INSTITUTO UNIVERSITÁRIO MILITAR

AMEAÇAS HÍBRIDAS – DESAFIOS PARA PORTUGAL

Coordenador

Tenente-coronel de Artilharia Diogo Lourenço Serrão

IUM – Centro de Investigação e Desenvolvimento (CIDIUM)
dezembro de 2023

Os **Cadernos do IUM** têm como principal objetivo divulgar os resultados da investigação desenvolvida no/sob a égide do IUM, autonomamente ou em parcerias, que não tenha dimensão para ser publicada em livro. A sua publicação não deverá ter uma periodicidade definida. Contudo, deverão ser publicados, pelo menos, seis números anualmente. Os temas devem estar em consonância com as linhas de investigação prioritárias do CIDIUM. Devem ser publicados em papel e eletronicamente no sítio do IUM. Consideram-se como objeto de publicação pelos Cadernos do IUM:

- Trabalhos de investigação dos investigadores do CIDIUM ou de outros investigadores nacionais ou estrangeiros;
- Trabalhos de investigação individual ou de grupo de reconhecida qualidade, efetuados pelos discentes, em particular pelos do CEMC e pelos auditores do CPOG que tenham sido indicados para publicação e que se enquadrem no âmbito das Ciências Militares, da Segurança e Defesa Nacional e Internacional;
- *Papers*, ensaios e artigos de reflexão produzidos pelos docentes;
- Comunicações de investigadores do IUM efetuadas em eventos científicos (e.g., seminários, conferências, *workshops*, painéis, mesas redondas), de âmbito nacional ou internacional, em Portugal ou no estrangeiro.

N.os Publicados:

1 – Comportamento Humano em Contexto Militar
Subsídio para um Referencial de Competências destinado ao Exercício da Liderança no Contexto das Forças Armadas Portuguesas: Utilização de um "Projeto STAfS" para a configuração do constructo
Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

2 – Entre a República e a Grande Guerra: Breves abordagens às instituições militares portuguesas
Coordenador: Major de Infantaria Carlos Afonso

3 – A Abertura da Rota do Ártico (*Northern Passage*). Implicações políticas, diplomáticas e comerciais
Coronel Tirocinado Eduardo Manuel Braga da Cruz Mendes Ferrão

4 – O Conflito da Síria: as Dinâmicas de Globalização, Diplomacia e Segurança
(Comunicações no Âmbito da Conferência Final do I Curso de Pós-Graduação em Globalização Diplomacia e Segurança)
Coordenadores: Tenente-coronel de Engenharia Rui Vieira
Professora Doutora Teresa Ferreira Rodrigues

5 – Os Novos Desafios de Segurança do Norte de África
Coronel Tirocinado Francisco Xavier Ferreira de Sousa

6 – Liderança Estratégica e Pensamento Estratégico
Capitão-de-mar-e-guerra Valentim José Pires Antunes Rodrigues

7 – Análise Geopolítica e Geoestratégica da Ucrânia
Coordenadores: Tenente-coronel de Engenharia Leonel Mendes Martins
Tenente-coronel Navegador António Luís Beja Eugénio

8 – Orientações Metodológicas para a elaboração de Trabalhos de Investigação
Coordenadores: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos
Tenente-coronel Técnico de Manutenção de Material Aéreo Joaquim Vale Lima

9 – A Campanha Militar Terrestre no Teatro de Operações de Angola. Estudo da Aplicação da Força por Funções de Combate
Coordenadores: Coronel Tirocinado José Luís de Sousa Dias Gonçalves
Tenente-coronel de Infantaria José Manuel Figueiredo Moreira

10 – O Fenómeno dos *"Green-on-Blue Attacks"*. *"Insider Threats"* – Das Causas à Contenção
Major de Artilharia Nelson José Mendes Rêgo

11 – Os Pensadores Militares
Coordenadores: Tenente-coronel de Engenharia Leonel José Mendes Martins
Major de Infantaria Carlos Filipe Lobão Dias Afonso

12 – *English for Specific Purposes* no Instituto Universitário Militar
Capitão-tenente ST Eling Estela do Carmo Fortunato Magalhães Parreira

13 – I Guerra Mundial: das trincheiras ao regresso
Coordenadores: Tenente-coronel de Engenharia Leonel José Mendes Martins
Major de Infantaria Fernando César de Oliveira Ribeiro

14 – Identificação e caraterização de infraestruturas críticas – uma metodologia
Major de Infantaria Hugo José Duarte Ferreira

15 – O DAESH. Dimensão globalização, diplomacia e segurança. Atas do seminário 24 de maio de 2016
Coordenadores: Tenente-coronel de Engenharia Adalberto José Centenico
Professora Doutora Teresa Ferreira Rodrigues

16 – Cultura, Comportamento Organizacional e *Sensemaking*
Coordenadores: Coronel Piloto Aviador João Paulo Nunes Vicente
Tenente-coronel Engenheira Aeronáutica Ana Rita Duarte Gomes S. Baltazar

17 – Gestão de Infraestruturas Aeronáuticas
Major Engenheira de Aeródromos Adelaide Catarina Gonçalves

18 – A Memória da Grande Guerra nas Forças Armadas
Major de Cavalaria Marco António Frontoura Cordeiro

19 – Classificação e Análise de Fatores Humanos em Acidentes e Incidentes na Força Aérea
Alferes Piloto-Aviador Ricardo Augusto Baptista Martins
Major Psicóloga Cristina Paula de Almeida Fachada
Capitão Engenheiro Aeronáutico Bruno António Serrasqueiro Serrano

20 – A Aviação Militar Portuguesa nos Céus da Grande Guerra: Realidade e Consequências
Coordenador: Coronel Técnico de Pessoal e Apoio Administrativo
Rui Alberto Gomes Bento Roque

21 – Saúde em Contexto Militar (Aeronáutico)
Coordenadoras: Tenente-coronel Médica Sofia de Jesus de Vidigal e Almada
Major Psicóloga Cristina Paula de Almeida Fachada

22 – *Storm Watching. A New Look at World War One*
Coronel de Infantaria Nuno Correia Neves

23 – Justiça Militar: A Rutura de 2004. Atas do Seminário de 03 de março de 2017
Coordenador: Tenente-coronel de Infantaria Pedro António Marques da Costa

24 – Estudo da Aplicação da Força por Funções de Combate - Moçambique 1964-1975
Coordenadores: Coronel Tirocinado de Infantaria Jorge Manuel Barreiro Saramago
Tenente-coronel de Infantaria Vítor Manuel Lourenço Ortigão Borges

25 – A República Popular da China no Mundo Global do Século XXI. Atas do Seminário de 09 de maio de 2017
Coordenadores: Professora Doutora Teresa Ferreira Rodrigues
Tenente-coronel de Infantaria Paraquedista Rui Jorge Roma Pais dos Santos

26 – O Processo de Planeamento de Operações na NATO: Dilemas e Desafios
Coordenador: Tenente-coronel de Artilharia Nelson José Mendes Rêgo

27 – Órgãos de Apoio Logístico de Marinhas da OTAN
Coordenador: Capitão-tenente de Administração Naval Duarte M. Henriques da Costa

28 – Gestão do Conhecimento em Contexto Militar: O Caso das Forças Armadas Portuguesas
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

29 – A Esquadra de Superficie da Marinha em 2038. Combate de alta Intensidade ou Operações de Segurança Marítima?
Capitão-de-mar-e-guerra Nuno José de Melo Canelas Sobral Domingues

30 – Centro de Treino Conjunto e de Simulação das Forças Armadas
Coronel Tirocinado de Transmissões Carlos Jorge de Oliveira Ribeiro

31 – Avaliação da Eficácia da Formação em Contexto Militar: Modelos, Processos e Procedimentos
Coordenadores: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro
Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

32 – A Campanha Militar Terrestre no Teatro de Operações da Guiné-Bissau (1963-1974). Estudo da Aplicação da Força por Funções de Combate
Coordenadores: Brigadeiro-general Jorge Manuel Barreiro Saramago
Tenente-coronel de Administração Domingos Manuel Lameira Lopes

33 – O Direito Português do Mar: Perspetivas para o Séc. XXI
Coordenadora: Professora Doutora Marta Chantal Ribeiro

8 – Orientações Metodológicas para a elaboração de Trabalhos de Investigação (2.ª edição, revista e atualizada)
Coordenadores: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos
Coronel Técnico de Manutenção de Material Aéreo Joaquim Vale Lima

34 – Coreia no Século XXI: Uma península global
Coordenadores: Professora Doutora Teresa Ferreira Rodrigues
Tenente-coronel Rui Jorge Roma Pais dos Santos

35 – O "Grande Médio Oriente" Alargado (Volume I)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Ricardo Dias Costa

36 – O "Grande Médio Oriente" Alargado (Volume II)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Ricardo Dias Costa

37 – As Forças Armadas no Sistema de Gestão Integrada de Fogos Rurais
Coordenador: Tenente-coronel Rui Jorge Roma Pais dos Santos

38 – A Participação do Exército em Forças Nacionais Destacas: Casos do Kosovo, Afeganistão e República Centro-Africana. Vertente Operacional e Logística
Coordenadores: Brigadeiro-general Jorge Manuel Barreiro Saramago
Major de Transmissões Luís Alves Batista
Major de Material Tiago José Moura da Costa

39 – Pensar a Segurança e a Defesa Europeia. Atas do Seminário de 09 de maio de 2019
Coordenador: Tenente-coronel Marco António Ferreira da Cruz

40 – Os Desafios do Recrutamento nas Forças Armadas Portuguesas. O Caso dos Militares Contratados
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

41 – Inovação na Gestão de Recursos Humanos nas Forças Armadas Portuguesas: Os Militares em Regime de Contrato. Atas das Comunicações do *Workshop* de 28 de janeiro de 2019
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

42 – Sistemas de Controlo de Gestão: Modelos, Processos e Procedimentos
Coordenador: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro

43 – Desafios Estratégicos para Portugal no Pós-Covid-19
Auditores Nacionais do Curso de Promoção a Oficial General 2019/2020

44 – Gestão Estratégica: Contributos para o Paradigma Estrutural da Marinha Portuguesa
Capitão-de-mar-e-guerra Nuno Sardinha Monteiro

45 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume I)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

46 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume II)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

47 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume III)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

48 – Estudos Estratégicos das Crises e dos Conflitos Armados
Coordenadores: Brigadeiro-general Lemos Pires
Tenente-coronel Ferreira da Cruz
Tenente-coronel Pinto Correia
Tenente-coronel Bretes Amador

49 – A Vulnerabilidade em Infraestruturas Críticas: Um Modelo de Análise
Tenente-coronel Santos Ferreira

50 – Função de Combate Proteção
Coordenadores: Coronel de Infantaria Paulo Jorge Varela Curro
Major de Cavalaria Rui Miguel Pinho Silva

51 – Estudos Estratégicos das Crises e dos Conflitos Armados
Coordenadores: Coronel de Cavalaria (Reformado) Marquês Silva
Tenente-coronel GNR Marco Cruz
Tenente-coronel ENGEL Silva Costa
Major Engenheiro Reis Bento

52 – Reinventar as Organizações Militares
Coordenador: Tenente-coronel de Administração Militar Carriço Pinheiro

53 – Estudos de Reflexão sobre as Informações Militares
Coordenador: Tenente-coronel de Infantaria Carlos Marques da Silva

54 – Convulsões Eurasiáticas. *in illo tempore* e agora
Coordenador: Coronel (Reformado) Carlos Manuel Mendes Dias

55 – Estratégias Marítimas – Uma Análise Comparativa (NATO, UE, Espanha, França, Itália, Portugal e Reino Unido)
Coordenadora: Capitão-tenente Sofia Saldanha Junceiro

56 – Ensino e Formação, Avaliação de Desempenho e Retenção do Talento: Dimensões para o Desenvolvimento da Liderança
Coordenador: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro

Como citar esta publicação:

Serrão, D. L. (Coord.) (2023). *Ameaças Híbridas – Desafios para Portugal*. Cadernos do IUM, 57. Lisboa: Instituto Universitário Militar.

Diretor
Tenente-General Hermínio Teodoro Maio

Editor-chefe
Coronel Delfim Zambujo das Dores

Coordenador Editorial
Coronel Delfim Zambujo das Dores

Capa – Composição Gráfica
Tenente-Coronel Técnico de Informatica Rui José da Silva Grilo

Secretariado
Assistente Técnica Gisela Cristina da rocha Basílio

Propriedade e Edição
Instituto Universitário Militar
Rua de Pedrouços, 1449-027 Lisboa
Tel.: (+351) 213 002 100
Fax: (+351) 213 002 162
E-mail: cidium@ium.pt
https://cidium.ium.pt/site/index.php/pt/publicacoes/as-colecoes

Paginação, Pré-Impressão e Acabamento
What Colour Is This?
Rua Roy Campbell Lt 5 -4º B
1300-504 Lisboa
Tel.: (+351) 219 267 950
www.wcit.pt

ISBN: 978-989-53460-9-7
ISSN: 2183-2129
Depósito Legal: 530580/24
Tiragem: 90 exemplares

Nota do Editor:

Os textos/conteúdos do presente volume são da exclusiva responsabilidade dos seus autores.

ÍNDICE

PREFÁCIO

Ao longo dos tempos, o desenvolvimento da humanidade traz-nos evoluções, muitas vezes em forma de revolução, quer na tecnologia, quer no ambiente social, com profunda transformação e sentida, com vertiginosa aceleração.

Os contextos contemporâneos enformam um ambiente estratégico, volátil e disruptivo, com níveis impressionantes de imprevisibilidade e de incerteza, com surpresas e incoerências, ao nível dos atores e competidores, na sua complexa relação e interconexão que exigem mais do que o tradicional portfólio de medidas e soluções baseadas em estratégias de previsão, de proteção e de resiliência. As alterações no modo de planear e conduzir a ação na conflitualidade, onde a paz e a guerra são um contínuo sem estado puro e onde as dimensões diversas da problematização em jogo se combinam em formas inesperadas, como as ameaças chamadas de híbridas e as operações multidomínio, impelindo a novas formulações estratégicas.

A compreensão das ameaças híbridas e o conceito de guerra híbrida têm fomentado muito a discussão aos vários níveis e mesmo alguns países, que são referência doutrinária para Portugal, têm-na adotado e preparado verdadeiros modelos de compreensão e resposta. Porém, no dizer de Horta Fernandes[1] "... a guerra híbrida pretende recobrir o espaço da guerra subversiva ou insurrecional, embora com muito mais limitações e insuficiência para dar conta da complexidade do fenómeno subversivo ou insurrecional." (Fernandes, 2021; p.99). Efetivamente, tal sobreposição verifica-se quer na questão das dimensões ou instrumentos de poder a considerar, quer no seu faseamento, quer na não predominância da luta armada e no caráter de imprevisibilidade e indeterminação da ação humana, na nebulosa que dificulta a atribuição em face dos limites legais, na diferença das guerras convencionais porque mais insidiosa, lembrando a subversão no início, etc. Enfim, tudo nos recorda a guerra subversiva e a sua complexidade, pelo que entende este especialista que estes conceitos não trazem rigorosamente nada de novo (Fernandes, 2021; p.111). André Beaufre ao erigir o conceito de estratégia indirecta, como aquela formulação que considera a decisão de utilização de outros meios, mais do que a vitória militar, utilizando como base o conceito de aproximação indireta de Liddel Hart, contido na estratégia militar direta, elege a chamada "estratégia do fraco ao forte" onde sobressaiu, na história, a utilização da guerra subversiva, sobretudo nas guerras pela autodeterminação, no período da guerra fria. Na sua estruturação e

[1] Fernandes, H. A., 2021. *O que É a Guerra. A Falácia do Conceito de Guerra Híbrida — Breve Excurso*. Nação e Defesa Nº 160, pp. 99-117.

faseamento, de vários modelos, assemelha-se em muito ao conceito da guerra híbrida e as suas ameaças e técnicas. Esta, com níveis tecnológicos mais evoluídos com expressão na ciberguerra, nas operações de informação, na ação externa e ocupando todos os domínios buscando a sinergia pela integração, parece diferenciar-se não especificamente na assimetria de meios entre o fraco e o forte, mas na assimetria de valores dos seus atores, Estados com dimensão de potências, com ênfase na derrogação dos parâmetros do direito internacional com expressão seja no direito internacional dos direitos humanos e no direito internacional humanitário.

A razão do seu estudo e investigação aparecem assim, mais do que pela sua novidade, pela necessidade de garantir a capacidade de prevenção e combate a esta forma de guerra, que também passará pela implementação de uma estratégia multissetorial e através de uma resposta integrada da sociedade. Está, no fundo, em causa a compreensão da natureza intemporal da Guerra com o seu caracter transmutável acelerado que coloca no tabuleiro, atores estatais e não estatais, mas ao serviço destes, com um vasto catálogo de possibilidades para manipular populações e corroer sociedades, criando stress nos processos de decisão dos Estados, ainda que com parco recurso ao instrumento militar. Estes desafios exigem respostas intra e intergovernamentais enquadradas por uma visão mais global e partilhada, e que tenham aplicação, através de políticas, estratégias e medidas também inovadoras e consistentes e que se configurem num dado nível de resiliência.

Com efeito, este assunto passou a ser prioridade nas agendas da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN). Em 2016, a Comissão Europeia e o Serviço Europeu para Ação Externa desenvolveram 22 medidas para aumentar a resiliência dos seus Estados membros. Também a OTAN, declarou um conjunto de medidas em julho de 2016 e atualizou-as em 2018. Porém, mais recentemente e ao nível nacional, a adesão de Portugal como país membro do Centro de Excelência para o Combate a Ameaças Híbridas (Hybrid CoE)[2], que conta com membros da UE e da OTAN, e a elaboração do documento de enquadramento nacional das ameaças híbridas, com uma perspetiva conjunta e interministerial sobre a posição de Portugal, foram respostas efetivas face à necessidade de melhor conhecer o fenómeno.

Neste exercício, o Instituto Universitário Militar (IUM), tem vindo, desde 2020, a investigar, debater e refletir nestes temas, procurando contribuir para o conhecimento nacional sobre o que se consideram as ameaças híbridas.

[2] Tem como finalidades: (i) constituir-se como uma plataforma de partilha das boas práticas das Nações; (ii) afirmar-se como um interlocutor entre a NATO e a UE para exercícios e (iii) liderar a discussão europeia sobre o combate a ameaças híbridas através da pesquisa e troca de informação.

Foi neste sentido que se organizou o seminário internacional intitulado "*Hybrid Threats and the use of cyber domain*", a 21 de outubro de 2020, com o duplo objetivo de compreender as relações entre as ameaças híbridas e o seu uso, preferencial, do domínio ciber e conhecer quais os instrumentos ao dispor dos Estados europeus para os melhor capacitar, aumentando os seus níveis de resiliência, nestes contextos.

Neste sentido, o IUM acolheu e participou no Exercício *Cyber Phalanx*, do tipo *Command Post Exercise*, que visou o planeamento de uma operação militar da UE, conduzida nos níveis estratégico-militar e nível operacional, num contexto de ameaças híbridas e *ciber*. Foi uma atividade pioneira em Portugal, financiada pela Agência Europeia de Defesa, no período de 27 de setembro a 01 de outubro de 2021 e que contou com a participação de 130 militares oriundos de 15 países da UE e de 11 organizações internacionais.

Participou, representativamente, no Grupo de Planeamento de Trabalho de Redação do Documento Nacional para o combate a ameaças híbridas, contando com este espaço para análise e reflexão enformando um palco óbvio de escopo à investigação e produção científica como escola de pensamento militar. Em particular, apresentou em 2021, na Reunião dos Pontos Focais Nacionais da Célula da Fusão Híbrida do Centro de Informações e Situação da União Europeia, todo o trabalho produzido contribuindo para uma discussão ao nível europeu de possíveis modelos nacionais de resposta.

Desenvolveram-se seis investigações, resultando duas do Curso de Promoção a Oficial General e quatro do Curso de Estado Maior, produzidas entre 2019 e 2021. Este acervo ergueu-se num contexto ímpar de oportunidade, pois ao nível nacional, buscava-se a razão da ciência para explicitar estas intituladas novas ameaças e nova forma de guerra e questionava-se o saber militar sobre como atuar face à sua natureza camaleónica, anónima e perpetradora de efeitos nefastos nas diferentes fontes de poder, extravasando o domínio militar, através da combinação de atividades e de uma ampla exploração do domínio operacional ciber.

Com a publicação dos resultados desta investigação, pretende-se assegurar a partilha e gerar mais discussão e outros projetos de investigação, com vista a auxiliar a promoção da formulação estratégica nestes domínios e fomentar a abertura à sociedade civil e a procura da resiliência do nosso Estado.

António Martins Pereira
Tenente-General

INTRODUÇÃO GERAL

Diogo Lourenço Serrão
Tenente-coronel de Artilharia do Exército Português
Docente do Instituto Universitário Militar (IUM) (1449-027 Lisboa)
Investigador Integrado do Centro de Investigação e Desenvolvimento do IUM (CIDIUM)
dlserrao@gmail.com

As ameaças híbridas resultam de uma estratégia baseada na combinação ampla e multidimensional de métodos convencionais e não convencionais, com ações abertas e encobertas, implementadas por atores estatais e não estatais. O principal objetivo de uma ameaça híbrida é criar desestabilização política e social, refletindo-se esse impacto nos governos e nas instituições oponentes, ao criar caos e vazio de poder.

Assim, em oposição ao clássico conceito de *Military Centric Warfare* que se ancora no uso do domínio militar, outras formas de atuação em conflito ganham expressão, num contexto tecnológico e de torrente informacional que facilita a sobrevivência das ameaças híbridas, facultando-lhes prosperar anónimas e aproveitando os vazios legais (o Ciber é um bom exemplo).

A prevenção e o combate das ameaças híbridas constituem um desafio, pois estas atuam circunscritas, preferencialmente, ao âmbito do *soft* e *smart power* com expressões menores de *hard power*. O seu *modus operandis* enquadra-se num espaço com limites difusos e mal definidos no espectro do conflito, convencionado chamar-se de *grey zone*. Neste contexto de dinâmicas aceleradas e difíceis de conter, a tecnologia constitui um meio hábil para estes atores conseguirem desestabilizar, erodindo a confiança pública nas instituições governamentais e ferindo os valores fundamentais das sociedades democráticas.

Neste contexto, a prevenção e o combate às ameaças híbridas exige um quadro de intervenção, caracterizada por uma abordagem compreensiva da Defesa Nacional, alicerçada nos diferentes instrumentos de poder e de uma resposta integrada de toda a sociedade. Desta forma, a presente publicação visa apoiar os decisores, chefes militares e planeadores através de seis investigações produzidas no âmbito dos Cursos de Promoção a Oficial General e de Estado Maior, ao longo dos anos letivos de 2019/2020 e 2020/2021, sobre (i) realidades e potencialidades das ameaças híbridas; (ii) pensamento estratégico nacional e pensamento estratégico militar sobre tais ameaças; (iii) níveis de resiliência e proposta de variáveis e indicadores que permitam mensurar o estado das coisas em qualquer momento da dimensão "tempo". Os investigadores calcorrearam ao longo dos seus percursos

metodológicos, além de conceitos doutrinários e avaliação de contextos presentes, os domínios: (i) da estratégia nacional; (ii) da estratégia militar e das (iii) Operações Militares.

A primeira investigação intitulada "A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas", tem como objeto do estudo a Defesa Nacional em Portugal, numa abordagem *whole of government* e *whole of society*, considerando também as sinergias alcançáveis por Portugal, como Estado-membro da União Europeia. É posicionada no nível do pensamento estratégico nacional, com uma perspetiva de aplicação temporal alargada e abre espaço para os artigos seguintes.

Na segunda investigação com o título "A Defesa Nacional na prevenção e combate às ameaças híbridas", são propostas linhas de ação das Forças Armadas Portuguesas para o combate às ameaças híbridas. Assim, é uma investigação posicionada no patamar da estratégia militar e que procura apresentar conclusões que tenham ressonância no campo operacional, estrutural e genética e tradução nas Missões das Forças Armadas e no Sistema e Dispositivo de Forças.

Mas se as ameaças híbridas têm capacidade para, residindo no anonimato, perpetrarem ações e efeitos simultaneamente nos diferentes instrumentos de Poder do Estado alvo, então mais importante que diminuir as vulnerabilidades é avaliar a resiliência desses instrumentos de poder. Neste exercício prevalecerá a ideia de continuidade no funcionamento dos instrumentos de Poder, mesmo afetados, e recuperabilidade, melhorando a sua eficiência face ao estado inicial.

Fundamentalmente, importa estudar a resiliência, interpretando-a como metodologia que procura uma melhor preparação de sistemas complexos para uma variedade de ameaças, conhecidas ou não, onde tão bem se enquadram as ameaças híbridas. O estado de "resiliente" é um fim comum na estratégia nacional e na estratégia militar, uma vez que a capacidade de resistir e recuperar na adversidade é essencial para garantir a segurança e defesa do país.

Dessa forma as quatro seguintes investigações, têm o objetivo de propor variáveis e indicadores de resiliência, focando cada uma delas, as diferentes dimensões da análise estratégica DIME: (i) diplomático; (ii) informacional; (iii) militar e (iv) económico, entendendo-a como uma ferramenta de análise estratégica consistente e adequada.

Por fim pretendemos deixar nesta publicação um contributo objetivo, útil e motivador para continuar a investigar, refletir e debater sobre a área das ameaças híbridas.

DEFESA NACIONAL NA PREVENÇÃO E COMBATE A AMEAÇAS HÍBRIDAS

NATIONAL DEFENSE IN COUNTERING HYBRID THREATS

Autor
COR ART António José Ruivo Grilo

Orientador
CMG FZ Artur José Figueiredo Mariano Alves

1. INTRODUÇÃO

As Ameaças Híbridas (AH) e a Guerra Híbrida (GH) são conceitos que ganham expressão com os acontecimentos na Ucrânia em 2014, em que a Rússia desenvolveu ações sincronizadas, recorrendo aos diversos instrumentos de poder, de forma a explorar as vulnerabilidades dos seus adversários e a alcançar os seus objetivos políticos. Em consequência, a Organização do Tratado do Atlântico Norte (NATO) classificou tais ações como híbridas (Fernandes, 2016) e viria a referir-se, formalmente, ao termo "ameaças de guerra híbrida"[3], para caracterizar as ameaças aos países da Aliança no século XXI (North Atlantic Treaty Organization [NATO], 2014).

O atual ambiente operacional possibilita às AH a utilização de uma grande diversidade de métodos e atividades, incluindo a desinformação, a exploração da tendência crescente de dependência energética, os transportes, a chantagem económica, a pressão diplomática, o minar das instituições internacionais, o terrorismo, o crime organizado, as tecnologias disruptivas exponenciadas pelo domínio Ciber, resultando no aumento da insegurança. Em oposição ao conceito de *Military Centric Warfare* que se ancora no domínio militar, a GH procura orquestrar ações nos mais diversos domínios e usa a plasticidade e a dinâmica, para criar ambiguidade (*Countering Hybrid Threats Centre of Excellence* [Hybrid CoE], 2017).

Apesar dos conceitos de AH e GH não serem novidade, a revolução digital, iniciada no século passado, veio redimensioná-los. A dependência do armazenamento de informação, a análise integrada de dados, os avanços na inteligência artificial (IA) e a acessibilidade globalizada às tecnologias emergentes,

[3] Na Declaração Final da Cimeira da NATO de 2014.

são e serão, oportunidades de desenvolvimento nos diversos domínios, mas também riscos por potenciarem as AH (Ralph, 2016).

O combate das AH constitui, assim, um desafio, porque estas vivem no foro da impossibilidade de deteção imediata e usam elementos caracterizadores de *soft, hard* e *smart power*, atuando numa *Grey Zone* com limites difusos e mal definidos, para manipular a população e corroer os governos e as sociedades, criando *stress* nos processos de decisão dos Estados democráticos (Hybrid CoE, 2017), através da erosão da confiança publica nas instituições governamentais e do ataque aos valores fundamentais da sociedade (Comissão Europeia [CE], 2018).

É no contexto deste novo paradigma civilizacional, com desafios em termos de defesa e segurança, que as AH têm prosperado pelo potencial perturbador que trazem aos Estados de direito democrático (Pereira, 2018).

O assunto passou a ser prioridade nas agendas da União Europeia (UE)[4] e da NATO que apresentam um conjunto de linhas de ação e medidas de forma a assegurar aos Estados-Membros (EM) uma base forte que os apoie na luta coletiva contra as AH, alicerçada na colaboração interinstitucional (CE, 2016a). É, no entanto, ressalvado nesse quadro de atuação, a responsabilidade primária dos EM para fazer face às AH, pelo que deverão aumentar a sua resiliência, a fim de mitigar as vulnerabilidades nacionais (CE, 2016a).

Ao nível da documentação estratégica nacional não há, ainda, referência às AH. Contudo, as declarações da ex-Secretária de Estado da Defesa Nacional, Ana Santos Pinto, por ocasião da candidatura de Portugal a membro do Centro Europeu de Excelência para Combate de Ameaças Híbridas (CAH) (Hybrid CoE)[5], foram reveladoras da preocupação do governo no CAH. Declarou, então, que a adesão "*Resulta de um processo nacional, de reconhecimento que as AH são uma prioridade…*", acrescentando que são questões "*transversais a várias áreas do Governo*" (LUSA, 2019).

Mais recentemente, são ainda evidências da relevância e atualidade nacional do tema, o seminário sobre a importância das AH à segurança, realizado em março de 2021, organizado pela presidência portuguesa do Conselho da UE, bem como a elaboração do documento de enquadramento nacional das AH, orientado segundo uma abordagem *whole of government*, com uma perspetiva conjunta e interministerial sobre a posição de Portugal, procurando projetar os interesses

[4] A UE através da Comissão Europeia e do Serviço Europeu para Ação Externa (EEAS) desenvolveram, em 2016, medidas para aumentar a resiliência dos seus EM.
[5] A 29 agosto de 2019.

nacionais em matéria de combate de AH e como potenciar a participação nacional nas organizações internacionais.

Assim, este TII revela-se de elevada importância e acuidade, pela necessidade de reflexão sobre as linhas de ação em matéria de Defesa Nacional (DN), numa abordagem abrangente e fazendo a desconstrução conceptual da GH e das AH, para acomodar as principais linhas de orientação da UE e as sinergias criadas no âmbito da UE e da NATO.

O objeto do estudo é a DN face às AH, no contexto nacional e no âmbito dos compromissos assumidos com as organizações que integra (UE e NATO).

Atendendo à abrangência do tema, o trabalho foi delimitado nos seguintes âmbitos: tempo, conteúdo e espaço.

Em termos temporais, a investigação abrange o período a partir de 2016 por representar uma clara definição política da UE no CAH.

A investigação é delimitada ao nível do conteúdo na AH e nas medidas de orientação da UE para o CAH que tenham implicações nacionais.

No domínio espacial, delimita-se este estudo à recolha de informação tendo em conta o Espaço Estratégico de Interesse Nacional Permanente e, as prioridades da política externa e da DN no âmbito da UE e da NATO.

Com a finalidade de orientar o trabalho de investigação, foram formulados como objetivos de investigação, um objetivo geral (OG) e três objetivos específicos (OE): OG: Propor linhas de ação estratégicas no âmbito da Defesa Nacional para o Combate às Ameaças Híbridas; OE 1: Analisar o papel da Defesa Nacional no Combate às Ameaças Híbridas; OE2: Analisar o ambiente externo face às Ameaças Híbridas; OE3: Analisar o ambiente interno face às Ameaças Híbridas.

Assim, define-se uma Questão Central (QC) e três Questões Derivadas (QD): QC: Quais são as principais linhas de ação estratégicas para o Combate às Ameaças Híbridas ao nível da Defesa Nacional?; QD 1: Qual é o papel da Defesa Nacional no Combate às Ameaças Híbridas?; QD 2: Quais as principais ameaças e oportunidades da Defesa Nacional face às Ameaças Híbridas?; QD 3: Quais as principais potencialidades e vulnerabilidades da Defesa Nacional face às Ameaças Híbridas?

Para a sua realização adotou-se uma investigação baseada num raciocínio indutivo, a metodologia seguiu a estratégia de investigação qualitativa e um desenho de estudo de caso, recorrendo à análise documental e a entrevistas semiestruturadas, como instrumentos de recolha de dados e à análise de conteúdo e análise SWOT - *Strengths, Weaknesses, Opportunities* e *Threats* (respetivamente, Potencialidades, Vulnerabilidades, Oportunidades e Ameaças) como técnicas de tratamento de dados.

O trabalho de investigação é organizado em cinco capítulos. Após a introdução, no primeiro capítulo, é feito o enquadramento teórico e conceptual, no segundo capítulo. No terceiro capítulo, aborda-se o percurso metodológico nas suas diferentes fases e explicam-se o raciocínio, a estratégia de investigação, os instrumentos e as técnicas de recolha, análise e tratamento de dados utilizadas. No quarto, apresentam-se e analisam-se os resultados referentes a três assuntos: (i) a capacitação da DN face às AH, nomeadamente através dos domínios de poder; (ii) as medidas de CAH através do quadro da UE, identificando-se as principais ameaças e oportunidades para a DN no CAH, no ambiente externo e as vulnerabilidades e potencialidades, no ambiente interno; (iii) a projeção das linhas de ação estratégicas nacionais para o Combate às AH com recurso às provas da estratégia, adequabilidade, aceitabilidade e exequibilidade. Nas conclusões, no quinto capítulo, apresenta-se um breve enquadramento do trabalho, um sumário do procedimento metodológico seguido, uma súmula dos resultados obtidos e dos contributos para o conhecimento, as limitações e, sugestões para pesquisas futuras.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Neste capítulo pretende-se, inicialmente, apresentar a evolução do conceito das AH e GH e os seus contextos de aplicação. Após esse enquadramento, desconstruímos o conceito de AH, perscrutando a sua evolução e identificando o que o diferencia de outros termos comuns na fraseologia sobre os conflitos. Seguidamente, percorremos os trabalhos ao nível da NATO e UE para, como corolário, atender ao despertar nacional, revigorado no contexto da Presidência Portuguesa da UE (PPUE).

2.1. Estado da arte e revisão de literatura

A dificuldade na definição concetual das AH e GH tem limitado o seu entendimento internacional, existindo inclusive fortes divergências na interpretação do fenómeno, nas suas origens, bem como, na sua tipologia e forma de as combater. Um dos principais problemas de conceptualização tem a ver com a linguagem, existindo na literatura especializada uma panóplia de termos relacionados com esta temática, que são usados de forma indiscriminada sem definição consensual (AH, GH, conflito híbrido, influência híbrida, ataque híbrido, zona híbrida ou cinzenta). Nesse sentido, importa para a clareza concetual necessária, definir e distinguir os diferentes conceitos dentro de uma abordagem abrangente de segurança nacional

(*Multinational Capability Development Campaign* [MCDC][6], 2019).

Desta forma, o foco será o conceito de AH por enformar toda a investigação que percorre o quadro científico que sustente a apresentação final, de linhas de ação.

2.1.1. O elemento diferenciador das Ameaças Híbridas e suas manifestações

Tendo em conta a realidade que AH e GH correspondem a diferentes desafios à segurança nacional, o MCDC (2019), vem distinguir os dois conceitos. Para esta organização, as AH combinam uma ampla gama de meios não violentos para visar vulnerabilidades em toda a sociedade, a fim de minar o funcionamento, a unidade ou a vontade de seus alvos, degradando e subvertendo o *status quo*, sendo que este tipo de estratégia é usado para atingir gradualmente os objetivos dos perpetradores sem desencadear respostas decisivas, incluindo armadas. Em contraponto, a GH, consiste no desafio apresentado pela crescente complexidade do conflito armado, em que os adversários podem combinar diferentes tipos de guerra com meios não militares para neutralizar o poder militar convencional (MCDC, 2019).

