas normativa, entre homens e mulheres. Além disso, estes objetivos são desagregados nas grandes opções do plano, uma vez mais apenas no campo das forças armadas (XXII Governo Constitucional, 2020).

O aparente consenso parece ter gerado uma pré-disposição para se aceitar medidas neste campo e não é despiciente saber-se que o I plano de 2009 foi concebido por um Governo do Partido Socialista (PS), que em 2014 o II plano foi desenhado por um Governo de coligação do Partido Social Democrata (PSD) e do Partido Popular (CDS-PP) e que o III plano resultou de um Governo do PS com apoio parlamentar dos restantes partidos posicionados à sua esquerda. Seguramente, não existem muitas outras áreas com tanta diversidade e respeito pelos planos, o Governo do PS

só criou um plano em 2014 (conforme previa o I plano) e o II plano, do PSD, vigorou durante três anos com o Governo do PS a reverter muitas outras medidas. Recorda-se que os planos foram aprovados por uma resolução do Conselho de Ministros, na qual os *pontos de vetos* (Immergut, *et al*., 2009) são reduzidos, sendo por isso mais fácil a promoção de mudanças.

Além dos avanços de semântica, já frisados, as avaliações produzidas ao II plano apontam taxas de execução razoáveis de 76%, mas também sugerem limitações de natureza prática na transposição dos objetivos teóricos para as ações concretas, além da falta de metas e de dados para aferir sobre a efetiva execução de cada medida (Equipa de Avaliação Externa do II Plano, 2018).

O desenho do III plano incorporou algum efeito de aprendizagem e colmatou as limitações. Por exemplo, foram criadas medidas operacionais com indicadores e metas. No entanto, afigura-se que continuam a subsistir debilidades, sobretudo no campo das forças de segurança.

2. A Agenda MPS nas Forças de Segurança

O III plano estabelece um objetivo específico para disseminar a agenda MPS junto dos jovens, bem como nos conteúdos dos cursos ministrados em instituições de ensino e formação, mas, uma vez mais, somente na área da defesa nacional.

Por outro lado, as forças de segurança não são expressamente envolvidas no objetivo de *promover a participação das mulheres e dos jovens na prevenção dos conflitos armados e nos processos de construção da paz e* não se conhecem argumentos que contrariem a factualidade de a GNR e a PSP serem decisivas nesta área. Inclusive, o III plano amplia o conceito de segurança e compromete-se a integrar a perspetiva de género nos diferentes domínios de política pública (segurança), mas o facto é que o MAI não foi diretamente envolvido (PCM, 2019).

O III plano elenca um objetivo relativo ao *n.º de pessoas envolvidas no combate ao terrorismo formadas, por sexo,* determina que os responsáveis são o MAI, a GNR e a PSP e estabelece uma meta de 20 formandos por ano. Assim, se não existir um plano ministerial a esclarecer as ponderações por força de segurança, corre-se o risco de as entidades nada executarem na expectativa de que a outra instituição cumpra o objetivo, circunstancialismo que se repete em outros objetivos. Porém, no Ministério da Defesa Nacional (MDN) esta situação nunca sucede, na coluna relativa aos responsáveis nunca são mencionados os ramos, talvez este facto tenha incentivado a conceção do plano ministerial que já está em vigor (MDN, 2019).

Todos estes elementos, de aparente detalhe, potenciam a entropia e poderão influenciar os resultados num campo fundamental de ação (as forças de segurança), assim existe a convicção de que é crucial um reforço da atenção, por parte do MAI,

para este assunto, sob pena de o III plano ficar limitado no âmbito da sua ação. Reitera-se, não se contesta, que a identificação de bloqueios e condições de sucesso das políticas tenham vindo a constituir uma preocupação dos diversos atores envolvidos, mas a realidade faz sobressair problemas significativos no desenvolvimento desse esforço.

Um desses elementos é a taxa de feminização dirigente. Na GNR, em 2017, cifrava-se nos 0.9%, sendo que nos oficiais a taxa era de 8.1% (GNR, 2018). Neste mesmo ano, a percentagem de oficiais do sexo feminino na PSP situava-se nos 13.8% com 22.6% de mulheres nos quadros dirigentes (PSP, 2018).

Deste modo, parece resultar que os indicadores das forças de segurança não permitiam abrandar os esforços. No entanto, é importante olhar para os números destas forças em perspetiva, dentro da Administração Pública e ao longo do tempo (tabela 2).

Tabela 2

Taxa de feminização por carreiras da Administração Pública (2011-2019)

CARGO / CARREIRA / GRUPO	31 de dezembro de 2011			31 de março de 2019			Variação da Taxa de Feminização (19-11)
	Homens	Mulheres	Taxa de Feminização	Homens	Mulheres	Taxa de Feminização	
Outro Pessoal de Segurança	1 949	41	2.1	1 216	43	3.4	**1.3**
Bombeiro	2 193	71	3.1	2 259	84	3.6	**0.5**
Guarda Nacional Republicana	21 759	1 140	5.0	21 063	1 601	7.1	**2.1**
Polícia de Segurança Pública	20 293	1 641	7.5	18 459	1 649	8.2	**0.7**
Forças Armadas	29 921	4 593	13.3	22 788	3 057	11.8	**-1.5**
Guarda Prisional	3 776	536	12.4	3 727	596	13.8	**1.4**
Polícia Municipal	1 001	271	21.3	1 245	264	17.5	**-3.8**
Serviço Estrangeiros Fronteiras	602	154	20.4	644	154	19.3	**-1.1**
Polícia Judiciária	1 567	751	32.4	1 414	735	34.2	**1.8**
Total	299 364	428 421	58.9	273 503	416 576	60.4	**1.5**

Fonte: elaboração própria, a partir de dados da DGAEP (2020).

A análise da tabela 2 permite afirmar que as tendências na Administração Pública, nas várias instituições, caminham no sentido de se contribuir para os objetivos da igualdade de género preconizada pelas Nações Unidas (2020) devido à taxa de feminização de 60.4%. No entanto, os resultados apresentados pela GNR e PSP parecem estar longe de garantir a participação plena e eficaz das mulheres, bem como a igualdade de oportunidades de liderança em todos os níveis de tomada de decisão. Os resultados também suscitam dúvidas sobre o comprometimento das instituições com a agenda, face à evolução desigual do indicador desde 2011. Por exemplo, a

GNR teve um crescimento de 2.1% superior à média (1.5%) e a PSP teve uma evolução de 0.7%, abaixo da média.

Conhecedores dos dados anteriores, também não se pode deixar de enfatizar que as forças e serviços de segurança do MAI (GNR, PSP e Serviço de Estrangeiros e Fronteiras), contam com um total de 3.365 mulheres, 8% do efetivo total, e que existem cargos de direção, comando e chefia exercidos por mulheres (Gabinete do MAI, 2020). Também é relevante saber-se que a GNR iniciou a integração das mulheres em 1994/95 e 25 anos depois a instituição conta com mais de 1.500 mulheres, a prestarem serviço em mais de 500 postos territoriais existentes por todo o país, sendo que de entre as 79 mulheres oficiais, 16 são comandantes de destacamento (Gabinete do MAI, 2020a). Por seu lado, as primeiras mulheres foram admitidas na PSP em 1971/72 o que permite que atualmente também sejam mais de 1.500 e que já existam mulheres a comandar dois importantes comandos – o comando metropolitano do Porto e comando distrital de Aveiro – e nove divisões (Gabinete do MAI, 2020b).

Os dados anteriores também permitem constatar que se está perante uma abertura tardia das forças de segurança às mulheres. Este elemento influencia o acesso atual ao desempenho de cargos de topo, nestas duas instituições, devido aos tempos mínimos de permanência exigidos nos vários postos, mas tenderá a afetar, de igual modo, as diversas instituições. Este ponto é relevante, porque as explicações mais transversais, apontadas para as limitações da agenda, prendem-se com a eliminação tardia dos obstáculos à entrada das mulheres nos respetivos quadros (MAI, 2014). Ora, apesar de não se negar a influência do argumento, afigura-se que ele não é exclusivo das forças de segurança, a entrada das mulheres para as forças armadas também só ocorreu na década de 90 e, em alguns indicadores como a taxa de feminização (tabela 2), apresentam melhor desempenho (MDN, 2014). É por este motivo, mas também porque a existência de mulheres em todos os níveis ainda não é uma realidade, mesmo na PSP onde foram pioneiras [*e.g.* no balanço social de 2018 verifica-se que não existiam dirigentes superiores de 1.º e 2.º grau mulheres (PSP, 2019)], que é determinante aprofundar o conhecimento neste setor.

Cientes de que dos resultados anteriores que contribuem para o sucesso ou insucesso dos objetivos da agenda MPS sabemos que as aspirações propostas por esta são mais abrangentes. Verificando a participação das mulheres em missões das Nações Unidas, constata-se que a GNR projetou, desde o ano 2000 até 2013, um total de 2.982 militares, sendo 56 mulheres (Meireles, 2018). Na PSP, o número total de mulheres que participou em missões de paz é de 94, num total de 1.195 elementos policiais que participaram em missões de paz (PSP, 2020). Estes dados fazem sobressair uma taxa de participação das mulheres em missões de paz de 7.9% para PSP e de 1.9% para a GNR. Também não se pode deixar de sublinhar o potencial impacto que a presença de mulheres poderá ter em algumas atuações operacionais. Estamos certos de que as

mulheres nestas instituições contribuirão significativamente para reduzir situações que criem um *reputational risk* para as duas forças de segurança.

Também não se pode deixar de enfatizar que faz seis anos que o último plano de ação sobre a agenda MPS foi desenvolvido e amplamente divulgado pelo MAI (2014) e que a GNR não desenvolveu qualquer plano nem estabeleceu orientações na estratégia 2020 (GNR, 2015), bem como a PSP, que nas grandes opções estratégicas (2017-2020) nada refere sobre a agenda ou sobre a igualdade de género (PSP, 2016).

Deste modo, face aos parcos resultados em alguns dos indicadores que densificam a agenda e ao aparente conforto institucional com os mesmos, corroboradas pela inexistência de planos e objetivos concretos, torna-se relevante olhar para estudos sobre a avaliação da implementação institucional que vão para além da monitorização administrativa requerida pelos próprios planos.

Um dos estudos mais recentes neste campo tentou perceber o modo como está a ser adotada e que fatores influenciam a implementação da agenda MPS na GNR (Malheiro, 2019). Embora o estudo tenha como objeto a GNR, o III plano, o uso do modelo unificado de inovação (Berry e Berry, 2007) e estabeleça uma comparação entre a GNR, a Marinha, a Força Aérea e o Serviço de Estrangeiros e Fronteiras, foram identificados fatores que afetam a adoção da agenda.

A investigação concluiu que a implementação da agenda na GNR está num estádio inicial, sobressaiu a motivação para a adoção, que é determinante a alocação de recursos específicos e em permanência e que os desafios serão superiores se não existir comprometimento do planeamento estratégico. Também sugere que as pressões reduzidas no campo do recrutamento podem potenciar a inercia na criação de estratégias mais diversificadas para atrair as mulheres.

As pistas anteriores ajudam a aumentar o conhecimento sobre a agenda, mas afigura-se que é relevante continuar a aprofundar o estudo para responder à questão que motiva a investigação – que elementos podem reforçar a implementação da agenda MPS nas forças de segurança em Portugal – até porque na pesquisa citada a PSP não foi objeto de análise.

Face à renovada centralidade das funções de segurança no mundo líquido e às incivilidades que se reconfiguram, a opção para se aprofundar o conhecimento recaiu sobre o estudo das perceções dos futuros líderes das duas forças de segurança sobre a presença e importância das mulheres nas duas instituições.

3. Perspetivas dos Futuros Decisores

O inquérito por questionário aplicado em 2016 aos cadetes que frequentavam os cursos de formação de oficiais das duas forças de segurança, permitiu-nos obter uma taxa de participação de 99.4% na GNR (87.3% homens e 12.7% mulheres num

total de 167) e de 70.9% na PSP (74.6% homens e 25.4% mulheres num total de 172). Numa escala em que 0 = muito difícil e 10 = muito fácil, foi perguntado aos cadetes como avaliam a forma como tem decorrido o processo de integração das mulheres nas forças de segurança. Quando se analisam agregadamente, independentemente da força de segurança a que pertencem, os cadetes tendem a apresentar médias acima do que é considerado o valor médio (5.00), o que permite afirmar que os mesmos percecionam que integração está de certa forma a ser facilitada (M = 6.02; DP = 2.25). Porém, verifica-se que esta perceção é mais forte nos cadetes da PSP (M = 6.33; DP = 1,78) do que nos cadetes da GNR (M = 5.81; DP = 2.50). Relembra-se o facto de que a PSP admitiu as primeiras mulheres no seu dispositivo em 1971, enquanto a GNR só em 1994 é que integrou as primeiras mulheres.

Quisemos aprofundar como esta realidade é percecionada pelos cadetes em função do sexo, tendo-se concluído que os cadetes femininos da PSP consideram que a integração está a ser facilitada (M = 5.74; DP = 1.78), enquanto aos cadetes femininos da GNR percecionam que está a ser dificultada (M = 4.33; DP = 2.13). Por seu lado, os cadetes masculinos, nas duas forças de segurança, consideram a que a integração está a ser mais fácil, sendo que essa perceção é mais elevada nos cadetes masculinos da PSP (M = 6.58; DP = 1.73) do que nos cadetes masculinos da GNR (M = 6.04; DP = 2.48).

Continuando a análise, procurou-se compreender como é que os cadetes percecionam o que mais facilitou ou dificultou a integração das mulheres nas forças de segurança recorrendo para tal a cinco perguntas que passamos a analisar com ajuda da tabela 3.

Tabela 3
Fatores que dificultaram ou facilitaram a integração das mulheres nas forças de segurança por força de segurança (média e desvio-padrão)

	GNR						PSP						Total PSP/GNR	
	Femininos		Masculinos		Total		Femininos		Masculinos		Total			
Questões	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**
A forma como os polícias homens aceitaram a presença das mulheres	4.71	2.26	6.31	2.55	6.09	2.56	4.68	2.39	5.83	1.84	5.50	2.07	6.13	2.31
O desempenho que as mulheres demonstraram nas tarefas	7,24	2.57	5.88	2.72	6.07	2.73	7.90	1.45	6.10	1.95	6.60	1.99	5.96	2.46
A forma como a sociedade vê as mulheres que ingressaram nas respetivas forças	7.10	2.90	6.81	2.36	6.85	2.43	6.84	2.22	6.25	1.64	6.42	1.83	6.60	2.13
O espírito de camaradagem existente entre homens e mulheres	6.00	2.53	6.18	2.42	6.15	2.43	6.87	2.30	6.14	2.27	6.33	2.29	6.16	2.36
A igualdade com que as respetivas forças tratam homens e mulheres	4.00	2.08	6.44	2.72	6.11	2.77	6.87	2.45	6.33	2.61	6.48	2.57	6.40	2.67

Fonte: inquérito por questionário aos alunos dos cursos de oficiais da GNR e da PSP no ano de 2016.
Escala: 0 = muito difícil e 10 = muito fácil.

Assim, quando nos focámos nos valores totais verificou-se que os cadetes consideram que a integração das mulheres nas forças de segurança tem sido facilitada, sendo que a forma como "a sociedade vê as mulheres que ingressaram nas respetivas forças" (M = 6.60) e a "igualdade com que as respetivas forças tratam homens e mulheres" (M = 6.40) são o que mais contribui para facilitar essa integração. Por outro lado, o "desempenho que as mulheres demonstraram nas tarefas" (M = 5.96) é o que menos facilita a integração das mulheres nas forças de segurança.

Quando redirecionámos o nosso olhar e analisámos as mesmas perguntas por sexo dos cadetes, em relação aos fatores que mais dificultaram ou facilitaram a integração das mulheres nas forças de segurança, verificou-se que para os cadetes femininos, independentemente da força de segurança, o que mais facilitou a integração foi "a capacidade demonstrada pelas mulheres no desempenho das tarefas que lhe são atribuídas", sendo que os cadetes femininos da PSP (M = 7.90) têm essa convicção mais reforçada do que os cadetes femininos da GNR (M = 7.24). Já no que diz respeito aos cadetes masculinos há uma diferente perceção sobre os fatores que facilitaram a integração das mulheres nas forças de segurança, para os cadetes masculinos da GNR (M = 6.81) é "a forma como a sociedade vê as mulheres que ingressaram nas respetivas forças" e para os cadetes masculinos da PSP (M = 6.33) é "a forma igual como as respetivas forças tratam homens e mulheres".

No que concerne ao que menos facilitou a integração das mulheres nas forças de segurança, os cadetes da PSP, independentemente do sexo, coincidem na escolha do fator que é a "forma como os polícias homens aceitaram a presença das mulheres" [cadetes femininos (M = 4.68); cadetes masculinos (M = 5.83)]. No que diz respeito aos cadetes da GNR, não se verificou a escolha de um fator em comum. Os cadetes femininos (M = 4.00) percecionam que é a "falta de igualdade na forma como as duas forças tratam homens e mulheres" que menos facilitou a integração das mulheres nas forças de segurança. Enquanto que para os cadetes masculinos (M = 5.88) o que mais dificultou a integração das mulheres é o "desempenho que as mesmas demonstraram nas tarefas".

Está-se perante diferentes perceções sobre a integração das mulheres nas forças de segurança que poderão ser ainda o reflexo de um condicionamento relativamente antigo da forma como esta profissão, quer queiramos ou não, ainda é conjugada no masculino. Por exemplo, na PSP o fator que mais dificultou a integração das mulheres é a "forma como os polícias homens aceitaram as mulheres", enquanto que na GNR os cadetes femininos afirmam ser a "falta de igual tratamento entre homens e mulheres", mas para os cadetes masculinos é o "desempenho demonstrado pelas mulheres no desempenho das tarefas". Crê-se que ambas as instituições ainda têm um longo caminho a desbravar, e muitas ações a desenvolver, para que esta profissão passe a ser percecionada de forma neutra – para homens e mulheres – e sem quaisquer distinções estigmatizadoras.

Quando foi perguntado aos cadetes sobre se a presença das mulheres nas forças de segurança acarreta mais ou menos vantagens para as referidas instituições, numa escala em que "0 = muitas desvantagens/difícil e 10 = muitas vantagens", verificou-se, quando analisados agregadamente, que os cadetes consideram que a presença de mulheres se traduz em mais vantagens do que desvantagens para as respetivas forças de segurança, mas são os cadetes da PSP (M = 7.57) que consideram que a presença das mulheres é mais vantajosa, por oposição aos cadetes da GNR (M = 5.97). No que concerne ao sexo, independentemente da força de segurança, verificou-se que os cadetes femininos (M = 8.57) consideram que a presença de mulheres nas forças de segurança implica, sem dúvida, mais vantagens para as forças de segurança do que desvantagens, por comparação com os cadetes masculinos (M = 6.17) que apresentam uma média mais baixa.

Porém, quando se refinou a análise por sexo e por força de segurança, verificou-se que são os cadetes da PSP [femininos (M = 8.94) e masculinos (M = 7 .04)] os mais convictos de que as mulheres representam mais vantagens do que desvantagens, quando comparados com os cadetes da GNR [femininos M = (8.00) e masculinos (M = 6.68)], mas note-se que os cadetes femininos em ambas as forças apresentam médias mais elevadas quando comparada com os cadetes masculinos, o que de certa forma seria expectável.

Para aquilatar sobre o que deveria ser feito pelas forças de segurança no que concerne ao recrutamento de mulheres, foram apresentadas cinco afirmações aos cadetes solicitando-lhes que indicassem o seu grau de concordância ou discordância numa escala em que "1 = discordo completamente e 5 = concordo totalmente completamente". Através da análise da tabela 4, verificou-se que, em média, adotam uma posição de neutralidade no que concerne às forças de segurança "manterem o número de mulheres" (M = 3.02), "recrutarem mais mulheres" (M = 3.11) ou "implementarem provas de admissão iguais para homens e mulheres" M = (3.31) e tendem a discordam que as forças de segurança "deixem de recrutar mulheres" (M = 1.87) ou que "tornem as provas de seleção mais fáceis" (M = 1.60).

Quando se procedeu à análise por força de segurança e por sexo, verificou-se que os cadetes da PSP optaram por uma atitude de relativa neutralidade, salientando-se a proximidade das médias em relação às questões "manter o número de mulheres [femininos (M = 3.03); masculinos (M = 3.04)] "recrutar mais mulheres" [femininos (M = 3.25); masculinos (M = 3.27)], e tendem a discordar totalmente, sendo que as médias nas mulheres são ligeiramente menores, que as forças de segurança deixem de recrutar mulheres" [femininos (M = 1.19); masculinos (M = 1.57) e que "tornem as provas de seleção mais fáceis" [femininos (M = 1.48); masculinos (M = 1.73)]. Por outro lado, tendem a discordar que se "implementem provas de admissão iguais para homens e mulheres" [femininos (M = 2.03); masculinos (M = 2.65)]. Esta proximidade de opiniões no seio dos cadetes da PSP, independentemente do sexo, pode-

rá ser o corolário de todo o trabalho institucional que tem sido desenvolvido para que a presença das mulheres seja aceite e incentivada nos seus quadros, bem como a sua presença desde 1971.

Tabela 4
Atitude das forças de segurança em relação ao recrutamento de mulheres para os seus quadros (média e desvio-padrão)

	GNR						PSP						Total PSP/GNR	
	Femininos		Masculinos		Total		Femininos		Masculinos		Total			
Questões	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**	**M**	**DP**
Manter o número de mulheres	2.76	1.09	3.04	1.23	3.00	1.13	3.03	.96	3.04	.81	3.04	.85	3.02	1.03
Recrutar mais mulheres	3.71	1.19	2.90	1.1	3.01	1.21	3.25	1.11	3.27	.96	3.26	1.00	3.11	1.13
Deixar de recrutar mulheres	1.19	.40	2.29	1.27	2.15	1.25	1.19	.48	1.57	.74	1.46	.70	1.87	1.11
Tornar as provas de seleção mais fáceis	1.62	.81	1.55	.96	1.56	.94	1.48	.77	1.73	.82	1.66	.81	1.60	.88
Implementar provas de admissão iguais para homens e mulheres	2.90	1.18	4.04	1.21	3.89	1.26	2.03	.89	2.65	1.25	2.49	1.20	3.31	1.41

Fonte: inquérito por questionário aos alunos dos cursos de oficiais da GNR e da PSP no ano de 2016.
Escala: 1 = discordo totalmente e 5 = concordo totalmente.

No que diz respeito aos cadetes da GNR é importante mencionar que as diferenças entre cadetes masculinos e femininos são mais evidentes do que na PSP. Assim, a posição de relativa neutralidade sobre as cinco afirmações é menor nos cadetes da GNR. Os cadetes masculinos manifestam essa neutralidade no que refere à "manutenção do número de mulheres nas forças de segurança" (M = 3.04), enquanto que os cadetes femininos a manifestam no "recrutar mais mulheres" (M = 3.71). Continuando a análise, verifica-se ainda que os cadetes femininos discordam totalmente que se "deixe de recrutar mais mulheres" (M = 1.19) e que se torne as "provas de seleção mais fáceis" (M = 1.62). Também discordam, com uma tendência para neutralidade, que se "implementem provas de admissão iguais para homens e mulheres (M = 2.90) e que se "mantenha o número de mulheres" nas forças de segurança (M = 2.76).

Por seu lado, os cadetes masculinos da GNR apresentam, em média, uma posição neutra em relação ao "manter o número de mulheres" (M = 3.04) e "recrutar mais mulheres" (M = 2.90). Discordam que se deixe de "recrutar mulheres" (M = 2.29) e discordam totalmente que se "tornem as provas de seleção mais fáceis" (M = 1.55). Porém, são os únicos a concordar que devem ser "implementadas provas de admissão iguais para homens e mulheres" (M = 4.04). Talvez, esta concordância encontre eco numa cultura institucional que ainda se conjuga bastante no masculino e que só recentemente abriu as suas portas às mulheres e garantiu o acesso gradual a todo o tipo de atividades.

Será, pois, este acesso a todas atividades que procuramos compreender ao questionar os cadetes quais são as tarefas que as mulheres deveriam desempenhar.[3]

Analisados agregadamente, 39,8% dos cadetes da GNR referem que as mulheres devem desempenhar todo o tipo de tarefas, incluído as de combate; enquanto 37,3% preconiza que devem desempenhar apenas tarefas de apoio administrativo-logístico e técnico e 22,9% indica que devem efetuar tarefas operacionais com exceção das funções de combate. Quando se refina a análise por sexo, verifica-se que 42,1% dos cadetes masculinos e 4,8% dos cadetes femininos responderam que as mulheres devem desempenhar tarefas de apoio administrativo-logístico e técnico. Por outro lado, 20,7% dos cadetes masculinos e 38,1% dos cadetes femininos referem que as mulheres devem efetuar todas as tarefas operacionais, com exceção das tarefas de combate e finalmente, 37,2% dos cadetes masculinos e 57,1% dos cadetes femininos concordam que as mulheres devem desempenhar todo o tipo de tarefas, incluindo as de combate.

Afigura-se que as mulheres, na GNR, ainda têm um caminho difícil a trilhar para que possam desempenhar na íntegra todas as tarefas próprias da profissão de polícia, mas a consciencialização para a concretização dessa igualdade já começa a ganhar raízes nas instituições policiais e a ascensão das mulheres, a curto prazo, aos postos mais elevados da hierarquia, permitirá, com certeza, que uma grande parte das condicionantes à plena integração das mulheres nas forças de segurança sejam suprimidas.

Para terminar, não podemos deixar de analisar como os cadetes da PSP percecionam este mesmo assunto. Quando analisados agregadamente, 86,7% dos cadetes respondeu que as "mulheres devem desempenhar todo o tipo de tarefas, sem exceções" e 13,3% que devem "executar apenas tarefas de apoio administrativo-logístico e técnico". Quando analisados por sexo, verifica-se que 96,8% dos cadetes femininos e 83,1% dos cadetes masculinos concordam que as mulheres devem desempenhar todo o "tipo de tarefas, sem exceções," enquanto que 3,2% dos cadetes femininos e 16,9% dos cadetes masculinos respondem que as mulheres "devem executar apenas tarefas de apoio administrativo-logístico e técnico."

Crê-se poder afirmar que a PSP já deixou de conjugar a profissão de polícia no masculino e que a presença das mulheres na instituição é já uma realidade que se encontra bastante consolidada.

3 Importa realçar que os cadetes da GNR foram questionados sobre tarefas nas forças armadas e os da PSP nas forças de segurança, razão pela qual nos limitaremos a apresentar a informação sem comparação entre as duas forças de segurança. Mesmo assim, julgamos relevante apresentar os resultados.

Conclusões

Motivada pela já consolidada maioridade dos vinte anos da agenda Mulheres, Paz e Segurança o presente artigo procurou identificar respostas à questão: *que elementos podem reforçar a implementação da agenda MPS nas forças de segurança em Portugal?*

Este *olhar* sobre as forças de segurança procurou discutir e despertar a atenção para os baixos níveis de implementação que alguns indicadores apresentam nesta área e o latente potencial de melhoria, sobretudo pelo universo de mais de 44.000 mulheres e homens que constituem os quadros da GNR e da PSP.

A reflexão iniciou-se com o exame dos fatores que contribuíram para a implementação das medidas preconizadas pela agenda, onde foi possível identificar o contributo dos indicadores estatísticos para despertar a atenção, além de outros eventos focalizadores, para as atrocidades que são perpetradas contra mulheres e crianças, especialmente em zonas de conflito. Por seu lado, também se verificou que as políticas domésticas incorporam elementos da aprendizagem internacional, desde logo porque se optou pela utilização de planos de ação para transpor a agenda através de três diplomas aprovados em 2009, 2014 e 2019.

Pese embora as ambições dos planos internos, tal como sucedeu nas avaliações internacionais, as apreciações apontam para a existência de algumas lacunas. Apesar de não sugerirem a falta de comprometimento dos atores ou a falta de recursos, como se pode verificar nos diferentes relatórios das avaliações das Nações Unidas, sublinha-se a dificuldade em mensurar os resultados práticos das medidas.

Aprimorando o estudo e observando a aplicação da agenda nas forças de segurança foram identificadas limitações na taxa de feminização e nas baixas percentagens de mulheres nos escalões mais elevados da tomada de decisão.

O plano em vigor (III plano), e outros documentos estruturantes como o Programa de Governo, remetem a agenda para as forças armadas em áreas que deveriam ser transversais. O MAI, a GNR e a PSP são responsáveis pelo cumprimento de diversos indicadores, mas afigura-se que existem limitações nos planos ao nível ministerial e institucional.

Para se aprofundar o posicionamento dos futuros comandantes das duas forças de segurança que tomarão decisões no âmbito do último *ratio regum* sintetizado no lema *dulce et decorum est pro Patria mori,* e se perceber como percecionam as mulheres na instituição, como está a ser facilitada ou dificultada a sua integração, o que preconizam em relação ao seu recrutamento e quais as missões que deveriam desempenhar, foram analisados os dados recolhidos em 2016, através de um inquérito por questionário. Estes 288 cadetes, que correspondem a todos os anos de formação das escolas superiores, fazem sobressair que a profissão ainda é muito conjugada no masculino.