Este posicionamento, apresentado na Figura 1, de distinção conceptual das AH em relação à GH durante as diferentes fases de um conflito, sustenta que as AH podem ter lugar sem nunca se chegar à GH e ao confronto direto.

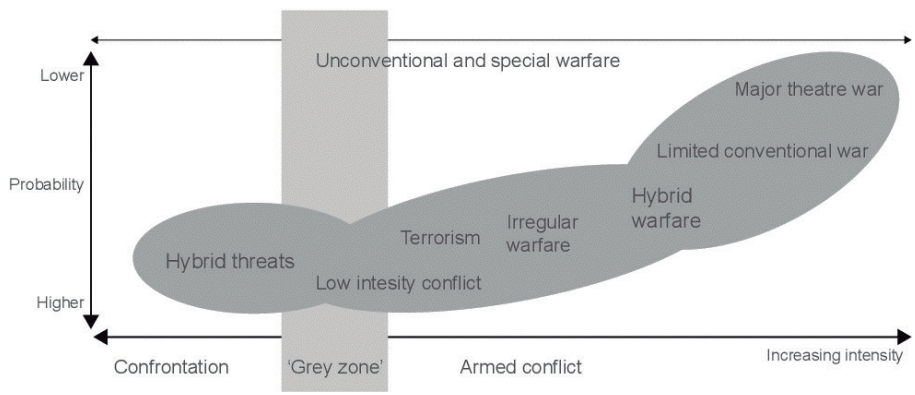


Figura 1 – Ameaças Híbridas vs Guerra Híbrida
Fonte: MCDC (2019; p. 4).

[6] MCDC *Countering Hybrid Warfare* foi um projeto que decorreu de jun17 a dez18 e incluiu 14 nações (Áustria, Canada, República Checa, Dinamarca, Alemanha, Espanha, Finlândia, Reino Unido, Noruega, Holanda, Polonia, República da Coreia, Suíça e Estados Unidos) e, envolveu a UE, a NATO e o Hybrid CoE.

Presentemente, a NATO possui uma Estratégia de CAH embora se centre fundamentalmente nas estratégias da GH fruto da sua vocação, motivo pelo qual o estudo se orienta para a UE mais centrada com a AH e o CAH, que desenvolveu um manual de instruções para combater AH[7] e criou, em Helsínquia, em 2017[8] um Hybrid Fusion Cel[9] e o Hybrid CoE (Pereira, 2018).

No âmbito da concetualização das AH, estas podem manifestar-se de diversas formas e em diferentes domínios, abrangendo "[…] desde as campanhas mediáticas à utilização de armas químicas, biológicas, radiológicas e nucleares, passando por ciberataques contra os sistemas informáticos de infraestruturas estratégicas ou pela utilização de meios de subversão da paz social ou da ordem económica" (Pereira, 2018, p. 11).

Segundo o MCDC (2019), as AH manifestam-se através de uma diversidade de tipologias de instrumentos expostas na Figura 2, forçosamente combinados (Alves, 2020) e podendo associar-se a uma variedade de cenários de guerra.

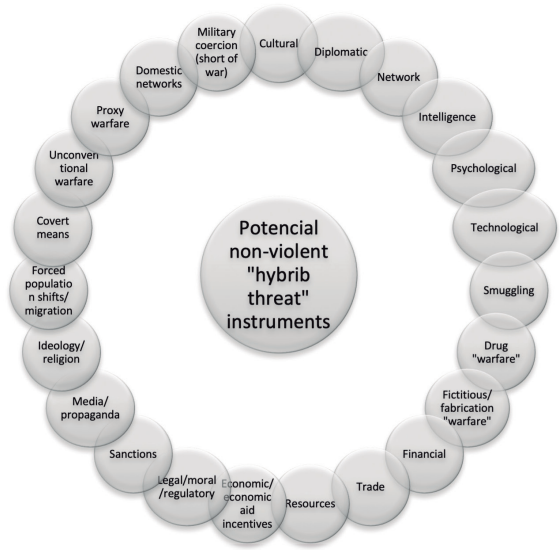


Figura 2 – Tipologia de instrumentos das Ameaças Híbridas
Fonte: Adaptado de Monaghan (2019; p.5).

[7] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.
[8] UE inaugura o *European Centre of Excellence for Countering Hybrid Threats*, 02Out17, www.hybridcoe.
[9] Vocacionado para recolha, processamento e análise de informações.

Sendo executadas "[…] quando um ator combina e sincroniza ações de forma deliberada, para atingir as vulnerabilidades sistémicas de sociedades democráticas, recorrendo a formas de atuação dos estados autoritários e outros atores para enfraquecer os sistemas democráticos" (Giannopoulos & Smith, 2019, p.4).

2.1.2. Linhas de ação da UE para o Combate de Ameaças Híbridas

Para a UE, a instabilidade nas regiões que lhe são confinantes e a evolução ao nível das ameaças, motiva um crescente número de desafios que se colocam em questões de paz, segurança e prosperidade. Assim o Presidente da Comissão Europeia, Jean-Claude Juncker salientou, nas suas orientações políticas de 2014, a necessidade de reforçar a Europa em assuntos de segurança e de defesa, enformando o que viria a ser um quadro conjunto com propostas para fazer face às AH e reforçar a resiliência da UE.

Nesse sentido, a Comissão Europeia e o Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, propuseram em abril de 2016 a adoção de um quadro comum com vinte e duas ações operacionais sustentado em 4 domínios estratégicos prioritários: (i) aumentar o conhecimento da situação; (ii) reforçar a resiliência; (iii) reforçar a capacidade dos EM e da União para prevenir e dar resposta às crises e para recuperar de forma coordenada e; (iv) reforçar a cooperação com a NATO a fim de assegurar a complementaridade das medidas (CE, 2016b).

Pretende este quadro dar aos EM uma base que os apoie na luta coletiva contra as AH, apoiado por instrumentos da UE e utilizando o potencial dos Tratados (CE, 2016b).

Mais recentemente, em junho de 2018, o Alto Representante da UE para os Negócios Estrangeiros e a Política de Segurança, em conjunto com a Comissão Europeia, publicaram uma comunicação conjunta, na qual ficaram definidas as principais linhas de orientação para CAH (CE, 2018).

Esta declaração realça a preocupação que estes desafios apresentam, mas também mostram que a capacidade de resposta deve ser combinada. Defendem assim, que o CAH deve assentar nos seguintes pilares: i) consciência situacional, tendo a UE criado, em 2017, o Hybrid Fusion Cell, que funciona no âmbito do UE Intelligence and Situation Centre Structure e do Serviço Europeu de Ação Externa, com a missão de recolha, processamento e análise de informações sobre as AH; ii) comunicação estratégica, sendo que um dos vetores de potencial sucesso das AH

reside na falta de comunicação e no isolamento dos países visados; iii) reforçar a resiliência e capacidade de contenção no setor da cibersegurança, tendo proposto a criação de um certificado de cibersegurança, o reforço das competências da Agência Europeia para a Cibersegurança, um quadro reforçado de cooperação entre EM e a UE em caso de ciberataque, bem como o conjunto de instrumentos de ciberdiplomacia e; iv) reforçar a resiliência perante atividades hostis de espionagem pretendendo, neste âmbito, melhorar a capacidade do UE Hybrid Fusion Cell no campo da contraespionagem (Pereira, 2018).

Um modelo conceptual[10] é desenvolvido pela UE em dezembro de 2019, para apoio das Nações na definição estratégias nacionais para o combate às AH, salientado atores, domínios e ferramentas e, sistematizando as bases para um plano adaptável às necessidades de cada EM da UE e da NATO (Hybrid CoE, 2020).

Neste contexto, o Hybrid CoE, sustenta que a comunicação conjunta da Comissão Europeia sobre AH, publicada em 2016, centra-se numa série de ações de nível operacional e que, por sua vez, a comunicação conjunta de 2018, fornece uma visão mais estratégica sobre o tema, claramente delineando a importância dos aspetos estratégicos como o reforço da resiliência (Giannopoulos & Smith, 2019).

2.1.3. Portugal e o conceito de Ameaças Híbridas

Entre um de janeiro e 30 de junho de 2021, Portugal assume a Presidência rotativa do Conselho da UE. O programa da Presidência assenta como principais prioridades expressas na Agenda Estratégica 2019-2024, a proteção dos cidadãos e das liberdades; o desenvolvimento de uma base económica forte e dinâmica; a construção de uma Europa com impacto neutro no clima, mais verde, mais justa e social e; a promoção dos interesses e valores europeus (CE, 2020).

No âmbito da Política Comum de Segurança e Defesa, realça-se que a capacidade de agir da UE, depende do que queremos ser capazes de fazer enquanto europeus. A análise das ameaças constituirá a base para o diálogo estratégico que contribua para um entendimento político comum e um plano de desenvolvimento de capacidades de defesa. O reforço da coesão e da capacidade de ação conjunta da NATO e da UE deverá incluir a defesa, a cibersegurança, bem como as AH (CE, 2020).

Neste âmbito da PPUE, realça-se a importância das AH, sendo reflexo disso o seminário intitulado "A importância das AH à segurança, na vizinhança sul da

[10] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.

Europa", realizado em março de 2021, organizado pela PPUE, pelo Ministério dos Negócios Estrangeiros (MNE) e pelo Hybrid CoE. Posteriormente, em abril de 2021, no seminário "AH, incluindo desinformação", organizado pelo MNE e pelo Serviço de Informações e Segurança, o Ministro dos Negócios Estrangeiros Augusto Santos Silva, alertou para as campanhas de desinformação, influência e interferência, patrocinados por rivais sistémicos da Europa, referindo-se a atores híbridos. Salienta-se ainda a constituição de um grupo de trabalho, liderado pelo MNE, de redação do documento de enquadramento nacional para fazer face às AH que, no fundo, constituirá a estratégia nacional de CAH.

2.2. Modelo de Análise

Este tema insere-se no Domínio das Ciências Militares e, enquadra-se, no âmbito da Área de Investigação das Operações Militares e do Estudo das Crises e Conflitos Armados (Decreto-Lei n.º 249, 2015), nas subáreas do Planeamento Operacional e no Planeamento Estratégico Militar.

Para além de artigos e trabalhos de investigação, de autores nacionais, utilizam-se, fontes bibliográficas de autores de origem americana e de países aliados, fundamentalmente da UE.

A dificuldade na definição concetual das AH e GH tem limitado o seu entendimento internacional, existindo divergências na sua interpretação, pelo que importa clarificar que esta investigação se foca nas AH, aproveitando fundamentalmente as sinergias da UE.

O Quadro 1 ilustra o Modelo de Análise.

Quadro 1 – Modelo de Análise

<table>
<tr><td>OBJETIVO GERAL</td><td colspan="6">Propor linhas de ação estratégicas no âmbito da Defesa Nacional para o CAH.</td></tr>
<tr><td rowspan="2">Objetivos Específicos</td><td>QUESTÃO CENTRAL</td><td colspan="5">Quais são as principais linhas de ação estratégicas para o CAH ao nível da Defesa Nacional?</td></tr>
<tr><td>QUESTÕES DERIVADAS</td><td>CONCEITOS</td><td>DIMENSÕES</td><td>INDICADORES</td><td>INSTRUMENTOS DE RECOLHA E TÉCNICAS DE TRATAMENTO DE DADOS</td><td>CRITÉRIOS DE AVALIAÇÃO</td></tr>
<tr><td>OE 1
Analisar o papel da Defesa Nacional no CAH.</td><td>QD 1
Qual é o papel da Defesa Nacional no CAH?</td><td rowspan="3">AH

CAH

Defesa Nacional

Instrumentos de Poder e Domínios

Tipologia das AH</td><td rowspan="3">Funções críticas PMESII

Ciberespaço

Conhecimento Situacional

Comunicação Estratégica

Resiliência

Prevenção e resposta a crises</td><td>Domínios
Whole of society</td><td>Análise documental</td><td rowspan="3">Entrevistas Confirmação
Adequabilidade
Aceitabilidade
Exequibilidade</td></tr>
<tr><td>OE 2
Analisar o ambiente externo face à AH.</td><td>QD 2
Quais principais ameaças e oportunidades da DN face à AH?</td><td>Ameaças

Oportunidades</td><td>Análise documental e entrevistas semiestruturadas

Análise de conteúdo e análise SWOT</td></tr>
<tr><td>OE 3
Analisar o ambiente interno face à AH</td><td>QD 3
Quais as principais potencialidades e vulnerabilidades da DN face à AH?</td><td>Potencialidades

Vulnerabilidades</td><td>Análise documental e entrevistas semiestruturadas

Análise de conteúdo e análise SWOT</td></tr>
</table>

3. METODOLOGIA E MÉTODO

Neste capítulo, inscreve-se a metodologia de investigação e o método utilizado nos instrumentos de recolha e técnicas de tratamento de dados.

3.1. Metodologia

O presente trabalho, necessariamente de investigação aplicada porque pretende elaborar contributos diretos em face da pesquisa realizada, seguirá as orientações metodológicas do Instituto Universitário Militar (IUM).

Para a abordagem metodológica deste tema, adota-se a posição ontológica construtivista, que considera que os fenómenos sociais e os seus significados são produzidos com base nas interações entre atores sociais e entre estes e a envolvente, pelo que estão em constante revisão (Bryman, 2012), e epistemológica interpretativa, que advoga que o mundo social, ao ser formado por indivíduos e pelas suas interações, não pode, nem deve ser estudado a partir dos princípios, ferramentas e técnicas das ciências naturais, competindo ao investigador não só verificar os fenómenos, mas também compreender os significados subjetivos desses mesmos fenómenos (Bryman, 2012).

Baseada num raciocínio indutivo, a metodologia segue a estratégia de investigação qualitativa e um desenho de pesquisa de estudo de caso, pela recolha de informação detalhada sobre uma unidade de estudo e análise de variação (Santos & Lima, 2019).

A Figura 3 ilustra a estrutura de investigação.

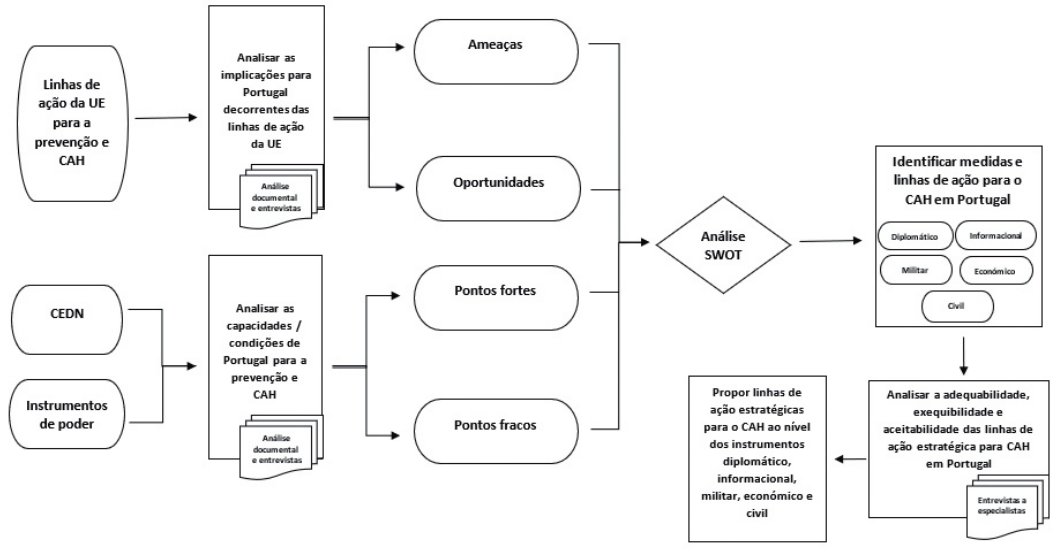


Figura 3 – Estrutura guia de investigação

3.2. Método

3.2.1. Participantes e procedimento

As entrevistas realizadas centraram-se na análise das áreas da DN do CAH. Constituíram-se em quatro entrevistas exploratórias, numa primeira fase e, posteriormente, em profundidade numa fase mais avançada, 17 entrevistas[11] dirigidas a personalidades especialistas na matéria, recorrendo à plataforma de vídeo conferência TEAMS e por email, no período de novembro a março.

As entrevistas que se constituem como uma amostra do tipo não probabilística ou empírica, intencional (Santos & Lima, 2019), foram estruturadas selecionando dois grupos de participantes. Um primeiro grupo de quatro entrevistas, a representantes de organismos centrais do estado e representantes dos diferentes instrumentos de poder que integram o grupo de trabalho liderado pelo MNE para a AH e, um segundo grupo de 13 entrevistas a estudiosos de reconhecida competência na matéria em estudo.

[11] Quantitativo enquadrado, inclusive por "excesso", na dimensão da amostra (N=12) de "informantes relativamente homogéneo", para um número de entrevistas que habitualmente permite obter saturação. (Rego, Cunha & Meyer, 2019, p. 53).

3.2.2. Instrumentos de recolha de dados

As técnicas de recolha de dados centraram-se na análise documental de fontes e origens diversas, recaindo prioritariamente nas áreas da DN, do CAH, complementada com entrevistas exploratórias, numa primeira fase e, posteriormente, entrevistas, do tipo semiestruturadas com recurso a tópicos e perguntas (Sarmento, 2013), a personalidades especialistas na matéria com o objetivo de analisar opiniões sobre os diferentes domínios considerados pertinentes para a pesquisa (Fachada, Ranhola, Marreiros & Santos, 2020).

3.2.3. Técnicas de tratamento dos dados

A análise de dados realiza-se na forma indutiva através da operacionalização de conceitos, onde as entrevistas semiestruturadas foram sujeitas a uma análise tipológica de conteúdo, para obter indicadores que permitiram inferência de conhecimentos (Fachada, et al., 2020).

A técnica de análise dos dados recolhidos é a análise categorial. Deste modo constituíram-se por questão, as unidades de contexto, determinam-se as unidades de registo e elabora-se o quadro com as unidades de contexto e registo. Seguidamente constrói-se o quadro com a análise conteúdo, onde se qualificam as unidades de registo pelas suas características comuns, as unidades de enumeração e se reagrupam em categorias (Sarmento, 2013, pp. 14-15 e 48-66). Finda análise de conteúdo por categoriais efetuou-se a análise interpretativa de resultados (Santos & Lima, 2019).

Posteriormente analisou-se o ambiente externo e o ambiente interno para permitir através de cinco Matrizes SWOT, para os domínios base das ameaças identificadas, analisar e apresentar os principais Objetivos Estratégicos e linhas de ação no CAH. As LA foram sujeitas a provas da estratégia, por validação por entrevistas de confirmação pelos critérios de adequabilidade, aceitabilidade e exequibilidade (Yarger, 2006), finalizando-se com a proposta das linhas de ação nacionais para o CAH.

4. APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

4.1. O papel da Defesa Nacional no Combate de Ameaças Híbridas: instrumentos de poder

As AH são foco de preocupação dos Estados de Direito Democrático, procurando-se uma resposta coletiva, participada e credível, através de uma

abordagem compreensiva da Defesa Nacional e uma resposta integrada de toda a sociedade.

A DN tem por objetivos garantir a soberania do Estado, a independência nacional e a integridade territorial de Portugal. Visa assegurar a liberdade e a segurança das populações e a proteção dos valores fundamentais da ordem constitucional contra qualquer agressão ou ameaça externas, e assegura ainda o cumprimento dos compromissos internacionais, de acordo com o interesse nacional (Declaração de Retificação n.º 52/2009, de 20 de julho, à Lei n.º 31-A/2009, de 7 de julho (2009)).

Salienta-se que para além da sua componente militar, a política de defesa nacional compreende as políticas sectoriais do Estado cujo contributo é necessário para a realização do interesse estratégico de Portugal e para o cumprimento dos objetivos da defesa nacional (Declaração de Retificação n.º 52/2009, de 20 de julho, à Lei n.º 31-A/2009, de 7 de julho (2009)).

O Conceito Estratégico de Defesa Nacional (CEDN), que define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional (Resolução do Conselho de Ministros n.º 19, 2013), deixou de ser um confronto exclusivamente entre forças militares, para obrigar à mobilização de todos os recursos da nação, pelo que face ao espectro das ameaças para o Estado, os recursos económicos, políticos, tecnológicos e psicológicos, transformaram-se eles próprios em instrumentos de coação (Barroso, 2008).

Por sua vez a doutrina NATO, salienta que os instrumentos do poder emanam das fontes de poder e são um conjunto de capacidades que o Estado pode utilizar para executar as suas estratégias, sistematizados em: (i) diplomático; (ii) informacional; (iii) militar e (iv) económico)[12] AJP-01 (2017).

A política de defesa nacional deve assim "[…] utilizar os instrumentos de poder político, económico, psicológico e militar de acordo com as diretivas políticas para criar os efeitos necessários à proteção dos interesses nacionais" (Yarger, 2006, p.1).

O MCDC "*Countering Hybrid Warfare Project*", salienta que um ator estatal ou não-estatal, usa numa abordagem *whole of society* os seus instrumentos de poder militar, político, económico, civil e informacional (MPECI), que também designa como funções críticas, nas vulnerabilidades política, militar, económica,

[12] Vulgarmente designados pelo seu acrónimo DIME.

social, informacional e de infraestruturas (PMESII) do seu oponente, ilustrado na Figura 4 (MCDC, 2019).

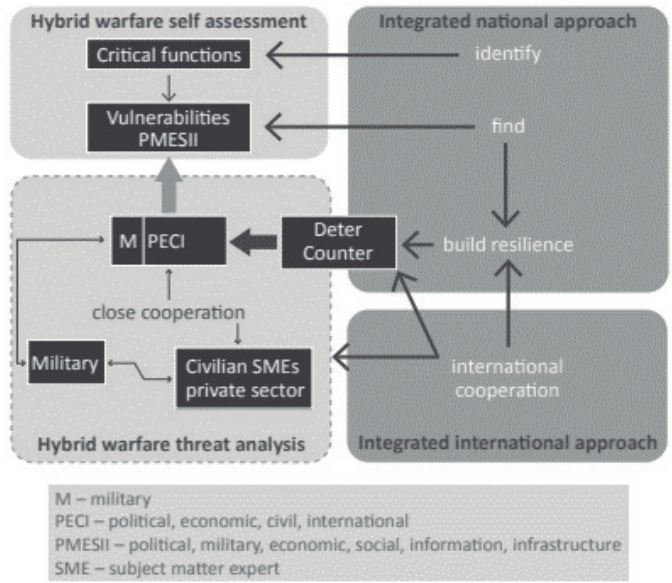


Figura 4 – Escalada da Guerra Híbrida
Fonte: MCDC (2017; p. 23).

A sua intensidade pode escalar verticalmente em intensidade e horizontalmente entre instrumentos de poder, para atingir os objetivos desejados (MCDC, 2019).

Finalmente, em dezembro de 2019[13], surge um modelo conceptual, desenvolvido pelo Hybrid CoE, para apoio das Nações na definição de estratégias nacionais para o CAH, que apresenta 13 domínios de poder e visa suprir as lacunas entre os domínios militar e civil e, ajudar a estabelecer uma base de entendimento comum e partilha entre civis e militares. De igual forma, pretende apoiar a conceção das ações certas para enfrentar as AH. A este respeito, refere-se que o modelo conceptual deve ser considerado como um ponto de referência para os decisores políticos, a fim de conceber políticas e ações eficazes e eficientes (Hybrid CoE, 2020).

[13] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.

Tendo a AH uma natureza adaptativa, que lhe possibilita prosperar no anonimato, sugere-se pensar na capacidade que os países têm para recuperar a estabilidade, apontando-se mais ao conceito de resiliência, do que propriamente, identificar fraquezas passíveis de explorar (vulnerabilidades), pelo que o CAH inclui a sua prevenção[14] (Giannopoulos & Smith, 2019).

4.1.1. Instrumentos de Poder e Domínios no Combate de Ameaças Híbridas

Considerando as diferentes abordagens aos instrumentos, funções críticas ou domínios de poder, sintetiza-se na Tabela 1 as diferentes abordagens anteriormente expostas.

Tabela 1 – Síntese de Instrumentos e Domínios de Poder

Fonte	Yarger	NATO	MCDC	Hybrid CoE UE
Instrumentos de Poder	Político		Político	Político
	Económico	Económico	Económico	Económico
	Psicológico			
	Militar	Militar	Militar	Militar e Defesa
		Diplomático		Diplomático
		Informacional	Informacional	Informacional
			Civil	
				Infraestruturas
				Ciber
				Espaço
				Cultural
				Administração Pública
				Legal
				Social
				Informações.

Fonte: Adaptado a partir de Hybrid CoE (2019), de MCDC (2019), de NATO (2017) e de Yarger (2006).

[14] O modelo conceptual procura fornecer os meios para abordar as vulnerabilidades, facilitar a deteção e fomentar a resiliência, adotando uma abordagem holística que considera devidamente a prevenção, preparação, resposta e recuperação. Também a NATO, aborda o CAH operacionalizado ao longo das três fases da sua estratégia*: Prepare – Detect – Deter*.

Apresentam-se os conceitos associados aos domínios de poder do CAH, identificados no modelo conceptual do Hybrid CoE para o CAH. Este modelo procura fornecer os meios para abordar as vulnerabilidades, facilitar a deteção e fomentar a resiliência, adotando uma abordagem global que considera devidamente a prevenção, preparação, resposta e recuperação.

O atual espectro das ameaças para o Estado, nomeadamente as AH, obriga à mobilização de todos os recursos da nação, numa abordagem compreensiva e multidisciplinar da Defesa Nacional, englobando a Segurança e Defesa de modo holístico. Com este enquadramento e considerando uma necessária abordagem *whole of society* da Defesa Nacional, para se definir quais as ações para prevenir e combater as AH, vamos valorizar os domínios do modelo conceptual como domínios de poder no CAH[15] e um ponto de referência para os decisores políticos, a fim de conceber políticas e ações eficazes e eficientes, especialmente quando se trata de deteção e de questões de atribuição destas ameaças de modo interministerial do Estado *(whole of government*) e holística multidisciplinar *(whole of society*).

Este modelo conceptual é ainda aberto, fornece um quadro flexível que permite a integração de novas ameaças e vulnerabilidades sem modificar significativamente os seus princípios fundamentais (Giannopoulos & Smith, 2019), e que pode ser adaptado às necessidades de cada EM da UE e da NATO. Face a este pressuposto, nesta fase e, dispondo de capacidades neste âmbito, o CAH assenta numa resposta articulada com a UE e a NATO. A maioria das ferramentas que podem visar o domínio espacial, explora a ligação do espaço com o ciberespaço e, com os outros domínios do CAH, realçando os potenciais efeitos em cascata, com forte ligação ainda, com o domínio militar, economia, infraestruturas, informacional e informações (Hybrid CoE, 2020), pelo que no caso nacional vamos associar este domínio ao domínio Ciber, pela exploração das suas capacidades.

Neste pressuposto, os domínios de poder do Estado para o CAH, nomeadamente da Defesa Nacional para apoiar a definição de estratégias nacionais são os: Político; Económico; Militar e Defesa; Diplomático; Informacional; Infraestruturas; Ciber e Espaço; Cultural; Administração Pública; Legal; Social; Informações.

[15] Conjunto de capacidades que o Estado pode utilizar para elaborar as suas estratégias de CAH.

4.1.2. Cooperação dos Domínios de Poder

Para a UE, esse esforço de cooperação é operacionalizado através da Criação da Célula de fusão da UE contra as AH para facilitar a partilha de conhecimento da situação, a fim de identificar qualquer alteração no contexto de segurança relacionada com uma atividade híbrida. Esta célula, ao apoiar a indicação das fontes e combater a desinformação concorre ainda em matéria de Comunicação Estratégica[16] dos EM. Através do Centro de Coordenação de Resposta de Emergência, a UE assegura a cooperação relativa à proteção da saúde pública, para a qual concorrem as capacidades de proteção civil (CE, 2016a).

Para a NATO, a cooperação e coordenação da estratégia de CAH, são operacionalizadas ao longo de três fases: *Prepare – Detect – Deter*. Nas fases *Prepare* e *Detect* através dos mecanismos de recolha, tratamento e partilha da informação controlados pelo *Hybrid analysis branch*, que providencia aos decisores informação sobre as AH. A coordenação e cooperação são chave na medida em que a transnacionalidade da AH impele a um trabalho conjunto dos serviços de informação dos Estados, para que se possa antecipar acontecimentos em determinados países em face dos que ocorrem, no presente, noutros países. Também a formação e o treino conjunto / combinado melhoram a qualidade das respostas (militares e não militares), estimulando a cooperação e coordenação entre todos os domínios de poder e do setor privado. Na fase *Deter*, a cooperação e coordenação já estabelecida é central para o processo de tomada de decisão política e operacionalização dos instrumentos de resposta (NATO, 2019).

Em termos de visão, importa referir que, no contexto internacional, as estratégias, tanto da UE como da NATO, orbitam em torno da cooperação e coordenação para fazer face às AH. Esta assunção realça a constatação de que, a edificação desta capacidade, deve estar alicerçada numa resposta articulada com a UE e a NATO, sendo irrealista uma posição nacional singular na definição de uma estratégica nacional.

Sendo as AH passiveis de prosperar no anonimato, importa ainda a cooperação transversal interministerial e coordenação para aumentar a resiliência, garantindo maior capacidade nacional para recuperar a estabilidade, também face a vulnerabilidades identificadas.

Como referido no contributo do Ministério da Defesa Nacional (MDN) para a redação do documento de enquadramento nacional para fazer face às AH,

[16] Essencial para este efeito a ligação com o Centro de Excelência em Comunicações Estratégicas da NATO e Divisão STRATCOM da European External Action Service.

apresentado ao MNE, em março de 2020, a resposta às AH só pode ser holística, abrangente, feita com todos e para todos.

Realça-se assim a necessidade de coordenação interministerial dos domínios das funções críticas da sociedade, tendente a uma avaliação interna e ligação externa à NATO[17] e UE[18]. A coordenação e cooperação são assim elementos-chave na medida em que a transnacionalidade das AH obriga a um trabalho conjunto de coordenação interministerial e dos serviços de informação dos Estados, para que se possa antecipar acontecimentos em face dos acontecimentos que ocorrem, no presente, noutros países.

Em 19 de Março de 2019, a UE adotou um regulamento[19] para criar um sistema de cooperação e troca de informações sobre investimentos de países não comunitários que possam afetar a segurança ou a ordem pública, tais como efeitos do investimento em infraestruturas e tecnologias críticas, fornecimento de inputs críticos (energia ou matérias-primas), acesso a informação sensível e capacidade de controlar a informação, ou a liberdade e pluralismo dos meios de comunicação social.

Perante este cenário, torna-se necessário apostar numa política de segurança interna e externa, cada vez mais assente numa maior colaboração e cooperação, integração e interdisciplinaridade interna e com a UE e os EM. Torna-se essencial redefinir o papel do Estado e reanalisar o conceito de Defesa Nacional, o Sistema de Segurança Interna (SSI) e, os modelos e sistemas de segurança e defesa.

O Estado Português tem como tarefas fundamentais, garantir a independência nacional e garantir os direitos e liberdades fundamentais e, promover o bem-estar e a qualidade de vida (art.º 9º da CRP).

As Forças de Segurança e as Forças Armadas (FFAA) assumem aqui um papel preponderante no âmbito da segurança do Estado, passando o seu conceito pela conjugação de áreas, consideradas "[…] estanques na dicotomia segurança interna/segurança externa e ao esforço coletivo na defesa" (Lopes, 2006, p. 10).

Pretende-se que a colaboração no âmbito do CAH, abranja a segurança e a defesa. Principalmente, pretendem-se políticas de segurança nacional, com uma maior cooperação e coordenação com políticas de segurança internacionais (NATO e UE), bem como uma gestão eficiente dos recursos humanos, das informações, das forças e serviços de segurança e de defesa, do poder judicial, do sector económico e financeiro, da tecnologia, da ciência e da diplomacia (Inácio, 2010).

---

[17] Hybrid analysis branch.
[18] Célula de fusão contra as AH.
[19] Regulation (UE) 2019/452 of the European Parliament and of the Council of 19 March 2019.

O SSI dispõe de órgão principal, o Conselho Superior de Segurança Interna (CSSI)[20]. Fazem ainda parte do SSI, um Secretário-geral[21] e o Gabinete Coordenador de Segurança[22]. O SSI, através dos seus três órgãos, detém assim mecanismos e competências para uma melhor interação com os outros sistemas internacionais da UE ou subsistemas nacionais, nomeadamente: o sistema de informações, a segurança aeronáutica e marítima, a segurança rodoviária e transportes, a segurança alimentar e económica e a segurança ambiental, o sistema criminal e a DN (Gabinete Coordenador de Segurança [GCS], 2008, p. 2).

Desde logo identificam-se necessidades de coordenação efetiva com os restantes domínios do CAH, nomeadamente Diplomático, Informacional; Ciber e Espaço; Cultura; Administração Pública; Legal; Social e o remanescente das Infraestruturas, bem como, no mesmo âmbito a efetiva coordenação no CAH com a UE e com a NATO.

No contexto nacional, aferimos a necessidade de um quadro legal de colaboração interministerial, e intersectorial (setor público e privado), que faça vigorar, a coberto de um documento nacional e respetivos planos operacionais a elaborar, medidas de coordenação e interoperabilidade de diferentes domínios de poder no âmbito da segurança nacional que não apenas o SSI[23] ou a DN. Embora não se enquadre no trabalho em curso, realçamos essa necessidade em face das observações evidenciadas por cinco entrevistados, questionados como visualizavam a centralidade da deteção, identificação, informação no âmbito das AH e, a colaboração interministerial, expressas na Tabela seguinte.

Tabela 2 – Registo de Observações à abordagem e coordenação interministerial

Entrevista	Observações
# 6	"…, Lei de Segurança Interna (LSI) não responde às AH,…, rever a LSI alavancando o Conceito de Segurança Nacional (que não existe no conceito jurídico),…, potenciar o papel do SGSSI como elemento de comando e controlo da segurança nacional e na coordenação intergovernamental,…, possível replica nacional do Hybrid Fusion Cell e comités transversais nas diferentes áreas,…, identificar o SGSSI como interlocutor horizontal e de disseminação vertical com UE Hybrid Fusion Cell e NATO Hybrid Branch,…"

[20] Órgão de audição e consulta do Primeiro-ministro (art.º 13.º, n.º 1 e 2, alínea a) e b) da LSI).
[21] Com competências de coordenação, direção, controlo e comando operacional (art.º 14 a 19º da LSI).
[22] Órgão especializado de assessoria e consulta para a coordenação técnica e operacional da atividade das forças de segurança e funciona na direta dependência do Primeiro-ministro (art.º 21.º e 22.º da LSI).
[23] Realça-se o caso australiano, que para além de comité coordenadores de diferentes áreas do SSI e DN, dispõe também de comités coordenadores transversais de natureza jurisdicional, (National Security Science and Innovation Strategy, 2009, cap. 6).

[Cont.]