Por exemplo, para os cadetes masculinos é o desempenho demonstrado pelas mulheres nas tarefas que mais condiciona a sua integração nas duas instituições. Os cadetes das duas forças consideram que a presença de mulheres se traduz em mais vantagens do que desvantagens, no entanto não existe uma posição claramente favorável a aumentos do número de mulheres nas instituições. Por outro lado, os dados relativos às funções que as mulheres podem desempenhar não são encorajadores, principalmente na GNR onde só 39,8% dos cadetes referem que as mulheres devem desempenhar todo o tipo de tarefas.

Como o explanado neste artigo, cremos poder afirmar que ainda não se atingiu o *break even point* da implementação da agenda MPS nas forças de segurança. O patamar mínimo de implementação só poderá ser atingindo se existir um esforço contínuo para se identificar e interferir positivamente nas variáveis que influenciam a implementação da agenda.

Apesar da consciência de que a implementação da agenda não passa apenas por *adicionar mulheres e mexer,* afigura-se que ajustamentos incrementais nas estratégias de recrutamento poderão ter impactos positivos.

Atendendo a que o papel das lideranças é crucial, desde logo, na difusão da mensagem de que a presença das mulheres contribui para a o sucesso das missões e que a igualdade de género é um multiplicador de força, considera-se pertinente reforçar a divulgação da agenda nas escolas superiores onde são formados os oficiais das forças de segurança.

Cientes de que muitos discursos e imagens institucionais já promovem as oportunidades das características estereotipicamente femininas – *e.g.* empatia, sensibilidade e comunicação – parece resultar como evidente a necessidade de se consolidar esta motivação em recursos efetivos e direcionados para diminuir os pontos fracos e potenciar os pontos fortes identificados como forma de consolidar a implementação da agenda.

Cônscios de que estas duas instituições perenes estão a caminhar a passos largos para uma maior implementação e consolidação da agenda, considera-se importante que seja operado um ajustamento e um redireccionamento das políticas aos contextos e limitações identificados neste estudo.

Referências Bibliográficas

Berry, F. e Berry, W., 2007. Innovation and Diffusion Models in Policy Reserarch. Em, P. Sabatier, ed., *Theories of the Policy Process.* Colorado: Westview Press, pp. 223-261.

Coligação Portugal à Frente, 2015. *Agora Portugal pode mais: programa eleitoral* [pdf]. Disponível em *Diário de Notícias*: https://www.dn.pt/DNMultimedia/DOCS+PDFS/Portugal%20%C3%80%20Frente%20-%20Agora,%20Portugal%20pode%20mais.pdf [acedido em 26 agosto 2019].

Comissão para a Cidadania e a Igualdade de Género (CIG), 2019. *Resolução do Conselho de Segurança das Nações Unidas n.º 1325 sobre Mulheres, Paz e Segurança 2019-2022* (RCSNU 1325). Disponível em CIG: https://www.cig.gov.pt/planos-nacionais-areas/rcsnu-1325/ [acedido em 22 agosto 2019].

Comissão para a Igualdade entre Mulheres e Homens (CIMH), 2017. *Valorizar o trabalho – Efetivar a igualdade* [pdf]. Lisboa: CIMH/CGTP-IN. Disponível em CGTP-IN: http://www.cgtp.pt/images/images/2017/04/Livro_Efectivar%20a%20Igualdade.pdf

Conselho de Segurança das Nações Unidas (CSNU), 2000. *Resolution 1325* [em linha]. Adopted by the Security Council at its 4213th meeting, on 31 October. United Nations Security Council. Disponível em: https://www.un.org/ga/search/view_doc.asp?symbol=S/RES/1325%282000%29 [acedido em 01 julho 2019].

Conselho de Segurança das Nações Unidas (CSNU), 2019. *Resolution 2493 (2019)*. Adopted by the Security Council at its 8649th meeting, on 29 October 2019. United Nations Security Council. [em linha] Disponível em: http://unscr.com/en/resolutions/doc/2493 [acedido em 30 abril 2020].

Direção-geral da Administração e do Emprego Público (DGAEP), 2020. Quadros 1.6 Emprego no sector das administrações públicas por cargo/carreira/grupo e sexo, segundo o subsector. *Boletim Estatístico do Emprego Público (BOEP)* [em linha]. Disponível em DGAEP: https://www.dgaep.gov.pt/index.cfm?OBJID=C0F56E62-5381-4271-B010-37ECE5B31017 [Acedido em 02 abril 2020].

Equipa de Avaliação Externa do II Plano, 2018. *Avaliação externa. II Plano Nacional de Acção para a implementação da Resolução do Conselho de Segurança das Nações Unidas n.º 1325* [pdf]. Disponível em CIG: https://www.cig.gov.pt/wp-content/uploads/2019/06/Avalia%C3%A7%C3%A3o-PNA-II.pdf [acedido em 15 agosto 2019].

Gabinete do Ministro da Administração Interna (MAI), 2020b. *Intervenção do Ministro da Administração Interna na Cerimónia Comemorativa do Dia Internacional da Mulher na PSP.* Ministério da Administração Interna. Disponível em Portal do Governo: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=0ba4cc2b-8d60-4ef3-8050-a16f1ec17721 [acedido em 30 abril 2020].

Gabinete do Ministro da Administração Interna (MAI), 2020. *Dia Internacional da Mulher – As Mulheres nas Forças e Serviços de Segurança.* Ministério da Administração Interna. Disponível em Portal do Governo: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=c9d6c433-8c06-4402-98f6-72293a2dc601 [acedido em 30 abril 2020].

Gabinete do Ministro da Administração Interna (MAI), 2020a. *Intervenção do Ministro da Administração Interna na Cerimónia Comemorativa do Dia Internacional da Mulher na GNR.* Ministério da Administração Interna. Disponível em Portal do Governo: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=a564925e-c66b-4bf9-839a-a364ab06d549 [acedido em 30 abril 2020].

Gabinete do Secretário-Geral do Sistema de Segurança Interna, 2019. *Relatório Anual de Segurança Interna 2018*. [em linha] Disponível em Portal do Governo: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=ad5cfe37-0d52-412e-83fb-7f098448dba7 [acedido em 30 Abril 2020].

Guarda Nacional Republicana (GNR), 2015. *Estratégia da Guarda 2020: Uma Estratégia de Futuro*. GNR [em linha]. Disponível em: https://www.gnr.pt/estrategia.aspx_[acedido em 01 maio 2020].

Guarda Nacional Republicana (GNR), 2018. *Relatório de Atividades 2017*. GNR [em linha]. Disponível em: http://www.gnr.pt/InstrumentosGestao/2017/RA2017.pdf [acedido em 13 janeiro 2019].

Immergut, E., Anderson, K. e Schulze, I., 2009. *The Handbook of West Europian Pensions Politics*. New York: Oxford University Press.

Malheiro, L., 2019. *A questão do género e os instrumentos de regulação internacional: a agenda mulheres paz e segurança na Guarda Nacional Republicana*. Trabalho de investigação final do Curso de Defesa Nacional. Lisboa: Instituto da Defesa Nacional.

Meireles, J. M. M., 2018. *A integração da perspetiva do género – um modelo para as organizações militares*. Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto. Instituto Universitário Militar. Disponível em RCAAP: https://comum.rcaap.pt/bitstream/10400.26/23216/1/MAJ%20Jorge%20Meireles.pdf [acedido em 2019].

Ministério da Administração Interna (MAI), 2015. *Plano para a Igualdade de Género (2014-2017)*, janeiro. MAI. Disponível em CIG: https://www.cig.gov.pt/wp-content/uploads/2016/01/Plano-de-A%C3%A7%C3%A3o-Setorial-para-a-Igualdade-de-G%C3%A9nero-Minist%C3%A9rio-da-Administra%C3%A7%C3%A3o-Interna.pdf [acedido em 28 dezembro 2018].

Ministério da Defesa Nacional (MDN), 2014. *Plano de Ação Setorial para a Igualdade: Setor Defesa Nacional e Forças Armadas 2014-2017*. Disponível em Portal do Governo: https://www.historico.portugal.gov.pt/media/1367793/20140314%20mdn%20PASI%202014_2017.pdf [acedido em 18 março 2019].

Ministério da Defesa Nacional (MDN), 2019. *Plano Setorial da Defesa Nacional para a Igualdade 2019-2021*. Disponível em Portal do Governo: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABAAzNzY3BADD5EyrBAAAAA%3d%3d [acedido em 01 julho 2019].

Partido Socialista, 2015. *Programa Eleitotal do Partido Socialista: Eleições Legislativas 2015*. Disponível em Partido Socialista: https://www.ps.pt/wp-content/uploads/2016/06/programa_eleitoral-PS-legislativas2015.pdf [acedido em 26 agosto 2019].

Polícia de Segurança Pública (PSP), 2016. *Grandes Opções Estratégicas da PSP para 2017-2020*. Direção Nacional da PSP, Gabinete do Diretor Nacional. Disponível em PSP: https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Documentos%20Estrat%C3%A9gicos/Op%C3%A7%C3%B5es%20Estrat%C3%A9gicas%202017-2020.pdf [acedido em 01 maio 2020].

Polícia de Segurança Pública (PSP), 2018. *Balanço Social da PSP 2017*. Maio de 2018. Departamento de Recursos Humanos. Disponível em PSP: https://www.psp.pt/Documents/Instrumentos%20de%20Gestão/Balanço%20Social/Balanço%20Social%20da%20PSP%20%202017.pdf [Acedido em 14 janeiro 2019].

Polícia de Segurança Pública (PSP), 2019. *Balanço Social da PSP 2018*. Maio de 2019 rectificado em outubro de 2019. Departamento de Recursos Humanos. Disponível em PSP: https://www.psp.pt/Documents/Instrumentos%20de%20Gest%C3%A3o/Balan%C3%A7o%20Social/Balan%C3%A7o%20Social%20da%20PSP%202018.pdf [acedido em 01 maio 2020].

Polícia de Segurança Pública (PSP), 2020. *A PSP em Missões Internacionais.* PSP [em linha]. Disponível em: https://www.psp.pt/Pages/sobre-nos/psp-global/missoes-internacionais.aspx [acedido em 30 abril 2020].

Presidência do Conselho de Ministros (PCM), 2009. Resolução do Conselho de Ministros n.º 71/2009. Aprova o Plano Nacional de Acção para Implementação da Resolução do Conselho de Segurança das Nações Unidas n.º 1325 (2000), adoptada em 31 de Outubro de 2000, sobre «mulheres, paz e segurança» (2009-2013). *Diário da República* n.º 164/2009, Série I de 2009-08-25. Disponível em CIG: https://www.cig.gov.pt/wp-content/uploads/2013/12/6.pdf [acedido em agosto 2019].

Presidência do Conselho de Ministros (PCM), 2014. Resolução do Conselho de Ministros n.º 50/2014. Aprova o II Plano Nacional de Ação para a Implementação da Resolução do Conselho de Segurança das Nações Unidas n.º 1325 (2000) sobre Mulheres, Paz e Segurança (2014-2018). *Diário da República* n.º 163/2014, Série I de 2014-08-26. Disponível em CIG: https://www.cig.gov.pt/wp-content/uploads/2014/08/II-Plano-Nacional-de-A%C3%A7%C3%A3o-para-a-implementa%C3%A7%C3%A3o-da-RCSNU-1325.pdf [Acedido em 14 julho 2019].

Presidência do Conselho de Ministros (PCM), 2019. Resolução do Conselho de Ministros n.º 33/2019. Aprova o III Plano Nacional de Ação para a Implementação da Resolução do Conselho de Segurança das Nações Unidas n.º 1325 (2000) sobre Mulheres, Paz e Segurança 2019-2022. *Diário da República* n.º 33/2019, Série I de 2019-02-15. Disponível em: https://dre.pt/web/guest/home/-/dre/119622096/details/maximized [acedido em 15 fevereiro 2019].

United Nations, 1995. *Report of the Fourth World Conference on Women*. Beijing, 4-15 September 1995. Nova Iorque: United Nations. Disponível em: https://www.un.org/womenwatch/daw/beijing/pdf/Beijing%20full%20report%20E.pdf [acedido em 4 agosto 2019].

United Nations, 2000. *Report of the Ad Hoc Committee of the Whole of the twenty-third special session of the General Assembly*. General Assembly, Official Records, Twenty-third special session, Supplement No. 3 (A/S-23/10/Rev.1). Nova Iorque: United Nations. Disponível em: https://undocs.org/en/A/S-23/10/Rev.1 [acedido em 4 agosto 2019].

United Nations, 2015. *Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council Resolution 1325*. UN Women. Disponível em: https://www.peacewomen.org/sites/default/files/UNW-GLOBAL-STUDY-1325-2015%20(1).pdf [acedido em 13 janeiro 2019].

United Nations, 2015a. *The Story of Resolution 1325 | Women, Peace and Security.* [em linha]. Disponível em YouTube: https://www.youtube.com/watch?v=mZH5hIOyU4Y [acedido em 2 agosto 2019].

United Nations, 2020. *Goal 5: Achieve gender equality and empower all women and girls.* Sustainable Development Goals [em linha]. Disponível em: https://www.un.org/sustainabledevelopment/gender-equality/ [acedido em 30 abril 2020].

XXII Governo Constitucional, 2020. *As Grandes Opções do Plano 2020-2023 do XXII Governo Constitucional*. [em linha] Disponível em: http://app.parlamento.pt/webutils/docs/doc.pdf?path=6148523063446f764c324679595842774f6a63334e7a637664326c756157357059326c6864476c3259584d7657456c574c33526c65485276637939776347777304c56684a5669356b62324d3d&fich=ppl4-XIV.doc&Inline=true [acedido em 25 abril 2020].

XXII Governo Constitucional, 2020a. *Programa do XXII Governo Constitucional (2019-2023).* [em linha] Disponível em: https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=54f1146c-05ee-4f3a-be5c-b10f524d8cec [acedido em 27 abril 2020].

Portugal e o Brasil entre a Ascensão do Indo-Pacífico e a Eventual Queda do Atlântico*

Bruno Cardoso Reis
Subdiretor do Centro de Estudos Internacionais, ISCTE-IUL.