# 8	"…, não temos sistema de resiliência no âmbito da DN alargada onde se inclua a segurança nacional e que monitorize e identifique ameaças e riscos,…, deixou de haver Gabinetes de Crise para monitorização,…, o mecanismo de resiliência deve ser de cúpula em âmbito ministerial,…, acima de LSI e SGSSI englobando segurança e defesa,…, com Gabinete de Crise para as Ameaças"
# 9	"…, precisamos de uma Estratégia Global do Estado, com um Conceito Nacional de Segurança e Defesa, complementar e coordenada com a UE e NATO, e Visão a 10 anos,…, necessitamos de um Conceito de DN com abordagem por domínios,…, órgão que faça levantamento de ameaças e análise,…, LSI não substitui um Conceito Estratégico de Segurança e Defesa,…, mais que uma revisão da LSI, para dar resposta à coordenação e complementaridade, precisamos de uma estratégia global e órgão que faça a articulação entre os diferentes pilares,…"
# 10	"…, não temos sistema de análise de ameaças e riscos (Sistema de Resiliência Nacional),…, o critico para o CAH é a deteção, identificação e reporte,…, LSI, não responde às necessidades,…, não temos Conceito de Segurança e DN e não se visualiza revisão constitucional, pelo que necessitamos de uma estratégia global do estado,…, um Secretariado junto 1ºministro (órgão de conselho) para a segurança e defesa, com representação alargada e com um coordenador (National Security Advisor), este secretariado vai inclui e juntar vários outros comités como terrorismo e ciber.…, Sistema de Informações (SIRP) com responsabilidades alargadas e meios de pesquisa, análise e relato ao secretariado,…"
#11	"…, resposta às AH deve ser interdepartamental,…, Conceito de DN abrangente e compreensiva,…, abordagem holística da DN, no âmbito multidisciplinar e global de segurança e defesa,…, Gabinete de crise de nível político para cooperação intergovernamental e para deteção, identificação e reporte de ameaças e riscos,…, na dependência do 1º ministro como responsável pela coordenação intergovernamental,…, se na dependência do MDN com uma abordagem compreensiva da DN, implica alteração da constituição,..."

Salienta-se a necessidade deste elemento de cooperação e coordenação interministerial para alimentar uma futura Estratégia Total no CAH, que promova a multidisciplinaridade dos domínios de poder, centralize a deteção, identificação, informação transversal e vertical com as estruturas da UE e NATO, das Ameaças e Riscos. Com base na informação recolhida e numa abordagem holística e multidisciplinar da Segurança e DN, visualiza-se um Gabinete ou Secretariado de Crise de nível político para cooperação intergovernamental e na dependência do Primeiro-Ministro como responsável pela coordenação intergovernamental. Órgão de conselho para a segurança e defesa, com representação alargada e com um coordenador, que seria responsável pela deteção, identificação e reporte de ameaças e riscos (incluindo assim vários outros comités atuais, como o do terrorismo e do ciber) e, orientando o esforço de pesquisa do Sistema de Informações (SIRP), como elemento central de pesquisa e relato. Este será um tema que se projeta para futuros desenvolvimentos, uma vez que não se constitui objeto deste trabalho.

4.1.3. Síntese Conclusiva

O atual espectro das ameaças para o Estado, nomeadamente as AH, obriga à mobilização de todos os recursos da nação, numa abordagem compreensiva e multidisciplinar da DN, englobando de modo holístico Segurança e Defesa, uma vez que para além da sua componente militar, a política de DN compreende as políticas sectoriais do Estado cujo contributo é necessário para a realização do seu interesse estratégico e para o cumprimento dos seus objetivos da DN.

As AH constituem, um desafio de natureza adaptativa, pelo que o seu combate inclui a sua prevenção, procurando preventivamente adquirir a consciência situacional e a resiliência nacional a esta ameaça, facilitando a sua deteção, a identificação e o combate, adotando um conceito que considere devidamente a prevenção, a preparação, a resposta e a recuperação. Nesta prevenção salienta-se a relevância da partilha de informação para um conhecimento situacional, sendo necessário a identificação dos elementos funcionais da rede de partilha, da rede de alerta e os elementos de combate; bem como o reforço da resiliência, nomeadamente a relativa à capacidade de garantir as funções vitais da sociedade numa situação de crise.

A análise dos documentos normativos estruturantes e a aplicação do contexto teórico de referência, permitiu a resposta à QD1 e o cumprimento do OE1, tendo identificado que os contributos da Defesa Nacional para o CAH, numa abordagem holística de Segurança e Defesa, concorrem com a utilização dos domínios de poder, Político, Económico, Militar e Defesa, Diplomático, Informacional, Infraestruturas, Ciber e Espaço, Cultural, Administração Pública, Legal, Social e, Informações, para o CAH e para a definição de estratégias nacionais e sectoriais.

Salienta-se ainda a necessidade de que, no contexto nacional, seja estudado um quadro de cooperação e coordenação interministerial, intersectorial e, entre setor público e privado e as organizações NATO e UE e, que se propõe, para futuros desenvolvimentos da temática das AH.

4.2. O ambiente externo face às Ameaças Híbridas

A análise do ambiente externo é relevante na definição de possíveis ameaças e riscos com as subsequentes oportunidades a alavancar. Ao ser, ainda, considerada a importância dos espaços cooperativos e colaborativos de que o país faz parte, assume-se relevante para Portugal a análise do quadro das AH enquanto membro da UE e da NATO, no âmbito dos espaços Político, Económico, Militar

e Defesa, Diplomático, Informacional, Infraestruturas, Ciber e Espaço, Cultural, Administração Pública, Legal, Social e, Informações.

O ambiente internacional é de grande imprevisibilidade, com a prevalência de ameaças e riscos de tipo não convencional e caráter por vezes difuso e transnacional, expressos desde logo nas regiões confinantes do continente europeu: o Norte da África, o Médio Oriente, a Europa de Leste, a África Subsariana e Atlântico, nomeadamente no Golfo da Guiné (Despacho n.º 2536, 2020, p.2).

O modelo conceptual do Hybrid CoE, desenvolvido pela UE em dezembro de 2019[24], pretende apoiar os EM na definição de estratégias nacionais para a prevenção e combate das AH, sustentando-se nos atores, domínios e ferramentas e, visa identificar as ligações entre estes, salientando-se a sua flexibilidade, podendo ser adaptado às necessidades de cada EM da UE e da NATO.

Importa, no caso nacional e tendo por base as ferramentas[25] das AH do modelo conceptual, expostas na Tabela 3, identificar, através das 17 entrevistas semiestruturadas a personalidades especialistas, as ameaças mais críticas e prováveis a Portugal, analisando também as possíveis oportunidades que se projetem em termos de ambiente externo, fruto do espaço geopolítico onde Portugal se integra.

Tabela 3 – Ferramentas do Combate de Ameaças Híbridas

Ferramenta
Operações físicas contra infraestruturas
Criar e explorar dependências em infraestruturas (incluindo dependência civil-militar)
Criar e explorar dependências económicas
Investimento direto estrangeiro
Espionagem industrial
Minar a economia nacional do adversário
Alavancagem de dificuldades económicas
Ciberespionagem
Operações Ciber
Violação do Espaço Aéreo
Violação das Águas Territoriais
Proliferação de Armas

[24] Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model*.
[25] Que combinadas, podem constituir AH.

[Cont.]

Operações militares convencional e não convencionais
Organizações Paramilitares
Exercícios Militares
Envolver as diásporas para influenciar
Financiamento de grupos culturais e de reflexão
Exploração de clivagens socioculturais (étnicas, religiosas e culturais)
Promover a agitação social
Manipular discursos sobre migração para polarizar as sociedades e minar as democracias liberais
Explorar as vulnerabilidades da Administração Publica (incluindo gestão de crises)
Promover e explorar a corrupção
Exploração de limites pouco claros, lacunas e ambiguidade da Lei
Alavancar argumentos, regras legais, processos, e instituições
Sistemas de Informações
Operações Clandestinas
Infiltração
Sansões Diplomáticas
Boicotes
Embaixadas
Criar confusão ou narrativas contraditórias
Migração como uma moeda de troca em relações internacionais
Desacreditação de lideranças e/ou candidatos
Apoio a atores políticos
Coerção de políticos e/ou governo
Exploração da imigração para influência política
Controlo e influência do Media
Campanhas de desinformação e propaganda
Influência curricular e académica
Operações eletrónicas (interferência de GNSS e falsificações)

Fonte: Hybrid CoE (2020).

4.2.1. Ambiente Externo – Quadro de Ameaças

A partir das respostas dadas à questão 1, elaboraram-se os quadros de análise das AH, com a respetiva análise categorial. Da análise dos quadros, é possível concluir quais as ameaças mais críticas a Portugal e que serão as consideradas para o desenvolvimento das principais linhas de ação estratégicas no âmbito da Defesa Nacional para o CAH, expostas na Tabela 4.

Tabela 4 – Ameaças mais críticas num quadro de AH a Portugal

Ameaças Criticabilidade Alta	Domínio Base	Domínios Afetados
38. Campanhas de desinformação e propaganda	Social	Informacional, Político, Ciber, Cultural, Administração Publica
8. Ciberespionagem	Infraestruturas	Espaço, Ciber, Militar e Defesa, Administração Publica
9. Operações Ciber	Infraestruturas	Espaço, Ciber, Social, Administração Publica, Militar e Defesa
37. Controlo e influência do Media	Informacional	Infraestruturas, Social, Cultural
3. Criar e explorar dependências económicas	Economia	Diplomático, Político, Administração Publica
25. Sistemas de Informações	Informações	Militar e Defesa
5. Espionagem industrial	Economia	Infraestruturas, Ciber, Espaço, Informações, Informacional
26. Operações Clandestinas	Informações	Militar e Defesa

Assim, de igual modo se pode inferir, que numa análise de domínio base (embora com uma afetação multidomínio), as ameaças mais críticas consideradas têm a seguinte distribuição expostas na Tabela 5:

Tabela 5 – Domínios base das Ameaças mais críticas

Domínio Base	Ameaças
Social	Campanhas de desinformação e propaganda
Infraestruturas	Ciberespionagem e Operações Ciber
Informacional	Controlo e influência do Media
Economia	Criar e explorar dependências económicas e Espionagem industrial
Informações	Sistemas de Informações e Operações Clandestinas

4.2.2 Ambiente Externo – Quadro das Oportunidades

Decorrente das respostas dadas à questão 2 das entrevistas, elaboraram-se quadros de análise das AH com a respetiva análise categorial. Da análise dos quadros do ambiente externo, referentes às oportunidades, é possível extrair o quadro de oportunidades consideradas mais relevantes e diretamente relacionadas com as ameaças mais críticas consideradas e respetivos domínios, expostos na Tabela 6.

Tabela 6 – Oportunidades do quadro de Ameaças críticas

Ameaça	Oportunidades
Campanhas de desinformação e propaganda	Gestão de perceções e educação social
	Comunicação estratégica
	Conhecimento situacional
	Estrutura de monitorização e identificação da ameaça e risco
Ciberespionagem e operações ciber	Estratégia de resiliência Ciber das Infraestruturas críticas
	Estrutura de monitorização e identificação da ameaça e risco
	Cooperação internacional NATO/UE
	Conhecimento situacional
Controlo e influência dos Media	Conhecimento situacional
	Estrutura de monitorização e identificação da ameaça e risco
Criar e explorar dependências económicas e espionagem industrial	Estratégia de resiliência económica em infraestruturas críticas
	Desenvolver indústria e planos de investimento
	Conhecimento situacional
Sistemas de Informações e Operações clandestinas	Cooperação internacional NATO/UE
	Estratégia de resiliência em ciberdefesa

4.2.3 Síntese Conclusiva

O ambiente internacional é de grande imprevisibilidade, com a prevalência de ameaças e riscos de tipo não convencional e caráter por vezes difuso e transnacional, expressos desde logo nas regiões limítrofes do continente europeu. Assim a análise do ambiente externo é clara na definição de possíveis ameaças e riscos com as subsequentes oportunidades a alavancar, devendo ser considerada a importância dos espaços cooperativos e colaborativos de que o país faz parte, nomeadamente como membro da UE e da NATO.

Através da análise categorial, das 17 entrevistas semiestruturadas às entidades especialistas, foi possível identificar os quadros de ameaças mais críticas e prováveis a Portugal no âmbito do CAH e as oportunidades consideradas mais relevantes no contexto do espaço geopolítico onde Portugal se integra. Deste modo, identifica-se a necessidade de que, no contexto nacional, a análise da ameaça dever ser valorada enquanto membros da UE e NATO, e que a nossa resiliência às AH está diretamente ligada à coesão e unidade destas organizações.

Estamos assim em condições de responder à QD2, cumprindo o OE2, de analisar o ambiente externo face às AH e expor na Tabela 7, as principais ameaças e oportunidades face às AH.

Tabela 7 – Quadro de Ameaças e Oportunidades

Ameaça	Domínio Base	Domínios afetados	Oportunidades
Campanhas de desinformação e propaganda	Social	Social, Informacional, Político, Ciber, Cultural, Administração Publica	Gestão de perceções e educação social
			Comunicação estratégica
			Conhecimento situacional
			Estrutura de monitorização e identificação da ameaça e risco
Ciberespionagem e operações ciber	Infraestruturas	Infraestruturas, Espaço, Ciber, Militar e Defesa, Administração Publica, Social	Estratégia de resiliência Ciber das Infraestruturas críticas
			Estrutura de monitorização e identificação da ameaça e risco
			Cooperação internacional NATO/UE
			Conhecimento situacional
Controlo e influência dos Media	Informacional	Informacional, Infraestruturas, Social, Cultural	Conhecimento situacional
			Estrutura de monitorização e identificação da ameaça e risco
Criar e explorar dependências económicas e espionagem industrial	Económico	Económico, Diplomático, Político, Administração Publica Infraestruturas, Ciber, Espaço, Informações, Informacional	Estratégia de resiliência económica em infraestruturas críticas
			Desenvolver indústria e planos de investimento
			Conhecimento situacional
Sistemas de Informações e Operações clandestinas	Informações	Informações, Militar e Defesa	Cooperação internacional NATO/UE
			Estratégia de resiliência em ciberdefesa

4.3. O ambiente interno face às Ameaças Híbridas

Apesar dos progressos registados nas últimas décadas, persistem ainda algumas fragilidades nacionais que condicionam o desenvolvimento. Acresce, a estes desafios estruturais, a desaceleração económica causada pela pandemia, a qual tem tido um impacto significativo ao nível interno. No seu percurso, Portugal deverá atender ao desafio de promover a recuperação decorrente dos choques causados pela pandemia, potenciando a convergência com a UE, ao qual não será alheio o seu plano de recuperação e resiliência, para explorar as potencialidades e colmatar as vulnerabilidades internas.

A análise do ambiente interno, assenta nos treze (13) domínios do CAH, para apoiar a conceção das ações certas a fim de enfrentar as AH. E conforme anteriormente referido, no presente trabalho vamos considerar doze (12) domínios,

expressos na Tabela 8, para o CAH e, para a análise categorial no ambiente interno: Político; Económico; Militar e Defesa; Diplomático; Informacional; Infraestruturas; Ciber e Espaço; Cultural; Administração Pública; Legal; Social; Informações.

Tabela 8 – Domínios de poder

Domínios de poder para o CAH
Político
Económico
Militar e Defesa
Diplomático
Informacional
Infraestruturas
Ciber e Espaço
Cultural
Administração Pública
Legal
Social
Informações

Fonte: Comissão Europeia (2018).

Importa, no caso nacional e tendo por base os domínios expressos, identificar, através das 17 entrevistas semiestruturadas às entidades especialistas, as potencialidades e vulnerabilidades que se perspetivam a Portugal, analisando o ambiente interno.

4.3.1. Ambiente Interno – Quadro de Potencialidades

A partir das respostas dadas à questão 3, no 2.º bloco de questões, elaboraram-se os quadros de análise das potencialidades, com a respetiva análise categorial. Da análise dos quadros, é possível concluir as potencialidades mais relevantes no ambiente interno num quadro de AH a Portugal e que no âmbito de trabalho em apreço serão as que vão ser consideradas para o desenvolvimento das principais linhas de ação estratégicas no âmbito da Defesa Nacional para o CAH, expostas na Tabela 9.

Tabela 9 – Potencialidades por Domínio

Domínio	Potencialidades
Político	Sistema político consolidado e estável
	Posicionamento geopolítico e pertença à NATO e UE
Económico	Inovação e indústrias tecnológicas digitais e espaciais
	Espaço UE de trocas comerciais e progresso económico
Militar e Defesa	Dispersão territorial e prontidão
	Integração NATO, UE e participação missões ONU
Diplomático	Diplomacia consolidada
	Ligação CPLP e Lusofonia
Informacional	Pluralidade e confiança na informação
	Diversidade plataformas eletrónicas de comunicação
Infraestruturas	Planos Resiliência Infraestruturas
	Infraestruturas abastecimento espaço europeu
Ciber e Espaço	Cibersegurança
	Centros de inovação e polos tecnológicos
Cultural	Identidade e Unidade Cultural
	Sociedade plural e multicultural
Administração Pública	Modernização governativa e cidadania eletrónica
	Saúde, Justiça e Educação gratuitos
Legal	Separação poderes legislativo e judicial
	Proximidade dos cidadãos à justiça
Social	Unidade nacional e coesão social
	Garantia direitos fundamentais e proteção necessitados
Informações (Intel)	Sistema integrado de centralização Intel
	Intercambio Intel com NATO e UE

4.3.2. Ambiente Interno – Quadro de Vulnerabilidades

Decorrente das respostas dadas à questão 4 do 2.º bloco de entrevistas, elaboraram-se os quadros de análise das vulnerabilidades nacionais, com a respetiva análise categorial. Da análise dos quadros do ambiente interno, é possível extrair o quadro de vulnerabilidades consideradas mais relevantes por domínios internos, expostos na Tabela 10.

Tabela 10 – Vulnerabilidades por Domínio

Domínio	Vulnerabilidades
Político	Falta consciencialização de ameaças e segurança
	Falta estratégia coordenação transversal e gestão crises integrada
Económico	Limitada competitividade económica e orçamental
	Dependência externa especialmente em recursos energéticos
Militar e Defesa	Falta de Investimento
	Resposta a ameaças multidominio e gestão crises
Diplomático	Pouca representatividade
	Falta Estratégia de cooperação e coordenação ameaças e riscos
Informacional	Consciencialização da ameaça
	Planos de ação e mecanismos de alerta
Infraestruturas	Falta Estratégia e planos de resiliência de infraestruturas
	Dependência Tecnológica
Ciber e Espaço	Estratégia espaço e resiliência ciber e digital
	Dependência tecnológica e dimensão económica
Cultural	Consciencialização da ameaça
	Capacidade económica
Administração Pública	Reforma digital e estrutural
	Falta de resiliência
Legal	Ferramentas legais pouco eficazes
	Sistema judicial moroso
Social	Literacia social
	Assimetrias sociais e demográficas
Informações (Intel)	Falta cultura e capacidades Intel
	Estratégia e resiliência Intel

4.3.3. Síntese Conclusiva

A nível interno, para além de desafios estruturais, a desaceleração económica causada pela pandemia, tem tido um impacto significativo. Portugal deverá atender ao desafio de promover a sua recuperação potenciando a convergência com a UE, ao qual não será alheio o seu plano de recuperação e resiliência, para explorar as potencialidades e colmatar as vulnerabilidades internas, de modo a preparar-se para a prevenção e CAH.

Através da análise categorial, das 17 entrevistas semiestruturadas às entidades especialistas, foi possível identificar os quadros de potencialidades

mais relevantes e vulnerabilidades mais críticas no âmbito da prevenção e CAH, considerando os diferentes domínios do ambiente interno.

Estamos assim em condições de responder à QD3, cumprindo o OE3, de analisar o ambiente interno face às AH. Assim, como resposta à QD3, as principais potencialidades e vulnerabilidades no ambiente interno, são expostas na Tabela 11.

Tabela 11 – Quadro de Potencialidades e Vulnerabilidades

Domínio	Vulnerabilidades	Vulnerabilidades
Político	Sistema político consolidado e estável	Falta consciencialização de ameaças e segurança
	Posicionamento geopolítico e pertença à NATO e UE	Falta estratégia coordenação transversal e gestão crises integrada
Económico	Inovação e indústrias tecnológicas digitais e espaciais	Limitada competitividade económica e orçamental
	Espaço UE de trocas comerciais e progresso económico	Dependência externa especialmente em recursos energéticos
Militar e Defesa	Dispersão territorial e prontidão	Falta de Investimento
	Integração NATO, UE e participação missões ONU	Resposta a ameaças multidominio e gestão crises
Diplomático	Diplomacia consolidada	Pouca representatividade
	Ligação CPLP e Lusofonia	Falta Estratégia de cooperação e coordenação ameaças e riscos
Informacional	Pluralidade e confiança na informação	Consciencialização da ameaça
	Diversidade plataformas eletrónicas de comunicação	Planos de ação e mecanismos de alerta
Infraestruturas	Planos Resiliência Infraestruturas	Falta Estratégia e planos de resiliência de infraestruturas
	Infraestruturas abastecimento espaço europeu	Dependência Tecnológica
Ciber e Espaço	Cibersegurança	Estratégia espaço e resiliência ciber e digital
	Centros de inovação e polos tecnológicos	Dependência tecnológica e dimensão económica
Cultural	Identidade e Unidade Cultural	Consciencialização da ameaça
	Sociedade plural e multicultural	Capacidade económica
Administração Pública	Modernização governativa e cidadania eletrónica	Reforma digital e estrutural
	Saúde, Justiça e Educação gratuitos	Falta de resiliência
Legal	Separação poderes legislativo e judicial	Ferramentas legais pouco eficazes
	Proximidade dos cidadãos à justiça	Sistema judicial moroso
Social	Unidade nacional e coesão social	Literacia social
	Garantia direitos fundamentais e proteção necessitados	Assimetrias sociais e demográficas

[Cont.]

Informações (Intel)	Sistema integrado de centralização intel	Falta cultura e capacidades Intel
	Intercambio intel com NATO e UE	Estratégia e resiliência Intel

4.4. Análise de *Strengths, Weaknesses, Opportunities* e *Threats* (SWOT) e Linhas de Ação Estratégicas

Este subcapítulo tem como objetivo apresentar as principais linhas de ação estratégicas para o CAH, deduzidas através da análise SWOT, correlacionando as potencialidades e vulnerabilidades, no ambiente interno, com as oportunidades e ameaças, do ambiente externo e a consequente confirmação por análise de validade.

A análise SWOT, tem por objetivo estabelecer prioridades de atuação e respetivas LA e baseia-se em quatro ideias chave: usar as potencialidades para obter vantagens sobre as oportunidades (PO); as oportunidades para superar as vulnerabilidades (VO); as potencialidades para evitar ameaças (PA); e em minimizar as vulnerabilidades para evitar ameaças (VA).

Para o efeito vão ser realizadas cinco análises SWOT, numa análise para cada domínio base (embora com uma afetação multidomínio) das ameaças mais críticas identificadas, com uma posterior correlação final e identificação dos principais Objetivos Estratégicos nacionais no CAH e propor as respetivas LAE de acordo com as provas da estratégia pela validação por critérios de adequabilidade, aceitabilidade e exequibilidade.

4.4.1. Objetivos Estratégicos e Linhas de Ação no CAH

Das análises SWOT realizadas aos domínios Social, Infraestruturas, Informacional, Económico e Informações e que se referem aos domínios base das ameaças mais críticas identificadas, identificam-se duas constatações. Identificam-se, desde logo, as principais linhas de ação (LA) no CAH que resultam das principais ameaças identificadas no âmbito do CAH e, simultaneamente assegura-se o seu enquadramento, agrupando as LA de acordo com as estratégias prioritárias identificadas nas dimensões do modelo de análise: (i) aumentar o conhecimento situacional; (ii) reforçar a resiliência; (iii) reforçar a capacidade de prevenir e dar resposta às crises e recuperar de forma coordenada na UE; (iv) reforçar a comunicação estratégica (CE, 2016b, 2018).

4.4.2. Confirmação das linhas de ação estratégicas

Toda a estratégia tem a sua própria lógica inerente que deve ser confirmada para determinar a sua validade, deve promover a adequabilidade de recursos, a aceitabilidade de conceitos e a exequibilidade, pela satisfação das metas e interesses (Yarger, 2006, p. 62).

Esta confirmação por validação de adequação, de exequibilidade e aceitabilidade, foi realizada com 4 entrevistas a entidades especialistas, que permitiram confirmar e consolidar as LAE no âmbito da Defesa Nacional para o CAH.

Assim, enquadrado nas provas da estratégia foi questionado, no âmbito da adequação, se a realização dos objetivos e LA propostas nos domínios indicados, vão produzir resultados; no âmbito da exequibilidade se as LA propostas, podem ser executadas com os recursos disponíveis; e no âmbito da aceitabilidade se os resultados esperados justificam as ações propostas nas LA.

As questões de adequação, exequibilidade, e aceitabilidade são questões para classificação de Elevada, Neutra ou Baixa incidem sobre a validade das propostas LA, pelo que é também questionado o risco, pela avaliação das prováveis consequências do sucesso e do fracasso das LA propostas, resultando num reescrever e melhoria das mesmas (Yarger, 2006, pg. 71).

4.4.3. Síntese Conclusiva

A dimensão multidimensional e transnacional das AH, vem reforçar a necessidade de existir uma visão alargada, com uma abordagem multi-instituicional, transversal e integrada *whole of government* e *whole of society* para se prevenir e combater a AH, aumentando a necessidade de reforçar a cooperação entre entidades no contexto nacional e no âmbito dos compromissos com as organizações de que faz parte (UE e NATO), através das sinergias da UE no âmbito da AH.

Através da análise SWOT centrada nos domínios Social, Infraestruturas, Informacional, Económico e Informações, foi possível identificar as 23 principais LA no CAH que resultam das principais ameaças identificadas no âmbito do CAH.

Posteriormente confirmaram-se as LA identificadas, através de entrevistas de validação de adequação, exequibilidade, e aceitabilidade, pelo que estamos em condições de responder à QC, cumprindo o OG e propondo 21 LAE no âmbito da Defesa Nacional para o CAH, como resposta à QC, expostas na Tabela 12.

Tabela 12 – Objetivos e LA Estratégicas

ObjEst	LAE
Aumentar o Conhecimento Situacional	LAE 1 - Criar mecanismos de integração, de vigilância e alerta e coordenação interministerial de ameaças e riscos.
	LAE 2 - Reforçar a partilha de informação da situação das ameaças com NATO e UE e entre estas.
	LAE 3 - Promover a informação publica e educação da sociedade no âmbito das ameaças e dos riscos, nomeadamente na educação da cidadania e educação governamental.
Reforçar a Comunicação estratégica	LAE 4 - Promover a Comunicação Estratégica no domínio Social e Informacional, em coordenação com o CoE em Comunicação Estratégica da NATO e Divisão STRATCOM da EEAS.
	LAE 5 - Promover a capacidade de combate à desinformação, através de deteção precocemente e desmentidos rápidos e firmes
Reforçar a Resiliência	LAE 6 - Criar equipas de apoio e resposta a ameaça multidomínio para apoio a entidades e civis.
	LAE 7 - Criar mecanismos de certificação e validação em segurança ciber com apoio e coordenação com a UE.
	LAE 8 - Promover coordenação e integração entre as estratégias de resiliência ciber da UE, NATO e a Estratégia Nacional de Segurança do Ciberespaço.
	LAE 9 - Reforço do papel da inovação e do capital humano como fatores catalisadores da cibersegurança nacional.
	LAE 10 - Criar mecanismos legais de enquadramento do controlo da desinformação.
	LAE 11 - Promover mecanismos de dissuasão de ameaças híbridas através de ações punitivas em coordenação com UE e NATO.
	LAE 12 - Apoiar tecnologias disruptivas emergentes como IA e *big data* para detetar desinformação e vigilância Intel.
	LAE 13 – Promover e incrementar a captação de investimento e inovação em infraestruturas críticas.
	LAE 14 - Diversificar dependências energéticas através da promoção de parcerias e investimentos preventivos estratégicos e de mecanismos de cooperação europeus.
	LAE 15 - Incrementar estratégias de cooperação e parcerias económicas entre estado e privados.
	LAE 16 - Promover uma cultura e capacidade Intel nos diversos domínios de segurança nacional, reforçando mecanismos de cooperação civil-militar.
Reforçar a capacidade de prevenir e dar resposta a crises	LAE 17 - Elaborar plano de resiliência em infraestruturas critica com salvaguarda de cibersegurança e contraespionagem.
	LAE 18 - Elaborar plano de resiliência económico.
	LAE 19 - Elaborar plano de resiliência de Informações.
	LAE 20 - Elaborar plano de resiliência Informacional.
	LAE 21 – Planear e promover exercícios com elementos híbridos para treinar a resiliência.

5. CONCLUSÕES

O ambiente de segurança atual é cada vez mais complexo. Estão a acabar os tempos em que a paz, a crise e o conflito eram três fases distintas, em que os conflitos eram resolvidos fundamentalmente com meios militares, e os adversários eram conhecidos. Os ataques cibernéticos estão posicionados no espectro do conflito, abaixo do limiar de um ataque militar, as campanhas de media social e a exploração de dependências económicas criam alternativas que procuram desestabilizar países e entidades políticas sem emprego de meios militares. Acresce a combinação "híbrida" de instrumentos militares e não militares, que cria ambiguidades e que torna de elevada complexidade a consciência situacional e dificulta a rápida tomada de decisão.

O assunto passou a ser prioritário nas agendas da UE e da OTAN e o CAH assumiu também relevância na agenda nacional, visível na criação do grupo de trabalho para a elaboração do documento de enquadramento nacional das AH, bem como na relevância académica que o tema está a merecer, com vários seminários, artigos e estudos, e onde se insere também este TII.

O objeto do estudo deste trabalho foi a Defesa Nacional face às AH, propondo-se apresentar as principais LAE para o CAH numa abordagem *whole of government* e *whole of society*, no âmbito nacional e dos compromissos com as organizações de que faz parte, através das sinergias da UE no campo da AH.

Para a sua realização adotou-se uma investigação baseada num raciocínio indutivo, a metodologia seguiu a estratégia de investigação qualitativa e um desenho de estudo de caso, recorrendo à análise documental e a entrevistas semiestruturadas, como instrumentos de recolha de dados e, à análise de conteúdo e análise SWOT como técnicas de tratamento de dados.

A análise dos documentos normativos estruturantes e a aplicação do contexto teórico de referência, permitiu a resposta à QD1 e o cumprimento do OE1, tendo identificado que os contributos da DN para o CAH, numa abordagem multidisciplinar da DN englobando de modo holístico a Segurança e a Defesa, concorrem com a utilização dos domínios de poder, Político, Económico, Militar e Defesa, Diplomático, Informacional, Infraestruturas, Ciber e Espaço, Cultural, Administração Pública, Legal, Social e, Informações, para o CAH e para a definição de estratégias nacionais globais e sectoriais.

Através da análise categorial, às 17 entrevistas semiestruturadas a entidades especialistas, foi possível identificar os quadros de ameaças mais críticas e prováveis

a Portugal no âmbito da prevenção e CAH e as oportunidades consideradas mais relevantes no contexto do espaço geopolítico onde Portugal se integra, respondendo assim à QD2, e cumprindo o OE2, de analisar o ambiente externo face às AH. O tratamento da mesma análise categorial às entrevistas, permitiu ainda identificar os quadros de potencialidades mais relevantes e vulnerabilidades mais críticas no âmbito da prevenção e CAH, considerando os diferentes domínios do ambiente interno, respondendo à QD3, cumprindo o OE3, de analisar o ambiente interno face às AH.

Através da análise SWOT, realizada aos domínios Social, Infraestruturas, Informacional, Económico e Informações, foi possível identificar as 23 LA que resultam das principais ameaças identificadas no âmbito do CAH.

O processo de confirmação das LA identificadas, por entrevistas, realizou-se por validação de critérios de adequação, exequibilidade e aceitabilidade e, permitiu respondermos à QC, cumprindo o OG, de propor as LAE no âmbito da DN para o CAH.

Como principais resultados e contributos para o conhecimento, resulta a proposta de 21 LAE para apropriar o País no CAH, ao nível da DN, num conceito alargado de Segurança e Defesa e numa abordagem *whole of society*. Estas LAE, decorrem da identificação das ameaças consideradas mais prováveis e críticas e, da análise do ambiente externo e do ambiente interno, expressas na Figura 5.

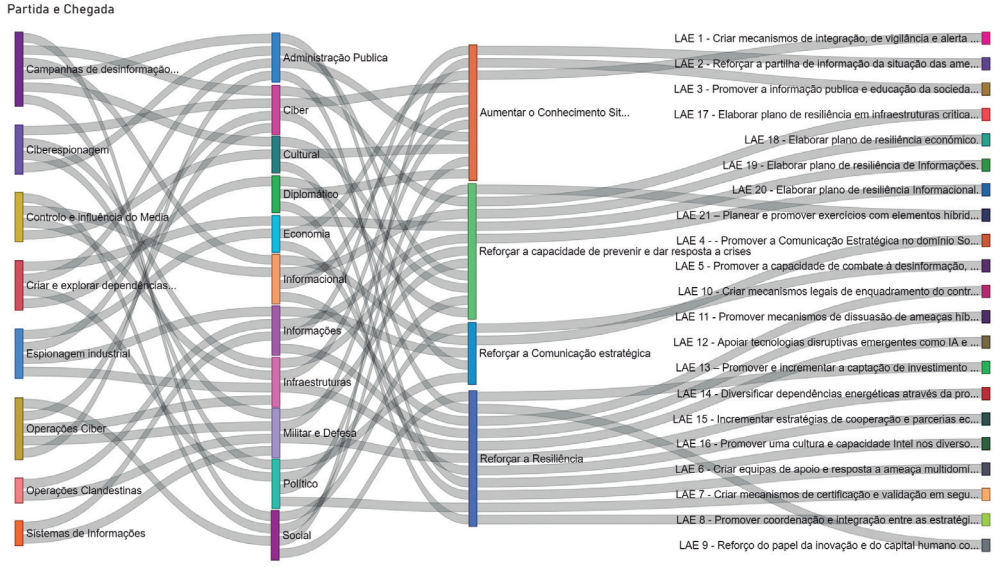


Figura 5 – Ameaças, Objetivos e Linhas de ação estratégicas no CAH

Em face dos Objetivos e LAE propõe-se a definição de uma estratégia nacional global para o CAH e a edificação das estratégias sectoriais no CAH para todos os domínios identificados, realçando que na análise da ameaça dever ser valorada a nossa posição enquanto membros da UE e NATO e, que a resiliência nacional face à AH está diretamente associada à coesão e unidade destas organizações.

Como limitação à investigação, salienta-se a necessidade de uma análise nacional centrada em cada uma das possíveis ameaças e não apenas nas mais prováveis de modo a constituir-se verdadeiramente num documento de apoio a uma estratégia global.

Para proposta de investigação futura, identifica-se a necessidade de que, no contexto nacional, seja estudado um quadro de cooperação e coordenação interministerial, intersectorial e, entre setor público e privado e as organizações NATO e UE. Salienta-se a necessidade deste mecanismo de cooperação e coordenação para alimentar uma futura estratégia nacional no CAH, que promova a multidisciplinaridade dos domínios de poder, centralize a deteção, identificação, informação transversal e vertical com as estruturas da UE e NATO, centralizando a observação e coordenação das Ameaças e Riscos.

REFERÊNCIAS BIBLIOGRÁFICAS

Alves, M. (2020). *A prevenção e o combate às ameaças híbridas: impacto para as forças armadas portuguesas*. (Trabalho de Investigação Individual CPOG 2019/20). Lisboa: Instituto Universitário Militar.

Barroso, L. (2008, abril). Análise conceptual do Conceito Estratégico de Defesa Nacional. *Revista Militar,* 2475. Retirado de https://www.revistamilitar.pt/artigo/274

Bryman, A. (2012). *Social Research Methods (4ª ed.)*. Oxford: Oxford University Press.

Comissão Europeia. (2016a). *Comunicação Conjunta ao Parlamento Europeu e ao Conselho. Quadro comum em matéria de luta contra as ameaças híbridas uma resposta da União Europeia*. Bruxelas: Comissão Europeia. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018&from=EN

Comissão Europeia. (2016b). Comunicado de imprensa - Segurança: *UE reforça resposta às ameaças híbridas*. Retirado de https://ec.europa.eu/commission/presscorner /detail/pt/

Comissão Europeia. (2018). *Increasing resilience and bolstering capabilities to address hybrid threats. Joint communication to the European Parliament, the European Council and the Council*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018JC0016&from

Comissão Europeia. (2020). *Programa do Conselho para 18 meses (1 de julho de 2020 – 31 de dezembro de 2021)*. Secretariado-Geral do Conselho.