Resumo

O impacto da pandemia da Covid-19 foi visto por alguns, já inclinados a subscrever esta ideia, como a confirmação do inevitável colapso das potências do Atlântico Norte e da ascensão irresistível das potências do Indo-Pacífico. Será realmente assim? E se sim, quais as implicações para Portugal e o Brasil? Este artigo tem como objetivo avaliar até que ponto as mudanças na política, na economia, e na segurança global das últimas décadas afetaram a centralidade das potências do Atlântico, em particular do Atlântico Norte, num sistema político global e globalizado em cuja construção estas últimas tiveram um papel fundamental nos últimos séculos.
O artigo defende que o que temos, para já, é um suave declínio relativo do peso global do Atlântico Norte face à ascensão da China e outras potências asiáticas. Porém, também reconhece que o Ocidente, e sobretudo a União Europeia e a OTAN, têm algumas vulnerabilidades e podem entrar em colapso. Apontamos para algumas das consequências prováveis destes dados para os interesses e as prioridades de Portugal e do Brasil, assim como para as respetivas relações bilaterais, sublinhando que não há ganhos nem perdas automáticas ou garantidas na política internacional.

Palavras-chave: Portugal; Brasil; Atlântico Norte; Indo-Pacífico; OTAN; China; Covid-19.

Abstract
Portugal and Brazil between the rise of the Indo-Pacific and the eventual fall of the Atlantic

The impact of the Covid-19 pandemic was seen by some, already inclined to subscribe to this idea, as the confirmation of the inevitable collapse of the North Atlantic powers and the irresistible rise of the Indo-Pacific powers. Is that really the case? And if so, what are the implications for Portugal and Brazil? This article aims to assess the extent to which changes in politics, the economy, and global security in recent decades have affected the centrality of the Atlantic powers, in particular the North Atlantic ones, in a global and globalized political system in whose construction the latter had a fundamental role in recent centuries. The article argues that what we have for now is a slight relative decline in the relative power of the North Atlantic in the face of China's and other Asian powers. However, it also recognizes that the West, and above all, the European Union and NATO, have some vulnerabilities and may collapse. We point to some of the likely consequences of these trends for the interests and priorities of Portugal and Brazil as well as for their respective bilateral relations, stressing that there are no gains, nor automatic or guaranteed losses in international politics.

Keywords: *Portugal; Brazil; North Atlantic; Indo-Pacific; NATO; China; Covid-19.*

Artigo recebido: 15.06.2020
Aprovado: 22.06.2020
https://doi.org/10.47906/ND2020.156.06

* Este artigo é o resultado de um projeto do Instituto da Defesa Nacional (IDN) em parceria com a Escola Superior de Guerra (ESG) do Brasil sobre o futuro da geoestratégia do Atlântico. Agradeço a todos os envolvidos no projeto, em particular ao General Vítor Rodrigues Viana, Diretor do IDN, por me ter confiado a direção do mesmo pelo lado do IDN, ao Almirante Antonio Ruy de Almeida Silva da ESG que comigo o coordenou, assim como ao Danilo Marcondes e ao Pedro Seabra que deram contributos inestimáveis para o mesmo. Agradeço ainda ao Almirante Alipio Jorge, Diretor da ESG, pelo apoio recebido no quadro deste projeto.

"Nos últimos anos, as pessoas têm afirmado que
o próximo século será o século da Ásia e do Pacífico, como se isso fosse
algo inevitável. Eu discordo dessa visão"
Deng Xiaoping (1988)

A intenção anunciada pelo presidente Barack Obama, em novembro de 2009, e reafirmada pela secretária de estado Hillary Clinton, em outubro 2011, de os EUA darem prioridade a um *pivot* ou *rebalancing* para o Pacífico tem sido frequentemente apontada como a prova decisiva da perda da centralidade do Atlântico no século XXI em favor do chamado Indo-Pacífico (Obama, 2009; Clinton, 2011). Se até os EUA, tradicionalmente vistos como a grande potência do Atlântico Norte, passam a dar prioridade sobretudo ao Indo-Pacífico, isso só pode significar que o predomínio global das potências do norte atlântico está a chegar ao fim. A eleição de Donald Trump pareceu acentuar essa viragem. Ele acentuou as divisões no Ocidente com a sua hostilidade a instituições multilaterais, mesmo as que desempenharam um papel fundamental no reforço da coesão do espaço Euro-Atlântico, como a União Europeia. Num gesto inédito por parte de um presidente dos EUA, chegou a declarar a Organização do Tratado do Atlântico Norte (OTAN) "obsoleta", no início de 2017 (BBC, 2017). Trump também passou a apontar a China de forma cada vez mais insistente como o grande rival geoestratégico dos EUA.

O culminar desta tendência foi, já em 2020, a publicação da estratégia para a China da administração Trump, que deixa clara a determinação de pôr de lado quaisquer ambiguidades e apostar numa postura de confrontação numa reedição da estratégia de contenção sistemática da Rússia soviética no pico da Guerra Fria (White House, 2020). Mesmo os líderes do Partido Democrático, nomeadamente o seu candidato e possível presidente, Joe Biden, parecem determinados a confrontar prioritariamente a China numa série de áreas estratégicas como as relações comerciais ou a segurança de novas tecnologias. E a União Europeia (UE) no seu documento orientador mais recente da relação com a China passou a referir-se a ela como um rival sistémico (European Commission, 2019). Mesmo que não necessariamente de forma simpática, todos as atenções parecem estar voltadas para o Indo-Pacífico.

Ao nível de análises da política global também não têm faltado autores de referência, como Fareed Zakaria (2011), Oliver Stuenkel (2017), ou Kishore Mahbubani (2018), a referirem-se à política global em termos de um século pós-americano, pós-ocidental, ou marcando um triunfo da Ásia. O impacto da pandemia da Covid-19 foi também visto por alguns, já inclinados a subscrever esta ideia, como a confirmação do inevitável declínio das potências do Atlântico Norte e da ascensão das potências do Indo-Pacífico. Mas será realmente assim?

Este artigo tem como objetivo avaliar até que ponto as dinâmicas em curso na economia, na defesa, na política global afetam a centralidade das potências do Atlântico.

Efetivamente, as potências do Atlântico Norte são geralmente reconhecidas como dominantes nos últimos séculos num sistema político global e globalizado em cuja construção tiveram um protagonismo fundamental. Este texto começará, por isso, nas suas seções iniciais por esboçar a história da construção do Atlântico como realidade geoestratégica sublinhando quão importante o processo foi para a ascensão de vários Estados do espaço Euro-Atlântico ao estatuto de grandes potências, mas também como o seu predomínio na distribuição de poder a nível global é relativamente recente, anormal e era insustentável a prazo. Depois irei apontar alguns erros fundamentais na forma como o tema do declínio ou colapso do Atlântico Norte e da ascensão do Indo-Pacífico é frequentemente abordado. Por fim, irei apontar algumas das consequências possíveis destas tendências para as prioridades estratégicas de Portugal e do Brasil.

Breve História da Ascensão do Atlântico e da Criação de Portugal e do Brasil

A história da ascensão das potências do Atlântico entre os séculos XV e XX ao topo de hierarquia de poder global é rica e complexa, repleto de heroísmos e vilanias, de progresso e de violência. Na breve síntese deste processo nas seções que se seguem iremos, dado o enfoque deste artigo, concentrar-nos sobretudo na dimensão da geoestratégica estatal. O objetivo desta seção é demonstrar que Portugal é um exemplo precoce e paradigmático da ascensão das potências marítimas europeias que garantiram a centralidade do Atlântico, em particular do Atlântico Norte, no sistema global que construíram. Iremos também sublinhar que a emergência do Brasil como colónia e como Estado independente só se percebe no contexto de guerras e de revoluções atlânticas.

Comecemos pelo princípio. Portugal foi criado como uma monarquia independente tendo por base a visão geopolítica dos primeiros monarcas que assentava num primado do Atlântico. Começando pelo rei fundador, D. Afonso Henriques (1139-1185), as suas ações deixam claro que desde o início a coroa portuguesa deu prioridade ao controlo da fachada costeira atlântica ocidental da Península Ibérica. A conquista do mais importante porto da costa ibérica ocidental, Lisboa, em 1147, foi estruturante na construção do novo reino. Isso fica evidente na rápida afirmação desta cidade como cabeça ou capital do novo reino.

O fundador da monarquia portuguesa percebeu que se queria ser reconhecido como rei no seio da Europa cristã, tinha de ser visto como dando um contributo eficaz para a expansão territorial e a segurança marítima da Cristandade, nomeadamente das rotas marítimas cada vez mais importantes que uniam o Norte europeu com o Mediterrâneo. Só assim o novo reino português poderia contar com os indispensáveis apoios externos para a consolidação do seu estatuto independente.

Foi assim nomeadamente com a participação crucial de uma frota de cruzados norte europeus na conquista de Lisboa. Esta dimensão marítima da chamada Reconquista, da expansão e construção da rede territorial da monarquia portuguesa tem vindo a ser cada vez mais estudada e documentada em anos mais recentes – ver, e.g., Borges (2013) e Silva (2009). Ela liga o rei D. Afonso Henriques no século XII ao infante D. Henrique no século XV.

Confrontado com um reino de Castela cada vez mais forte, controlando o centro da Península e com ambições evidentes de unificar todo o espaço peninsular, a monarquia portuguesa foi apostando em alianças fora da Península e no reforço das capacidades navais. Paradigmático é o empenho do rei D. Dinis (1279-1325), o primeiro monarca a reinar depois de terminada a ocupação do Algarve em 1249, no desenvolvimento de uma marinha de guerra, como fica claro pela nomeação do experiente marinheiro italiano, Manuel Pessanha, em 1317, como primeiro Almirante-mor do Reino. Depois do choque quase fatal para a independência portuguesa da crise dinástica de 1383-85, esta prioridade atlântica ganhou nova urgência e ímpeto. É neste contexto que o infante D. Henrique (1394-1460) se vai afirmar como principal articulador de uma visão estratégica de expansão atlântica da monarquia portuguesa, uma cruzada marítima com os meios e os homens da Ordem de Cristo, prosseguida sistematicamente durante décadas e dando origem aos chamados Descobrimentos (Oliveira e Costa, 2013).

É como resultado dos Descobrimentos que surgiu o espaço geopolítico do Atlântico como hoje o conhecemos. Com esta afirmação não estamos, claro, a negar a existência material do segundo maior oceano da Terra desde há algumas dezenas de milhões de anos. Estamos sim a destacar a importância vital do descobrimento dos contornos precisos das costas, do regime de ventos e correntes, dos melhores métodos de navegação do Atlântico, das suas ligações com os demais grandes oceanos da terra, o Índico e o Pacífico. Essa descoberta nada teve de natural ou de inevitável, e data de há cinco séculos atrás. Esta construção do Atlântico tal como o conhecemos ao longo do século XV foi indispensável precursora da globalização. Ela permitiu também a criação de um primeiro sistema de conhecimento geográfico de todo o globo e, consequentemente, de um primeiro sistema geoestratégico verdadeiramente global – e.g., Domingues (2016).

O descobrimento do Atlântico não foi, efetivamente, fruto de achamentos ocasionais. Ele resultou de um plano sistemático de exploração e expansão, mesmo que sujeito a naturais contingências. Ao dizê-lo não estamos apenas a avançar teses de historiadores atuais, mas sim a ler as prioridades da grande estratégia da expansão portuguesa tal como foram descritas na *Crónica dos Feitos da Guiné*, pelo cronista de D. Henrique, Gomes Eanes de Zurara no final do século XV. O respetivo capítulo VII é dedicado precisamente a explicitar as "razões por que o Senhor Infante [D. Henrique] foi movido de mandar buscar as terras de Guiné", a designação

que na época se dava à costa da África subsaariana. Aí fica claro que D. Henrique tinha as seguintes prioridades nesta sua empresa: a) mapear o poder do inimigo tradicional, os Estados islâmicos do Norte de África; b) explorar novos recursos estratégicos; c) procurar novas rotas comerciais, de acesso exclusivo, permitindo substanciais lucros; d) buscar novos aliados, nomeadamente reis cristãos desconhecidos; e) projetar o *soft power* português através da cristianização.

Esta grande estratégia foi elevada a um novo nível de ambição pelo príncipe e rei D. João II (1481-1495), que a começou a gerir ainda enquanto herdeiro da coroa. Este Príncipe Perfeito da *Realpolitik* do Renascimento passou a ter como prioridade contornar África e atingir diretamente a partir do Atlântico o Índico e as enormes riquezas da Ásia, até então apenas acessíveis aos europeus por via terrestre, indireta e mais custosa (Adão da Fonseca, 2011).

O sucesso desta prioridade estratégica portuguesa de procura de profundidade estratégica fora da Europa foi fundamental na consolidação de Portugal como um Estado independente. O sucesso da grande estratégia da expansão portuguesa foi tão grande que acabou por ser emulado por vários outros Estados atlânticos da Europa, desde logo a vizinha Espanha, e resultou na consolidação do Atlântico como o eixo central de um sistema de poder verdadeiramente global. A fragilidade relativa da Europa face aos grandes impérios da Ásia, como um sistema regional onde o poder era muito mais fragmentado, acabou por se revelar uma vantagem a prazo. Neste contexto altamente competitivo nenhum Estado, se quisesse sobreviver, podia correr o risco de deixar de inovar e de aperfeiçoar os seus meios de projeção de poder.

Muito antes da internet ou da aviação, o desenvolvimento pelos Estados euro-atlânticos de meios de navegação oceânica revelaram ser as inovações tecnológicas indispensáveis para permitir a construção de uma primeira rede global de comunicações, de trocas e de projeção de poder. Efetivamente o marco fundamental na geopolítica global que foi o Tratado de Tordesilhas de 1494, entre D. João II de Portugal e os Reis Católicos de Espanha, seria algo impensável sem uma primeira marinha de mar azul (*blue water navy*) com capacidade de navegação oceânica e bem como a capacidade de mapear as costas de todo o globo.

Mas porque nos importa especificamente neste texto o Tratado de Tordesilhas? Por duas razões. A primeira é que ele torna evidente a centralidade do Atlântico na emergente geopolítica global. O que esteve fundamentalmente em jogo nas duras negociações que levaram à assinatura deste acordo entre Portugal e Espanha, em 1494, foi uma demarcação de esferas de influência por via do controlo partilhado entre as potências ibéricas do Atlântico Norte e de uma garantia a Portugal do controlo exclusivo do Atlântico Sul. Este último aspeto era indispensável para garantir a segurança do monopólio português da rota marítima direta entre a Europa e o Indo-Pacífico. É significativo que seja neste último ponto que os negociadores portugueses mais insistem. Não sabemos se D. João II já conhecia a existência de

algumas das terras que vieram a ser o Brasil, embora haja alguns indícios nesse sentido (Domingues, 2012). Mas o que o rei português sabia é que era possível por via do Cabo da Boa Esperança chegar ao Índico a partir do Atlântico e que, para o fazer, os navios portugueses precisavam de contornar a zona de calmaria do Golfo da Guiné. Por isso, quaisquer territórios na região que hoje é a costa Brasil teriam de ficar em mãos exclusivamente portugueses, ou a rota para a Índia e a China ficaria vulnerável a quem os controlasse.

A segunda razão porque nos importa o Tratado de Tordesilhas é por ser o primeiro exemplo de uma geoestratégia pensada à escala global. Corresponde à primeira divisão em esferas de influência de todo o Mundo. Nesse sentido é semelhante, por exemplo, à Conferência de Ialta, no final da Segunda Guerra Mundial, em que se desenharam as esferas de influência soviéticas e norte-americanas, inaugurando a Guerra Fria Global, que se prolongou de 1945 até 1989. Ambos os acordos foram, aliás, intensamente contestados.

Efetivamente as potências emergentes da Europa Atlântica – França, Inglaterra, Países Baixos – não descansaram enquanto não começaram a desafiar o condomínio ibérico fixado em Tordesilhas, e mais concretamente o predomínio de Espanha no Caribe e nas Américas, e o predomínio naval de Portugal no Oceano Índico, o que sucedeu com cada vez maior eficácia a partir do final do século XVI. O monopólio português do comércio com o Indo-Pacífico, por via do controlo exclusivo do Atlântico Sul era um alvo demasiado apetecível para outros Estados europeus não procurem também lucrar com ele. Portugal não tinha, nem os homens, nem os recursos para contrariar esse esforço da parte de vários Estados europeus bem melhor dotados de pessoas e de meios.

A ocupação mais continuada e mais empenhado do que veio a ser a costa do Brasil por guarnições e colonos portugueses deveu-se precisamente à tentativa de Portugal contrariar a todo o custo essas tentativas de pôr em causa o seu domínio naval do Atlântico Sul: primeiro francesas, logo no século XVI, em torno do Rio de Janeiro, e depois holandeses em torno do Recife, no século XVII. No século XVI começou por se subcontratar a vários nobres portugueses a ocupação da costa do Brasil por via de capitanias, mas acabou-se, em 1549, por considerar necessário estabelecer um primeiro governador geral régio. A campanha terrestre e naval para recuperar o Nordeste do Brasil da ocupação holandesa foi bem mais exigente, e não teria sido possível sem o concurso ativo de armadas vindas da Europa e do esforço armado dos colonos portugueses e dos seus aliados locais, ilustrada paradigmaticamente pelas forças mobilizadas na chamadas Batalhas de Guararapes em 1648 e 1649. Na verdade, tão pesada foi esta guerra colonial com os holandeses que Portugal foi forçado a escolher, a definir prioridades.

Portugal passou, a partir de meados do século XVII, a dar prioridade ao seu império Atlântico, e abandonou grande parte do seu império naval asiático, que se tinha

dispersado num excessivo número de fortalezas, impossíveis de defender face a ataques repetidos na terra e no mar e frequentemente coordenados entre potências locais e potências europeias igualmente hostis a Portugal. O império português entrou em parcial colapso no Oriente, mas revelou-se bem mais resiliente no Atlântico, onde, longe de entrar em colapso foi até ganhando novos territórios e novos recursos estratégicos sobretudo no Brasil.

Até que ponto o Atlântico era a nova prioridade estratégica portuguesa ficou claro no facto de António Vieira – padre, pregador, diplomata e conselheiro destacado do novo rei português, D. João IV, restaurador de um reino independente de Espanha – ter chegado a defender a transferência da capital do Estado português para o Brasil, face à ameaça espanhola. E, de forma ainda mais marcante, no facto de isso ter efetivamente acontecido em 1808. A transferência dos órgãos centrais do Estado e da esquadra portuguesa para o Brasil, na impossibilidade de parar uma invasão napoleónica, vinha sendo discutida e planeada desde 1803. Concretizou-se quando as tropas francesas invadiram finalmente Portugal, no final do 1807 para tentar forçar o governo de Lisboa a abandonar a sua prioridade atlântica e alinhar com o sistema continental europeu dominado por Paris. Iniciou-se assim o processo que levou à criação das instituições estatais brasileiras que declaram a independência face ao governo de Lisboa, em 1822 (Pedreira e Costa, 2009).

O Atlântico como Chave da Inserção Internacional de Portugal e do Brasil

As potências lusófonas, apesar da independência do Brasil, continuaram a partilhar alguns elementos de uma cultura estratégica comum, que podemos corporizar em António Vieira ou em Alexandre de Gusmão, dois portugueses nados ou criados fora da metrópole e que tiveram grande influência na definição das prioridades da ação externa da coroa portuguesa no século XVII e XVIII[1]. Uma cultura estratégica em que a segurança marítima atlântica era vista como indispensável garantia da independência e defesa de interesses nacionais vitais. Isto implicava uma política externa em que a prioridade era uma aliança próxima com a potência naval dominante no Atlântico. O que não excluía a procura do máximo de autonomia possível face a esta última, nos limites desta necessidade geoestratégica.

Esta prioridade Atlântica na inserção no sistema global de Portugal e do Brasil manteve-se ao longo do século XIX e XX, apesar da separação dos dois Estados, e de serem atravessados por várias mudanças de regime: monarquias constitucionais, repúblicas constitucionais, repúblicas autoritárias. O chamado Terceiro Império português é um império centrado no Atlântico, numa relação simbiótica com a principal

1 Sobre estas continuidades cf. Paquette (2013).

potência atlântica no século XIX, a Grã-Bretanha. A ocupação por Portugal de vastos territórios na África Austral, em Angola e Moçambique, servia também os interesses estratégicos britânicos. Ela criava territórios tampão amigáveis nas mãos de um aliado fraco na vizinhança de importantes colónias britânicas, em particular a África do Sul. Esta última foi construída para defender a Colónia do Cabo, retirada à Holanda e anexada ao império britânico a pretexto do conflito com Napoleão, e permitia aos britânicos controlar solidamente a rota do Cabo, ligando o Atlântico ao Indo-Pacífico onde se encontrava a sua principal colónia, o Raj indiano.

O Brasil também procurou afirmar-se como um grande império do Atlântico Sul, até no seu nome oficial como Estado independente. Isso significava consolidar-se como um Estado credível no quadro do sistema de poder tradicional do Atlântico, ou seja, um Estado monárquico. Significou também manter uma relação de alinhamento próximo com a Grã-Bretanha, como garante último da segurança das suas costas e fronteiras, de financiamento e de mercado para a produção das plantações brasileiras. Isso fica bem evidente no facto do reconhecimento por Portugal da independência do Brasil, em 1825, ser negociado por via de diplomatas britânicos. Mais uma independência política do que uma descolonização em termos de modelo económico e social, a emancipação do Brasil face a Portugal tirou partido de um contexto atlântico favorável a revoluções independentistas nas Américas. O Brasil independente fez parte de uma vaga de independências nas Américas espanhola e portuguesa que encontraram um apoio decisivo em Londres. A Grã-Bretanha havia consolidado o seu predomínio naval com a derrota de Napoleão, controlando territórios chave para o controlo do Atlântico desde Halifax até às Bermudas, passando por Gibraltar, Ascensão, as Falklands ou o Cabo. Nesse contexto Londres apostou no apoio à independência das colónias americanas de Espanha e Portugal como a forma menos custosa de garantir o seu acesso em condições privilegiadas a vastos mercados que até aí lhe eram negados, criando uma esfera de influência que chegou a ser designado, por alguns autores, de império informal (Darwin, 2011).

Ou seja, para a maioria das elites governativas do Estado português e do Estado brasileiro, pareceu evidente, ao longo do século XIX e XX, a noção de que era uma prioridade estratégica manterem uma aliança próxima com a principal potência do Atlântico. Nem sempre gostavam ou partilhavam das prioridades britânicas. Basta pensar nas tensões criadas pelo violento tráfico de africanos escravizados por portugueses e brasileiros na primeira metade do século XIX (Bethell, 2009). Ou nas disputas territoriais no final do século XIX, com o Brasil em torno da Ilha da Trindade no meio do Atlântico, ou com Portugal, em torno da ambição de este unir os territórios da sua principal colónia atlântica, Angola, com a costa oriental africana de Moçambique, levando à chamada crise do *Ultimatum* de 1890. Mas em última análise, pragmaticamente, as elites portuguesas e brasileiras consideraram sempre que não havia melhor alternativa do ponto de vista dos seus interesses a

um alinhamento com a Grã-Bretanha, garantia última da sua independência, da segurança das suas costas e da sua navegação, e indispensável financiador da economia e do Estado em Portugal e no Brasil.

É verdade que no caso do Brasil se começou mais cedo a apostar na outra grande potência em ascensão no Atlântico, os EUA, logo a partir da proclamação da República brasileira em 1889 e sobretudo da revolta da Armada, de 1894, derrotada com a ajuda decisiva de meios navais norte-americanos (Herring, 2017, p. 8). Essa era também uma forma de ganhar autonomia face à tradicional dependência do poder naval e económico britânico. O chamado americanismo desenvolvido pelo Barão do Rio Branco à frente do Itamaraty (1902-1912), sempre foi muito pragmático e atento às possibilidades de reequilibrar com os EUA o tradicional peso da Grã-Bretanha – e.g., Santos (2018). Durante a década de 1930, tanto o Estado Novo português como o brasileiro, procuraram ganhar margem negocial face ao seu alinhamento tradicional e retirar vantagens do crescendo de tensões entre grandes potências, mas em última análise, a geopolítica prevaleceu sobre a ideologia (Cervo e Magalhães, 2000; Cervo, 2008; Pinheiro, 2004; Neto, 2011; Burges, 2017; Ricupero, 2017).

Portugal demorou mais tempo a fazer essa viragem. Mas a partir da Segunda Guerra Mundial, o governo de Lisboa, não teve alternativa senão reforçar as suas relações com os EUA, apesar das reservas do regime de Salazar face ao liberalismo político e económico norte-americanos. Elas foram, em parte, descansadas pela regra do consenso nas decisões tomadas pela Aliança Atlântica, ou OTAN, de que Portugal era membro fundador. E de esta Aliança Atlântica ter por objetivo estratégico principal manter a Rússia soviética e a subversão comunista fora da Europa Ocidental (Telo, 1996).

Evidentemente esta passagem de uma aliança prioritária com a Grã-Bretanha para uma aliança prioritária com os EUA não significou uma mudança radical na inserção internacional de Portugal ou do Brasil. Resultou, desde logo, da determinação das elites portuguesas e brasileiras de resistir ao comunismo, que viam como ameaça vital ao seu modo de vida, a todo o preço. Resultou, sobretudo, de uma mudança no equilíbrio de poder, refletindo o peso crescente dos EUA como a nova principal potência naval no Atlântico e a nível global.

O Ocidente e o Indo-Pacífico: Declínio, Colapso e Outros Erros

As seções anteriores permitem apontar um primeiro erro frequente na forma como se olha para esta questão. Os Estados europeus do Atlântico foram efetivamente as primeiras potências com capacidades verdadeiramente globais de projeção de poder, logo a partir do século XVI e XVII. Mas não eram ainda nessa altura as maiores potências do mundo em termos dos habituais indicadores agregados de poder

como a dimensão da população, da economia, ou dos exércitos. O pico de poder do Ocidente Euro-atlântico é muito mais tardio do que geralmente se pensa, só se consolidando claramente nos séculos XIX e XX. Durante grande parte da história conhecida a China foi a maior potência estatal do mundo. Ora, importa sublinhar que este grande peso da China ou de outras potências orientais não impediu o Ocidente de prosperar (Darwin, 2008).

O Estado chinês atingiu efetivamente a sua máxima extensão territorial no final do século XVIII, com a dinastia manchu dos Qing (1648-1911). A maioria dos historiadores considera que, pelo menos até ao início do século XIX, o imperador chinês, a partir da sua capital, em Pequim, continuava a controlar não só o maior território e a maior população do mundo, como também a maior economia, a maior burocracia estatal e o maior exército. O que faltava ao Estado chinês era uma significativa capacidade naval oceânica, pois Pequim tinha decidido, em 1439, que o modelo de sociedade chinesa era incompatível com essas inovações tecnológicas perigosas que eram os navios oceânicos. O que faltava à Pequim imperial era uma grande estratégia global que fosse para além da procura de uma hegemonia regional na Ásia Central e Oriental. O que lhe faltava cada vez mais, como resultado disso, era também uma economia dinâmica, inovadora e globalizada. Esta falta de uma visão estratégica global do império chinês, confrontado com desafios geoestratégicos continentais bem pesados, é certo, teve um preço elevado, resultando no chamado século das humilhações chinesas de meados do século XIX até meados do século XX – e.g., Westad (2012). Os riscos da complacência de uma grande potência habituada a ser o centro do mundo – China significa literalmente império central – merecem alguma reflexão no Ocidente atual.

Isto não significa, evidentemente, que desvalorizemos a importância do controlo precoce pelas potências da fachada atlântica da Europa de um sistema de comércio global com um potencial de crescimento enorme. Esta abertura para o mundo, esta intensa competição entre Estados do Atlântico Norte levou, nomeadamente, a um crescendo de inovações. A chamada Revolução Industrial, do século XVIII em diante, veio consolidar a Grã-Bretanha, pioneira neste processo e afortunadamente dotada de amplos recursos estratégicos em carvão, como a potência dominante no Atlântico e na geoestratégia global.

A invenção da invenção, ou seja, a rotinização da constante inovação tecnológica e da sua aplicação produtiva, sobretudo quando se traduziu numa revolução na produção de energia por via dos motores a vapor, levou a um crescimento explosivo dos indicadores de poder do espaço Euro-Atlântico. Levou, nomeadamente, à multiplicação de capacidades militares únicas dos Estados do Atlântico Norte: dos navios a vapor e depois a diesel, couraçados e carregados de artilharia pesada, até à produção em massa de armas automáticas capazes de disparar milhares de balas por minuto, do surgimento de explosivos avançados como a dinamite até aos

carros de combate, à aviação militar e ao armamento nuclear. Estes meios aumentaram exponencialmente a assimetria de poder económico e militar entre os Estados Euro-Atlânticos e os demais Estados. Pelo menos, até se começarem a difundir amplamente por Estados não-ocidentais, e até por atores não estatais, a partir de meados do século XX. Foi este processo de maximização da inovação tecnológica e de revolução energética que levou à afirmação das potências do Atlântico Norte com um nível de preponderância de poder entre grosso modo 1850-1950, que, sendo aquele a que nos habituámos, foi relativamente recente, breve, e absolutamente excecional na história (Headrick, 1981; McNeill, 1984).

Um segundo erro fundamental resulta de se confundir um suave declínio relativo das potências do Atlântico Norte com o seu colapso. Talvez o peso na cultura política Ocidental de Roma e da sua famosa ascensão e queda, ajude a explicar a importância destas correntes declinistas. Mas realmente um suave declínio relativo, ou um colapso completo são coisas bem diferentes.