Declaração de Retificação n.º 52/2009, de 20 de julho, à Lei n.º 31-A/2009, de 7 de Julho (2009). *Rectifica a forma e o número da Lei n.º 31-A/2009, de 7 de Julho, publicada no Diário da República, 1.ª Série, n.º 129 (suplemento), de 7 de Julho de 2009, que se rectifica como Lei Orgânica n.º 1-B/2009, de 7 de Julho, e republicação integral da mesma*. Diário da República, 1ª Série, 138. Lisboa: Assembleia da República.

Decreto-Lei n.º 249/2015, de 28 de outubro (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar*. Diário da República, 1.ª Série, 211, 9298-9311. Lisboa: Ministério da Defesa Nacional.

Despacho n.º 2536/2020, de 24 de fevereiro. (2020). *Diretiva Ministerial de Planeamento de Defesa Militar - quadriénio 2019-2022*. Diário da República, 2.ª Série, 38, 36-41. Lisboa: Ministério da Defesa Nacional.

Fachada, C. P. A., Ranhola, N. M. B., Marreiros, J. P. R., & Santos, L. A. B. (2020). *Normas de Autor no IUM* (3.ª Ed., revista e atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.

Fernandes. (2016). As Novas Guerras: O Desafio da Guerra Híbrida. *Revista de Ciências Militares*, p. 20.

Gabinete Coordenador de Segurança. (2008). *Relatório Anual de Segurança Interna*. Lisboa: Ministério da Administração Interna.

Giannopoulos, G., & Smith, H. (2019). *The Landscape of Hybrid Threats: A conceptual model*. Brussels: European Commission.

Hybrid CoE. (2017). *Hybrid Threats*. The European Centre of Excellence for Countering Hybrid Threats: https://www.hybridcoe.fi/hybrid-threats/

Hybrid CoE. (2019). *Countering Hybrid Threats - Understanding Hybrid Warfare*. Retirado de https://www.hybridcoe.fi/hybrid-threats/

Hybrid CoE. (2020). *The Landscape of Hybrid Threats: A conceptual model*. Brussels:

Inácio, C. (2010). *Políticas Públicas de Segurança – novo paradigma* (Dissertação de Mestrado em Ciência Política). Secção Autónoma de Ciências Sociais, Jurídicas e Políticas, Universidade de Aveiro.

Lopes, A. (2006). Segurança e Cidadania: conceitos e políticas. Grupo de estudo e reflexão de estratégia. *Cadernos Navais*, 19. Edições culturais da marinha. Out/Dez.

LUSA. (2019). *Candidatura ao Centro Europeu de Excelência para Combate às Ameaças Híbridas*. Retirado de https://combatefakenews.lusa.pt/fake-news-governo-quer-plano-nacional-para-combater-desinformacao-e-ciberataques-c-audio/

Monaghan. (2019). *Countering Hybrid Warfare: Concetual Foundations and Implications for Defence Forces - Information note*. *MCDC Countering Hybrid Warfare Project*.

Multinational Capability Development Campaign. (2017). Countering Hybrid Warfare Project: Understanding Hybrid Warfare. *MCDC January 2017*.

Multinational Capability Development Campaign. (2019). *Countering Hybrid Warfare Information Note*. Gov.UK Ministry of Defence. Retirado de https://www.gov.uk/government/publications/countering-hybrid-warfare-project-understanding-hybrid-warfare

National Security Science and Innovation Strategy. (2009). *The National Security Science and Innovation Strategy*. Australian Government.

North Atlantic Treaty Organization. (2014). *Wales Summit Declaration, Heads of State and Government participating in the meeting of the North Atlantic Council in Wales*. Retirado de https://www.nato.int /cps/en/natohq/official_texts_112964.htm

North Atlantic Treaty Organization. (2017). *Allied Joint Doctrine Edition E Version 1*. AJP-1. NATO Standardization Office (NSO). NATO.

North Atlantic Treaty Organization. (2019). *NATO*. Retirado de www.nato.int: https://www.nato.int/cps/en/natohq/topics_156338

Pereira, J. (2018). *As ameaças híbridas - Uma abordagem conceptual no quadro da OTAN e da UE*. CEDIS.

Ralph. (2016). *Hybrid Warfare - On redisign of National Security*. ISPS Strategics studies.

Rego, A., Cunha, M. P., & Meyer, V.. (2019). Quantos participantes são necessários para um estudo qualitativo? Linhas práticas de orientação. *Revista de Gestão dos Países de Língua Portuguesa*, 45-57. Retirado de https://doi.org/ 10.12660/rgplp.v17n2.2018.78224.html

Resolução do Conselho de Ministros n.º 19/2013, de 21 de março (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República 1.ª Série, 67, 1981-1995. Lisboa: Presidência do Conselho de Ministros.

Santos, L. B. & Lima, J. V. (Coords.) (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação* (2.ª ed, revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sarmento, M. (2013). *Metodologia Científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada.

Yarger, H. (2006). *Strategic Theory for the 21st Century: The Little Book on Big Strategy, Carlisle: Strategic Studies Institute*. USAWC.

A PREVENÇÃO E O COMBATE ÀS AMEAÇAS HÍBRIDAS: IMPACTO PARA AS FORÇAS ARMADAS PORTUGUESAS

PREVENTION AND TACKLING OF HYBRID THREATS: IMPACT ON THE PORTUGUESE ARMED FORCES

Autor
CMG FZ Artur José Figueiredo Mariano Alves

Orientador
COR TIR ART António José Pardal dos Santos

1. INTRODUÇÃO

A globalização desregulada e o sistema internacional em transição, com novos alinhamentos geopolíticos, tende a gerar uma nova ordem mundial e a criar uma crescente instabilidade no ambiente de segurança, propiciando uma maior projeção de novas ameaças, de carácter difuso e transnacional, interdependentes, de múltiplas naturezas, dinâmicas, híbridas, assimétricas e globais, que afetam a segurança dos Estados (Garcia, 2017). A par destas ameaças, a gama de métodos e atividades empregues por atores estatais e não-estatais, é cada vez mais ampla e de cariz combinada. A desinformação, a exploração das vulnerabilidades de carácter logístico, como a dependência energética e os transportes, a chantagem económica, a pressão diplomática, a deterioração das instituições internacionais, o terrorismo, o crime organizado, ampliadas pela nova dimensão das tecnologias disruptivas e o domínio do Ciberespaço, contribuem para o aumento de forma desmedida da insegurança. De facto, vivemos numa era de Ameaças Híbridas (AH), as quais se têm afirmado com um dos principais desafios securitários da atualidade (The European Centre of Excellence for Countering Hybrid Threats [Hybrid CoE], 2018).

Estas ameaças vivem no foro da impossibilidade de deteção imediata e usam elementos caracterizadores de *soft, hard* e *smart power*, atuando numa *gray zone* com limites difusos e mal definidos, onde procuram a paridade no desenvolvimento tecnológico e na sua acessibilidade, usando as redes sociais como arma de propaganda e desinformação, manipulando e influenciando as populações de forma a corroer governos e sociedades (Schmid, 2019). É no contexto deste novo paradigma civilizacional que o Combate às Ameaças Híbridas (CAH) constitui um verdadeiro desafio, com reptos inigualáveis em termos de defesa e segurança, os

quais têm vindo a causar apreensão e preocupação acrescidas dos Estados-Membros da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN), "[…] pelo potencial subversivo que acarretam para o Estado de direito democrático" (Pereira, 2018, p. 1). Os conceitos de AH e Guerra Híbrida (GH), apesar de não serem novidade, ganharam definitivamente dimensão, com os acontecimentos na Ucrânia em 2014, país em que a Rússia desenvolveu ações de forma astuciosa, sincronizada e combinada, de forma a explorar as vulnerabilidades dos adversários e alcançar os seus objetivos políticos, o "[…] que levou a NATO a classificá-la como uma abordagem híbrida à guerra e a atribuir-lhe uma elevada importância na preparação do combate às futuras ameaças da Aliança" (Fernandes, 2016, p. 20).

De facto, desde 2014 até à atualidade, têm-se multiplicado as tentativas de desestabilização dos países ocidentais, através da erosão da confiança das instituições governamentais e de ataques aos valores fundamentais da sociedade (e.g. ciberataques, campanhas de desinformação e ações militares hostis) (Comissão Europeia [CE], 2018). De forma a combater esta realidade, a UE e a OTAN têm vindo a desenvolver um conjunto de medidas e Linhas de Ação (LA) de forma a assegurar aos Estados-Membros e Aliados, uma base que os apoie na luta coletiva contra as AH, que evidencie a necessidade de colaboração interinstitucional e a utilização potencial dos respetivos tratados (CE, 2016a). As declarações no dia 29 agosto de 2019, da ex-Secretária de Estado da Defesa Nacional, Ana Santos Pinto, à agência Lusa, por ocasião da formalização da candidatura portuguesa ao Hybrid CoE, ilustram bem a prioridade e preocupação do governo no CAH e a importância atribuída a esta temática.

Quando inquirida sobre a necessidade da candidatura Ana Pinto respondeu: "[…] resulta de um processo nacional de reconhecimento que as ameaças híbridas são uma prioridade e, portanto, tentamos não só adaptarmo-nos do ponto de vista interno, mas aprender com as boas práticas e perceber o que podemos utilizar". Realçou ainda: "[…] são ameaças que, do ponto de vista do conceito, são não tradicionais no que respeita à conflitualidade". Por essa razão, continuou, "[…] são questões transversais a várias áreas do Governo, não só na Defesa, nos Negócios Estrangeiros, mas também das Finanças, por ataques […] que vêm de várias áreas e regiões". E finalmente concluiu: "[…] aquilo que é uma responsabilidade nacional, mas sem capacidade de resposta exclusivamente nacional, só tem uma forma de resposta, que é do ponto de vista cooperativo, através da UE e da NATO" (LUSA, 2019).

Por outro lado, o Conceito Estratégico de Defesa Nacional (CEDN) refere de forma clara, que devem ser potenciadas as capacidades civis e militares para uma abordagem integrada na resposta às ameaças transnacionais (AT) (e.g. crime organizado transnacional e cibercriminalidade), através de respostas estratégicas multissectoriais e integradas (Resolução do Conselho de Ministros [RCM] n.º 19/2013, de 05 de abril, pp. 1989-1990). Ao nível das Forças Armadas (FFAA), o próprio Conceito Estratégico Militar (CEM) mostra a necessidade de edificar capacidades diversificadas, interoperáveis e integráveis, de forma a garantir a participação nacional nas Organizações Internacionais (OI), de segurança e defesa coletiva, nomeadamente na UE e OTAN (Ministério da Defesa Nacional [MDN], 2014).

Desta forma, torna-se necessária a definição de linhas de ação para o CAH ao nível das FFAA, que acomodem simultaneamente, as principais Linhas de Orientação Estratégica (LOE) da UE e da OTAN e as sinergias criadas no âmbito destas organizações, justificando-se assim o presente estudo. O objeto de estudo centra-se nas AH e está delimitado nos domínios: (i) temporal, desde o início do século XXI até à atualidade; (ii) espacial, ao Espaço Estratégico de Interesse Nacional (EEIN); (iii) e de conteúdo, centrando-se nas AH e no seu significado para o instrumento militar, nas LOE da UE e da OTAN e nas capacidades das FFAA para o CAH. A presente investigação encontra-se alicerçada no Objetivo Geral (OG) e nos Objetivos Específicos (OE) definidos na Figura 1.

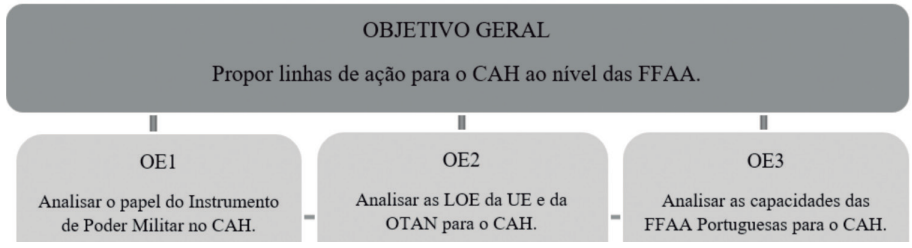


Figura 1 – Objetivos da investigação

O trabalho está organizado em cinco capítulos. O primeiro capítulo introduz a investigação e o segundo capítulo apresenta o enquadramento teórico e conceptual. O terceiro capítulo aborda a metodologia, em detalhe. O quarto capítulo apresenta os dados e os resultados, designadamente (i) o papel do Instrumento de Poder Militar (IPM) no CAH, (ii) as principais LOE da UE e da OTAN para o CAH com implicações para as FFAA e as capacidades de CAH ao nível das FFAA.

O quarto capítulo é finalizado com propostas de LA para o CAH, através duma análise SWOT (*Strengths, Weaknesses, Opportunities e Threats*), respondendo-se à QC. Finaliza-se com as conclusões do trabalho, a avaliação dos resultados obtidos em relação aos objetivos traçados e a resposta ao problema de investigação.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

No presente capítulo, apresenta-se a revisão da literatura com enfoque nas AH.

2.1. Estado da arte e revisão de literatura

Uma das principais dificuldades para se pensar claramente sobre os desafios "híbridos" é a diversidade de termos existentes na literatura especializada (e.g. AH, GH, conflito híbrido, influência híbrida, ataque híbrido), e que são usados de forma indiscriminada e sem definição consensual (*Multinational Capability Development Campaign* [MCDC], 2019a), pelo que importa ter a necessária clareza conceptual.

Nesse sentido, descreve-se a evolução dos conflitos, de forma sucinta, para se perceber como o carácter da guerra tem vindo a alterar-se até à GH do presente. A partir desta conceptualização, efetua-se o enquadramento e explicação do conceito de AH, das suas principais características e tipologias.

2.1.1. Evolução dos conflitos, das Velhas às Novas Guerras

Clausewitz (1987) dizia que a guerra tem duas componentes que perduram ao longo do tempo: a sua natureza que permanece constante e o seu carácter que se altera conforme o contexto. Esta alteração provoca sucessivas transformações na forma de fazer a guerra, levando a maioria dos pensadores militares a classificar a evolução dos conflitos armados em várias gerações, colocando-se, no entanto, o debate, se serão "novas" ou apenas, as guerras de sempre. Para vários autores, conforme refere Serrano (2013, pp. 66), "[…] a adaptação da natureza da guerra mantem válida a trindade de Clausewitz – Povo, Governo e Militares" e representa a continuidade da política por outros meios, com a finalidade de forçar o adversário a submeter-se à vontade do oponente.

Outros pensadores contrapõem, dizendo que os novos conflitos já não se enquadram nesta definição clássica de Clausewitz, adicionando "novas" à classificação das guerras. Mary Kaldor, defende que as "velhas guerras" estão

relacionadas com a versão bélica, que caracterizou a Europa entre os finais do século XVIII e meados do século XX, período em que os Estados combatiam com militares uniformizados, procurando a derrota do inimigo através da batalha decisiva. (2013, p. 1).

Kaldor (2013, p. 2) contrasta as diferenças entre "velhas guerras" e "novas" pelos atores intervenientes, objetivos, métodos e formas de financiamento como ilustra a Figura 2, realçando que a distinção entre Estados e não Estados, público ou privado e mesmo entre a guerra e a paz está cada vez mais a esbater-se.

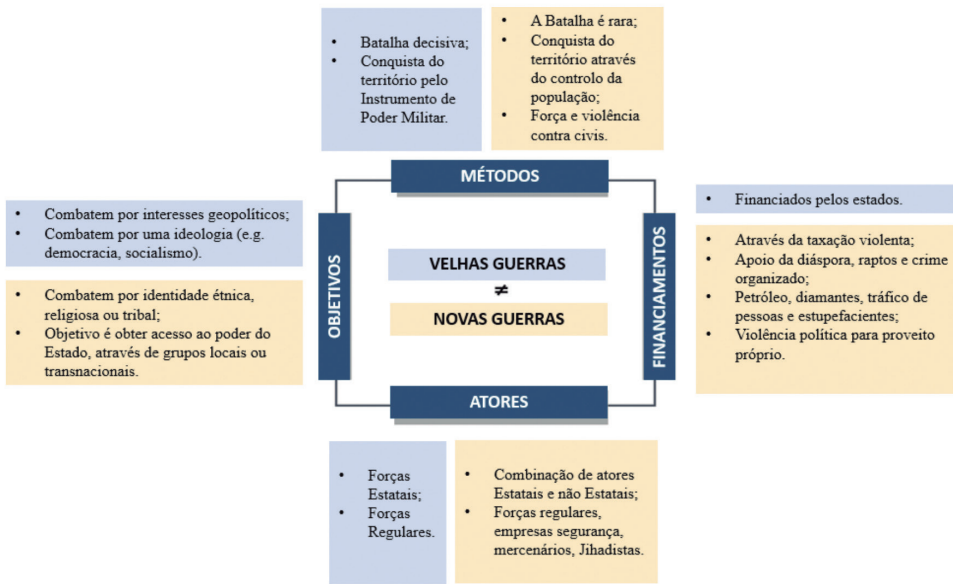


Figura 2 – Diferença entre velhas e novas Guerras
Fonte: Adaptado de Kaldor (2013, p. 3).

De facto, desde o fim da Guerra Fria, diversos conceitos têm vindo a ser propostos na tentativa de se explicar a realidade dos conflitos contemporâneos. Termos como guerra tradicional, composta e de quarta geração, fundiram-se num guarda-chuva teórico de conceitos denominado GH, classificação que surge da necessidade de preencher uma lacuna conceptual (Casalunga, s.d.).

2.1.2 Guerra Híbrida

O conceito de GH é uma noção emergente. Refere-se ao uso de métodos não convencionais como parte de uma abordagem de combate em múltiplos

domínios, que visam interromper e anular as ações de um oponente sem haver um envolvimento em hostilidades abertas (Treverton et al., 2018).

Embora o conceito não seja novo, os seus efeitos e resultados começaram a aparecer com frequência na literatura especializada, desde a abordagem híbrida da Rússia à Ucrânia, que envolveu uma combinação de atividades, incluindo desinformação, manipulação económica, uso de forças paramilitares e milícias, pressão diplomática e ações militares (Guindo, 2015). No entanto, o conceito de GH só começou a aparecer no vocabulário militar em 2005, evidenciando que a superioridade convencional dos Estados Unidos da América estava a criar uma lógica, que iria levar os seus oponentes a abandonarem a maneira tradicional de travar a guerra (Guindo, 2015). O termo GH, originalmente referia-se a atores não--estatais irregulares com capacidades militares avançadas. Por exemplo, na Guerra Israel-Líbano de 2006, o Hezbollah empregou uma série de táticas diferentes contra Israel,que incluíram a guerrilha, o uso inovador da tecnologia e campanhas efetivas de informação, coordenadas com operações militares convencionais, guerra cibernética e atividades criminosas, procurando dessa forma anular a superioridade tecnológica de Israel (Hoffman, 2009).

Desde então, surgiram outros conflitos que se encaixavam neste novo modo de atuação, como a intervenção da Rússia na Ucrânia e as ações do Estado Islâmico do Iraque e do Levante, por apresentarem características que a distinguiam de conflitos anteriores. (Fernandes, 2016). Após o conflito da segunda guerra do Líbano, Frank Hoffman, volta a desempenhar um papel importante, expandindo os termos de AH e GH para descrever conflitos onde se empregam várias táticas em simultâneo. Para este investigador, "[…] hybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion and criminal disorder" (Hoffman, 2007, p. 14).

Desde então, têm sido propostos vários modelos para se obter um melhor entendimento da GH, muitas vezes complexos, mas que Schmid (2019) vem explicar de forma simples. Para este investigador do Hybrid CoE, ao contrário do *Military-Centric-Warfare*, a GH passa por orquestrar diversas operações nos diferentes domínios, procurando explorar Centros de Gravidade não militares que, mutáveis no tempo, criam ambiguidade e impedem a compreensão da situação por parte do oponente.

Essas operações são conduzidas fundamentalmente numa "*gray zone*", designação sugestiva quanto à complexidade de identificação dos seus elementos

e fronteiras, que compreende múltiplas interfaces (e.g. paz e guerra, amigo e inimigo, militar e civil) e destinam-se a enfraquecer a segurança interna, para que a pressão nos sistemas, exponha vulnerabilidades do país a explorar. Nesse sentido a GH não é mais do que uma mistura de *soft power* com *hard power,* catalisado com a criatividade do smart power (Schmid, 2019).

2.1.3 As ameaças híbridas

Derivado do conceito de GH surge a conceção do termo AH, que tem evoluído ao longo do tempo, na tentativa de se adaptar ao progresso proporcionado pelas inovações tecnológicas, do mundo das telecomunicações e cibernético, e ainda, pela capacidade dos atores internacionais utilizarem, cada vez mais, todo o tipo de ferramentas (não cinéticas) para alavancar a sua influência geopolítica (Hybrid CoE, 2018).

Para se entender melhor as AH na atualidade, deve-se examinar as tendências geopolíticas e a interação que existe entre os atores internacionais em termos de "competição" e "influência". De facto, para se "[…] entender o híbrido tem de se entender o conceito de influência híbrida, que é uma influência premeditada consciente exercida por […] atores, que utilizam métodos diversos para alcançar determinado objetivo" (A.G. Marques entrevista presencial 14 de fevereiro 2020). Nesse sentido, as AH, não são mais do que a personificação e alavancagem dessa influência através de ferramentas híbridas e dos instrumentos de poder (e.g. político, económico e militar).

Talvez por isso, o Hybrid CoE, incumbido, recentemente, pela UE e pela OTAN, de aprofundar o conhecimento sobre as AH, as entenda simplesmente, como "[…] methods andactivities that are targeted towards vulnerabilities of the oponent". Segundo este Centro de Excelência, estas ameaças possuem as seguintes características:

> […] coordinated and synchronised action, that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means. […] the activities to exploit the thresholds of detection and attribution as well as the different interfaces (war-peace, internal-external, local-state, national and international, friend-enemy). […] the aim of the activity is to influence different forms of decision making […]. (Hybrid CoE, s.d.)

3. METODOLOGIA E MÉTODO

Este trabalho enquadra-se no âmbito das Áreas de Investigação das Operações Militares e do Estudo das Crises e Conflitos Armados (Decreto-Lei n.º 249, de 28 de outubro de 2015), nas subáreas do Planeamento Operacional e no Planeamento Estratégico Militar e tem um carácter científico, pois satisfaz o requisito de possuir um objeto reconhecível e definido, identificável pelos outros e que possa ter utilidade.

A posição ontológica face ao objeto da investigação é o "construtivismo", tendo por base que todo o conhecimento é, puramente, uma construção social, e a epistemológica é o "interpretativismo", por se considerar "[…] que o mundo social, ao ser formado por indivíduos e pelas suas interações, não pode, […] nem deve ser estudado a partir dos princípios e instrumentos das ciências naturais" (Santos & Lima, 2019, p. 18).

Na investigação adota-se o raciocínio indutivo, já que a partir da observação de factos singulares e da sua associação estabelece-se uma lei ou uma teoria (Santos & Lima, 2019). A estratégia de investigação é qualitativa, por se considerar "[…] que existe uma relação indissociável entre o mundo real e a subjetividade do sujeito, que não é passível de ser traduzida em números" (Santos & Lima, 2019, p. 27). O desenho de pesquisa é o estudo de caso, já que se procura "[…] recolher informação detalhada sobre uma única unidade de estudo […]" (Santos & Lima, 2019, p. 36). O Horizonte Temporal é transversal, porque pressupõe a recolha de dados a partir de mais de um caso, num determinado instante de tempo (Bryman, 2012). O percurso metodológico integra as fases exploratória, analítica e conclusiva (IUM, 2018), conforme apresentado na Figura 3.

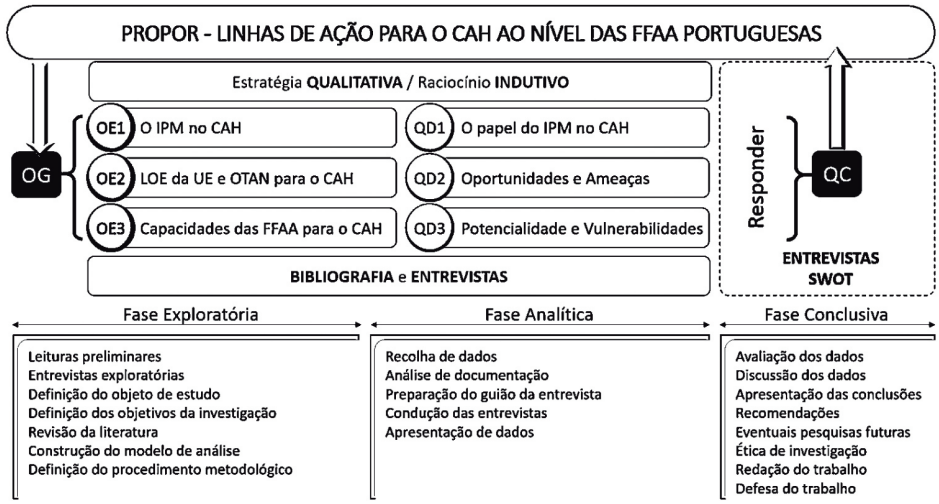


Figura 3 – Percurso metodológico

A população do estudo é constituída por militares e civis (*experts*) com conhecimentos ou trabalhos elaborados no âmbito das AH. Constitui-se uma amostra do tipo não probabilística, intencional (Santos & Lima, 2019, p. 71), composta por dez participantes do Ministério dos Negócios Estrangeiros, MDN, Estado-Maior das Forças Armadas (EMGFA), Marinha e Exército, por serem os mais representativos da população, devido à especificidade do tema e aos cargos que desempenham, considerando-se por isso a dimensão adequada (Rego, Cunha, M. P, Meyer & Victor, 2018).

A técnica de recolha de dados para todas as QD assenta em entrevistas, apoiadas em Análise Documental (AD) com os seguintes critérios:

– As entrevistas são do tipo semiestruturadas (Sarmento, 2013, p. 34), com recurso a tópicos e perguntas, alinhadas com os problemas e principais eixos da pesquisa. O guião contém quatro perguntas: as duas primeiras são orientadas para responder à QD1, a terceira à QD2 e a quarta à QD3.

– A AD é utilizada fundamentalmente para consolidar os instrumentos necessários na recolha de dados e baseia-se essencialmente nas seguintes áreas e fontes: literatura de metodologia científica; estudos desenvolvidos pelo Hybrid CoE; estudos desenvolvidos pela MCDC; literatura da especialidade; legislação e documentação estruturantes das FFAA.

A técnica de análise dos dados recolhidos nas entrevistas é a análise categorial. Por questão, procede-se da seguinte forma: (i) constituem-se as unidades

de contexto, determinam-se as unidades de registo e elabora-se um quadro com as unidades de contexto e registo; (ii) constrói-se um quadro com a análise conteúdo, no qual as unidades de registo são quantificadas de acordo com as suas características comuns (unidades de enumeração: soma e percentagem na amostra) e reagrupadas em categorias, a que se atribui uma designação; (iii) elaboram-se as conclusões, evidenciando os resultados ≥ 50% e enfatizando os ≥ 80% (verificação das unidades de registo: não verificadas se x < 50%; parcialmente verificadas se estiverem no intervalo 50% ≤ x < 80%; verificadas se x ≥ 80%) (Sarmento, 2013, pp. 14-15 e 48-66).

No caso da QD1, os resultados obtidos são ainda tratados segundo o conceito da MCDC, que será explanado em detalhe no próximo capítulo.

A obtenção da resposta à QC inclui uma análise SWOT das unidades de registo verificadas ou parcialmente verificadas na QD2 e QD3, na qual se tem em consideração as conclusões da QD1 para propor as LA.

O tratamento dos dados realiza-se com o auxílio da folha de cálculo Excel e os gráficos são elaborados através do *Software Power Business Intelligence* (Power BI).

4. APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

4.1. O papel do Instrumento do Poder Militar no Combate a Ameaças Híbridas

O presente subcapítulo tem por objetivo analisar o papel do IPM no CAH. Para esse efeito: examinam-se as principais componentes que devem ter uma estratégia de CAH; explica-se o conceito de análise desenvolvido pela MCDC e a sua adequabilidade às AH; analisa-se empiricamente a atividade híbrida no conflito da Rússia com a Ucrânia; e apresentam-se os dados e a análise das entrevistas, correlacionando as variáveis e indicadores com recurso ao Power BI.

4.1.1. Estratégia de combate às ameaças híbridas

A maioria das instituições que estudam as AH, defendem, que a estratégia para o seu combate deve basear-se nas seguintes componentes; detetar, deter ou dissuadir e se necessário, responder aos ataques híbridos (MCDC, 2019b).

A Figura 4 resume as principais ações no âmbito dessas três componentes.

Figura 4 – Estratégia CAH
Fonte: Adaptado da MCDC (2019a, p. 5).

4.1.2. Conceito análise das ameaças híbridas da MCDC

A MCDC (2017) desenvolveu uma estrutura analítica que permite interpretar a GH, através de três características principais: instrumentos de poder; vulnerabilidades das funções críticas visadas; ações e efeitos não lineares. Quando se analisa a descrição destes vetores, conclui-se que são muito semelhantes à descrição e características das AH feita pelo Hybrid CoE, pelo que, utiliza-se essa mesma estrutura para entender também a dinâmica destas ameaças.

Os instrumentos de poder são os vetores que os atores estatais ou não estatais têm para alcançar os seus objetivos políticos e genericamente podem ser divididos; em Militar, Político, Económico, Civil e Informacional (MPECI) (MCDC, 2017).

As funções críticas são definidas como atividades ou operações distribuídas no espectro Político, Militar, Económico, Social, Informacional e das infraestruturas (PMESII) que se forem descontinuadas, podem levar a uma interrupção ou disrupção dos serviços ou de determinadas funções de que uma sociedade ou um Estado dependem (MCDC, 2017). A estrutura analítica que se ilustra na Figura 5 permite refletir esses vetores de poder de um ator face às vulnerabilidades do seu oponente, no espectro das funções mais críticas da sociedade, e apresenta um exemplo prático de visualização.

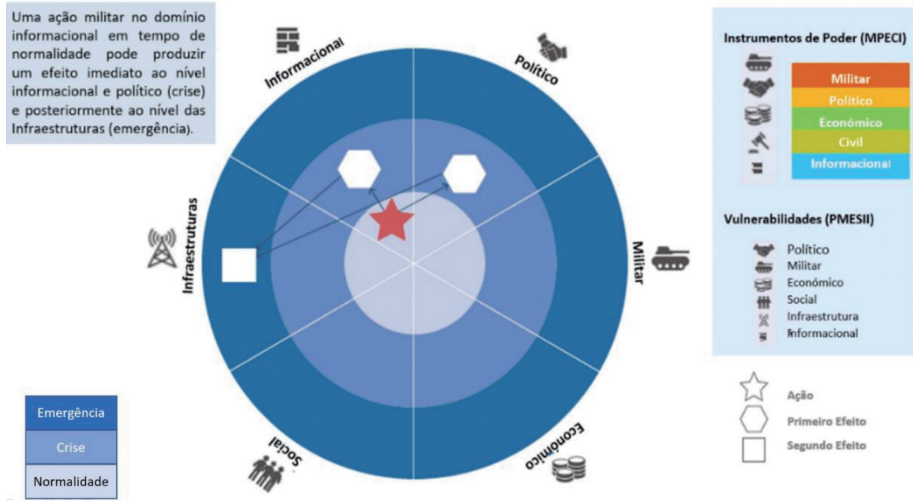


Figura 5 – Instrumentos de poder e funções críticas
Fonte: Adaptado MCDC (2017, p. 15).

Por outro lado, esta é apenas uma maneira de dividir as funções críticas de um Estado, muitas outras variações podem ser feitas. Neste estudo, os domínios do "Ciberespaço" (C) e o "Legal" (L) foram acrescentados face à sua importância na atualidade.

4.1.3. A atividade híbrida no conflito Rússia/Ucrânia

Apesar dos antecedentes históricos, a crise prolongada na Ucrânia começou em 21 de novembro de 2013, quando o então presidente Viktor Yanukovych suspendeu os trabalhos que visavam um acordo de associação com a UE. Essa decisão provocou graves protestos, precipitando uma revolução que levou à sua destituição em fevereiro de 2014. Desta manifestação resultou um novo Governo interino que não foi reconhecido pela Rússia, levando a que esta realizasse uma série de incursões no Leste da Ucrânia, que vieram a culminar na anexação da Península da Crimeia e na revolta dos ucranianos pró-russos da região de Donetsk e Luhansk (Figura 6) (J.M.P. Teixeira entrevista presencial, 11 de março de 2020).

Figura 6 – Agitação pró-russa
Fonte: Adaptado de Wikimedia (s.d.).

Constatou-se que a Ucrânia teve vários desafios políticos e ao nível do seu capital social, "[…] foi fácil para a Rússia desencadear operações na Crimeia e no leste da Ucrânia, explorando as divisões regionais e as tensões nacionais polarizadas, pela diferença da língua e da cultura" (J.M.P. Teixeira, *op. cit.*). Roberts descreve de forma resumida a gama de capacidades e meios, que foram empregues pela Rússia neste conflito, incluindo a camuflagem, deceção, negação, subversão, sabotagem, espionagem, propaganda e operações psicológicas.

> Maskirovka 2.0 is a continuation of the old military approach, to which we must add new whole-of-government tools, such as: coercion, media manipulation, the employment of fossil fuel energy access and price as a weapon, cyber-attacks, political agitation, use of agents provocateurs, the deployment of military forces in clandestine status, and the development of surrogate forces by providing arms, equipment, training, intelligence, logistic support, and command and control. (Roberts, 2015)

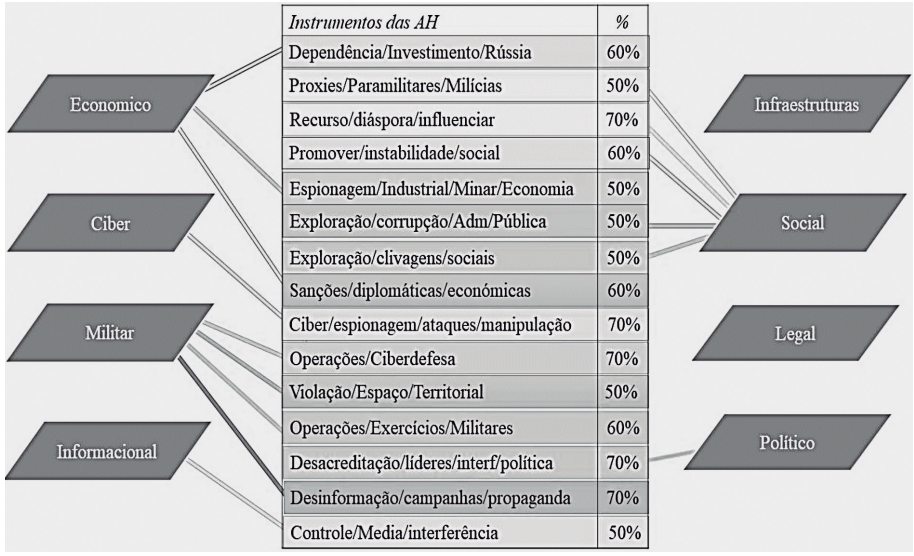
Ao nível operacional, a Rússia estabeleceu a interligação entre as suas ações táticas com operações de informação. Implementou ações de deceção, efetuando exercícios militares ao longo da sua fronteira com a Ucrânia, desviando assim, as atenções de outras operações que estavam a ocorrer em simultâneo.

Desta forma, introduziu no território ucraniano armamento e forças paramilitares que alegadamente iriam prestar ajuda humanitária (Davis, 2015).

Concomitantemente, empregou militares encobertos, os *little green men*, dando início a uma campanha psicológica, informacional e subversiva junto da população local, com o propósito de desacreditar o governo ucraniano (Davis, 2015). Em súmula, a Rússia explorou ativamente as divisões da sociedade ucraniana e o seu governo instável com FFAA mal equipadas, utilizando uma ampla gama de instrumentos, desde a alavancagem económica, forças especiais, ciberataques, a influência da diáspora e a desinformação, entre outros.

4.1.4. Apresentação e discussão de resultados da QD1

A partir das respostas dadas à pergunta 1, elaboraram-se os quadros com a respetiva análise categorial. A Figura 7 apresenta as unidades de registo verificadas (resultados ≥ 50%) e permite visualizar a correlação direta das principais ferramentas híbridas utilizadas pela Rússia (ação direta) contra as funções críticas da Ucrânia.



Instrumentos das AH	%
Dependência/Investimento/Rússia	60%
Proxies/Paramilitares/Milícias	50%
Recurso/diáspora/influenciar	70%
Promover/instabilidade/social	60%
Espionagem/Industrial/Minar/Economia	50%
Exploração/corrupção/Adm/Pública	50%
Exploração/clivagens/sociais	50%
Sanções/diplomáticas/económicas	60%
Ciber/espionagem/ataques/manipulação	70%
Operações/Ciberdefesa	70%
Violação/Espaço/Territorial	50%
Operações/Exercícios/Militares	60%
Desacreditação/líderes/interf/política	70%
Desinformação/campanhas/propaganda	70%
Controle/Media/interferência	50%

Figura 7 – Unidades de registo verificadas da pergunta 1

Os resultados obtidos foram também escrutinados e relacionados criticamente através da folha de cálculo *Excel* e do *software* Power BI, para se ter uma visualização mais holística que permita identificar os efeitos lineares e não

lineares que ocorreram em todo o espectro da sociedade, onde se inclui o IPM. A Figura 8 ilustra um exemplo aleatório das unidades de registo ≥ 50%, em concreto a Violação do Espaço Territorial da Ucrânia, para melhor esclarecer o potencial deste tipo de visualização integrada, que permitiu complementar a análise efetuada. Este exemplo tem a seguinte explicação:

– Para 50% dos entrevistados, a Rússia com o IPM efetuou a ação híbrida "Violação do Espaço Territorial da Ucrânia", visando diretamente o domínio Militar desse país (coluna PMESII-CL). Esta ação tem impacto não linear nos domínios Político e Legal. Se a Ucrânia tivesse aplicado a estratégia de CAH da MCDC, a atuação expectável nos domínios Militar e Político seria detetar, deter e se necessário responder, e no domínio Legal seria dissuadir e se necessário responder.

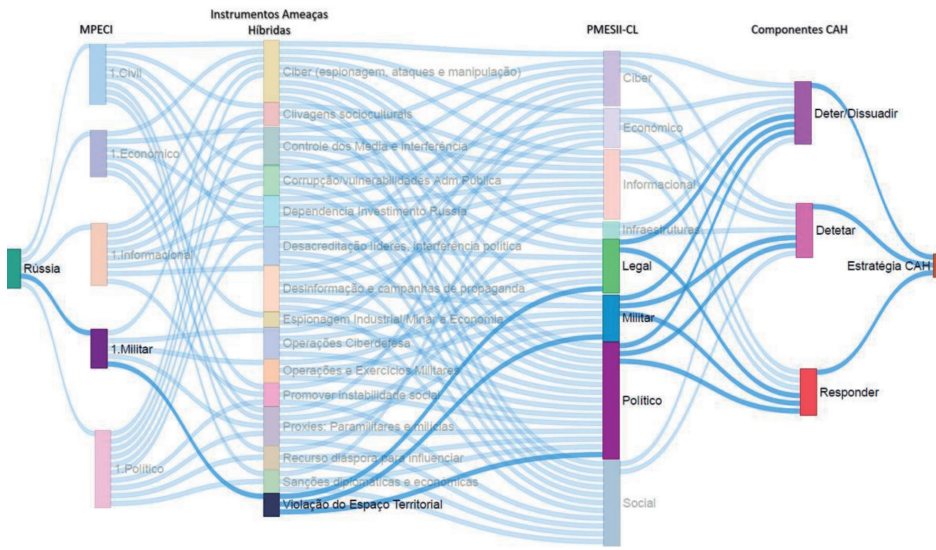


Figura 8 – Exemplo – Violação do Espaço Territorial

Este gráfico de visualização integrada conjuntamente com os resultados da análise de conteúdo permitem inferir o seguinte:

– A natureza transversal e multi-domínio das AH manifesta-se através de ações coordenadas e sincronizadas dos vários elementos/instrumentos de poder;

– Cada ferramenta híbrida utilizada pela Rússia teve como alvo uma ou mais funções críticas da Ucrânia, ou a interface entre elas;

– O capital social e político como sendo as funções críticas mais visadas em termos de efeitos lineares e não lineares;

– As ações mais preponderantes tiveram origem no domínio do Ciberespaço e Informacional com efeitos transversais em quase todas as funções críticas;

– Os domínios Político e Militar são os que podem dar uma resposta mais abrangente através das três componentes do CAH.

A ferramenta Power BI permite ainda verificar de forma individual as ações e respostas que deveriam ter sido dadas. A Figura 9 ilustra a atuação expectável da Defesa Militar, face às principais ferramentas que foram utilizadas pela Rússia contra esse domínio. Dela pode-se inferir que as principais ferramentas híbridas com ação direta e efeitos não lineares no domínio militar dizem respeito ao ciberespaço, desinformação e campanhas de propaganda, operações de ciberdefesa, operações e exercícios militares, forças paramilitares e milícias e violação do espaço territorial.

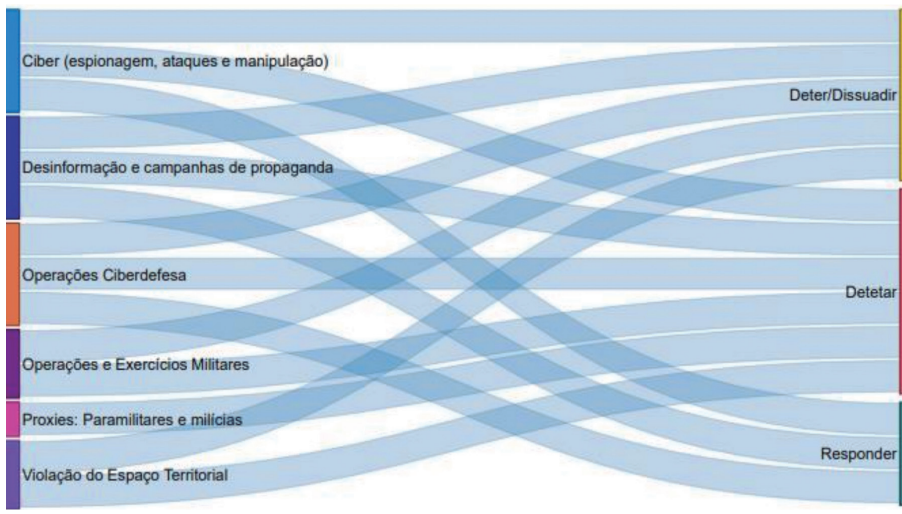


Figura 9 – Visualização do domínio Militar

A partir das respostas à pergunta 2, elaboraram-se os quadros com a respetiva análise categorial. A Figura 10 apresenta as unidades de registo principais (resultados ≥ 50%).

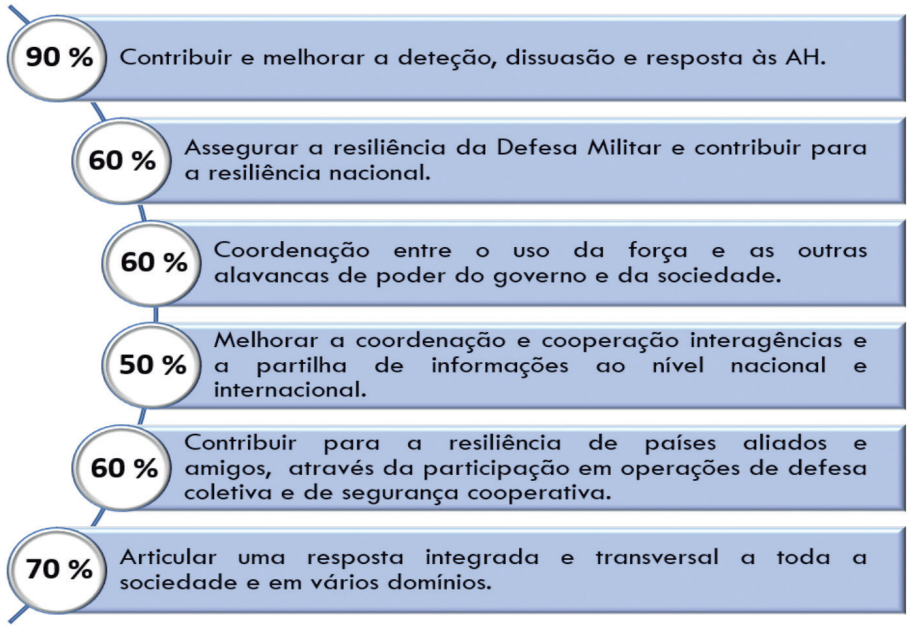


Figura 10 – Desafios do IPM face às AH

Esta análise permite inferir os principais desafios das FFAA no CAH, que se consubstanciam em: assegurar a resiliência da Defesa Militar e contribuir para a resiliência nacional; coordenar o uso da força com os outros instrumentos de poder do Governo numa estratégia de segurança cooperativa e integrada de toda a sociedade; melhorar a cooperação e coordenação interagências e a partilha de informações ao nível nacional e internacional; contribuir para a resiliência de países Aliados e amigos, através da cooperação e participação em operações de defesa coletiva e segurança cooperativa; e o contributo para a deteção, detenção e resposta às AH, que foi mencionado pela maioria dos entrevistados (90%). Neste âmbito, importa enfatizar que a atuação militar ao nível da deteção não será substancialmente diferente da prática existente, embora requeira, conforme refere A.J.G. (Marques, *op. cit.*) "[…] uma cooperação mais estreita com os nossos Aliados e parceiros e deverá explorar sobretudo a partilha de informação, a inteligência estratégica e os recursos técnicos e físicos a que tem acesso no âmbito da comunidade militar internacional".

Em termos de dissuasão e resposta, os militares devem garantir a sua dissuasão convencional e eventual escalada para um conflito armado, quer em termos nacionais quer no âmbito dos compromissos internacionais de defesa.

Nesse sentido, devem "[…] continuar a assegurar capacidades para conduzir operações credíveis de negação (i.e., coagir, interromper, negar e impedir), no âmbito da defesa naval, terrestre e aérea, inclusive nos novos domínios do espaço e do ciberespaço" (J.M. Coelho, entrevista presencial em 3 de março de 2020). Nesse contexto, o papel das FFAA, passa obrigatoriamente "[…] por assegurar a sua própria resiliência para continuar a cumprir as suas missões e contribuir para a resiliência nacional na prevenção e resposta a crises, através de uma abordagem coordenada, transversal, transdisciplinar e multi-institucional com toda a sociedade" (J.M. Coelho, *op. cit.*).

Concluindo, apesar do CAH ser uma responsabilidade de todo o Governo ou até mesmo de toda a sociedade, dependendo na maioria das vezes de ferramentas não militares, o IPM tem um papel muito importante, devido às capacidades únicas que possui, em termos nacionais e internacionais, para detetar ameaças, dissuadir agressores e responder a ataques híbridos.

Para que esse papel seja determinante, torna-se necessário: (i) garantir uma melhor coordenação entre o uso da força e as outras alavancas de poder do Governo e dos Aliados e parceiros, assegurando-se que essa contribuição para o CAH seja apropriada e eficaz, nomeadamente ao nível da deteção e partilha de informação; (ii) garantir capacidades para conduzir operações credíveis no âmbito da defesa militar, incluindo nos domínios do espaço e do ciberespaço, mantendo a necessária dissuasão convencional; (iii) contribuir para a resiliência nacional e assegurar a própria resiliência, face às AH. Com esta súmula, apresentou-se o papel do IPM, o que responde à QD1 e cumpre o OE1.

4.2. Linhas de orientação estratégica da UE e da OTAN para o CAH

Este subcapítulo tem por objetivo analisar as LOE da UE e da OTAN (ambiente externo) para concluir quais são as principais ameaças e oportunidades para o CAH ao nível das FFAA.

4.2.1. Ambiente externo e as novas ameaças híbridas

A dinâmica da revolução tecnológica transformou o mundo numa aldeia global, com um nível de progresso e integração sem precedentes, criando, ao mesmo tempo, terreno fértil para uma difusão equivalente de ameaças e riscos em todas as dimensões, que se alimentam desenfreadamente das tecnologias

disruptivas e do potencial devastador do ciberespaço (Training and Doctrine Command [TRADOC], 2019).

Neste contexto de homogeneização, Portugal e a Europa enfrentam um vasto leque de ameaças, riscos e desafios, potencialmente geradores de conflitos e passíveis de serem utilizados em campanhas híbridas (Despacho n.º 2536/2020 do MDN, de 24 de fevereiro).

A Leste, a ameaça de uma campanha híbrida consubstancia-se pela conjugação de operações de desinformação, ataques cibernéticos e constantes violações do espaço aéreo de diversos países, à já reanexação da Crimeia pela Rússia e no seu apoio aos separatistas de Donbass (Treverton et al., 2018).

No flanco Sul-Médio-Oriente, a instabilidade endémica com a implantação do Daesh, a guerra na Síria e no Iémen, a intensificação da crise na Líbia, a par do recrudescimento de Estados frágeis nas regiões da África subsariana e Sahel, configuram desafios securitários que podem ser instrumentalizados para fins que não a sua natureza, designadamente o terrorismo, pirataria, criminalidade organizada, tráfico humano e sobretudo o incremento exponencial de fluxos migratórios e das vagas de refugiados (Rodrigues & Borges, 2016). Para além destes desafios, a exígua cooperação ao nível de segurança e defesa, potenciada pelos ataques cibernéticos, a guerra das perceções, o *Information gathering*, o *Big Data*, a desinformação, as assimetrias económicas e as divergências políticas no continente europeu, propiciam o desenvolvimento e a confirmação das AH, como uma das principais preocupações securitárias e militares (Treverton et al., 2018).

Estas ameaças não reconhecem fronteiras e manifestam-se em todas as funções críticas de um Estado, requerendo por isso uma resposta global e uma aproximação concertada de toda a sociedade. A maioria dos países ainda não está preparada para essa realidade. Nesse sentido, "[…] é recomendável seguir de perto o que se está a fazer neste âmbito na UE e na OTAN, adaptando a doutrina e as boas práticas à nossa realidade e procurando total interoperabilidade e coordenação com essas organizações" (A.J.G. Marques, *op. cit.*).

No que respeita à UE, em abril de 2016, a CE e a Alta Representante adotaram um quadro comum para fazer face às AH e reforçar a resiliência da UE, dos seus Estados-Membros e dos países parceiros e, simultaneamente, aumentar a cooperação com a OTAN. Esse quadro propõe vinte e duas ações operacionais destinadas a dar aos Estados-Membros uma base para a luta coletiva contra as AH e é apoiado por um vasto leque de instrumentos e iniciativas, incluído a utilização

de todo potencial dos Tratados (CE, 2016b). Mais tarde, no dia 13 de junho de 2018, a Alta Representante para a UE, em conjunto com a CE, publicou uma comunicação conjunta, na qual ficaram definidas as principais LOE para combater as AH (CE, 2018). Esta declaração evidencia que o CAH deve basear-se fundamentalmente nas seguintes áreas: melhorar a consciência situacional; reforçar a resiliência; reforçar a prevenção e a resposta a situações de crise; e melhorar a cooperação internacional e interagências (CE, 2018). Estes vetores prioritários constituem as variáveis do modelo de análise do presente estudo.

Por sua vez, a NATO apresenta, desde 2015, uma estratégia para combate à GH, garantindo que os Aliados estão suficientemente preparados e apoiados para combater ataques híbridos. A mesma prevê medidas robustas, incluindo a evocação do artigo 5.º, e vem consolidar as decisões da cimeira de Gales de 2014, tendentes ao reforço da Postura de Defesa e Dissuasão, através da: (i) aprovação do Readiness Action Plan (ii) identificação e respostas aos desafios impostos pelas AH (iii) criação do Centro de Comunicações Estratégicas na Letónia, (iv) exercícios com foco nas AH (v) melhoria da coordenação interagências, (vi) melhoria da capacidade de antecipação estratégica (vii) e desenvolvimento do Defence Planning Package (OTAN, 2015).

No entanto, no que concerne às AH, a Aliança declarou um conjunto de medidas em julho de 2016 e atualizou-as em 2018. Estas propostas contemplaram também um conjunto de ações para incrementar a cooperação e delinear uma estratégia comum (OTAN, 2018a). Apesar de ser perentória em afirmar, que a principal responsabilidade de responder a AH recai sobre o país-alvo e na sua capacidade de resiliência, a Aliança tem vindo a disponibilizar um conjunto de mecanismos de cooperação e colaboração para aprofundar o conhecimento e contribuir para a criação de sinergias, que se estendem por várias medidas, em áreas civis e militares (OTAN, 2019). Destas medidas destacam-se as seguintes: incrementar e incentivar a partilha de informações entre Aliados através do Hybrid Analysis Branch; incrementar os eventos híbridos nos exercícios (e.g. Crisis Management Exercise); implementar o uso das Counter Hybrid Support Teams (CHST); intensificar a cooperação com parceiros e organizações, nomeadamente a UE; encorajar o fortalecimento da resiliência nacional ao nível do planeamento civil de emergência; encorajar o uso das comunicações estratégicas para contrariar e denunciar campanhas híbridas; continuar a desenvolver o esforço na Ciberdefesa; considerar opções de resposta coletiva no CAH (Ibid).

De facto, existe uma forte cooperação OTAN-EU. Desde logo, a criação do Hybrid CoE em 11 de abril de 2017. A iniciativa teve origem na CE (2016b)

tendo sido aprovada no conjunto comum de propostas para a implementação da Declaração Conjunta, endossada pelo Conselho da UE e pelo Conselho do Atlântico Norte em 6 de dezembro de 2016 (OTAN 2016a). Estas propostas contêm um conjunto de medidas para incrementar a cooperação OTAN-UE no CAH, o que permitiu que estas organizações começassem a trabalhar em estreita ligação no sentido desenvolver *playbooks* e operacionalizar procedimentos conjuntos, nomeadamente nas seguintes áreas: consciência situacional; prevenção e resposta a crises; segurança cibernética; comunicação estratégica; e realização de exercícios de AH (OTAN, 2016b).

Esta declaração conjunta vem reforçar a necessidade de aumentar a cooperação entre as estruturas mais relevantes destas organizações, ao mesmo tempo, que os países avaliam as suas próprias vulnerabilidades, de forma a garantir uma resposta horizontal "*whole-of society*" apoiada por ambas instituições. A Figura 11 reflete essa abordagem abrangente, que passa por uma resposta conjunta e integrada em termos nacionais e internacionais, onde se privilegia o conhecimento situacional, a prontidão e a resiliência, numa dinâmica de segurança cooperativa (OTAN, 2018b).

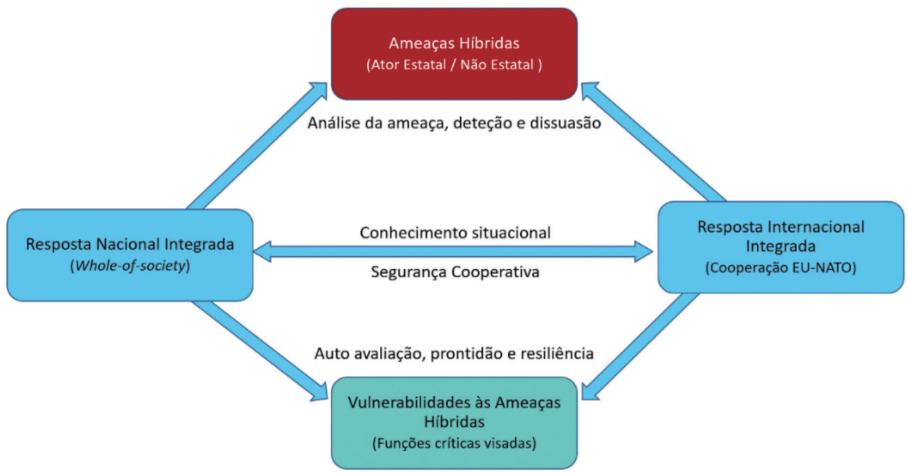


Figura 11 – Abordagem abrangente da UE e OTAN às AH
Fonte: Adaptado de OTAN (2018b, p. 1).

4.2.2. Apresentação e discussão de resultados da QD2

A análise das principais ameaças e oportunidades baseia-se nas respostas à pergunta 3 do guião e na AD efetuada no âmbito desta dimensão.

Decorrente da AD, conclui-se que existe um conjunto de ferramentas e de oportunidades no âmbito das estratégias delineadas pela UE e OTAN para apoiar os EstadosMembros, Aliados e parceiros, nomeadamente:

– Na melhoria do conhecimento situacional, mediante a criação de mecanismos específicos para a troca de informação;

– Na criação de sinergias ao nível da comunicação estratégica;

– No reforço da resiliência, abordando setores estratégicos e críticos, como a cibersegurança e as infraestruturas críticas;

– Na prevenção e resposta a crises, definindo procedimentos eficazes, examinando a aplicabilidade dos tratados e acordos de defesa coletiva, caso ocorram ataques híbridos de grande amplitude;

– Na cooperação com os parceiros internacionais, assegurando um esforço conjunto no CAH.

Relativamente à análise de conteúdo, inferiram-se 11 oportunidades e dez ameaças. A Figura 12 apresenta as seis oportunidades e as seis ameaças que foram verificadas ($x \geq 80\%$) ou parcialmente verificadas ($50\% \leq x < 80\%$).

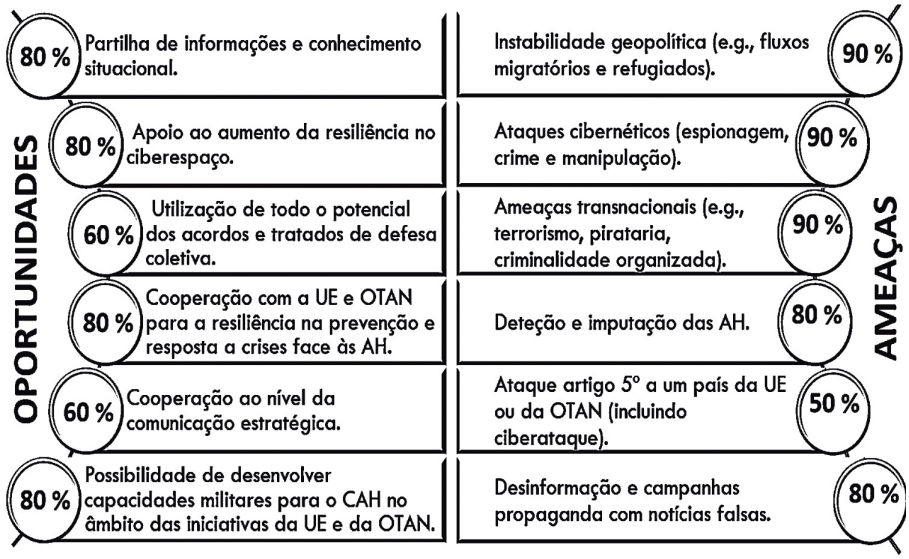


Figura 12 – Oportunidades e ameaças

Relativamente às oportunidades, merecem especial destaque por se terem verificado com 80 % dos entrevistados as seguintes: partilha de informações e a melhoria do conhecimento situacional, apoio ao aumento da resiliência no

ciberespaço, cooperação com a UE e OTAN para a resiliência na prevenção e resposta a crises e a possibilidade de desenvolver capacidades para o CAH no âmbito das iniciativas da UE e da OTAN. As ameaças que mais se destacaram são: (i) com 90 %, o aumento da instabilidade geopolítica, os ataques cibernéticos e as AT; (ii) com 80 %, a dificuldade de deteção e imputação das AH e a desinformação e campanhas de propaganda.

Conclui-se que existe um conjunto de ferramentas e de oportunidades no âmbito das estratégias delineadas pela UE e OTAN para apoiar os Estados-Membros, Aliados e Parceiros, que podem potenciar as capacidades nacionais para o CAH. Ainda neste âmbito, deduziu-se que a melhor forma de consolidar uma estratégia nacional, passa por acomodar as principais LOE destas organizações, que assentam nos seguintes pilares: melhorar o conhecimento situacional; reforçar a resiliência; reforçar a prevenção e resposta a crises; e melhorar a cooperação internacional e interagências.

Tendo em conta essas variáveis do ambiente externo, a análise de conteúdo permitiu inferir e validar, seis oportunidades (quatro verificadas e duas parcialmente verificadas) e seis ameaças (cinco verificadas e uma parcialmente verificada). Responde-se assim à QD2 e cumpre-se o OE2.

4.3 Capacidade das Forças Armadas para o combate às ameaças híbridas

Este subcapítulo tem por objetivo analisar a capacidade das FFAA para o CAH, para concluir quais são as principais vulnerabilidades e potencialidades. Examina-se o ambiente interno e apresentam-se os resultados da análise das entrevistas realizadas no âmbito desta dimensão.

4.3.1 Análise ambiente interno e as novas ameaças híbridas

A localização geográfica de Portugal, a extensão dos seus limites marítimos e a sua vulnerabilidade económica no âmbito da UE, constituem um terreno fértil para a influência híbrida e para o uso combinado de ameaças associadas, das quais se destacam: (i) crime organizado transnacional, branqueamento de capitais, tráfego de estupefacientes e imigração ilegal; (ii) ciberataques; (iii) terrorismo transnacional; (iv) espionagem ao nível político, militar e económico; (v) definhamento económico-financeiro; (vi) disputa de recursos; (vii) pirataria; (vii),

vagas de refugiados e fluxos migratórios (RCM n.º 19/2013, de 05 de abril). Estas ameaças podem manifestar-se de forma mais cinética, através de impactos físicos diretos, através do uso da força, e de forma menos cinética, que tem mais a ver com a perceção, influência e manipulação (Duarte, 2020).

Comparado a outros Estados europeus, Portugal não tem sido um alvo significativo de ataques híbridos cinéticos devido à sua dimensão geopolítica. No entanto, não escapa ao que está a acontecer na Europa, que cada vez mais, tem vindo a ser alvo de ataques não cinéticos, especialmente através do ciberespaço, em campanhas de desinformação e por pressões económicas e financeiras (Ibid.). Neste contexto, a Tabela 1 evidencia os dados estatísticos das ocorrências das AH em Portugal durante os anos de 2017 a 2018 com realce para a debilitada situação financeira portuguesa, que tem propiciado vulnerabilidades de âmbito económico, principalmente chinesas. A Tabela 2 realça a evolução dos ataques cibernéticos no mesmo período.

Tabela 1 – AH em Portugal - 2017/2018

Tipo Ameaça	Ocorrências			Perpetrador		
	Sim	Não	Factual	Rússia	China	Outros
Ações cinéticas						
Ações *proxies*		x				
Conflitos não declarados		x				
Grupos paramilitares		x				
Ações não cinéticas						
Operações de narrativa, redes sociais, media	x		x	x	x	x
Financeiro	x		x	x	x	
Pressão económica	x				x	
Ciberataques	x		x	x	x	x

Fonte: Duarte (2020, p. 15).

Tabela 2 – Evolução dos ataques cibernéticos em Portugal - 2017/2018

Tipo de Classificação	Número de Ocorrências	
	2017	2018
Comando & controlo	11,345	21,626
Distribuição	n/d	822
Desconhecido	0	n/d
Spam	n/d	119
Malware	22,665	405,866
Phishing	1,496	58,142
Alertas Ids	5,081	7,830
Blacklist	959,361	2,885,640
Comprometimentos	27,218	7,937
Brute-force	700	405,866
Botnet drone	562,521	1,030,717
Serviços vulneráveis	41,363,567	51,071,703
Scanner	2,189	68,748
Total	42,956,143	55,964,075

Fonte: Duarte (2020, p. 16).

Importa enquadrar legislativamente a atuação das FFAA, pensando que para o CAH ser tratado com eficácia, "[…] nenhuma área governativa deve chamar a si essa responsabilidade […] já que é um assunto transversal, em que todas as áreas ou vetores do Estado devem analisar o que podem fazer, e estarem prontos e resilientes para esse efeito" (A.J.G. Marques, *op. cit.*).

Não obstante esta necessidade imperativa, a Constituição da República Portuguesa (CRP) é perentória em atribuir a defesa militar da República às FFAA, a satisfação dos compromissos internacionais e a participação em missões humanitárias e de paz, no quadro dos compromissos internacionais assumidos (Lei Constitucional n.º 1/2005, de 12 de agosto, p. 4682).

Por outro lado, o CEDN (2013) refere que a "[…] tipologia das ameaças transnacionais, como […] o crime organizado transnacional, a cibercriminalidade […], exige respostas estratégicas multissectoriais e integradas [devendo o Estado potenciar] as capacidades civis e militares existentes e impulsionar uma abordagem integrada na resposta […]" (RCM n.º 19/2013, de 05 de abril, pp. 1989-1990). Sendo esta realidade, consubstanciada por normativos subsequentes, tais como a Lei de Defesa Nacional (Lei Orgânica n.º 5/2014, de 29 de agosto) e a Lei Orgânica de Bases da Organização das Forças Armadas (Lei Orgânica n.º 6/2014, de 01 de setembro).

Ainda de acordo com o CEDN (2013), Portugal deverá garantir em todos os momentos a funcionalidade dos sistemas vitais de segurança nacional,

nomeadamente a capacidade de vigilância e controlo do território nacional e do espaço interterritorial, incluindo a fiscalização do espaço aéreo e marítimo, as redes de energia, comunicações, transportes, abastecimentos e informação assegurando a resiliência nacional (RCM n.º 19/2013, de 05 de abril, pp. 1989-1990). Finalmente, e não menos importante, as FFAA também têm um papel fundamental na estabilização da vizinhança próxima alargada, fundamental para defender os interesses nacionais, nomeadamente através da Cooperação no Domínio da Defesa (CDD), reforçando as capacidades dos nossos Parceiros para uma resposta às AH mais eficaz (MDN, 2020).

Partindo do enquadramento legislativo efetuado, reflete-se seguidamente sobre a Estratégia de desenvolvimento de capacidades. A Diretiva Ministerial Orientadora do Ciclo de Planeamento de Defesa Militar (DMPDM) "[…] estabelece o Ciclo de Planeamento de Defesa Militar (CPDM), baseado em capacidades militares, […] articulado com o ciclo de planeamento da OTAN e com o Processo de Desenvolvimento de Capacidades da UE" (MDN. 2020, p. 36).

Esta modalidade de planeamento está prevista no CEDN (2013) e contempla o processo de planeamento da UE, assegurando a partilha de capacidades em todos os ciclos e a articulação da programação e do planeamento. Para esse efeito, Portugal participa no debate do desenvolvimento de capacidades, que contribui para o sistema de *Smart Defense* da OTAN e para o *Pooling & Sharing* da UE, orientado pela Agência Europeia de Defesa (AED) (RCM n.º 19/2013, de 05 de abril).

Por outro lado e tendo em conta os cenários de atuação perspetivados e as ameaças à segurança nacional, foi definido como prioridade, o desenvolvimento de capacidades que possam contribuir para: (i) a manutenção da capacidade de dissuasão; (ii) a vigilância e defesa das áreas sob jurisdição nacional; (iii) a participação em teatros internacionais; (iv) a participação em missões humanitárias e de apoio ao desenvolvimento e bem-estar das populações; (v) e o aumento da capacidade de atuar no ciberespaço e no espaço (MDN, 2020).

Neste contexto, deve ser considerado "[…] o desenvolvimento da economia nacional, promovendo a indústria nacional, em parceria com os centros de investigação e as universidades nacionais" (MDN, 2020, p. 37). No entanto, para o CAH importa desenvolver e consolidar outras capacidades fundamentais, bem como, adaptar de forma conjunta, o conceito de "Batalha MultiDomínio" através de "[…] estruturas e organizações mais flexíveis, modelares, com menor sustentação logística […] tirando o máximo partido de programas de I&D [Investigação e Desenvolvimento] e de edificação de capacidades […], em desenvolvimento na NATO e na UE" (Pires, 2018, p. 44).

Quanto ao impacto desta estratégia na Lei de Programação Militar, convém avivar que um dos principais objetivos do Plano de Desenvolvimento de Capacidades (CDP/2018), aprovado pela Agência Europeia de Defesa, consiste na identificação das capacidades prioritárias de defesa, no curto, médio e longo prazos, assim como, na identificação das áreas tecnológicas críticas até 2040 (AED, s.d.).

A gama de capacidades prevista no CDP/2018 contempla: operações no ciberespaço; operações de combate terrestre; C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*); superioridade de informação; capacidades de apoio logístico e médico; projeção de força; e as tecnologias disruptivas (Correia, 2019).

A Lei de Programação Militar (LPM), correspondente ao período de 2019 a 2030, estipula o investimento público das FFAA em matéria de armamento e equipamento, tendo em vista os seguintes objetivos: modernizar, operacionalizar e sustentar o sistema de forças nacional; promover o duplo-uso das capacidades militares; potenciar o investimento na economia nacional; e responder, na medida do possível, às exigências instrumentais da UE e OTAN em termos de desenvolvimento de capacidades e de prontidão e disponibilização de forças, estruturas e meios de defesa (Lei Orgânica nº 2/2019, 17 de junho de 2019). A Figura 13 ilustra os principais programas da LPM.

Figura 13 – Principais programas da LPM
Fonte: Correia (2019).

A Figura 14 mostra, a inter-relação dos programas da LPM, por áreas de capacidades, com o CDP/2018, o que permite inferir a existência de uma percentagem bastante significativa de prevalência entre projetos, propiciando condições favoráveis para aceder a fundos do Fundo Europeu de Defesa (FED) (Correia, 2019).

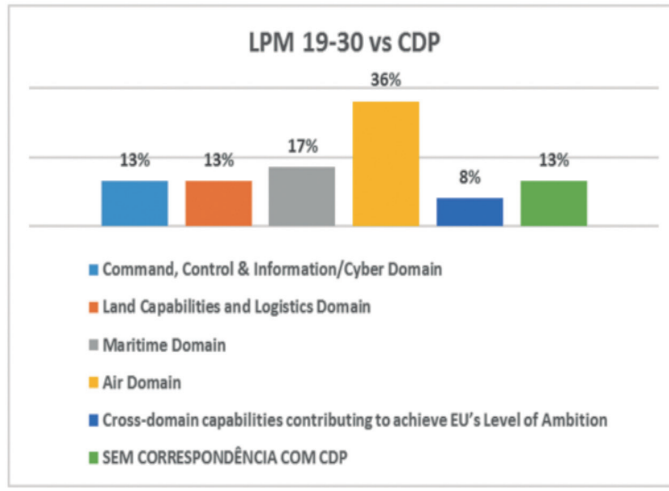


Figura 14 – Programas da LPM vs CDP/2018
Fonte: Correia (2019).

4.3.2 Apresentação e discussão dos resultados do Q3

A atuação das FFAA no CAH encontra-se vertida de forma implícita no normativo legislativo vigente, essencialmente pela natureza transnacional, transversal e multidisciplinar deste tipo de ameaças e a sua similitude com as existentes. Neste âmbito, a resposta às AH deve incluir as FFAA, as Forças e Serviços de Segurança (FSS) e o Sistema de Proteção Civil, assumindo uma responsabilidade primária do Estado, a que se devem associar os cidadãos, numa estratégia de segurança cooperativa.