Este suave declínio relativo do Ocidente não é, aliás, algo recente, está a acontecer há décadas. Mais, ele era inevitável tendo em conta que se partia de uma concentração de poder e riqueza nos EUA e nos seus aliados Europa Ocidental absolutamente anormal na história. O final da Segunda Guerra Mundial resultou num pico insustentável de poder económico e militar do espaço Euro-Atlântico. Estima-se que em 1945 a América do Norte sozinha tinha talvez 25% do PIB global e quase 35% do total da produção industrial global. E, claro, os EUA, até 1949, tiveram a posse exclusiva do armamento nuclear. Apesar de enfraquecidos pelos custos gigantescos de uma guerra que teve lugar no seu continente, os Estados europeus controlavam ainda todo o continente africano, com exceção da Etiópia e da Libéria assim como vastas extensões da Ásia. Mesmo a Alemanha derrotada ainda tinha, em 1945, 75% da sua capacidade industrial e, portanto, uma base sólida para uma reconstrução rápida do seu poder económico quando os EUA, através do Plano Marshall, se disponibilizaram para a apoiar (Kennedy, 1989; Ferguson, 2005; Steil, 2018).

Por que não temos dúvida em afirmar que esta concentração de poder no hemisfério Norte Atlântico era insustentável? Por três razões principais:

Primeiramente, porque é um padrão conhecido e estudado da política internacional que uma grande concentração de poder num Estado, gera uma reação dos demais Estados no sentido de contrabalançar esse risco para a sua sobrevivência e interesses. Para esse efeito é de sublinhar a eficácia particular de métodos não-convencionais para reduzir essa assimetria, em particular o recurso a insurreições armadas, a arma preferida dos fracos contra os fortes pelo seu enorme poder de desgaste de atores mais poderosos (Reis, 2017).

Em segundo lugar, porque as inovações tecnológicas resultantes da Revolução Industrial que começaram por favorecer as potências coloniais europeias e a sua capacidade de expansão pela força a um custo muito baixo, inevitavelmente difundiram-se.

Se há uma constante na história humana é o da difusão global de ferramentas de sucesso. Para dar um exemplo particularmente relevante para os temas que nos ocupam: a difusão de explosivos e de armas automáticas extremamente eficazes acabaram por resultar no enorme aumento da capacidade das insurreições armadas, de grupos dedicados à guerrilha e ao terrorismo, provocarem um tremendo desgaste mesmo em Estados coloniais militarmente muito mais poderosos. Foi tanto mais assim, quanto muitas destas insurreições armadas nos impérios europeus foram transformadas em guerras por procuração pela Rússia soviética ou pela China comunista, que passaram a financiar, armar, treinar, apoiar politicamente estes grupos independentistas como forma de contrabalançar o peso do Ocidente.

Uma terceira razão de ser insustentável a prazo esta concentração de poder no Atlântico Norte são os próprios interesses económicos dessas potências do Atlântico. Para que as economias dos EUA e da Europa Ocidental pudessem continuar a crescer a um ritmo acelerado elas precisavam de exportar. E para terem clientes novos para quem exportar precisavam que as demais regiões do globo crescessem economicamente. Mais, no quadro de uma Guerra Fria global entre os EUA e a URSS, que era também uma disputa entre dois modelos ideológicos e de desenvolvimento económico, era fundamental demonstrar que o capitalismo ocidental era mais eficaz do ponto de vista de promover o crescimento económico da periferia do que o comunismo soviético ou chinês.

O declínio relativo e suave do poder relativo do Ocidente desde o pico do seu poder tem, portanto, vindo a ter lugar desde a década de 1950. Tem também, naturalmente, sofrido oscilações importantes. Ele foi acelerado, por exemplo, pela descolonização. Ela afetou mais o poder do Ocidente do que os EUA esperavam, convencidos que estavam de que conseguiriam passar a ter relações privilegiadas com as ex-colónias europeias, emulando o que a Grã-Bretanha fizera com as ex-colónias espanholas e portuguesas nas Américas. Na verdade, muitas antigas colónias em África e na Ásia transformaram o seu capital de queixa contra o colonialismo ocidental em regimes com simpatias pelo bloco soviético. O declínio relativo do espaço Euro-Atlântico foi novamente acentuado pela forte crise económica que atingiu fortemente o Ocidente como resultado dos chamados choques petrolíferos, de 1973 em diante, que pôs fim a décadas de crescimento económico extraordinário.

Em contraste, o desfecho da Guerra Fria, em 1989-91 pareceu sinalizar uma recuperação notável do poder da Europa e dos EUA depois de algumas décadas de dificuldades. Efetivamente, as décadas finais do século XX e o início do século XXI, pelo menos até à Grande Recessão de 2008, pareceram a muitos representar o triunfo definitivo e global do modelo político e económico da região Euro-Atlântica. Esse triunfalismo exagerado teve a sua tradução no argumento de Francis Fukuyama (2006) no *The End of History*: o Ocidente tinha encontrado *a* fórmula para o desenvolvimento humano: liberalismo + capitalismo.

Seria, porém, do meu ponto de vista, um erro crasso substituir o triunfalismo de então, pelo declinismo de agora. Na verdade, logo em 1989, a repressão de manifestações a favor da liberalização do sistema político, pelo governo da República Popular da China, deveria ter-nos levado a questionar os limites deste aparente triunfo definitivo do Ocidente. Porque na história não há nada definitivo. E porque o regime comunista chinês claramente optava por uma adoção muito seletiva e parcial do modelo ocidental, que não incluía a liberalização política ou o fim do papel central do Estado na economia. Os líderes chineses incorporaram pragmaticamente aspetos da economia de mercado, para garantir a modernização da economia e um crescimento económico acelerado, mas nunca aceitaram ceder o seu controlo último sobre o Estado, a economia, a sociedade (Joseph *et al.*, 2019).

Vimos nascer na China um Leninismo de Mercado. Será esta China governada pelo Partido Comunista e enriquecida pelo mercado o sinal do triunfo de Grandes Potências autoritárias, como afirma Azar Gat (2007)? Talvez. Será que ela sinaliza o colapso inevitável do Ocidente Euro-Atlântico? Não me parece. E, mais importante, o próprio fundador desde modelo chinês de Leninismo de mercado, Deng Xiaoping (1978-1992/97) também duvidava da inevitabilidade de o século XXI ser um século (de predomínio absoluto) asiático, como se pode ver pela citação sua usada como epígrafe no início deste texto.

Vale, portanto, a pena, ponderar se autores como Paragat Khanna (2019) ou Kishore Mabubhani (2008 e 2018), que criticaram justamente alguma complacência do Ocidente no pós-Guerra Fria, não correm eles próprios o risco de alguma complacência simplista na sua análise da ascensão irresistível da Ásia e o declínio inevitável do Ocidental. Diga-se que nomeadamente Mabubhani (2020) depois de anos em que avançou essas teses, parece, no seu último livro reconhecer a necessidade de qualificar esse juízo. Nomeadamente, estas teses correm o risco de confundir variações conjunturais com mudanças estruturais, declínio relativo com colapso absoluto. Sobretudo, correm o risco de nos levar a cair num terceiro erro fundamental, apresentar o espaço Indo-Pacífico como tendo uma harmonia interna que está longe de ser a realidade, no fundo, e ironicamente, de oferecerem da Ásia uma imagem à semelhança da Europa, como um alter ego do Ocidente com um nível de coesão que não é, de todo, comparável.

Seria preciso um grande grau de cegueira para negar a excecional ascensão económica da China, com décadas de crescimento do seu PIB que passou de 2% do total global em 1960 para 15% em 2018, mas cabe notar que ainda assim face aos 23% dos EUA. Ainda mais significativo é o facto de a China não se ter contentado com ser o estaleiro do mundo, mas ter investido cada vez mais na inovação, no desenvolvimento de tecnologias de ponta como o 5G ou a Inteligência Artificial, e em novas infraestruturas. Isso traduz-se no facto de hoje se estimar que a China produz 70% dos telemóveis existentes no mundo. No combate à Covid-19 isso também ficou

evidente, com a maioria das farmacêuticas envolvidas na procura de uma cura ou de uma vacina a estarem baseadas nos EUA ou na China, mais do que na Europa. Ou com a China a produzir metade do equipamento de proteção médica a nível global. E na Ásia temos ainda a Índia também a crescer a ritmo acelerado. A China e a Índia são os únicos Estado com uma população superior a 1 bilião de pessoas. E claro que há muitos outros Estados economicamente muito dinâmicos e muito populosos no espaço Indo-Pacífico. Os asiáticos representam quase 60% da população global face a 15% de europeus e norte-americanos. A Ásia, por outras palavras, é muito maior e mais populosa do que a Europa e tem mostrado grande dinamismo económico. O Pacífico é uma bacia oceânica duas vezes maior do que a do Atlântico. Isto traz vantagens quando se trata de olhar para indicadores agregados. Mas cria enormes problemas de convergência de interesses – e.g., Silver (2020).

É, portanto, fundamental evitar um quarto erro fundamental que resulta do anterior que é o de tentar somar os indicadores de poder, desde logo militar, das potências do Indo-Pacífico, da mesma forma que o fazemos com as potências da Aliança Atlântica. Ora, a China não investe na sua defesa com o Japão. A Índia não investe na sua defesa com o Paquistão. Os gastos militares chineses devem ser vistos como sendo em grande parte gastos contra o Japão. Os gastos militares indianos devem ser vistos como sendo em grande parte gastos contra o Paquistão. E o mesmo se aplica a outros grandes Estados asiáticos. Não queremos com isto dizer que uma guerra entre a China e o Japão ou entre a Índia e o Paquistão, ou mesmo entre a Índia e a China, sejam inevitáveis. Desde logo, porque vários destes Estados têm armas nucleares ou estão protegidos por elas. Mas conflitos armados, mesmo que limitados, são bem possíveis e têm ocorrido na Ásia: as tensões no Mar do Sul da China ou nos Himalaias são apenas exemplos recentes e mais noticiados disso mesmo.

Talvez essa dinâmica se venha a alterar. Talvez a Organização de Cooperação de Xangai se transforme numa verdadeira aliança de algumas das principais potências militares euroasiáticas, nomeadamente da China, Índia, Paquistão, Rússia e eventualmente o Irão. Mas ainda estamos longe de ter na Ásia uma comunidade de segurança, onde a guerra é impensável e a cooperação é a regra, semelhante à que existe entre os países membros da OTAN e da UE. Estamos longe de uma dinâmica, como aquela que se verifica na OTAN, em que os Estados realmente investem em meios militares que podem usar mediante doutrina, treino e uma estrutura de comando comum. Estamos longe da dinâmica que se verifica no seio da UE em que os Estados investem em projetos nacionais, mas também, cada vez mais, investem de forma coordenada em capacidades militares através dos chamados projetos da cooperação estruturada permanente (PESCO), com base em orientações da Agência Europeia de Defesa e também através do orçamento comum por via do chamado Fundo Europeu de Defesa.

As potências do Atlântico Norte estão, portanto, longe de ter colapsado no campo militar. Em 2019, os EUA sozinhos ainda gastam quase tanto nas suas Forças Armadas quanto o conjunto das 14 maiores potências militares seguintes do mundo: 684 biliões de dólares face a 181 biliões da China. E neste grupo de 14 grandes potências militares, além do EUA, estão outros quatro membros europeus da OTAN – a Grã-Bretanha em sexto, a França em sétimo, a Alemanha em nono, e a Itália em décimo – isto para não falar de aliados extraeuropeus como o Japão em oitavo, ou a Coreia do Sul em décimo. A OTAN ainda hoje é, incontestavelmente, a mais poderosa, robusta, bem organizada e coesa aliança militar do mundo. Em suma, se há algo que suaviza muito o declínio relativo do Ocidente Atlântico é a sua coesão e coordenação institucionalizada. Se há algo que pode sinalizar um eventual colapso do Ocidente será o fim de organizações como a OTAN ou a UE (IISS, 2020).

Claro que um quinto erro fundamental em que não podemos cair é o de pensar que o estado atual das coisas não pode ser alterado, inclusive de forma significativa. Creio que as páginas anteriores mostram que se há uma lição da história global é que nenhum Estado, nenhuma instituição, por mais poderosa e antiga que seja, está livre do risco de colapso. E é claro que isso se aplica aos EUA, à OTAN, ou à União Europeia. Esta última é uma confederação, ou seja, uma associação de Estados que a qualquer momento a podem abandonar, portanto vulnerável a qualquer crise significativa. Os EUA são uma federação, mas com um sistema de poder repartido, de *checks and balances* muito vulnerável a uma polarização política excessiva.

Porém, e de acordo com esta mesma lógica, o risco de colapso também existe relativamente à China. A história mostra que as grandes potências asiáticas também não são imunes a crises económicas, sociais ou políticas significativas ou mesmo a um colapso do Estado. A elite chinesa parece não só estar bem ciente, mas até, segundo alguns autores, vive obcecada com o risco do colapso do Estado chinês. Afinal, foi essa a experiência traumática que a China viveu nos cem anos desde meados do século XIX até 1949 (Khan, 2018). Aliás, tendo em conta a Formosa/Taiwan este processo de reunificação da China ainda não está sequer concluído, certamente não na perspetiva dos líderes e de muitos nacionalistas chineses.

Relativamente a esta questão central defendo que o colapso do núcleo de poder económico e militar concentrado no Atlântico Norte não pode ser dado como uma certeza, mas não é impossível. O ponto fundamental que me importa deixar bem claro é que o colapso do Ocidente não será causado automaticamente pelo simples facto de outras potências ganharem riqueza e poder noutras partes do Mundo. Um verdadeiro colapso do Ocidente, pode até ser facilitado ou acelerado por fatores exógenos, mas só se verificará, em última análise, por razões endógenas, como resultado de tensões e divisões internas, de opções políticas tomadas ou não no Ocidente.

A intensificação de uma polarização cada vez mais conflituosa nos países europeus e nos EUA, e entre a Europa e a América do Norte, será um sinal de alarme importante

que tornará o colapso do Ocidente mais provável. Essa tendência a continuar a acentuar-se poderá levar ao fim da UE e da OTAN, ou, pelo menos à sua paralisia e queda na irrelevância. Efetivamente a paralisação ou mesmo uma fragmentação da UE não é inconcebível, à luz do Brexit, e da ascensão de líderes nacionalistas como Órban na Hungria. Um triunfo de Salvini e grupos ainda mais à direita na Itália, de Marine Le Pen em França, e da Alternativ for Deutschland na Alemanha poderiam levar a dinâmicas de colapso ou paralisia das instituições europeias.

Os EUA são uma federação e não uma confederação como é o caso da UE, e, por isso, são menos vulneráveis a crises conjunturais, mesmo profundas. Mas a polarização crescente, de que a presidência de Trump é um exemplo paradigmático e, também, um fator de agravamento, pode levar a sérios conflitos internos, diminuindo a capacidade e a vontade norte-americana de se envolver em questões globais. Poderá mesmo, no limite, pôr em questão a viabilidade da OTAN, uma organização que seria difícil de conceber sem os EUA ativamente engajados, e que é um pilar do poder do Ocidente.

Há aliás, sinais de que rivais estratégicos do Ocidente como a Rússia ou a China percebem este facto fundamental: o Ocidente só irá colapsar por dentro. Logicamente, procuram tirar partido destas tendências polarizadoras, e até promovê-las, numa linha de dividir para reinar recorrendo a métodos não-convencionais de desinformação e propaganda. Porém, volto a recordar que não é apenas o Ocidente que tem problemas de coesão. Como vimos, a Ásia é um continente gigantesco com grandes tensões e conflitos territoriais por resolver entre os seus principais Estados. Em particular a China e o respetivo regime enfrentarão um teste difícil quando a economia chinesa deixar de crescer de forma tão acelerada como tem sido o caso nas últimas décadas (Pei, 2020).

A pandemia da Covid-19, com o seu enorme e prolongado custo em vidas e em modos de vida, com a enorme incerteza que trouxe relativamente à melhor forma de conciliar saúde e economia, será um teste à solidez de qualquer Estado, de qualquer regime, de qualquer organização. O vírus veio relembrar o papel da contingência, dos eventos imprevistos, das crises inesperadas na evolução da política global. Pode ser que acelere a ascensão da China. Pode ser que atinja mais o Ocidente. Mas o contrário também é possível. Teremos de ver. O que é certo é que Portugal e o Brasil terão de se preparar para um mundo ainda mais incerto do que tem sido habitual.

Implicações para Portugal e o Brasil do Indo-Pacífico *Up* e do Atlântico *Down*

Algo que é certo e evidente, mas nunca é demais relembrar em face das modas do momento, é que o Atlântico pode estar a perder peso relativo em termos da geopolítica e da geoeconomia global, mas continuará a ser vital para Portugal e para o Brasil,

para o bem ou para o mal. Não se trata apenas de ter em conta a história, o facto de que a criação de Portugal e do Brasil e a sua inserção internacional estão ligadas à ascensão do Atlântico como eixo central da geopolítica global. Trata-se sobretudo de ter em conta que Portugal e o Brasil são dois Estados com uma enorme faixa costeira atlântica, onde se concentra grande parte da sua população e da sua produção. De ter em conta que é pelos portos e pelas rotas do Atlântico que Portugal e o Brasil escoam grande parte das suas exportações e recebem grande parte das suas importações. De ter em conta que é através de cabos de comunicação que atravessam o Atlântico que Portugal e o Brasil recebem e enviam grande parte dos dados vitais para a sua economia digital. As mudanças que afetem o espaço atlântico continuarão, portanto, a ser vitais para o futuro dos dois países de língua portuguesa.

Claro que a grande importância do Atlântico tanto para Portugal quanto para o Brasil não significa que ambos os países sejam afetados da mesma forma pelo declínio relativo ou pelo colapso das principais potências do Atlântico Norte. Portugal é um Estado do Atlântico Norte e tem interesses vitais investidos na relação bilateral com os EUA, na OTAN e na União Europeia, organizações de que é membro e que têm sido vitais para garantir ao país um elevadíssimo grau de segurança e prosperidade a um preço bastante comportável. Já o Brasil é um grande Estado do Atlântico Sul e um membro dos BRICS e do G20, vistos como paradigmáticos de um mundo mais multipolar e onde o Sul Global ganha peso face ao Atlântico Norte. Aliás, há muitas décadas que a elite brasileira se queixa, com alguma razão, de que a ordem global dominada pelo Ocidente Atlântico não lhes tem dado o peso devido, por exemplo, ao não ser incluído como membro permanente do Conselho de Segurança da ONU (Garcia, 2012).

Porém, também me parece simplista pensar que o Brasil beneficiará automaticamente e significativamente com a uma ascensão das potências do Indo-Pacífico. A ascensão da China ou da Índia está longe de ser equivalente de uma ascensão de todo o Sul Global. Os interesses e as prioridades do Estado chinês ou indiano no campo da economia ou da segurança e da defesa não são necessariamente convergentes com os interesses e as prioridades estratégicas do Brasil. Basta pensar no impacto do peso crescente da China como parceiro comercial do Brasil na inversão da tendência histórica para o reforço do peso da indústria na economia brasileira, que era uma prioridade estratégica tradicional do desenvolvimentismo brasileiro. Basta pensar no peso crescente da China em África. A China estabeleceu mesmo a sua primeira base militar no exterior no Djibuti, quebrando assim um tabu importante. Está cada vez mais presente inclusive nos Estados africanos ribeirinhos do Atlântico Sul e parte da ZOPACAS (Seabra, 2017). Em novembro de 2019 pela primeira vez navios militares chineses estiveram em manobras com navios russos e sul-africanos ao largo do Cabo. Não seria estranho que a China se venha a tornar mais presente militarmente no Atlântico, introduzindo uma nova grande potência

estranha à região. Claro que se pode decidir que, afinal, a agroindústria é a melhor aposta para o Brasil. Claro que se pode decidir que a ZOPACAS pode funcionar bem sem implicar a exclusão da presença militar de potências exteriores à região. O ponto crucial é que para o Estado chinês a prioridade é importar recursos naturais e exportar tecnologia, defender as rotas e os recursos vitais para a China. Para a China a prioridade é, independentemente dos interesses de outras potências, reforçar a sua influência em África ou na América Latina, onde, por exemplo, estabeleceu uma estação de rastreamento espacial na Argentina, em Neuquén. Em suma, se não exista uma convergência automática de interesses e prioridades estratégicas entre o Brasil e as potências do Atlântico Norte, ela também não me parece que exista com a China ou outras potências do Indo-Pacífico.

Convém ainda notar que, se para Portugal um colapso do Ocidente teria um custo muitíssimo elevado, é possível argumentar que o Estado português pode talvez retirar algumas vantagens do declínio relativo das grandes potências do Atlântico Norte, e de uma maior presença de outras grandes potências no espaço do Atlântico, seja uma Rússia fortalecida ou uma China emergente. Isto se Portugal souber usar este contexto para captar mais apoios de aliados tradicionais. E se o Estado português conseguir voltar a valorizar a concessão de acesso aos seus recursos estratégicos ou bases, na vasta mancha de território sob responsabilidade portuguesa no Atlântico entre o território continental e os arquipélagos dos Açores e da Madeira aos EUA, num contexto geoestratégico mais competitivo e exigente.

Por outro lado, também é possível argumentar que, menos do que Portugal, mas também o Brasil provavelmente perderia alguma coisa, pelo menos no curto prazo, com um colapso súbito das potências do Atlântico Norte. O colapso das potências do Atlântico Norte não iria resultar automaticamente e facilmente numa ordem internacional mais multilateral e mais democrática, mais justa, mais equilibrada. Parece mais provável que, pelo menos no curto prazo, um colapso do Ocidente levasse, se não ao caos, pelo menos a um período de grande incerteza e grave crise económica global, e a mais conflitos para preencher o vazio de poder criado. Numa nova ordem global que se construísse no contexto do colapso das potências do Atlântico Norte não haveria, evidentemente, lugares garantidos para ninguém no topo.

Um maior peso do Brasil na ordem internacional pode ser mais ou menos facilitado pelo contexto externo, mas evidentemente nunca acontecerá de mão-beijada. Não me parece evidente que uma ordem global mais centrada no Indo-Pacífico irá necessariamente favorecer mais o peso das potências do Atlântico Sul como o Brasil. Se olharmos para a história da política externa brasileira no último século parece-me fazer sentido argumentar que os períodos de maior sucesso do ponto de vista da afirmação da sua autonomia – da sua margem de manobra e capacidade de barganha – foram aqueles em que, mesmo que privilegiando mais as relações com potências do Ocidente, procurou alguma diversificação. Foi assim

com o Barão do Rio Branco no início do século jogando com a Grã-Bretanha e os EUA. Foi assim com Getúlio Vargas olhando para os EUA, mas também para as potências revisionistas europeias como a Alemanha de Hitler. Foi assim no período de *détente* à brasileira de Azeredo da Silveira na década de 1970 (Spektor, 2017). Se a completa equidistância parece difícil na política internacional, o pragmatismo e alguma diversificação de relações pode ser uma aposta interessante. Porque deveria o Brasil optar *a priori* entre os BRICS ou a OCDE, entre as relações com a China, com os EUA, ou com a UE? Parece possível argumentar que o grau de investimento nas diferentes relações e organizações deve ser função do que possa daí resultar para os interesses do Brasil.

Para concluir, quais serão alguma das implicações para as relações entre Portugal e o Brasil destes cenários futuros no Atlântico? Apontaria para as seguintes consequências fundamentais:

1. Não se deve esperar, simplesmente por via de uma língua comum e de uma história partilhadas, uma convergência automática entre Portugal e o Brasil quanto à forma como veem o Atlântico e definem as suas prioridades estratégicas perante os desafios globais atuais**.** A simpatia mútua e a facilidade de comunicação são úteis, mas não bastam.
2. Terá, portanto, de se trabalhar ativamente no sentido de uma mais forte relação entre Brasil e Portugal em torno do Atlântico, identificando divergências, procurando evitar mal-entendidos, e buscando pontos de convergência de interesses, assim como mecanismos de melhor cooperação. Adianto alguns exemplos nos pontos seguintes.
3. Reforçar o diálogo inter-regional. Desse ponto de vista, quer Portugal, quer o Brasil podem apostar na ratificação do acordo entre o Mercosul e a UE. Mesmo que o acordo possa ter ainda deficiências que se possa trabalhar por melhorar, parece-me, no contexto atual, mais importante do que nunca este acordo como um seguro mútuo contra os riscos de uma desglobalização caótica.
4. Investir na segurança do Atlântico. Portugal tem procurado, por exemplo com o projeto de criação de um novo Atlantic Center multinacional baseado nos Açores, contribuir para o desenvolvimento das dinâmicas de cooperação no campo da segurança e defesa no conjunto do Atlântico com o envolvimento em condições iguais de Estados e organização de todo este espaço. É verdade que, por vezes, alguns dos Estados do Atlântico Norte parecem ver-se como garantes da segurança de todo o Atlântico, sem terem em grande conta os pontos de vistas dos Estados do Atlântico Sul. Seja por essa via, ou por outras, parece, em todo o caso, fundamental reforçar os mecanismos de debate franco entre todos os Estados ribeirinhos do Atlântico sobre estes problemas. Afinal, riscos como os resultantes das mudanças climáticas ou ameaças como as do terrorismo, da pirataria ou de outras formas de criminalidade transnacional

> não reconhecem fronteiras, seja entre países, seja entre o norte e o sul do Atlântico. Isto não significa ignorar que há grandes desigualdades no seio do Atlântico, ou que há divergências de perceções e de interesses entre os Estados ribeirinhos. Significa sim procurar mecanismos para: discutir essas divergências, minorar mal-entendidos, criar confiança e encontrar os pontos de convergência possível numa cooperação que sirva os interesses de todos. Esta parece-me ser um objetivo em que Portugal e o Brasil teriam um interesse partilhado em trabalhar em conjunto.

Portugal e o Brasil têm muitas opções a fazer num mundo em que abunda a incerteza. Mas não têm a opção de deixar de ser Estados Atlânticos. Esta é uma caraterística definidora que os dois Estados partilham, que terão de ter em conta na definição das suas prioridades estratégicas. O Atlântico é um importante caminho possível para uma maior cooperação entre Portugal e o Brasil, assim o saibamos navegar no interesse de ambos os países.

Referências

BBC, 2017. Trump worries Nato with 'obsolete' comment. *BBC News* [em linha], 16 de janeiro. Disponível em https://www.bbc.com/news/world-us-canada-38635181 (acesso: 26.1.2017).

Bethell, L., 1970. 2009. *The Abolition of the Brazilian Slave Trade: Britain, Brazil and the Slave Trade Question*. Nova Iorque: Cambridge University Press.

Borges, M. O., 2013. Em torno da preparação do cerco de Lisboa (1147) e de uma possível estratégia marítima pensada por D. Afonso Henriques. *História: Revista FLUP,* vol. III, No. 3, pp. 123-144.

Burges, S., 2017. *Brazil in the world: The International Relations of a South American Giant*. Manchester: Manchester University Press.

Cervo, A., 2011. *A Parceria Inconclusa: As Relações entre Brasil e Portugal*. Belo Horizonte: Fino Traço.

Cervo, A., 2008. *Inserção Internacional: formação dos conceitos brasileiros*. São Paulo: Ed. Saraiva.

Cervo, A. e Magalhães, J. C., 2000. *Depois das Caravelas: as relações entre Portugal e Brasil, 1808-2000*. Brasília: Ed. Unb.

Clinton, H., 2011. America's Pacific Century. *Foreign Policy* [em linha], 11 de outubro, 12:41 AM. Disponível em http://foreignpolicy.com/2011/10/11/americas-pacific-century/ (acesso: 12.9.2013).

Darwin, J., 2011. *The Empire Project: The Rise and Fall of the British World-System, 1830-1970*. Cambridge: Cambridge University Press.

Darwin, J., 2008. *After Tamerlane: The Rise and Fall of Global Empires, 1400-2000*. Londres: Penguin.

Domingues, F. C., dir., 2016. *Dicionário da História da Expansão*. Mem Martins: Círculo de Leitores. 2 vols.

Domingues, F. C., 2012. *A Travessia do Mar Oceano - A Viagem de Duarte Pacheco Pereira ao Brasil em 1498*. Lisboa: Tribuna da História.

European Commission, 2019. *EU-China – A strategic outlook*. European Commission and HR/VP contribution to the European Council, 12 March. JOIN(2019) 5 final. Joint Communication to the European Parliament, the European Council and the Council, Strasbourg. Disponível em https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf

Ferguson, N., 2005. *Colossus: The rise and fall of the American Empire*, Reprint. Londres: Penguin.

Fonseca, L. A., 2011. *D. João II*. Lisboa: Temas e Debates.

Fukuyama, F., 2006. *The End of History and the Last Man*, 2nd ed. Nova Iorque: Free Press.

Garcia, E., 2012. *O Sexto Membro Permanente: o Brasil e a Criação da ONU*. Rio de Janeiro: Contraponto.

Gat, A., 2007. The Return of Authoritarian Great Powers. *Foreign Affairs*, vol. 86, no. 4, pp. 59-69.

Headrick, D. R., 1981. *The Tools of Empire: Technology and European Imperialism in the Nineteenth Century*. Oxford: Oxford University Press.

Herring, G. C., 2017. *The American Century and Beyond: U. S. Foreign Relations, 1893-2014*. Oxford: Oxford University Press.