A LPM contempla programas e, nesses, a possibilidades de ajustar projetos para fazer face às AH, que se enquadram nas iniciativas da OTAN e da UE, nomeadamente: a ciberdefesa; os serviços de informações e comunicações baseados no espaço; as capacidades de apoio logístico e médico; a superioridade de informação; a projeção de força; e as tecnologias disruptivas. Ao comparar as capacidades indicadas na LPM com o CDP/2018, verifica-se que existe uma significativa sintonia entre os diferentes programas e projetos, que podem contribuir para a edificação e consolidação de

capacidades essenciais para o CAH. Tendo em conta o enquadramento do ambiente interno e a análise de conteúdo inferiram-se 12 potencialidades e 11 vulnerabilidades. Desse resultado selecionaram-se seis potencialidades e sete vulnerabilidades que se apresentam na Figura 15, por terem sido verificadas ou parcialmente verificadas, todas com uma frequência de registos ≥ 50%.

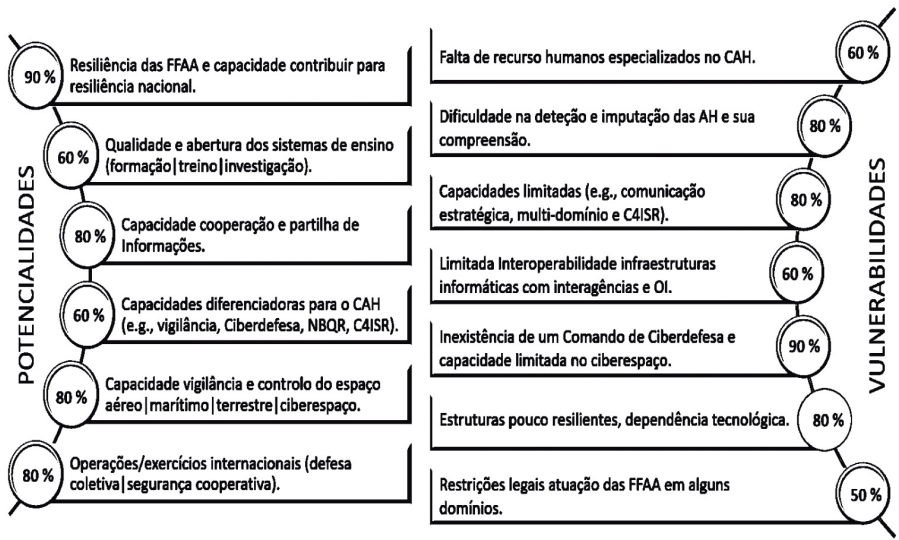


Figura 15 – Potencialidades e Vulnerabilidades

As potencialidades que mais se destacam são, a resiliência das FFAA e a capacidade de contribuir para a resiliência nacional com 90% e com 80%, as seguintes: capacidade de cooperação e partilha de Informações; capacidade de vigilância e controlo do espaço aéreo, marítimo, terrestre e do ciberespaço; e a experiência em operações e exercícios internacionais.

Relativamente às vulnerabilidades, merece especial destaque: a inexistência de um Comando de Ciberdefesa; a capacidade limitada no ciberespaço, por se ter verificado com 90%, a par da dificuldade na deteção e imputação das AH e sua compreensão; as capacidades limitadas em comunicação estratégica, multi-domínio e C4ISR; e as estruturas pouco resilientes, com forte dependência tecnológica, por se terem verificado com 80% dos entrevistados.

Em suma, a atuação das FFAA está enquadrada de forma implícita no normativo legislativo vigente. Nesse sentido, a resposta às AH deve incluir a cooperação civil-militar e a articulação interagências nomeadamente com o Sistema de Proteção Civil,

numa estratégia de segurança cooperativa de toda a sociedade. Neste contexto, as FFAA desempenham uma função única, pelos seus recursos materiais, humanos, capacidades diferenciadoras, infraestruturas e treino, que permitem assegurar a sua própria resiliência e contribuir para a resiliência nacional.

Tanto a LPM, como os projetos, de I&D e de edificação de capacidades, na UE e na OTAN, refletem presentemente, a maioria das necessidades para o CAH, pelo que, bastará adaptar os projetos que estão em curso às lacunas mais prementes nas FFAA. Este capítulo permitiu analisar o ambiente interno face às AH e examinar a estratégia de desenvolvimento de capacidades de forma a enquadrar a análise de conteúdo, permitindo inferir e validar seis potencialidades (quatro verificadas e duas parcialmente verificadas) e sete vulnerabilidades (quatro verificadas e três parcialmente verificadas). Responde-se assim à QD3 e cumpre-se o OE3

4.4 Análise SWOT e resposta à QC

Este subcapítulo tem como objetivo apresentar as principais LA para o CAH ao nível da FFAA, deduzidas através de uma análise SWOT, correlacionando as potencialidades e vulnerabilidades, no ambiente interno, com as oportunidades e ameaças, do ambiente externo, validadas pelos resultados das QD2 e QD3 e enquadrados pelos resultados da QD1 e da respetiva AD.

4.4.1 Desafios estratégicos

De forma a assegurar o devido alinhamento com o meio envolvente, as LA devem assentar, primordialmente, nos seguintes Desafios Estratégicos (DE) (CE, 2018):

DE1 – Melhorar o conhecimento situacional e reconhecer a natureza das AH, com o objetivo identificar as principais vulnerabilidades e contribuir para a sua deteção e resposta adequada. Desafio que passa sobretudo, pelo processamento e análise de informações sobre as AH, incluindo as ameaças NBQR, a contraespionagem e as ciberameaças, articulando esforços e criando sinergias neste âmbito através da cooperação com a UE e OTAN;

DE2 – Reforçar a resiliência das FFAA, nomeadamente no setor da cibersegurança, no desenvolvimento de capacidades da Defesa Militar e na segurança das infraestruturas críticas;

DE3 – Reforçar capacidade para prevenir e responder a situações de crise, de forma a dar uma resposta rápida aos acontecimentos desencadeados pelas

AH. O objetivo é que as FFAA participem no planeamento e desenvolvimento das atividades que concorrem para a resiliência nacional de modo a prevenir, responder e recuperar de crises, de forma rápida e coordenada;

DE4 – Fomentar a cooperação com a UE, a OTAN e as regiões vizinhas e países terceiros de forma a articular estratégias, medidas e modelos de atuação, para prevenir, impedir e dar resposta às AH, robustecendo a dimensão alargada de segurança no CAH.

4.4.2. Análise SWOT

A análise SWOT, tem por objetivo estabelecer prioridades de atuação e respetivas LA e baseia-se em quatro ideias chave: usar as potencialidades para obter vantagens sobre as oportunidades (PO); as oportunidades para superar as vulnerabilidades (VO); as potencialidades para evitar ameaças (PA); e em minimizar as vulnerabilidades para evitar ameaças (VA). A Figura 16 sintetiza a matriz SWOT efetuada.

AMBIENTE EXTERNO	AMBIENTE INTERNO: POTENCIALIDADES	AMBIENTE INTERNO: VULNERABILIDADES
	P1 - Resiliência das FFAA e capacidade contribuir para resiliência nacional. P2 - Qualidade e abertura dos sistemas de ensino (formação|treino|investigação). P3 - Capacidade cooperação e partilha de Informações P4 - Capacidades diferenciadoras para o CAH (e.g., vigilância, Ciberdefesa, NBQR, C4ISR). P5 - Capacidade vigilância e controlo do espaço aéreo|marítimo|terrestre|ciberespaço. P6 - Operações/exercícios internacionais (defesa coletiva|segurança cooperativa).	V1 - Falta de recurso humanos especializados no CAH. V2 - Dificuldade na deteção e imputação das AH e sua compreensão. V3 - Capacidades limitadas (e.g., comunicação estratégica, multi-domínio e C4ISR). V4 - Limitada Interoperabilidade infraestruturas informáticas com interagências e OI. V5 - Inexistência de um Comando de Ciberdefesa e capacidade limitada no ciberespaço. V6 - Estruturas pouco resilientes, dependência tecnológica. V7 - Restrições legais atuação das FFAA em alguns domínios.
OPORTUNIDADES O1 - Partilha de informações e conhecimento situacional. O2 - Apoio ao aumento da resiliência no ciberespaço. O3 - Utilização de todo o potencial dos acordos e tratados de defesa coletiva. O4 - Cooperação com a UE e OTAN para a resiliência na prevenção e resposta a crises face às AH. O5 - Cooperação ao nível da comunicação estratégica. O6 - Possibilidade de desenvolver capacidades militares para o CAH no âmbito das iniciativas da UE e da OTAN.	**CRESCIMENTO** PO1 - Incrementar o intercâmbio, partilha de informações sobre AH com a UE, OTAN e as entidades nacionais competentes. [P2, P3, P4, P5, P6] - [O1, O2, O4, O6] PO2 - Reforçar o contributo para a operacionalização da cibersegurança e da capacidade de ciberdefesa nacional face às AH. [P1, P4] - [O1, O2, O4, O6] PO3 - Dinamizar o ensino, a investigação e desenvolvimento em parceria com entidades nacionais e internacionais com enfoque no CAH. [P2, P6] - [O1, O4, O6]	**DESENVOLVIMENTO** VO1 - Desenvolver capacidades de comunicação estratégica e a resiliência perante a desinformação e campanhas híbridas. [V1, V2, V3, V5, V6, V7] - [O1, O2, O3, O4, O5, O6] VO2 - Integrar, explorar e coordenar as ações militares no CAH, otimizando os programas de desenvolvimento e edificação de capacidades definidas pela LPM e no âmbito da UE e da OTAN. [V1, V2, V3, V4, V5] - [O1, O4, O5, O6] VO3 - Alinhar as estratégias militares, nos domínios genético, estrutural e operacional de forma mais efetiva para o CAH. [V1, V3, V4, V5, V6] - [O2, O4, O6]
AMEAÇAS A1 - Instabilidade geopolítica (e.g., fluxos migratórios e refugiados). A2 - Ataques cibernéticos (espionagem, crime e manipulação). A3 - Ameaças transnacionais (e.g., terrorismo, pirataria, criminalidade organizada). A4 - Deteção e imputação das AH. A5 - Ataque artigo 5º a um país da UE ou da OTAN (incluindo ciberataque). A6 - Desinformação e campanhas propaganda com notícias falsas.	**MANUTENÇÃO** PA1 - Consolidar e expandir a capacidade de conhecimento situacional no EEIN, incluindo o ciberespaço face às AH. [P1, P3, P4, P5, P6] - [A1, A2, A3, A4, A6] PA2 - Desenvolver planos de articulação operacional, incluindo a necessária coordenação interagência para o combate às AH, às AT e proteção de infraestruturas críticas. [P1, P3, P4, P5] - [A1, A2, A3, A4, A5] PA3 - Consolidar o apoio e a cooperação com as regiões vizinhas, países amigos e aliados, parceiros nacionais e internacionais no CAH. [P1, P2, P3, P4, P5, P6] - [A1, A3, A4, A6]	**DEFESA** VA1 - Explorar todo o potencial dos tratados de defesa coletiva em caso de ocorrência de AH graves. [V2, V3, V4, V5, V6, V7] - [A1, A2, A3, A5, A6] VA2 - Melhorar a coordenação entre as FFAA e os outros instrumentos de poder do Estado e agentes da proteção civil na prevenção e resposta a crises. [V1, V3, V4, V6] - [A1, A2, A3, A5] VA3 - Articular estratégias e modelos de atuação com a UE e OTAN, no contexto da resposta a crises e emergências complexas, ampliando a resiliência militar e os principais vetores da resiliência nacional. [V1, V2, V3, V4, V5, V7] - [A1, A2, A3, A4, A5, A6]

Figura 16 – Análise SWOT

4.4.3. Linhas de Ação

De forma a orientar e facilitar a superação dos desafios decorrentes das LOE da UE e da OTAN, importa enquadrar as principais iniciativas e medidas concretas a desenvolver. Nessa ótica, no Quadro 1 apresenta-se a associação das LA que resultaram da análise SWOT aos desafios, a qual constitui uma orientação para o processo de uma estratégia futura para o CAH ao nível das FFAA.

Quadro 1 – Linhas de ação

Desafios	Linhas de Ação
DE1	LA1 Incrementar o intercâmbio, partilha de informações sobre AH com a UE, OTAN e as entidades nacionais competentes. LA2 Dinamizar o ensino, a investigação e desenvolvimento em parceria com entidades nacionais e internacionais com enfoque no CAH. LA3 Consolidar e expandir a capacidade de conhecimento situacional no EEIN, incluindo o ciberespaço. LA4 Desenvolver capacidades de comunicação estratégica para fazer face à desinformação e campanhas híbridas.
DE2	LA5 Reforçar o contributo para operacionalização da cibersegurança e da capacidade de Ciberdefesa nacional. LA6 Desenvolver planos de articulação operacional, incluindo a necessária coordenação interagência para o combate às AH, AT e proteção de infraestruturas críticas. LA7 Alinhar as estratégias militares, nos domínios genético, estrutural e operacional de forma mais efetiva para o CAH.
DE3	LA8 Melhorar a coordenação entre as FFAA e os outros instrumentos de poder do Estado e agentes da proteção civil na prevenção e resposta a crises. LA9 Articular estratégias e modelos de atuação com a UE e OTAN, no contexto da resposta a crises e emergências complexas, ampliando a resiliência militar e os principais vetores da resiliência nacional.
DE4	LA10 Consolidar o apoio e a cooperação com as regiões vizinhas, países amigos e Aliados, parceiros nacionais e internacionais no CAH. LA11 Explorar todo o potencial dos tratados de defesa coletiva em caso de ocorrência de AH graves. LA12 Integrar, explorar e coordenar as ações militares no CAH, otimizando os programas de desenvolvimento e edificação de capacidades definidas pela LPM, no âmbito da UE e da OTAN.

4.4.4. Síntese conclusiva e resposta à QC

A dimensão multidimensional e transnacional das AH, vem reforçar a necessidade de existir uma visão alargada, com uma abordagem multi-instituicional, transversal e integrada de toda a sociedade para se enfrentar este novo espectro de ameaças, aumentando a necessidade de reforçar a cooperação civil-militar (com entidades públicas e privadas) nos diferentes patamares de decisão, exigindo, na

máxima extensão possível, sinergias nacionais e internacionais, de acordo com o quadro de alianças e acordos existentes.

As FFAA devem por isso estar preparadas para antecipar, prevenir e defenderem-se contra as AH, dissuadindo potenciais atores hostis, tornando ineficientes os seus ataques e limitando o seu impacto. Para esse efeito, devem procurar um alinhamento institucional, nos domínios genético, estrutural e operacional (e.g. edificação de novas capacidades multidomínio, estruturas mais flexíveis e fomentando a necessária resiliência através do treino e formação) para apropriar as suas capacidades de forma mais efetiva para o CAH. De forma a acomodar as principais LOE da UE e da OTAN neste âmbito, as FFAA deverão procurar superar, no âmbito da sua estratégia para o CAH, os seguintes desafios: aumentar o conhecimento situacional; aumentar a resiliência nomeadamente no domínio do ciberespaço, da comunicação estratégica e na segurança das suas infraestruturas críticas; potenciar as suas capacidades para prevenir e responder a situações de crise e recuperar de forma rápida; e fomentar a cooperação civil-militar nacional e internacional. A resposta a estes desafios, culmina neste capítulo com uma avaliação SWOT e a dedução das correspondentes LA para o CAH ao nível das FFAA, tendo por base o papel do IPM e as análises efetuadas ao ambiente interno (ameaças e oportunidades) e externo (potencialidades e vulnerabilidades). Assim, considera-se respondida a QC e cumprido o OG.

5. CONCLUSÕES

A emergência das AH, exponenciadas pela globalização e a informatização da vida moderna, com as mudanças tecnológicas associadas e a incerteza que daí advém, tem levado a sociedade a confrontar-se com um novo paradigma civilizacional, onde o tema das AH se assume cada vez mais, como um dos principais desafios securitários da atualidade.

Este conceito é tão antigo quanto os conflitos e as guerras, mas com um novo rótulo, robustecido por novas ferramentas e tecnologias voltadas para explorar e influenciar vulnerabilidades em vários domínios, de uma maneira sem precedentes, afetando a confiança nas instituições e os valores centrais das sociedades, de forma a alavancar a influência e o poder geopolítico.

O assunto passou a ser prioridade nas agendas da UE e da OTAN. Em 2016 a CE e o Serviço Europeu para Ação Externa desenvolveram 22 medidas para aumentar a resiliência dos seus Estados-Membros. A OTAN declarou um conjunto de ações em

2016 e atualizou-as em 2018. Estas propostas contemplaram também um conjunto de medidas para incrementar a cooperação e delinear uma estratégia comum.

O CEDN refere que devem ser potenciadas as capacidades civis e militares para uma abordagem integrada na resposta às AT e garantir o desenvolvimento de capacidades para assegurar os compromissos assumidos perante Organizações Internacionais a que Portugal pertence, pelo que, o estudo desta temática revelou-se atual, de especial relevância e acuidade.

Tendo por base este enquadramento, a investigação teve como OG propor as principais linhas de ação para o CAH ao nível das FFAA Portuguesas, acomodando simultaneamente, as principais linhas orientadoras estratégicas da UE e da OTAN.

O presente estudo utilizou o raciocínio indutivo, assente numa estratégia de investigação qualitativa, consubstanciada num estudo de caso como desenho de pesquisa. Os instrumentos de recolha de dados utilizados foram a entrevista semiestruturada, aplicada a uma amostra homogénea não-probabilística intencional de dez militares e civis com créditos e conhecimentos nesta matéria, bem como a análise documental, designadamente na QD1.

No que respeita à estrutura, após a introdução no primeiro capítulo, enquadrou-se conceptualmente a investigação, sobressaindo os seguintes aspetos:

– A constatação que GH e AH correspondem a diferentes desafios à segurança nacional, sobretudo quando nos focalizamos nas possíveis ameaças que podem surgir sem a necessária existência de um conflito armado;

– A GH consiste no desafio apresentado pela crescente complexidade do conflito armado, em que os adversários podem combinar diferentes tipos de guerra com meios não militares para neutralizar o poder militar convencional.

– As AH consistem em ações coordenadas e sincronizadas, que visam deliberadamente as vulnerabilidades sistémicas dos Estados e instituições democráticas, através de uma ampla gama de meios, explorando os limiares de deteção e imputação, com o principal objetivo de influenciar e alavancar a vantagem sobre o adversário.

No terceiro capítulo descreveu-se a metodologia e o método e no quarto capítulo, foi analisado, inicialmente, o papel do Instrumento de Poder Militar no CAH, tendo como referência o conflito da Rússia na Ucrânia. Para tal, foi efetuada uma análise de conteúdo das respostas às perguntas 1 e 2, permitindo inferir as principais ferramentas híbridas que foram utilizadas pelos instrumentos de poder da Rússia nas funções críticas da Ucrânia, em termos de ações e efeitos.

Posteriormente, realizou-se uma análise integrada com todas as variáveis e indicadores desta dimensão, representadas graficamente pelo *software Power Business Intelligence*, o que permitiu responder à QD1 e alcançar o OE1. Dos resultados obtidos, concluiu-se que:

– As principais ferramentas híbridas com ação direta e efeitos não lineares no domínio militar dizem respeito ao ciberespaço, desinformação e campanhas de propaganda, operações de ciberdefesa, operações e exercícios militares, forças paramilitares e milícias e violação do espaço territorial;

– O CAH requer uma aproximação e resposta de toda a sociedade, dependendo na maioria das vezes de ferramentas não militares. No entanto, o papel da Defesa Militar continua a ser muito importante, devido às contribuições únicas que possui, em termos nacionais e internacionais, para detetar, dissuadir e responder a ataques híbridos.

Para que esse papel seja determinante, torna-se necessário: (i) garantir uma melhor coordenação entre o uso da força e as outras alavancas de poder do Governo e dos países Aliados e parceiros; (ii) garantir capacidades para conduzir operações credíveis no âmbito da defesa naval, terrestre e aérea, incluindo nos domínios do espaço e do ciberespaço, mantendo a necessária dissuasão convencional; (iii) e contribuir para a resiliência nacional.

No decurso do quarto capítulo, respondeu-se também à QD2 e QD3 respetivamente, o que permitiu alcançar o OE2 e OE3. Para esse efeito, foi efetuada a análise de conteúdo às perguntas 3 e 4, que conduziram as respostas dos entrevistados para a elaboração de uma matriz SWOT. As respostas à pergunta 3 foram enquadradas com a análise do ambiente externo, tendo por base os principais documentos, que enformam as LOE da UE e da OTAN, o que permitiu inferir como principais:

– Ameaças: instabilidade geopolítica; ataques cibernéticos; AT; dificuldade de deteção e imputação das AH; desinformação e campanhas de propaganda; ataque a um país da UE ou da OTAN (artigo 5.º);

– Oportunidades: partilha de informações e a melhoria do conhecimento situacional; apoio ao aumento da resiliência no ciberespaço; cooperação com a UE e OTAN para a resiliência na prevenção e resposta a crises; apoio ao aumento da resiliência no ciberespaço; utilização de todo o potencial dos tratados de defesa coletiva da OTAN e UE; e cooperação ao nível da comunicação estratégica.

Analogamente, as respostas à pergunta 4 foram reforçadas com o estudo do

ambiente interno, inferindo-se como principais:

– Potencialidades: a resiliência das FFAA e a capacidade de contribuir para a resiliência nacional; capacidade de cooperação e partilha de Informações; capacidade de vigilância e controlo do espaço aéreo e marítimo, terrestre e do ciberespaço; experiência em operações e exercícios internacionais; capacidades diferenciadoras das FFAA para o CAH; e a qualidade dos sistemas de ensino e de investigação e na área da formação e treino;

Vulnerabilidades: inexistência de um Comando de Ciberdefesa e capacidade limitada no ciberespaço; dificuldade na deteção e imputação das AH e sua compreensão; capacidades limitadas; estruturas pouco resilientes, com forte dependência tecnológica; restrições legais para a atuação das FFAA em alguns domínios; e limitada interoperabilidade das infraestruturas informáticas que assegure as ligações interagência, com as organizações nacionais e internacionais. Finalizou-se, respondendo à QC, através duma matriz SWOT, que foi realizada com base nas respostas às QD, permitindo propor 12 LA, apresentadas em 4.4.3.

O papel dos meios militares na dissuasão ou defesa contra AH ainda não está totalmente esclarecido. A permanente competição interestatal recorre cada vez mais a ações híbridas, como ataques cibernéticos, campanhas de desinformação ou interferência nas eleições, sendo neste âmbito, pouco provável, a necessidade do emprego militar.

Não obstante, o domínio militar é uma ferramenta do Estado e ao mesmo tempo, uma função crítica da sociedade, sujeito a ser visado nas suas vulnerabilidades, pelo que se revela importante assegurar a sua própria resiliência e o seu contributo para a resiliência nacional. Neste contexto, e como corolário desta investigação e principal contributo para o conhecimento, relevam-se a proposta de 12 LA para o CAH ao nível das FFAA, que visam constituir-se como elementos orientadores para o processo de alinhamento de uma estratégia futura, e um contributo para a clareza conceptual e compreensão das AH do papel das FFAA no seu combate.

Nesse sentido, recomenda-se que seja dado conhecimento deste trabalho ao EMGFA, como contributo para a eventual delineação de uma estratégia futura ao nível das FFAA, contribuindo também para uma reflexão militar sustentada, que permita colaborar num documento enquadrante das AH a nível nacional.

O presente estudo compreende algumas limitações que importam ter em consideração: a primeira prende-se com a novidade do conceito e a pouca

informação e conhecimento existente em Portugal, pelo que, o presente estudo teve de se basear, quase em exclusivo, nos estudos internacionais e nas entrevistas realizadas; a segunda é o facto de não existir uma estratégia nacional para o CAH e um órgão central de tomada de decisão e coordenação com agilidade e autoridade suficiente para delinear orientações estratégicas, o que permitiria enquadrar de uma forma mais pragmática a análise efetuada e os resultados obtidos.

Para estudos futuros e em complemento das LA propostas, identificam-se três áreas que requerem uma investigação adicional: analisar o contributo da Defesa Militar para a resiliência nacional e as medidas necessária para garantir a sua própria resiliência; analisar os recursos e as capacidades necessárias para combater as AH ao nível da estratégia genética, estrutural e operacional; e analisar opções de resposta militar abaixo do limiar do conflito armado para dissuadir e responder a ataques híbridos.

REFERÊNCIAS BIBLIOGRÁFICAS

Agência Europeia de Defesa. (s.d.). *Capability Development Plan* [Página online]. Retirado de https://www.eda.europa.eu/what-we-do/our-currentpriorities/capability-development-plan

Bryman, A. (2012). *Social Research Methods* (4ª ed.). Oxford: Oxford University Press.

Cadle, J., Paul, D., & Turner, P. (2010). Business Analysis Techniques: 72 Essential Tools for Success. Swindon: British Informatics Society Limited.

Casalunga, F.H. (2018). *Guerra Híbrida Cibernética: uma análise do conflito RussiaUcrânia (2014-2016) sob a perspetiva da tecnologia da informação*. 10.º Encontro Nacional da Associação Brasileira de Estudos de Defesa, 2018, São Paulo. Anais eletrônicos, 2018. v. 1.

Clausewitz, C. (1984). *Da Guerra*. Nova Jersey: Princeton University Press

Comissão Europeia. (2016a, 06 de abril). *Joint Communication - Joint Framework on countering HT a European Union response* [Página online]. Retirado de https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:52016JC0018&from =EN

Comissão Europeia. (2016b, 06 de abril). Comunicado de imprensa - *Segurança: UE reforça resposta às ameaças híbridas* [Página online]. Retirado de https://ec.europa.eu/commission/presscorner/detail/pt/IP_16_1227

Comissão Europeia. (2018). *Joint Communication: Increasing resilience and bolstering capabilities to address hybrid threats* [Página *online*]. Retirado de https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_a nd_bolstering_capabilities_to_address_hybrid_threats.pdf

Correia, A.M. (2019). *A Cooperação Estruturada Permanente, o Fundo Europeu de Defesa e a Lei de Programação Militar 2019-2030* – Atualização [Página online]. Retirado de https://www.eurodefense.pt/a-cooperacao-estruturada-permanente-o-fundoeuropeu-de-defesa-e-a-lei-de-programacao-militar-2019-2030/#_ednref61

Couto, A. C. (1988). *Elementos de Estratégia - Apontamentos para um curso*. Vol. I. Pedrouços: Instituto de Altos Estudos Militares.

Davis Jr., J. R. (2015). *Continued Evolution of Hybrid Threats. The Russian Hybrid Threat Construct and the Need for Innovation*. The Three Swords Magazine. Retirado de https://pdfs.semanticscholar.org/08c6/b9e234cd5c918f36dfd91b88967725a2be97.pdf?_ga=2.253064073.1650783760.1591290871-352523493.1591290871

Decreto-Lei n.º 249, de 28 de outubro. (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar*. Diário da República n.º 211/2015, 1.ª Série. Lisboa: Ministério da Defesa Nacional.

Despacho n.º 2536/2020, de 24 de fevereiro. (2020). *Diretiva Ministerial de Planeamento de Defesa Militar — quadriénio 2019-2022*. Diário da República, 2.ª Série, 38, 36- 41. Lisboa: Defesa Nacional - Gabinete do Ministro.

Dias, A. L., Varela, M. e Costa, J. L. (2013). *Excelência Organizacional*. Lisboa: Editora Bnomics.

Duarte, F. P. (2020). *Non-kinetic hybrid threats in Europe – The Portuguese case study (2017-18)*. Retirado de https://www.emerald.com/insight/1750-6166.htm

Fleming, B. (2011). *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*. School of Advanced Military Studies.

Garcia, F.P. (2017). *O Espaço do Atlântico e os principais desafios à segurança*. Revista de Ciências Militares, V (2), 95-116.

Guerra, I. (2006). *Pesquisa Qualitativa e Análise de Conteúdo. Sentidos e formas de uso*. Lisboa: Princípia.

Guindo, M. (2015). *La guerra híbrida: Nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales*. Instituto Español de Estudios Estratégicos (IEEE).

Hoffman, F. G. (2007). *Conflict in the 21 st Century: The Rise of Hybrid Wars*. Potomac Institute for Policy Studies, Arlington. Retirado de http://www.potomacinstitute.org/

Hoffman, F. G. (2009). *Hybrid Warfare and Challenges*. National Defense University Press.

Lei Constitucional n.º 1/2005, de 12 de agosto (2005). *Sétima revisão constitucional*. Diário da República, 1.ª Série-A, 155, 4642-4686. Lisboa: Assembleia da República.

Lei Orgânica n.º 6/2014, de 01 de setembro (2014). *Procede à primeira alteração à Lei Orgânica de Bases da Organização das Forças Armadas, aprovada pela Lei Orgânica n.º 1-A/2009, de 7 de julho*. Diário da República, 1.ª Série, 167, 4597-4611. Lisboa: Assembleia da República.

Lei n.º 2/2019, de 17 de junho (2019). *Aprova a lei de programação militar e revoga a Lei Orgânica n.º 7/2015*. Diário da República n.º 114/2019, 1.ª Série. 114. Assembleia da República.

Lusa. (2019). Candidatura ao Centro Europeu de Excelência para Combate às Ameaças Híbridas. Retirado de https://combatefakenews.lusa.pt/fake-newsgoverno-quer-plano-nacional-para-combater-desinformacao-e-ciberataques-caudio/

Luthar, S. S, Cichetti, D., & Becker, B, (2000). *The construct of resilience: A critical evaluation and guidelines for future work*. Child Development, 71, 3, 543-562.

Ministério da Defesa Nacional. (2014). *Conceito Estratégico Militar (CEM)*. Lisboa: Autor.

Ministério da Defesa. (s.d.). Glossário. Retirado de https://www.defesa.gov.br/glossario/

Multinational Capability Development Campaign. (2017, s.d.). *Understanding Hybrid Warfare* [Versão PDF]. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attach ment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Multinational Capability Development Campaign. (2019b, s.d.). *Conceptual Foundations and Implications for Defence Forces* [Versão PDF]. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/

uploads/attach ment_data/file/840513/20190401-MCDC_CHW_Information_note_- _Conceptual_Foundations.pdf A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas. 49

Nye Jr, J. (2008). *The Powers to Lead*. Oxford University.

Organização do Tratado do Atlântico Norte. (2010, 01 de maio). NATO 2020: Assured security; dynamic engagement. [Página online]. Retirado de https://www.nato.int/cps/en/natohq/topics_85961.htm

Organização do Tratado do Atlântico Norte. (2015). *Hybrid Warfare: NATO's New Strategic Challenge*.

Organização do Tratado do Atlântico Norte. (2016a, 08 de julho). *Joint declaration* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_133163.htm? selectedLocale=en

Organização do Tratado do Atlântico Norte. (2016b, 06 de dezembro). *Statement on the implementation of the Joint Declaration* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_138829.htm

Organização do Tratado do Atlântico Norte. (2016c, 09 de julho). *Warsaw Summit Communiqué, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016*. [Página *online*]. Retirado de https://www.nato.int/cps/ic/natohq/official_texts_133169.htm

Organização do Tratado do Atlântico Norte. (2018a, 12 de julho). *Brussels Summit Declaration, issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels 11-12 July* [Página *online*]. Retirado https://www.nato.int/cps/en/natohq/official_texts_156624.htm

Organização do Tratado do Atlântico Norte. (2018b, 23 de novembro). *Cooperating to counter hybrid threats* [Página *online*]. Retirado de https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counterhybrid-threats/index.html

Organização do Tratado do Atlântico Norte. (2019, 08 de agosto). *NATO's response to hybrid threats* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas. 50

Organização do Tratado do Atlântico Norte. (2020, 31 de março). *Resilience and Article 3* [Página *online*]. Retirado de https: http://www.nato.int/cps/en/natohq/topics_132722.htm

Pereira, J. (2018). *As ameaças híbridas - Uma abordagem conceptual no quadro da OTAN e da UE*. CEDIS.

Pires, N. C. (2018). *O Novo Conceito de "Multi-Domain Battle" e suas Implicações na Edificação de Capacidades Militares do Exército*. Lisboa: Instituto Universitário Militar.

Kaldor, M. (2005). *Old Wars, Cold Wars, New Wars, and the War on Terror*. International Politics, 42(4), 491–498.

Kapusta, P. (2015). *Gray Zone*. *Special Warfare,* October 2015. Retirado de https://www.soc.mil/SWCS/SWmag/archive/SW2804/GrayZone.pdf

Rego, A. R., Cunha, & Jr, M. (2018, s.d.). *Quantos participantes são necessários para um estudo qualitativo?* Linhas práticas de orientação [Página online]. Retirado de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-44642018000200004

Resolução do Conselho de Ministros n.º 19/2013, de 5 de abril. (2013). *Aprova o Conceito Estratégico de Defesa Nacional*. Diário da República, 1.ª Série, 67, 1981-1995. Lisboa: Presidência do Conselho de Ministros.

Roberts, J. Q. (2005, s.d.). *Maskirovka 2.0: Hybrid Threat, Hybrid Response* [Versão PDF]. Retirado de https://apps.dtic.mil/dtic/tr/fulltext/u2/1007494.pdf

Rodrigues, T. F., & Borges, J.V. (Coord.) (2016). *Ameaças e Riscos Transnacionais no novo Mundo Global*. Porto: Fronteira do Caos.

Santos, J. (2017). *O Emprego da Artilharia em Operações contra as Ameaças Híbridas*. (Trabalho de Investigação Aplicada - Mestrado Integrado). Academia Militar. Lisboa.

Sarmento, M. (2013). *Metodologia Científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora. A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas. 51

Serrano, M. (2013). *A Guerra é Filha Única*. Coleção Meira Mattos - Revista das Ciências Militares. 7(28), 65–78.

The European Centre of Excellence for Countering Hybrid Threats. (s.d.). *Hybrid Threats* [Página *online*]. Retirado de https://www.hybridcoe.fi/hybrid-threats/

The European Centre of Excellence for Countering Hybrid Threats. (2018, s.d.). *Helsinki in the era of hybrid threats – Hybrid influencing and the city* [Página *online*]. Retirado de https://www.hel.fi/static/kanslia/Julkaisut/2018/hybridiraportti_eng_neti.pdf

Training and Doctrine Command. (2017). *Multi-Domain Battle* - Frequently Asked Questions. Virginia: United States Army.

Training and Doctrine Command. (2019). *The Operational Environment and the Changing Character of Warfare*. Virginia: United States Army.

Treverton, G., Thvedt, A., Chen, A., Lee, K. & McCue, M. (2018). *Addressing Hybrid Threats*. Swedish Defence University.

Tzu. S. (2009). *The Art of War*. Edição em Português. Betrand Editora. United States Government Accountability Office (2010). U.S. GAO [Versão PDF]. Retirado de: http://www.gao.gov/assets/100/97053.pdf

Wikimedia. (s.d.). *Pro-Russian unrest in Ukraine*. [Página *online*]. Retirado de https://commons.wikimedia.org/wiki/File:2014_proRussian_unrest_in_Ukraine.png

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA, VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS. (DIPLOMÁTICO)

PREVENTION AND TACKLING OF HYBRID THREATS: IDENTIFYING MEASUREMENT INSTRUMENTS, VARIABLES AND NATIONAL RESILIENCE INDICATORS AGAINST HYBRID THREATS (DIPLOMATIC)

Autor
MAJ ART Albino José Pinheiro de Jesus

Orientador
MAJ ART Diogo Lourenço Serrão

1. INTRODUÇÃO

Uma leitura atenta a *magnum opus* de *Carl Von Clausewitz, Vom Krieg,* leva-nos a concluir que a guerra é uma atividade social entre atores com vontade própria, sentimentos, emoções e intenções hostis. Esta hostilidade pode não ter limite na aplicação do uso da força, com a finalidade única de fazer capitular o inimigo (Landmeter, 2018).