International Institute for Strategic Studies (IISS), 2020. Comparative Defence Statistics (Chap.). Em, IISS, ed., *Military Balance 2020*. Londres: IISS/Routledge.

Kennedy, P., 1989. *The Rise and Fall of the Great Powers: Economic Change and Military Conflict from 1500 to 2000*. Londres: Vintage.

Khan, S. W., 2018. *Haunted by Chaos: China's Grand Strategy from Mao Zedong to Xi Jinping*. Cambridge MA: Harvard University Press.

Khanna, P., 2019. *The Future Is Asian*. Nova Iorque: Simon & Schuster.

Mahbubani, K., 2020. *Has China Won? The Chinese Challenge to American Primacy*. Nova Iorque: Public Affairs.

Mahbubani, K., 2018. *Has the West Lost It? A Provocation*. Londres: Penguin.

Mahbubani, K., 2009. *The New Asian Hemisphere: The Irresistible Shift of Global Power to the East*. Nova Iorque: Public Affairs.

McNeill, W. H., 1984. *The Pursuit of Power: Technology, Armed Force, and Society since A. D. 1000*. Chicago: University of Chicago Press.

Mixin Pei, M., 2020. China's Coming Upheaval: Competition, the Coronavirus, and the Weakness of Xi Jinping. *Foreign Affairs*, vol. 99, no.3, pp. 82-94.

Neto, O. A., 2011. *De Dutra a Lula: A Condução e os Determinantes da Política Externa Brasileira*. Rio de Janeiro: Campus Elsevier.

Obama, B., 2009. Full Text: Barack Obama's speech in Tokyo. *Financial Times* [em linha], 14 de novembro. Disponível em https://www.ft.com/content/9e985a46-d0c2-11de-af9c-00144feabdc0 (acesso: 14.06.2020).

Oliveira e Costa, J. P., 2013. *Henrique, o Infante*. Lisboa: A Esfera dos Livros.

Paquette, G., 2013. *Imperial Portugal in the age of Atlantic revolutions: the Luso-Brazilian world, c. 1770-1850*. Cambridge: Cambridge University Press.

Pedreira, J. e Costa, F. D., 2009. *D. João VI*. Lisboa: Temas e Debates.

Pinheiro, L., 2004. *Política Externa Brasileira (1889-2002)*. Rio de Janeiro: Zahar Editor.

Reis, B. C., 2017. *Novo Século, Novas Guerras Assimétricas? Origem, Dinâmica e Resposta a Conflitos não-Convencionais como a Guerrilha e o Terrorismo*. Lisboa: Instituto da Defesa Nacional.

Ricupero, R., 2017. *A Diplomacia na Construção do Brasil: 1750-2016*. Rio de Janeiro: Versal.

Santos, L. V., 2018. *Juca Paranhos, o Barão do Rio Branco*. Rio de Janeiro: Companhia das Letras.

Seabra, P., 2017. Stretching the Limits? Strengths and Pitfalls of South Atlantic Security Regionalism. *Contexto Internacional*, vol. 39, no. 2, pp. 77-99.

Silva, J. M. M., 2009. Operações Navais e Estratégia Marítima na Reconquista e Consolidação do Território Nacional (1147-1349). *Revista Militar*, N.º 2487. Disponível em https://www.revistamilitar.pt/artigo/469

Silver, C., 2020. The Top 20 Economies in the World. Ranking the Richest Countries in the World. *Investopedia* [em linha], Mar 18. Disponível em https://www.investopedia.com/insights/worlds-top-economies/ (acesso, 1.6.2020).

Soares, M. R. e Hirst, M. 2006. Brazil as an intermediate state and regional power: action, choice and responsibilities. *International Affairs,* vol. 82, no. 1, pp. 21-40.

Spektor, M., ed., 2010. *Azeredo da Silveira: um depoimento*. Rio de Janeiro: Fundação Getúlio Vargas.

Steil, B., 2018. *The Marshall Plan: Dawn of the Cold War*. Nova Iorque: Simon & Schuster.

Stuenkel, O., 2017. *Post-Western World: How Emerging Powers Are Remaking Global Order*. Cambridge: Polity Press.

Teixeira, N. S., Domingues, F. C. e Monteiro, J. G., 2017. *História Militar de Portugal*. Lisboa: A Esfera dos Livros.

Telo, A. J., 1996. *Do Tratado de Tordesilhas à guerra fria: reflexões sobre o sistema mundial*. Blumenau: Ed. da FURB.

Westad, O. A., 2011. *Restless Empire: China and the World Since 1750*. Nova Iorque: Basic Books.

White House, 2020. United States Strategic Approach to the People's Republic of China. *The White House* [em linha], Foreign Policy, May 26. Disponível em https://www.whitehouse.gov/wp-content/uploads/2020/05/U.S.-Strategic-Approach-to-The-Peoples-Republic-of-China-Report-5.20.20.pdf (acesso: 30.3.2020).

Williams, J. A., ed., 2019. *Politics in China: An Introduction*, 3rd ed. Oxford: Oxford University Press.

Zakaria, F., 2011. *Post-American World: Release 2.0*. Nova Iorque: W.W. Norton.

REVISTA NAÇÃO E DEFESA

Números temáticos publicados

1998	84	Inverno	Uma Nova NATO numa Nova Europa
	85	Primavera	Portugal e o Desafio Europeu
	86	Verão	O Desafio das Águas: Segurança Internacional e Desenvolvimento Duradouro
	87	Outono	O Estado em Mudança
1999	88	Inverno	Mulheres nas Forças Armadas
	89	Primavera	Portugal na NATO: 1949-1999
	90	Verão	Economia & Defesa
	91	Outono	Operações de Paz
2000	92	Inverno	Portugal e as Operações de Paz na Bósnia
	93	Primavera	Novos Rumos da Educação para a Cidadania
	94	Verão	Democracia e Forças Armadas
	95/96	Outono-Inverno	Prevenção de Conflitos e Cultura da Paz
2001	97	Primavera	Nova Ordem Jurídica Internacional
	98	Verão	Forças Armadas em Mudança
	99	Outono	Segurança para o Século XXI
	100	Inverno	De Maastricht a Nova Iorque
2002	101	Primavera	Europa e o Mediterrâneo
	102	Verão	Repensar a NATO
	103	Outono-Inverno	Novos Desafios à Segurança Europeia
	Extra	Dezembro	Cooperação Regional e a Segurança no Mediterrâneo (C4)
2003	104	Primavera	Evolução das Nações Unidas
	Extra	Abril	A Revolução nos Assuntos Militares
	105	Verão	Soberania e Intervenções Militares
	106	Outono-Inverno	A Nova Carta do Poder Mundial
2004	107	Primavera	Forças Armadas e Sociedade. Continuidade e Mudança
	Extra	Julho	Educação da Juventude. Carácter, Liderança e Cidadania
	108	Verão	Portugal e o Mar
	109	Outono-Inverno	Segurança Internacional & Outros Ensaios
2005	110	Primavera	Teoria das Relações Internacionais
	111	Verão	Raymond Aron. Um Intelectual Comprometido
	112	Outono-Inverno	Número não Temático
2006	113	Primavera	Número não Temático
	114	Verão	Segurança na África Subsariana
	115	Outono-Inverno	Portugal na Europa Vinte Anos Depois

2007	116	Primavera	Número não Temático
	117	Verão	Número não Temático
	118	Outono-Inverno	Políticas de Segurança e Defesa dos Pequenos e Médios Estados Europeus
2008	119	Primavera	Transição Democrática no Mediterrâneo
	120	Verão	Número não Temático
	121	Outono-Inverno	Estudos sobre o Médio Oriente
2009	122	Primavera	O Mar no Pensamento Estratégico Nacional
	123	Verão	Portugal e a Aliança Atlântica
	124	Outono-Inverno	Que Visão para a Defesa? Portugal-Europa-NATO
2010	125	Primavera	Visões Globais para a Defesa
	126		O Conceito Estratégico da NATO
	127		Dinâmicas da Política Comum de Segurança e Defesa da União Europeia
2011	128		O Mar no Espaço da CPLP
	129		Gestão de Crises
	130		Afeganistão
2012	131		Segurança em África
	132		Segurança no Mediterrâneo
	133		Cibersegurança
2013	134		Ásia-Pacífico
	135		Conselho de Segurança da ONU
	136		Estratégia
2014	137		Reflexões sobre a Europa
	138		Brasil
	139		Portugal na Grande Guerra
2015	140		Nuclear Proliferation
	141		Arquipélago dos Açores
	142		India
2016	143		Terrorismo Transnacional
	144		The EU Comprehensive Approach: Concepts and Practices
	145		Leituras da Grande Guerra
2017	146		Drones
	147		Brexit
	148		Grupos Islamistas Radicais

2018	149		Europe and Refugees
	150		European Defence
	151		Geopolítica Aplicada
2019	152		Terrorismo e Violência Política
	153	Agosto	Segurança Energética e Economia do Gás
	154	Dezembro	Pontes Sobre o Atlântico
2020	155	Abril	Desafios Europeus

Política Editorial

A *Nação e Defesa* proporciona um espaço de reflexão que privilegia diferentes paradigmas e perspetivas relevantes para o conhecimento e análise de questões no quadro da segurança e defesa, no plano teórico e aplicado. A revista encontra-se vocacionada para a compreensão, exame crítico e debate de matérias no âmbito da segurança e defesa internacional e nacional.

Tem como prioridade promover o conhecimento e a reflexão pluridisciplinar, nomeadamente no campo dos Estudos de Segurança, Estudos Estratégicos, Ciência Política, História, Estudos Diplomáticos, Relações Internacionais, Sociologia, Direito Internacional Público e Economia.

Nação e Defesa é uma publicação periódica de natureza científica, que adota o sistema de arbitragem por pares na admissão e aprovação dos artigos submetidos.

Editorial Policy

Nation and Defense provides a space for reflection that privileges different paradigms and perspectives relevant to theoretical and applied analysis of security and defense matters. The journal is dedicated to the critical examination and scientific debate on international security and defense.

Its priority is to promote a multidisciplinary approach to Security Studies, Strategic Studies, Political Science, History, Diplomatic Studies, International Relations, Sociology, International Law and Economics.

Nation and Defense is a scientific publication, which adopts the peer review system in the admission and approval of submitted articles.

NORMAS DE COLABORAÇÃO

O artigo proposto para publicação, em português ou inglês, deve ser enviado via correio eletrónico para idn.publicacoes@defesa.pt devendo observar as seguintes normas:

- Ter entre 5.000 a 8.000 palavras (espaços incluídos) em Word;
- Ser acompanhado de um resumo em português e em inglês (até 150 palavras cada);
- Ter título e palavras-chave em português e inglês;
- Ser redigido de acordo com o sistema de referências de Harvard.

Os textos submetidos devem ser inéditos, não editados ou apresentados em quaisquer outras publicações.

O artigo, sem indicação do autor e acompanhado pela Ficha de Identificação (disponível em https://www.idn.gov.pt/conteudos/documentos/FichadeAutor.pdf devidamente preenchida, será apreciado em regime de anonimato (*blind peer review*).

A revista *Nação e Defesa* adota o sistema de referência bibliográfica de Harvard, disponível em https://library.aru.ac.uk/referencing/harvard.htm. Este sistema emprega a referência autor e data no corpo do texto e uma lista de referências bibliográficas no final do artigo escrito, organizada por ordem alfabética. A lista de referências contém uma relação detalhada dos livros, revistas e fontes eletrónicas citadas.

Os artigos publicados são da inteira responsabilidade do autor.

Cada autor receberá dois exemplares da revista na morada indicada.

Ao submeter um manuscrito à revista, o(s) autor(es) declara(m) que autoriza(m), a título gracioso, a digitalização, o carregamento e a divulgação do referido artigo nas plataformas de conteúdos digitais do IDN e em repositórios e bases de dados bibliográficos. Os casos não especificados nestas normas de colaboração deverão ser apresentados ao Editor.

COLLABORATION RULES

The article submitted for publication, in Portuguese or English, must be sent by email to idn.publicacoes@defesa.pt observing the following rules:

- Length between 5,000 and 8,000 words (spaces included) in a Word format;
- Abstract in Portuguese and English (up to 150 words each);
- Title and keywords in Portuguese and English;
- Adoption of the Harvard reference system.

Submitted texts must be unpublished, unedited or presented in any other publications.

The article, without the author name and accompanied by the Identification Form available in https://www.idn.gov.pt/conteudos/documentos/author_form.pdf duly completed, will be evaluated anonymously (blind peer review).

Nation and Defense adopts the Harvard bibliographic reference system - https://library.aru.ac.uk/referencing/harvard.htm. This system uses the author and date in the text body and a list of references at the end of the article, organized in alphabetical order. The reference list contains a detailed list of cited books, journals and electronic sources.

Published articles are the sole responsibility of the author.

Each author will receive two copies of the journal.

By submitting a manuscript to the journal, the author (s) declare that they gracefully allow the digitization, upload, and dissemination of the article on IDN digital content platforms, repositories and bibliographic databases. Cases not specified in these collaboration rules should be submitted to the Editor.

NAÇÃO E DEFESA

Revista quadrimestral

Nome/Name _____

_____

Morada/Adress _____

_____

Localidade/City _____

Cód. Postal/Zip _____ - _____ _____

_____ NIF _____

Country _____

E-mail _____

Tel./Phone _____

☐ Renovação/Renewal – Assin. nº/Subscrip. nr. _____

☐ Nova assinatura/New subscription

Assinatura/Signature _____

Data/Date _____

Assinatura Anual/Annual Subscription (3 nºs /issues)

☐ Instituições/Institutions 40,00 €

☐ Individuais/Individuals 25,00 €

☐ Estudantes/Students 20,00 € (anexar comprovativo deste ano)

Números Anteriores/Previous Issues – 8,50 € cada/each + portes/ /postage charges

☐ ☐ ☐ ☐ ☐ ☐

Pré-Pagamento/Prepayment

☐ **Numerário**

☐ **Cheque** nº _____ Banco _____ à ordem do IDN

☐ **Transferência Bancária** NIB 0781 0112 0000 000 7777 20
(anexar comprovativo da Transferência)

☐ **Bank Transfer** (compulsory for foreign subscriptions)

IBAN – PT50 0781.0112 0000 000 7777 20
BIC (SWIFT) – IGCPPTPL

INSTITUTO DA DEFESA NACIONAL
Calçada das Necessidades, 5, 1399-017 Lisboa
PORTUGAL

www.idn.gov.pt
idn.publicacoes@defesa.pt
tel. + 351 21 392 46 00 Fax + 351 21 392 46 58

idn nação e defesa

idn Instituto da Defesa Nacional

ISSN 0870-757X
00156
9 770870 757007