É reconhecido a Clausewitz , a trindade da guerra, baseado na violência, no acaso e na razão, também associável a outra trindade: o povo, as Forças Armadas (FFAA) e o governo unidos como bem expressa o seguinte triangulo (vide Figura 1) (Landmeter, 2018).

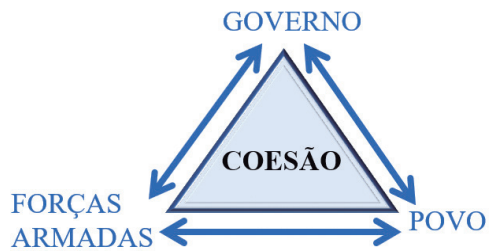


Figura 1 – Possível interpretação de trindade de Clausewitz
Fonte: Adaptado a partir de Evans (2016).

O elemento-chave desta relação é a coesão como garantia da manutenção dos interesses vitais, transpondo tal ideal para a Constituição da República Portuguesa. Com efeito, através dos artigos 273.º, 275.ºe 276.º define-se a obrigação ao Estado de assegurar a defesa nacional, às FFAA a responsabilidade pela defesa militar da República e a todos os portugueses o direito e dever da defesa da Pátria. (Constituição da República Portuguesa, 1976).

Este trabalho aborda uma das atuais ameaças à coesão nacional, as ameaças híbridas.

Ora a redação de uma qualquer estratégia, deve simultaneamente considerar uma avaliação da ameaça e das capacidades utilizáveis para lhe fazer face. Nesse contexto, o conceito que melhor acomoda essas características é a resiliência, sendo quotidianamente utilizado nesta, como em muitas outras áreas do conhecimento, da economia às ciências sociais (Linkov & Palma-Oliveira, 2016).

É assim fundamental que numa fase anterior a uma formulação estratégica, haja capacidade para a avaliar e, se possível, quantificar a resiliência nacional nos diferentes instrumentos de poder. Assim se justifica a importância da presente investigação, procurando contribuir com a determinação de variáveis e indicadores de resiliência, focado no instrumento de poder diplomático.

Uma vez que as ameaças híbridas são preocupação das alianças que Portugal integra, o desenvolvimento de uma estratégia nacional para lhes fazer face, conta com uma parcela atribuível às FFAA, como garante da soberania nacional. Desta forma, foi identificado como objeto de estudo, o Instrumento de poder do Estado Diplomacia, enquadrando o tema, nas ciências militares, no âmbito da Área de Investigação das Operações Militares e do Estudo das Crises e Conflitos Armados (Decreto-Lei N.o249, 2015).

O objeto de estudo foi delimitado temporalmente a partir de 2017, justificando-se como o ano de criação do Hybrid CoE; espacialmente, na zona geográfica Euro-atlântica, respeitando os três primeiros eixos da política externa Portuguesa, a Europa, o Atlântico e a Língua Portuguesa (Pereira, 2018a); e quanto ao conteúdo, concentramo-nos na investigação da resiliência, como a característica óbvia para precaver combater tais ameaças.

O objetivo geral (OG) da presente investigação é: Propor instrumentos de medida da Resiliência do instrumento de poder Diplomático contra ameaças híbridas. Concorrendo para este desiderato estabeleceram-se os seguintes objetivos específicos (OE):

OE1: Identificar o papel do instrumento de poder diplomático na soberania nacional;

OE2: Analisar a afetação do Instrumento de poder diplomático pelas ameaças híbridas;

OE3: Analisar variáveis e indicadores de resiliência do instrumento de poder diplomático.

Em sintonia com o procedimento metodológico de Quivy e Campenhoudt (2003, p. 44), que estabelece como primeira etapa "[...] a pergunta de partida[…]", que deve ter uma intenção de compreensão dos fenómenos, ser precisa, concisa e unívoca. Neste contexto, a Questão Central (QC) da investigação é: Como determinar a resiliência do Instrumento de poder diplomacia face a ameaças híbridas? Como facilitador do pensamento desta derivam três questões derivadas (QD):

QD1: Qual o contributo do instrumento de poder diplomático na soberania nacional?

QD2: Como é o instrumento de poder diplomático afetado pelas ameaças híbridas?

QD3: Quais as variáveis e indicadores de resiliência do instrumento de poder diplomático?

Na presente investigação seguiu-se uma metodologia de raciocínio indutivo, assente numa estratégia de investigação qualitativa com reforço quantitativo a fim de robustecer "os resultados qualitativos" (Bryman, 2012), substanciada num estudo de caso como desenho de pesquisa, conforme apresentado por Santos e Lima (2019).

Respeitante aos instrumentos e técnicas de recolha de dados, realizaram-se duas rondas de questionários respeitando a metodologia de *Delphi* a fim de assegurar maior concordância dos especialistas quanto aos indicadores de resiliência. Aplicaram-se metodologias científicas para aferir a concordância e a fórmula final de cálculo, como o coeficiente de correlação de postos de Kendall e sujeitou-se ainda à prova final de validação através de uma entrevista ao coordenador nacional do grupo de redação.

Em face do que antecede, a presente investigação está organizada, em três capítulos. Após a introdução à temática, o primeiro capítulo constitui o enquadramento teórico e concetual onde se apresenta o quadro teórico de referência. No segundo capítulo, explica-se a metodologia seguida, para no terceiro capítulo se descrever a diplomacia, a sua relação com a soberania nacional e analisar a atuação das ameaças híbridas para determinar as variáveis e os indicadores de resiliência, ponderados de acordo com a importância. Por último apresentamos as conclusões.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Este capítulo é composto por uma revisão de conceitos.

2.1. Revisão da literatura

Quando em 2013, o Chefe de Estado-Maior General da Rússia, publicou o seu artigo anunciando uma forma de conduzir a Guerra, estaria bem longe de imaginar que estava a apresentar algo bastante relevante na área dos conflitos híbridos, que ficaria conhecido como a doutrina *Gerasimov*, aludindo à combinação de ações convencionais e não convencionais. Esta nova "doutrina" veio alertar os países ocidentais do modo como conseguir alcançar os objetivos políticos e estratégicos através das ameaças híbridas (Bartles, 2016).

As ameaças híbridas podem ser empregues por Estados tirando partido das suas FFAA, mas também por outros atores, tais como terroristas ou grupos extremistas. Apesar de não ser um fenómeno recente, a forma como tem sido explorado, bem como a escala do seu uso tem sido surpreendente, utilizando ferramentas antigas associadas a novas tecnologias (Richterová, 2015). Nessa medida, o Poder *Cyber* tem-se revelado preponderante visto constituir-se como catalisador da hibridização, na medida em que os novos interfaces complexam a comunicação entre sistemas, surgindo novos alvos e acrescendo dificuldade na identificação das origens. Por outro lado, o domínio *Cyber* também funciona como vetor da comunicação, elemento-chave para a manipulação social, uma constante na estratégia das ameaças híbridas (Serrão, 2019).

Evidentemente que os decisores políticos e militares necessitam de compreender o potencial disruptivo associado às novas tendências tecnológicas, que podem permitir novas formas de violência, associadas ao uso da força num contexto de conflito híbrido. Os novos avanços tecnológicos sugerem que as ameaças híbridas irão expandir-se rapidamente (Artimová et al., 2019).

O quadro comum UE-NATO de 22 medidas apresentadas em 2016, foi um despertar sério para a temática, merecendo subsequentemente relatórios anuais de avaliação de implementação das medidas e impulsionando novos quadros de ações para áreas ainda pouco desenvolvidas, como o caso da Comunicação sobre a segurança de eleições europeias justas[26] e o Plano de Ação contra a desinformação[27].

[26] em setembro de 2018.
[27] em dezembro de 2018.

Esta dinâmica é bem demonstrativa da preocupação atual que esta organização tem, visando potenciar as suas capacidades para fazer face as alterações da cena internacional. A EU reconhece que está a tentar contrariar as ações hostis da Rússia (Fiott & Parkes, 2019), que foram apresentadas num artigo, antes mesmo de serem postas em prática, no contexto da Crimeia em 2016.

2.1.1 Diplomacia

Um outro conceito importante para este trabalho é a diplomacia, enquanto instrumento de poder do Estado, empregue para atingir objetivos nacionais estratégicos. Os instrumentos de poder nacional são utilizados de forma coordenada através da ação governativa.

A diplomacia de acordo com o departamento de estado norte-americano é o principal instrumento para se relacionar com outros Estados ou organizações, na defesa de valores, interesses e objetivos norte-americanos. Consideram ainda que é este o instrumento principal para organizar alianças e coligações (U.S. Joint Chiefs of Staff, 2013).

Numa visão mais nacional, o General Cabral Couto define "[…] diplomacia como a arte de convencer sem o emprego de força, utilizando a persuasão, negociação e mediação […]" (Couto, 1988, p. 95).

Olhando para um diplomata, a definição do Embaixador Calvet de Magalhães, diz-nos que a diplomacia é um instrumento da política externa para o estabelecimento e desenvolvimento dos contactos pacíficos entre os governos de diferentes Estados, pelo emprego de intermediários mutuamente reconhecidos pelas respetivas partes (Gomes, 1990). Apresenta como as suas tarefas fundamentais: a representação, a proteção, a informação e a negociação, atualmente acrescida de informação ativa, a promoção económica e a expansão cultural (Gonzaga-Ferreira, 1984).

A diplomacia é o modo privilegiado de execução da política externa, desenvolvendo-se na comunidade internacional, prosseguindo os objetivos estratégicos do Estado, obedecendo a um conjunto de princípios e regras na sua execução (Gomes, 1990). Esta execução estende-se hoje a todos os domínios da atividade humana, estabelecendo-se laços de aproximação e cooperação, por exemplo no desporto, na saúde, no trabalho, na emigração, nas atividades económicas, na cultura etc… (Gonzaga-Ferreira, 1984).

2.1.2 Resiliência

O último conceito que se reverte de importância para este estudo é a resiliência.

Esta é definida pela Academia Nacional de Ciências como a capacidade de planear e preparar para absorver, recuperar e adaptar face a um evento adverso (Linkov & Palma-Oliveira, 2016).

O rápido aumento na evolução tecnológica, o crescimento da população e do consumo, são característicos do complexo e dinâmico sistema antropocêntrico que caracteriza o século XXI, em que o Homem e a sua criação são centrais. Este sistema volátil e incerto, especialmente na forma como o Homem se relaciona com a natureza, o ambiente e a tecnologia, contribui para que a expressão resiliência esteja associada aos diversos sistemas em que o Homem é o elemento central (Pavlov & Hadjitorov, 2019).

Associando o fenómeno globalização, a esta circunstância, compreendemos que existe hoje, uma maior conectividade e interdependência entre vários domínios do ser humano, criando um sistema de sistemas.

Assim, podemos aceitar a definição de resiliência como a capacidade de uma pessoa, organização ou sistema, possui para se preparar, responder, recuperar e prosperar face a um perigo (Figura 2), sem nunca quebrar o seu ciclo (SIEMENS, 2013).

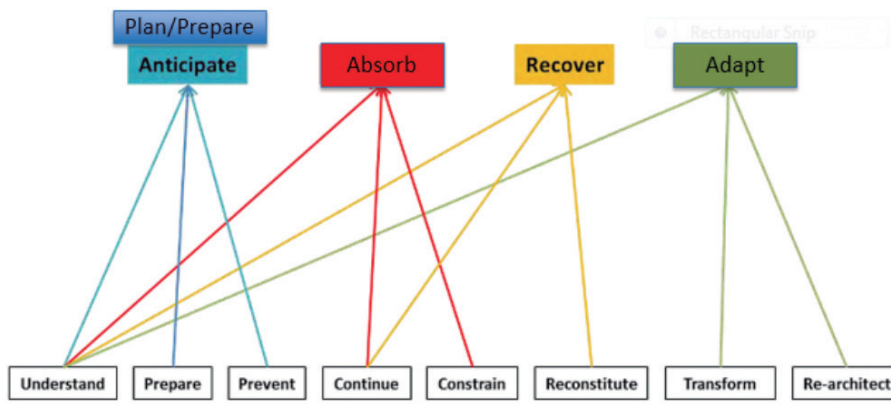


Figura 2 – Resiliência aplicada a um modelo Ciber
Fonte: Kott et al. (2018).

A análise da resiliência tem o seu foco nos perigos diários da organização, infraestrutura, ou sistema, relacionando probabilidade de acontecer determinado impacto negativo com o seu efeito mais ou menos destrutivo (Figura 3) (Linkov & Palma-Oliveira, 2016).

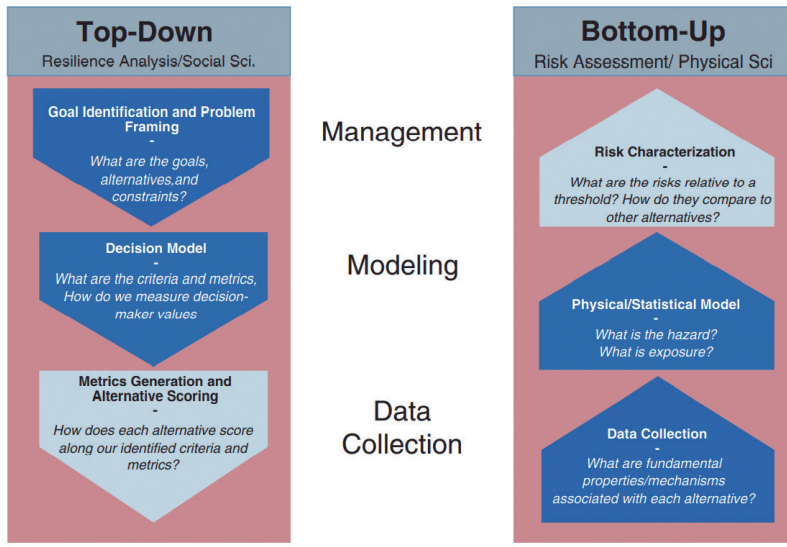


Figura 3 – Integração de Risco e Resiliência
Fonte: Linkov e Palma-Oliveira (2016).

A resiliência de um sistema pode ser representada graficamente relacionando o desempenho com o tempo (Figura 4), face a um evento adverso.

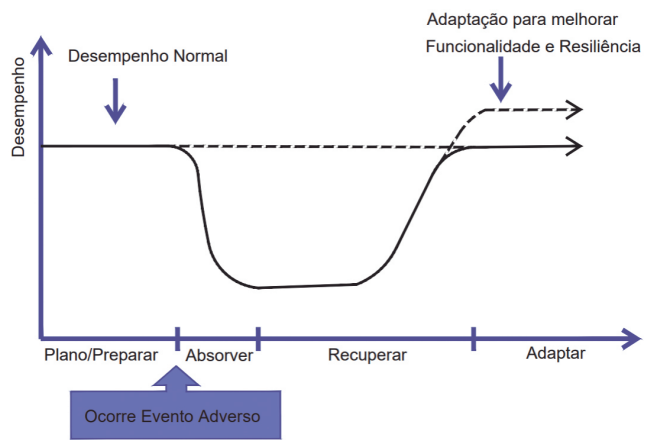


Figura 4 – Noção gráfica de Resiliência
Fonte: Adaptado a partir de Linkov e Kott (2019).

Resiliência pode ser definida como a capacidade de uma sociedade resistir com facilidade e recuperar rapidamente face a um choque ou evento negativo (NATO, 2020). No entanto, o facto da expressão resiliência poder ser aplicada, quer a um humano, um animal, ou um sistema, por exemplo, gera confusão, pelo que, definimos resiliência, para a presente investigação, como a capacidade de um sistema retornar ao seu estado inicial após uma perturbação (Pavlov & Hadjitorov, 2019).

2.2. Modelo de análise

Os conceitos estruturantes resultantes do modelo de análise escolhido para este estudo são apresentados no Quadro 1, e têm como finalidade ajudar-nos na racionalização do estudo (Quivy & Campehoudt, 2003, p. 260).

Quadro 1 – Modelo de Análise

<table>
<tr><td>OBJETIVO GERAL</td><td colspan="6">Propor instrumentos de medida da Resiliência do instrumento de poder Diplomático contra ameaças híbridas</td></tr>
<tr><td rowspan="2">Objetivo Específico</td><td>Questão Central</td><td colspan="5">Como determinar a resiliência do Instrumento de poder diplomacia face a ameaças híbridas?</td></tr>
<tr><td>Questões Derivadas</td><td>Conceitos</td><td>Dimensões</td><td>Variáveis</td><td>Indicadores</td><td>Técnicas de recolha de dados</td></tr>
<tr><td>OE 1
Identificar o papel do instrumento de poder diplomático na soberania nacional</td><td>QD 1
Qual o contributo do instrumento de poder diplomático na soberania nacional?</td><td>Diplomacia</td><td rowspan="4">Política externa

Estrutura diplomática Portuguesa

Diplomacia Económica

Diáspora</td><td>Europeia
Atlântica
Língua Portuguesa</td><td>N.º de representações diplomáticas junto das OI
N.º de propostas, projetos apresentados nas OI</td><td>Pesquisa documental e Questionários</td></tr>
<tr><td rowspan="3">OE 2
Analisar a afetação do Instrumento de poder diplomático pelas ameaças híbridas</td><td rowspan="3">QD 2
Como é o instrumento de poder diplomático afetado pelas ameaças híbridas?</td><td rowspan="3">Ameaças Híbridas</td><td>Constituintes da Rede Diplomática Portuguesa</td><td>Número de Embaixadas, consulados, Missões</td><td rowspan="3">Pesquisa documental e Questionários</td></tr>
<tr><td>Influências económicas</td><td>Boicotes
Sanções</td></tr>
<tr><td>Narrativas Contraditórias</td><td>Existência de Fact Checkers
Listas de emigrantes</td></tr>
<tr><td></td><td></td><td></td><td>Violação da Integridade Territorial</td><td>Pedido de Explicação</td><td>Número de violações</td><td></td></tr>
</table>

[Cont.]

OE 3 Analisar variáveis e indicadores de resiliência do instrumento de poder diplomático	**QD 3** Quais as variáveis e indicadores de resiliência do instrumento de poder diplomático?	Resiliência	Estrutura diplomática Portuguesa	Missões de apoio à internacionalização	Número de missões culturais Número de missões económicas	Pesquisa documental e Questionários
			Diplomacia Económica	Dificuldades económicas	Existência de legislação para proteção da economia	
			Diáspora	Influencias sobre comunidades estrangeiras	Número de fundações ou instituições influenciadoras	
			Violação da Integridade Territorial	Formalidade	Número de violações	

3. METODOLOGIA E MÉTODO

A metodologia de investigação segue as orientações metodológicas para elaboração de trabalhos de investigação seguidas no Instituto Universitário Militar (Santos et al., 2019), dividindo este percurso em duas fases, a fase I e a fase II.

3.1. Metodologia

Este estudo é de investigação aplicada, uma vez que ele assenta numa metodologia em que se formulam enunciados, para posteriormente os tentar verificar (Popper, 2012, p. 27).

O investigador encara o objeto da investigação numa perspetiva objetivista, segue procedimentos padronizados para conseguir as coisas (Bryman, 2012, p. 32). Por conseguinte epistemologicamente é positivista, uma vez que considera que só é possível chegar ao conhecimento com a confirmação das leis desenvolvidas (Bryman, 2012, p. 28).

Foi seguida uma metodologia de raciocínio indutivo, baseado na observação e categorização de factos particulares que, associados, permitam chegar a uma teoria, para confirmar (Sousa & Baptista, 2010, p. 8). Desta forma recorremos a uma estratégia de investigação qualitativa que alvitra a existência de uma relação indissociável entre o mundo real e a subjetividade do sujeito (Vilelas, 2009) com reforço quantitativo (Bryman, 2012), atendendo a se quantificar, pela atribuição de pesos relativos, a importância dos indicadores de resiliência.

Quanto ao desenho de pesquisa, seguiu-se um procedimento metodológico desenvolvido com base no estudo de caso, buscando descrever o objeto de estudo de forma completa, recorrendo a técnicas de recolha de dados diversas (Ponte, 2006, cit. por Freixo, 2011, p. 121), apoiado num horizonte temporal transversal em que dados quantitativos associados permitem determinar padrões (Figura 5) (Santos et al., 2019, p. 33).

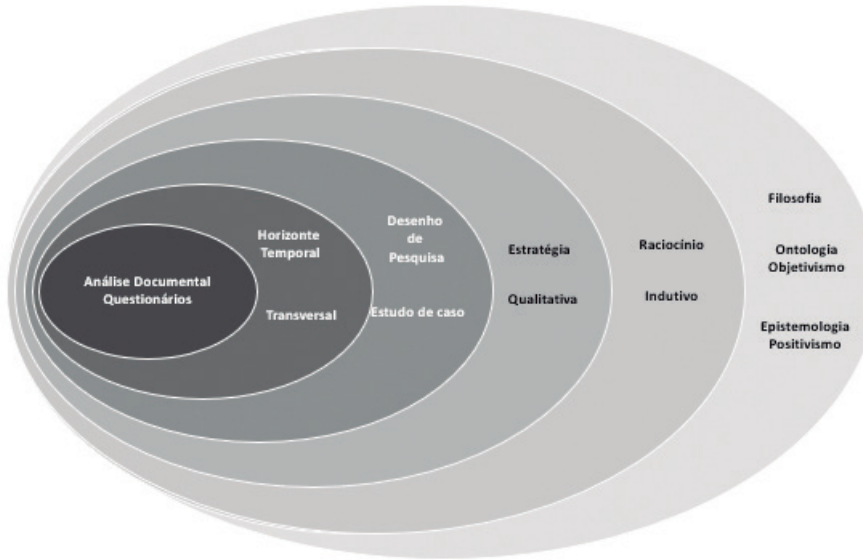


Figura 5 – Desenho de Investigação

3.2. Método

O caminho para chegar a instrumentos de medida da resiliência do instrumento de poder diplomático parte de uma revisão bibliográfica, apurando-se o estado da arte e inferindo-se as possíveis ameaças híbridas que afetam este instrumento de poder.

Após listadas tais ameaças, importa validá-las no panorama nacional, através de uma análise temporal, a três anos. Assim, através do método da análise de fatores, conclui-se quais as ações passíveis de conter as ameaças híbridas e, simultaneamente, os indicadores que confirmam tal aplicação. Os indicadores concluídos são apreciados por *experts* (académicos e em funções na área diplomática), utilizando o método de *Delphi*, para substantivamente os validar, através do grau de concordância obtido.

A técnica ou método de *Delphi* é uma ferramenta estratégica utilizada para conseguir a convergência de opinião sobre um assunto, através da realização de questionários, em rondas sucessivas, a um grupo de peritos (EMGFA, 2020). Foi desenvolvido na década de 50 do século passado pela Rand Corporation com o intuito de obter o mais confiável consenso de um grupo de especialistas, através de uma série de questionários de opinião (rondas). (Linstone & Turoff, 2002).

Com a finalidade de robustecer cientificamente o instrumento de medida concluído, este foi sujeito à apreciação final do coordenador do grupo de trabalho para a redação do documento de enquadramento Nacional das ameaças híbridas.

3.2.1. Participantes e procedimento

A escolha dos participantes atende, em bom rigor, à capacidade e aptidão. Capacidade pelo conhecimento reconhecido pela comunidade científica e aptidão por trabalharem atualmente num grupo de reflexão e execução do documento formal nacional, que analisa o contexto presente das ameaças híbridas. Assim assegura-se um conjunto de indivíduos com uma ou mais características comuns (Sarmento, 2013, p. 71).

A amostra foi constituída por um conjunto de elementos retirados da população, representativos e significativos (Sarmento, 2013, p. 71), num total de dez, que responderam aos questionários, respeitando a metodologia de *Delphi*.

Inicialmente, com os indicadores de resiliência inferidos, foi elaborado um inquérito com o objetivo de, com clareza e rigor, confirmar a concordância dos peritos com os indicadores apontados. Foi enviado a dez elementos, via *email*, uma vez que o questionário foi preparado com recurso à plataforma académica do Instituto.

Após as respostas iniciais, melhoraram-se os indicadores, tendo por base as respostas às questões abertas, sendo elaborado novo questionário, que foi posteriormente enviado com a finalidade de aumentar a concordância entre os especialistas, face às melhorias introduzidas.

3.2.2. Instrumentos de recolha de dados

Partindo de uma base documental por via de pesquisa bibliográfica, utilizaram-se, seguidamente dois inquéritos, para confirmação dos dados inferidos na pesquisa. Ambos os inquéritos previam a classificação dos indicadores apresentados através da escala de *Likert* de cinco níveis. O elemento diferenciador dos questionários é uma pergunta aberta para possibilitar o comentário

"especialista" ao indicador, justificando a avaliação dada. É esta informação que possibilita melhorar a redação do indicador para a segunda ronda.

Finalmente, com o objetivo de uma validação final dos resultados, efetuou-se uma entrevista confirmatória ao chefe do grupo de redação do documento de enquadramento nacional das ameaças híbridas (Sarmento, 2013, p. 33).

3.2.3 Técnica de tratamento dos dados

Como referido anteriormente, para este estudo recorreu-se a inquéritos. Os dados obtidos foram tratados, recorrendo à função estatística, coeficiente de correlação de postos de *Kendall*. Este coeficiente correlaciona dados obtidos em diferentes observações, prevendo um para total concordância e menos um para total dissonância (Kendall, 1938). Ora conjugando este coeficiente com a escala de *Likert* de cinco níveis, resulta no Quadro 2.

Quadro 2 – Transformação da Escala de Likert em valores numéricos, baseado no coeficiente de correlação de postos de Kendall

Concordo totalmente	Concordo	Indeciso	Discordo	Discordo totalmente
1	**0,5**	0	-0,5	-1

4. APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DOS RESULTADOS

Neste capítulo analisa-se os dados recolhidos e responde-se às QD e QC, apresentando as induções realizadas que permitiram chegar aos indicadores de resiliência nacional face às AH no domínio diplomático e aos resultados, após aplicação do método de Delphi, para validação.

4.1 A Diplomacia e a Soberania Nacional

Ao longo dos séculos, a relação entre os Estados foi assegurada pela diplomacia, sendo um dos instrumentos de prossecução dos seus interesses. Esta visa a utilização de mecanismos pacíficos para a resolução de divergências e controvérsias, associadas muitas vezes a interesses comerciais divergentes (Bueno et al., 2017).

A diplomacia sofreu transformações em função das épocas. A partir do século XV, a diplomacia serve como instrumento de afirmação da ação Real, mas

é no século XVII, com a assinatura dos tratados de Vestefália, que a diplomacia passa a focar-se nas relações entre Estados, ganhando fulgor enquanto atividade governativa e administrativa (Cardim, 2004, p. 12).

A atividade diplomática como a conhecemos hoje, foi regulada em 1961 na Convenção de Viena sobre Relações Diplomáticas, complementada pela Convenção de Viena sobre Relações Consulares de 1963. Foi neste contexto que se definiu as práticas diplomáticas ainda vigentes, desde a representação dos Estados ao seu relacionamento no seio de Organizações Internacionais (Magalhães, 2001, p. 6).

Porém, a relações entre Estados projeta "jogos" de influência, levando neste particular, Henry Kissinger (1994) a estabelecer o que ficou conhecido como "a nova ordem global", ao caracterizar o período que se seguiu ao fim da Guerra Fria.

Assim, fruto do desenrolar da atividade internacional, dá-se um salto para uma nova forma de diplomacia, "a nova diplomacia", por oposição à diplomacia clássica. Tal qual a revolução nos assuntos militares, fruto do impacto das novas tecnologias disruptivas na condução da Guerra, também a diplomacia mudou, tornando-se mais dinâmica, com Estados a perderam o monopólio da política externa e outros atores a erguerem-se (Moita, 2006).

Com o eclodir da nova forma de conduzir a diplomacia, surge a "diplomacia pública" que tem o objetivo de promover uma correta imagem do país, afirmando as suas valências e fatores diferenciadores (MNE, 2020a) junto de atores não Estatais, através da informação, comunicação e interação com a sociedade civil.

Nesta nova forma, destaca-se a Agência para o Investimento e Comércio Externo de Portugal (AICEP) responsável por fomentar a internacionalização das empresas portuguesas e apoiar a sua atividade exportadora, captar investimento estruturante e promover a imagem de Portugal, através de uma rede externa que conta com mais de 50 localizações no estrangeiro (AICEP, s.d.).

Adicionalmente, O Camões, Instituto da Cooperação e da Língua, promove a língua e cultura portuguesa, executando políticas de ensino do português no estrangeiro e é apoiado por uma rede de mais de 60 representações, repartidas pelos diversos continentes, com a sua ação orientada pela Diplomacia Nacional (Camões, 2016).

Importa, contudo, afirmar, que a forma clássica da ação diplomática não se extinguiu, mantendo-se uma vasta rede composta por embaixadas, consulados e missões.

A rede diplomática portuguesa, composta por 76 embaixadas, 48 postos consulares e nove representações e missões permanentes, conforme Figura 6, permite

a Portugal ocupar o 23º lugar, num índice de representação diplomática segundo o Lowy Institute (2019), numa lista de 61 países, encabeçada pela China e EUA.

Através de uma sondagem de opinião pública[28], 49,8% dos entrevistados consideraram a representação diplomática portuguesa no mundo como média (Moita et al., 2019).

Figura 6 – Mapa da Rede Diplomática Portuguesa
Fonte: Ministério dos Negócios Estrangeiros (2020b).

4.1.1. Diplomacia enquanto instrumento de Soberania Nacional

Para a presente investigação, a diplomacia é entendida como instrumento de poder do Estado, que o permite projetar (poder). Ora para Magalhães a diplomacia é " [..] um instrumento da política externa, para o estabelecimento e desenvolvimento de contactos pacíficos entre os governos de diferentes Estados, pelo emprego de intermediários, mutuamente reconhecidos pelas respetivas partes […]"(1996, p. 90), realçando-se o elemento pacifista na procura dos objetivos de política externa.

[28] Em 2017.

A política externa portuguesa é caracterizada por possuir três principais eixos de ação, que são condicionantes da posição geográfica que Portugal ocupa no mundo. Em primeiro lugar, a sua condição de país europeu, que define o eixo europeu, que passa pela pertença de Portugal à EU, assumindo a conservação da paz, a prosperidade e a promoção dos valores fundamentais como seu desígnio. Um segundo eixo condicionado pela sua posição atlântica, o eixo atlântico, que tem na organização NATO a sua maior relevância, numa lógica de projeção de segurança. Por último, o eixo língua portuguesa, consequência da localização estratégica nacional, que incutiu nos nossos antepassados, uma vontade de conhecer novos mundos, e dessa forma projetar a língua portuguesa, hoje congregada na Comunidade dos Países de Língua Portuguesa (CPLP) (Pereira, 2018b, p. 271).

Pelo referido anteriormente, o instrumento de poder diplomacia é fundamental e firma-se na integração de Portugal nas grandes alianças, promovendo a relação formal entre os Estados e agilizando atividades comuns. Como exemplo, importa recordar o virar de página nas relações com Espanha, a entrada no espaço ibero-americano por via das relações com o Brasil e a familiaridade com Timor-Leste e os novos Estados africanos pela cultura (Gama, 1997, p. 48). Desta forma, o multilateralismo, é o eixo da diplomacia portuguesa, dado pertencer às organizações internacionais de relevância[29], e dessa forma reconhecer como atuar e influenciar na cena internacional, de forma a prosseguir com os objetivos prioritários da sua política externa (MNE, 2018)

Por conseguinte, a política externa seguida por Portugal, fundamentada em valores humanitários, no diálogo inter-racial, apoiado pela sua inserção em múltiplos espaços globais, faz de Portugal um reconhecido *Honest Broker*, cultivando a imagem de mediador imparcial, disponível para compreender e dar voz às preocupações de outros Estados, procurando promover o bem comum, no respeito pelo direito internacional (MNE, 2018).

Portugal tem procurado afirmação, como bem atesta as suas nove representações diplomáticas junto das principais organizações onde se insere (*vide* Tabela 1). Por via destas[30], participa na dinâmica externa, com voz ativa nos projetos e atividades, cumprindo a dupla finalidade de se mostrar ativo e comprometido com os valores destas organizações.

[29] Ocupando cargos de grande relevo, como o caso da eleição por aclamação de António Guterres para a função de Secretário-geral das Nações Unidas, (Pereira, 2018b, pp. 280–282).
[30] Além das Missões Permanentes, podem ser criadas temporárias.

Tabela 1 – Missões Diplomáticas Portuguesas junto de Organizações Internacionais

Organização	Localização	Tipo de missão	Número de diplomatas
Organização das Nações Unidas	Nova Iorque	Permanente	9
Nações Unidas e Organizações Internacionais	Genebra	Permanente	6
Organização do Tratado do Atlântico Norte	Bruxelas	Permanente	5
Conselho da Europa	Estrasburgo	Permanente	2
Comunidade Países de Língua Portuguesa	Lisboa	Permanente	2
Organização para a Cooperação e Desenvolvimento Económico	Paris	Permanente	2
Organização para a Segurança e Cooperação na Europa	Viena	Permanente	3
União Europeia	Bruxelas	Permanente	21
Organização das Nações Unidas para a Educação, a Ciência e a Cultura	Paris	Permanente	2

Fonte: Ministério dos Negócios Estrangeiros (2020b).

Além do referido, não somos alheio ao facto de Portugal servir-se da rede diplomática como braço de apoio à sua comunidade emigrante, possibilitando serviços vários, como a renovação de cartão do cidadão, ação eleitoral e acesso a serviços públicos nacionais (Correia, 2006).

4.1.2. Síntese conclusiva

Em súmula, verificou-se neste capítulo que o instrumento de poder diplomacia contribui para a projeção de poder de Portugal, em particular junto das organizações internacionais que integra, através das missões permanentes ou temporárias. É esta realidade que constrói um Portugal multilateralista, já reconhecido pela sua capacidade mediadora e que vem merecendo a nomeação para altos cargos das organizações internacionais a que pertence. A conjugação destes fatores fortalece toda uma imagem que facilita a projeção da língua, cultura e ciência, e cooperação, também noutros domínios.

Concorrentemente, é possível compreender um esforço de internacionalização, da economia e da língua, a que se associam a promoção da cultura e da ciência.

4.2. As Ameaças Híbridas à Diplomacia

Recentemente o conceito de ameaças híbrida é amplamente refletido no domínio da segurança e defesa[31]. No entanto, este conceito é muitas vezes confundido com guerra híbrida, apresentado à comunidade científica e militar por Frank Hoffman através do estudo realizado sobre a ação de atores não estatais como o Hezbollah e a Al-Qaeda (Friedman, 2018).

As ameaças híbridas referem-se à manipulação, interferência e intervenção de forma deliberada, com recurso a uma série de ferramentas, tais como a desinformação ou descontextualização da informação, interferência nas narrativas, interferência na eleições, cyber ataques e uso de instrumentos económicos para persuadir (Giannopoulos et al., 2019).

4.2.1 Ameaças Híbridas

Concetualmente, as ameaças híbridas são um conjunto de ferramentas, vetores e atividades que, de forma coordenada e com intenção, pretendem atingir um determinado objetivo, associado a um ator hostil (Kersanskas, 2020). O facto de poderem ser nefastas, criando efeitos destrutivos nos processos de decisão dos Estados alvo, antes mesmo de serem identificadas, leva-nos a crer que o seu combate requer conjugação de esforços entre os Estados aliados e parceiros.

Por conseguinte a EU constitui-se como plataforma base para esta partilha de informação, necessária para a deteção de sinais e padrões que possam indicar ação de uma ameaça híbrida. Assim, já em 2018, a CE relatou ter realizado mais de 100 avaliações, pareceres e briefings sobre estas matérias (European Comission, 2018).

No mesmo alinhamento, uma recente investigação[32] afirma que o modelo conceptual de ameaças híbridas assenta em quatro principais pilares, (i) os atores estatais e não estatais (ii) os domínios de poder, um ou múltiplos, em que se focam as ameaças, (iii) as ferramentas, uma ou a combinação de várias, que são utilizadas para aplicar as ameaças, (iv) e as fases em que atuam as ameaças, preparação, destabilização e coesão (Giannopoulos et al., 2019).

Um dos grandes resultados do estudo *The Landscape of Hybrid Threats* é uma identificação clara das 40 ferramentas utilizadas pelas ameaças híbridas para

[31] Uma pesquisa no sítio da NATO sobre este termo resulta num total de 474 entradas (NATO, 2021)
[32] Publicada pelo Joint Research Center, com o patrocínio da EU e sob supervisão da Hybrid CoE, com a finalidade de auxiliar a elaboração de políticas europeias apoiadas com conhecimento científico.

afetarem os 11 domínios considerados no trabalho e que se podem identificar no modelo apresentado na Figura 7. Segundo Giannopoulos, estas ferramentas procuram explorar as vulnerabilidades e oportunidades, multidomínio, visando atingir a coesão de um Estado, a sua capacidade de realizar decisões e criar segurança (2019, p. 26).

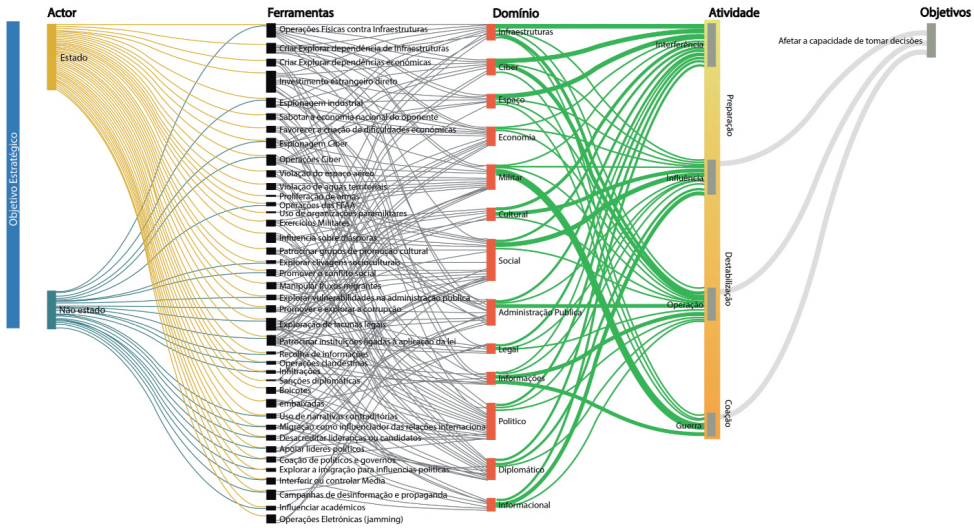


Figura 7 – Visualização do Modelo Conceptual de Ameaças Híbridas
Fonte: Adaptado a partir de Giannopoulos et al. (2019 p. 13).

Destas 40, 15 afetam diretamente o domínio diplomático (Giannopoulos et al., 2019).

4.2.2. Diplomacia

Como vimos anteriormente a Diplomacia é um instrumento de ação externa que pode ser afetada diretamente ou indiretamente pelas ações de ameaças híbridas. Este atuar perpetra-se por inúmeras ferramentas. O elemento diferenciador deste instrumento de poder para com outros é o contexto espacial. Enquanto o instrumento de poder informacional, militar e económico atua no território português, a diplomacia afeta o ambiente externo e liga-se aos portugueses que vivem fora da fronteira. Esta realidade enforma uma vulnerabilidade latente que pode ser explorada por campanhas de desinformação que interferem no processo de tomada de decisão.

Pelo modelo concetual das ameaças híbridas, confirma-se também que a diplomacia relaciona-se com um conjunto de outros domínios, tal como o económico, o político e o social (Giannopoulos et al., 2019).

Por afinidade das ações conduzíveis por tais ferramentas, foram estas agrupadas em quatros áreas (Quadro 3).

Quadro 3 – Ferramentas e áreas das Ameaças Híbridas que afetam o domínio da diplomacia

Ferramentas das Ameaças Híbridas	Áreas
Criar ou explorar dependências económicas	Diplomacia Económica
Comprometer a economia nacional do opositor	
Potenciar dificuldades económicas	
Sanções diplomáticas	
Boicotes	
Violação do Espaço Aéreo	Violação da soberania nacional
Violação de Águas territoriais	
Exercícios Militares	
Exploração de lacunas legais	
Patrocinar instituições ligadas à aplicação da lei	
Embaixadas	Estruturas físicas da Diplomacia
Influência sobre diásporas	Diásporas
Patrocinar grupos de promoção cultural	
Uso de narrativas contraditórias	
Migração como influenciador das relações internacionais	

4.2.3. Síntese Conclusiva

Com este capítulo pretendeu-se esclarecer de que forma o instrumento de poder diplomacia é afetado pelas ameaças híbridas. Da investigação resulta que a utilização de ferramentas por atores que apresentam um *modus operandi* híbrido visa desestabilizar o ambiente interno de um país, mas também afetar a coesão/unidade das organizações internacionais e até os países com comunidades emigrantes. A diplomacia é particularmente afetável, pelo externalizar dos efeitos nefastos criados ao nível interno.

As principais áreas utilizadas pelas ameaças híbridas para afetar o domínio diplomático prendem-se com a diplomacia económica, em estreita colaboração com o domínio económico, as violações da soberania nacional, as estruturas físicas da diplomacia, e as diásporas, externa e interna.

4.3. Indicadores de Resiliência da Diplomacia

Reconhecido por um numeroso conjunto de autoridades, a melhor forma de enfrentar as ameaças híbridas, é aumentar a resiliência face a esta tipologia de ameaça. A EU, inclusive, tem acompanhado o tema, reconhecendo a sua importância particularmente durante a pandemia de corona virus disease 2019 (COVID-19), conforme se atesta pela intervenção do ministro do interior alemão, Markus Kerber, durante a presidência alemã da EU, "[…] a pandemia de COVID-19 deixou claro que são necessários esforços intensificados para proteger a EU, os seus Estados-Membros, as suas sociedades e as instituições da EU contra ameaças híbridas […] reforçando a nossa resiliência e reforçando ainda mais os instrumentos ao nível da EU e dos Estados-Membros […]" (Conselho Europeu, 2020).

Efetivamente, resiliência tem sido um termo muito usado inclusive na sequência da recuperação económica pós COVID-19 para classificar o plano que suporta as medidas económicas de incentivo à recuperação da economia.

Baseado nas ameaças à diplomacia anteriormente identificadas, infere-se quais os indicadores de resiliência (Quadro 4).

Quadro 4 – Raciocínio para os indicadores propostos

Áreas	Raciocínio	Explicação	Indicadores propostos
Diplomacia Económica	Existem empresas estratégicas que influenciam a economia nacional. As estratégias de ameaças híbridas procuram influenciar negativamente essas empresas. Portugal tem uma moeda igual a 19 países. A coesão da moeda da EU influencia a economia nacional	A aquisição de empresas estratégicas em diversos setores públicos pode influenciar negativamente as ações da diplomacia nacional	Lei que permite ao Governo bloquear inves-timentos estrangeiros em empresas estratégicas
		As ameaças híbridas tiram partido das dificuldades económicas para ferir a moral e coesão de uma nação, economias fortes resistem melhor a esta ameaça	Existência de uma taxa positiva de crescimento económico nacional
Violação da soberania nacional	As ameaças híbridas utilizam a violação do espaço aéreo e marítimo de um país soberano	A violação do espaço de soberania de um país é muitas vezes utilizada pelas ameaças híbridas para provocar um sentimento de insegurança na população	Violação do espaço de soberania nacional com solicitação de justificação do ato
Diásporas Estrangeiras	As ameaças híbridas procuram influenciar as comunidades estrangeiras residentes num país	A melhor forma de influenciar comunidades inteiras é, com recurso, a instituições culturais, muitas vezes fundações com autonomia económica	Existência de uma lei que permite ao Estado dissolver uma fundação ou instituição
Diásporas Nacionais	As comunidades residentes em países estrangeiros são potencialmente mais vulneráveis a ameaças híbridas. Pelo seu isolamento, essas comunidades podem ser mais facilmente manipuladas. Os órgãos de comunicação social são muitas vezes utilizados para passar mensagens ou narrativas contraditórias	O número de Portugueses residentes no estrangeiro é elevado. A proteção diplomática é tão mais efetiva quanto mais atualizado se estiver sobre o cidadão.	Existência de listagens atualizadas de Portugueses residentes no estrangeiro
		Ter planos para socorrer cidadãos nacionais face a determinados atos hostis, tem impacto positivo na ação diplomática em caso de estratégia híbrida sobre a nossa comunidade	Existência de protocolos próprios de apoio aos portugueses residentes no estrangeiro em caso de emergência
		Potenciar os órgãos de comunicação social como locais para deturpar mensagens ou introduzir narrativas contraditórias é muitas vezes utilizado para gerar sentimentos de insegurança	Existência de processos de identificação de *fake news* nos Órgãos de Comunicação Social mais relevantes com influência na diáspora portuguesa

[Cont.]

Estruturas físicas da Diplomacia	A rede diplomática nacional baseia-se em embaixadas, consulados e missões	As instalações físicas (embaixadas, consulados e missões) são potenciais alvos para as ameaças híbridas, tirando partido do seu isolamento	Existência de uma rede de infraestruturas diplomáticas (embaixadas, consulados e missões) segura
	Missões económicas de apoio a internacionalização da economia, são potencializadoras da presença nacional	A existência de instalações dedicadas a promoção da economia (exemplo da AICEP) consegue potenciar a presença da diplomacia noutros territórios	A existência de missões económicas (por exemplo delegações AICEP)
	Missões culturais de apoio a internacionalização da economia, são potencializadores da presença nacional	A existência de instalações dedicadas a promoção da cultura (exemplo do instituto Camões) consegue potenciar a presença da diplomacia noutros territórios	A existência de missões culturais (por exemplo delegações do Instituto Camões)
	A troca da informação entre os diferentes órgãos da diplomacia é essencial ao seu funcionamento	Pela sua especificidade a utilização de uma rede segura para troca de informação entre os órgãos da diplomacia é essencial, esta rede tem de cumprir requisitos de segurança para não ser alvo de ameaças híbridas	Existência de uma rede informática diplomática para troca de informação segura
Comum a todas as ferramentas	Portugal está inserido num grande número de organizações internacionais, relacionando-se através da diplomacia	Para assegurar uma maior robustez face a ameaças híbridas, Portugal necessita de estar e demonstrar estar coeso com as organizações internacionais a que pertence	Número de cargos ocupados junto das organi-zações internacionais
			Número de iniciativas propos-tas/ desenvolvidas por Portugal no seio das organizações internacionais
	Portugal é membro da Hybrid CoE, o que lhe permite ter acesso a rede de partilha de informação sobre ameaças híbridas	A diplomacia nacional tem de ter acesso a informa-ção que advém da rede de partilha de informação EU e NATO sobre ameaças híbridas	A partilha de informação da rede de apoio às ameaças híbridas da EU e NATO

4.3.1 Apresentação de resultados

Como já se explicou, foi elaborado um questionário para colocar à consideração dos especialistas, tendo por base os indicadores propostos:

A – Existência de uma lei que permita conter investimentos estrangeiros em empresas estratégicas;

B – Taxa positiva de crescimento económico nacional;

C – Violação do espaço de soberania nacional com solicitação de justificação do ato;

D – Existência de uma lei que permite ao Estado dissolver uma fundação ou instituição;

E – Existência de listagens atualizadas de Portugueses residentes no estrangeiro;

F – Existência de protocolos próprios de apoio aos portugueses residentes no estrangeiro em caso de emergência;

G – Existência de processos de identificação de *fake news* nos Órgãos de Comunicação Social mais relevantes com influência na diáspora portuguesa;

H – Existência de uma rede de infraestruturas diplomáticas (embaixadas, consulados e missões) segura;

I – Existência de missões económicas (por exemplo delegações AICEP);

J – Existência de missões culturais (por exemplo delegações do Instituto Camões);

K – Existência de uma rede informática diplomática para troca de informação segura;

L – Número de cargos ocupados junto das organizações internacionais;

M – Número de iniciativas propostas/desenvolvidas por Portugal no seio das organizações internacionais;

N – A partilha de informação da rede de apoio às ameaças híbridas da União Europeia e NATO com a rede diplomática

Os resultados do questionário, foram expressos numa escala numérica, conforme explicado no ponto 2.2.3.

Assim foi possível elaborar o Quadro 5, que relaciona os especialistas com os indicadores e permite obter os coeficientes de concordância, recorrendo à função estatística média, apresentada em percentagem.

Quadro 5 – Relação dos fatores de concordância entre especialistas por Indicador (1ª ronda)

Especialistas / Indicadores	1	2	3	4	5	6	7	8	9	10	Taxa de Concordância
A	1	0,5	1	0,5	1	-0,5	0,5	0,5	0,5	0,5	55%
B	1	0,5	0,5	0,5	0,5	1	0,5	0,5	1	0,5	65%
C	1	1	0,5	0,5	1	1	0,5	0,5	0,5	1	75%
D	1	1	0,5	0,5	1	-1	0	0	0,5	0	35%
E	1	1	0,5	0,5	1	1	1	0,5	0,5	-0,5	65%
F	1	1	1	0,5	1	1	0,5	0,5	1	-0,5	70%
G	1	0,5	0,5	0,5	0,5	1	0,5	1	1	0,5	70%
H	0,5	1	1	1	1	1	1	1	1	0,5	90%
I	1	0,5	0,5	1	0,5	1	0,5	1	1	0,5	75%
J	1	0,5	1	1	0,5	1	0,5	0,5	1	0,5	75%
K	1	1	1	1	0,5	1	1	1	1	1	95%
L	1	0,5	0,5	-1	0,5	1	0,5	0,5	-0,5	0,5	30%
M	0,5	0,5	0,5	0,5	0	1	0,5	1	1	1	60%
N	1	1	0,5	0,5	-0,5	1	0,5	1	1	1	70%

Da análise dos contributos dos especialistas, através das respostas às questões abertas sobre os indicadores foi possível refinar os indicadores de resiliência. Foi apontado pelos especialistas que o indicador A deveria estar inserido numa estratégia nacional, bem como foi alertado que existem normativos europeus que já obrigam os Estados-Membros a controlarem o investimento estrangeiro em empresas estratégicas. Sobre o indicador D, de forma a evitar o uso de instrumentos que poderiam parecer autocráticos, recomendou-se investigar as fundações. Relacionado com o indicador K foi referida a necessidade da rede segura diplomática permitir trocas de informação com outras redes, enquadrada por uma estratégia de âmbito nacional de combate a ameaças híbridas. O indicador L, que tem a taxa de concordância mais baixa, foi repensado, uma vez que, se conclui pela análise dos dados que os elementos que ocupam cargos em organizações internacionais, defendem os interesses dessas organizações e não as do seu país. Assim procurou-se um indicador relacionado com as missões permanentes juntos das principais organizações que integram Portugal. No refinamento do indicador M, considerou-se a indicação de um perito que refere que, além do número de propostas, a importância que elas possuem, é também relevante para o indicador. Por último, o indicador N, apoiado pelas referências constantes à necessidade de uma estratégia nacional, sofre alterações no sentido de acomodar esta visão.

Com base nestes resultados e nas respostas obtidas das perguntas abertas, foi possível refinar os indicadores, colocando-os de novo à consideração dos peritos, numa tentativa de aumentar a concordância e validar os indicadores.

Esta segunda ronda teve os resultados que se indicam no Quadro 6:

Quadro 6 – Relação dos fatores de concordância entre especialistas por indicador (2ª ronda)

Especialistas / Indicadores	1	2	3	4	5	6	7	8	9	10	Taxa de Concordância
A	1	0,5	1	0,5	1	0,5	0,5	0,5	1	1	75%
B	1	1	,5	0,5	1	1	0	1	1	1	80%
C	1	0,5	1	0,5	0,5	1	1	0,5	0,5	1	75%
D	1	1	0,5	-0,5	1	1	0	1	1	0,5	65%
E	1	1	1	0,5	1	1	1	0	0,5	0	70%
F	1	1	1	1	1	1	0,5	0,5	1	-0,5	75%
G	1	0,5	1	0,5	0,5	1	0,5	1	1	0,5	75%
H	1	0,5	1	1	1	1	1	1	1	0,5	90%
I	1	0,5	0,5	0,5	1	1	0,5	0,5	1	0	65%
J	1	0,5	1	1	0,5	1	0,5	0,5	1	0,5	75%
K	1	0,5	1	1	1	1	1	1	1	1	95%
L	1	1	0,5	-0,5	0,5	1	-0,5	0,5	0,5	0	40%
M	1	0,5	0,5	0,5	0	1	0,5	1	1	0,5	65%
N	1	1	1	1	0,5	1	0,5	1	1	1	90%

Desta forma, porque definimos como valor mínimo para a taxa de concordância dos indicadores, os 70%, cinco indicadores não foram considerados validados, resultando num total de dez indicadores.

4.3.2. Síntese conclusiva

Durante o decorrer desta investigação foi possível encontrar indicadores de resiliência para o instrumento de poder diplomático, no entanto, dos 14 indicadores induzidos, após a utilização da técnica de *Delphi* junto de uma equipa de dez especialistas na área das ameaças híbridas, apenas dez indicadores foram validados, com taxas de concordância acima do 70% (Quadro 7). Desta forma, foi possível identificar os indicadores da resiliência do instrumento de poder diplomacia face a ameaças híbridas.

Quadro 7 – Lista de Indicadores Finais

	Indicadores Finais	Concordância
A	Transposição dos normativos europeus sobre investimentos estrangeiros em em-presas estratégicas, apoiada por uma estratégia nacional de combate as ameaças híbridas	75%
B	Existência de uma taxa positiva de crescimento económico nacional	80%
C	Violação do espaço de soberania nacional com solicitação de justificação do ato (através de nota verbal)	75%
E	Existência de listagens atualizadas de Portugueses residentes no estrangeiro	70%
F	Existência de protocolos próprios de apoio aos portugueses residentes no estran-geiro em caso de emergência	75%
G	Existência de processos de identificação de *fake news* nos Órgãos de Comunica-ção Social mais relevantes com influência na diáspora portuguesa	75%
H	Existência de uma rede de infraestruturas diplomáticas (embaixadas, consulados e missões) segura	90%
J	A existência de missões culturais (por exemplo delegações do Instituto Camões)	75%
K	Existência de uma rede informática diplomática, integrada com outras redes, para troca de informação segura, apoiada por uma estratégia nacional para o combate a ameaças híbridas	95%
N	Partilha de informação da rede de apoio às ameaças híbridas da União Europeia e NATO com a rede diplomática, enquadrada pela partilha de informação numa rede interministerial (nacional)	90%

4.4 Determinação da resiliência da diplomacia

Uma vez determinados os indicadores de resiliência do instrumento de poder diplomacia face a ameaças híbridas, tendo por base a taxa de concordância entre os especialistas, podemos considerar que estes indicadores tem uma importância relativa entre si.

4.4.1 Pesos relativos

Para mensurar, o grau de importância dos indicadores, recorreu-se a uma associação das taxas de concordância dos *experts* com um determinado peso relativo para esse indicador, utilizando para suportar esse pensamento o Quadro 8:

Quadro 8 – Relação entre as taxas de concordância e os pesos relativos

Intervalo de concordância	Peso relativo
[90% a 100%]	3
[80% a 90%[	2
[70% a 80%[	1

Desta forma cada indicador ganha um peso relativo, que traduz a sua importância para o cálculo da resiliência, onde naturalmente alguns indicadores são mais valiosos que outros. Esta relação entre indicadores e o seu peso relativo é traduzida no Quadro 9:

Quadro 9 – Relação Indicadores - Pesos Relativos

	Indicadores	Peso relativo
A	Transposição dos normativos europeus sobre investimentos estrangeiros em em-presas estratégicas, apoiada por uma estratégia nacional de combate as ameaças híbridas	1
B	Existência taxa positiva de crescimento económico nacional	2
C	Violação do espaço de soberania nacional com solicitação de justificação do ato (através de nota verbal)	1
E	Existência de listagens atualizadas de Portugueses residentes no estrangeiro	1
F	Existência de protocolos próprios de apoio aos portugueses residentes no estran-geiro em caso de emergência	1
G	Existência de um *trakking* de *fake news* nos Órgãos de Comunicação Social mais relevantes com influência na diáspora portuguesa	1
H	Existência de uma rede de infraestruturas diplomáticas (embaixadas, consulados e missões) segura	3
J	A existência de missões culturais (por exemplo delegações do Instituto Camões)	1
K	Existência de uma rede informática diplomática, integrada com outras redes, para troca de informação segura, apoiada por uma estratégia nacional para o combate a ameaças híbridas	3
N	Partilha de informação da rede de apoio às ameaças híbridas da União Europeia e NATO com a rede diplomática, enquadrada pela partilha de informação numa rede interministerial (nacional)	3

4.4.2 Formulação

Nesta lógica, podemos dizer que a avaliação da resiliência (Ar) é resultado do somatório do produto do valor que o indicador assumir com o seu peso relativo, traduzido matematicamente na fórmula:

$$Ar = \sum_{i=1}^{10} \text{Valor indicador}_i \times Peso\ rel_i$$

Aqui, o valor do indicador, corresponde à avaliação do respetivo indicador realizado por uma qualquer entidade, considerando como norma, a mesma referência para todos os indicadores e o peso relativo resulta do grau de concordância que os especialistas tiveram sobre os indicadores.

Foi apresentado este raciocínio ao chefe do grupo de redação do documento de enquadramento nacional das ameaças híbridas para validação dos resultados.

4.4.3 Síntese conclusiva

Determinar algo tão abstrato como o grau de resiliência do instrumento de poder da diplomacia face a ameaças híbridas, vai sempre depender do grau de perceção que determinada entidade terá na avaliação da mesma. Para esta avaliação propõe-se o uso de dez indicadores, que influenciados pela importância que um grupo de especialistas lhes atribuiu, terão significados relativos, traduzidas em pesos relativos. Desta forma considerámos que a fórmula proposta, que representa o somatório dos produtos do valor dos indicadores propostos pelo seu peso relativo será uma forma de determinar a resiliência deste instrumento de poder.

5. CONCLUSÕES

Este estudo debruçou-se sobre o instrumento de poder do Estado diplomacia e a forma como é afetado pelas ameaças híbridas e surge num momento de necessidade do estabelecimento de uma estratégia de combate, inserida numa perspetiva "*whole of government*" e "*whole of society*", como terá de ser toda a estratégia de combate às ameaças híbridas, já que o seu foco é a coesão que liga os cidadãos ao seu Estado, e a unidade, partilha e complementaridade de todos os instrumentos de poder. Estamos perante uma ameaça que surge quando e onde menos se espera, com efeitos diretos no sentimento de segurança da população, ferindo a coesão nacional e o equilíbrio da trindade da guerra de *Clausewitz*. É evidente que conjugando *soft*, *hard* e *smart power*, tirando partido dos vazios da lei, para atacar ocupando espaço na "*Gray Zone*" que as protege de uma deteção em tempo útil, permite uma corrosão dos processos de decisão prolongada e cínica, extremamente difícil de antecipar.

Num momento em que toda a Europa, se preocupa com o tema, urge identificar a forma de atuar das ameaças híbridas, de forma a encontrar ferramentas que permitam resistir a tais ameaças. A dificuldade na antecipação impõe erguer uma capacidade resiliente, que permita ao sistema continuar a funcionar após o efeito produzido pela ameaça, aguentando o impacto e retornar com celeridade ao seu estado normal.

O objeto de estudo escolhido para esta investigação é a diplomacia, enquanto instrumento de projetar poder de um Estado e, por conseguinte, foi o

foco da presente investigação, de forma a analisar as ameaças a que está sujeito, que são passíveis de o influenciar com vista a afetar a coesão dos cidadãos para com o seu governo e assim, a unidade nacional.

A análise de modelos de avaliação da resiliência visou constituir um contributo para um possível modelo de medição da resiliência de um Estado no domínio diplomacia.

Seguiu-se, desta forma, uma metodologia apoiada num raciocínio indutivo. Em primeiro lugar, determinaram-se as ferramentas das ameaças híbridas, baseado em publicações apoiadas pela Hybrid CoE e, de seguida, recorrendo a uma estratégia qualitativa, induziram-se 14 possíveis indicadores de resiliência, para a diplomacia. Estes possíveis indicadores foram postos à consideração de um grupo de especialistas tendo-se, através do recurso à técnica de *Delphi*, robustecido os indicadores através das apreciações qualitativas dos especialistas fruto da primeira ronda de entrevistas. Uma segunda ronda foi aplicada para aumentar a taxa de concordância, que permitiu no final, determinar dez indicadores. A relação das concordâncias foi transformada em peso relativo dos indicadores validados de forma a concluir uma possível fórmula de cálculo da resiliência.

Com esta investigação, foi possível compreender que a diplomacia contribui para a projeção de poder, principalmente através da relação com as organizações internacionais, em particular na complexa teia de negociações que aí decorrem, associadas muitas vezes a objetivos económicos e que também servem outros fins, tais como a cooperação. Esta afirmação de poder, permite a Portugal ser reconhecido na comunidade internacional como *Honest Broker*, papel de mediador imparcial. Ainda apoiado pela diplomacia, em particular as missões de cariz permanente, está o papel ativo nacional no panorama internacional traduzível pela nomeação de portugueses para altos cargos em organizações internacionais.

Concomitantemente, concluiu-se que as principais ferramentas das ameaças híbridas que afetam o domínio diplomático podem ser agrupadas em quatro áreas, em função da afetação no domínio, destacando-se as ameaças ao nível da (i) diplomacia económica, que procuram comprometer a economia do opositor através da exploração de dependências económicas, as que se prendem com a (ii) violação da soberania nacional, explorando lacunas legais que permitem violar os espaços de soberania do um Estado, as que se fixam nas (iii) estruturas físicas da diplomacia, na rede diplomática propriamente dita, embaixadas consulados, redes que permitem a troca de informação entre estes locais, e as que buscam influenciar as (iv) diásporas, sejam as residentes num determinado território, ou as

que se encontram fora da sua pátria mãe, com recurso a grupos de promoção de narrativas contraditórias, sob a imagem de promoção cultural.

Resultou da segunda ronda de inquéritos, por não ser substancialmente importante continuar para uma terceira, em virtude dos resultados alcançados, a determinação de dez indicadores de resiliência do instrumento de poder do Estado diplomacia, pois todos apresentam um grau de concordância superior a 70%. Baseado nestas taxas de concordância, foi possível estabelecer uma relação entre eles, atribuindo aos indicadores um grau de importância que eles têm entre si, através de pesos relativos, contributos pertinentes para a formulação realizada e que, por conseguinte, permitem a possibilidade do cálculo da resiliência da diplomacia de um Estado.

Considera-se a presente investigação, um contributo para o conhecimento nesta área, que se encontra presentemente em evolução contínua.

Os constrangimentos causados pela COVID-19 poderão ter limitado o trabalho, em particular na interação com os especialistas, que poderia ter sido presencial, não fossem as restrições existentes.

A aplicação da fórmula de cálculo concluída a um Estado, com o valor de resiliência no domínio da diplomacia já determinado, poderia ser um bom exercício pratico, para validação formal desta fórmula, através de uma comparação de valores.

Como estudos futuros, sugere-se o estudo da resiliência de organizações internacionais, até para ver a similaridade de indicadores com a diplomacia, fruto da proximidade entre ambos.

Por último, recomenda-se que a aplicação da fórmula de cálculo da resiliência recorra a uma única escala para determinação do valor dos indicadores, sob pena de se falsear o raciocínio tido na obtenção desta fórmula.

REFERÊNCIAS BIBLIOGRÁFICAS

Abreu, R., David, F., & Augusto, L. (s.d.). *Avaliação das Fundações em Portugal: Passado, Presente e Futuro* [Página *online*]. Retirado de https://www.occ.pt/news/comcontabaudit/pdf/121.pdf.

AICEP- Agência para o Investimento e Comércio Externo de Portugal. (s.d.). AICEP *Portugal Global, o seu parceiro de confiança* [Página *online*]. Reirado de https://www.portugalglobal.pt/PT/sobre-nos/Paginas/sobre-nos.aspx.

Alves, A. J. F. M. (2020). *A Prevenção e o Combate às Ameaças Hibridas: Impacto para as Forças Armadas Portuguesas* (Trabalho de Investigação Individual do Curso de Promoção a Oficial General). Instituto Universitário Militar, Lisboa.

Artimová, P., Czulda, R., Dordevic, V., Lippert, T., Macko, P., Rhodes, M., & Schmid, J. (2019). *NATO at 70*. Bratislava: NATO.

Barreiros, P. M. C. M. (2010). *Associativismo e práticas culturais como veículo de integração dos imigrantes* (Dissertação de Mestrado em Serviço Social). Universidade Fernando Pessoa, Porto.

Bartles, C. K. (2016). Getting Gerasimov Right. *Military Review The Professional Journal of the U.S. Army*, Janeiro-Fevereiro, 30–38.

Bryman, A. (2012). *Social Research Methods* (4.a Edition). Oxford: Oxford University Press.

Bueno, E. de P., Freire, M., & Oliveira, V. A. P. de. (2017). As origens históricas da diplomacia e a evolução do conceito de proteção diplomática dos nacionais. *Anuario Mexicano de Derecho Internacional, XVII*, 623-649.

Camões- Instituto da Cooperação e da Língua. (2016). *Identidade* [Página *online*]. Retirado de https://www.instituto-camoes.pt/sobre/sobre-nos/identidade.

Cardim, P. (2004). A prática diplomática na Europa do Antigo Regime. Em: L. Rodrigues & F. Martins. *História e Relações Internacionais*. Évora: Publicações do Cidehus, Edições Colibri.

Comissão Europeia. (2016). *Comunicação Conjunta ao Parlamento Europeu e ao Conselho - Quadro comum em materia de luta contra as ameaças híbridas uma resposta da União Europeia* [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A52016JC0018.

Conselho Europeu. (2020). *Council calls for strengthening resilience and countering hybrid threats, including disinformation in the context of the COVID-19 pandemic*. Press Realease de 15 de dezembro de 2020 [Página *online*]. Retirado de https://www.consilium.europa.eu/en/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation.

Constituição da República Portuguesa. (1976). *Constituição da República Portuguesa*. Diário da República, 1.aSerie, 86, 738-775. Lisboa: Presidência da República.

Correia, J. de M. (2006). A integração na União Europeia e o Papel do Ministério dos Negócios Estrangeiros. *Nação e Defesa, 3*(115), 29-81.

Couto, A. C. (1988). *Elementos de Estratégia, Apontamentos para um Curso Volume I* (2.a Edição). Lisboa: Fundação Casa Carvalho Cerqueira.

Decreto-Lei N.o 249, de 28 de outubro (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar*. Diário da República, 1.a Série, 211, 9298-9311. Lisboa: Ministério da Defesa Nacional.

Deshpande, V. (2018). Hybrid Warfare and the Changing Character of Conflict. *The Quarterly Journal, 15* (2). doi: 10.11610/connections.15.2.05.

Duarte, F. P. (2020). *Non-kinetic hybrid threats in Europe – the Portuguese case study* (2017-18) [Página online]. Retirado de https://www.emerald.com/insight/1750-6166.htm.

EMGFA. (2020). *Manual para o Planeamento Estratégico Militar do Estado-Maior-General das Forças Armadas* [EMGFA]. Lisboa: Autor.

European Comission. (2018). *Joint Communication to the European Parliament, the European Council and the Council Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*. Brussels: High Representative of the Union for Foreign Affairs and Security Policy [Página online]. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018JC0016.

Evans, T. (2016). *SSR and Clausewitz's "remarkable trinity."* [Página *online*]. Retirado de https://issat.dcaf.ch/mkd/Share/Blogs/ISSAT-Blog/SSR-and-Clausewitz-s-remarkable-trinity.

Faria, R. (2020). *Espanha reforça blindagem de empresas estratégicas ao investimento estrangeiro*. *Jornal de Negócios*, de 18 de novembro. Retirado de https://www.jornaldenegocios.pt/economia/detalhe/espanha-reforca-blindagem-ao-investimento-estrangeiro-em-empresas-estrategicas#loadComments.

Fiott, D., & Parkes, R. (2019). Protecting Europe: The EU's response to hybrid threats. *Chaillot Paper, 151* (Abril). doi: 10.2815/679971.

Fonseca, M. L. (2003). Integração dos Imigrantes: Estratégias e Protagonistas. *I Congresso Imigração em Portugal - Diversidade, Cidadania e Integração*. Congresso organizado pela Fundação Calouste Gulbenkian, Lisboa.

Freixo, M. J. V. (2011). *Metodologia Científica: Fundamentos, Métodos e Técnicas (4.a Edição)*. Lisboa: Instituto Piaget.

Friedman, O. (2018). *Russian Hybrid Warfare-Resurence and Politicisation*. Londres: Hurst.

Gama, J. (1997). A Política Externa. *Revista Nação e Defesa* (83), 45-57.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2019). *The Landscape of Hybrid Threats: A Conceptual Model Public Version*. Bruxelas: European Comission.

Gomes, G. S. C. (1990). A Politica Externa e a Diplomacia numa Estratégia Nacional. *Nação e Defesa, 15*(56), 55-75.

Gonzaga-Ferreira, L. (1984). Estratégia Política e Diplomática no Interior do Adversário [Página *online*]. Retirado de http://comum.rcaap.pt/bitstream/10400.26/2798/1/NeD030_LuisGonzagaFerreira.pdf

Hoffman, F. G. (2007). *Conflict in the 21st Century: The Rise of Hybrid Wars*. Virginia: Potomac Institute for Policy Studies.

Kendall, M. G. (1938). A new measure of Rank Correlation. *Biometrika, 30* (1-2), 81-93. doi: 10.1093/biomet/30.1-2.81.

Kersanskas, V. (2020). *Hybrid CoE Paper 2 Deterrence: Proposing a more strategic approach to countering hybrid threats*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats.

Kissinger, H. (1994). *Diplomacy*. New York: Simon & Schuster.

Kott, A., Blakely, B., Henshe, D., Wehner, G., Rowell, J., Evans, N., Muñoz-González, L., Leslie, N., French, D. W., Woodard, D., Krutilla, K., Joyce, A., Linkov, I., Mas-Machuca, C., Sztipanovits, J., Harney, H., Kergl, D., Nejib, P., Yakabovicz, E., … Møller, A. (2018). *Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization*. Maryland: US Army Research Laboratory

Landmeter, D. E. (2018). *The relevance of Clausewitz's On War to today's conflicts*. *Militaire Spectator*, 386–398 [Página *online*]. Retirado de:https://www.militairespectator.nl/sites/default/files/teksten/bestanden/Militaire Spectator 7-8-2018 De Landmeter.pdf.

Linkov, I., & Kott, A. (2019). *Fundamental Concept of Cyber Resilience: Introduction and Overview*. Nova Iorque: Springer International Publishing.

Linkov, I., & Palma-Oliveira, J. M. (2016). *Resilience and risk studies*. Amsterdão: Springer.

Linstone, H. A., & Turoff, M. (2002). The Evolution of Delphi. *The Delphi Method Techniques and Applications* (pp- 5-12). Portland: Portland State University.

Lowy Institute. (2019). *Global Diplomacy Index* [Página *online*]. Retirado de https://globaldiplomacyindex.lowyinstitute.org/country_rank.html.

LUSA. (2019). *Governo quer plano nacional para combater desinformação e ciberataques - Combate às Fake News, uma questão democrática* [Página *online*]. Retirado de https://combatefakenews.lusa.pt/fake-news-governo-quer-plano-nacional-para-combater-desinformacao-e-ciberataques-c-audio/.

Magalhães, J. C. (1996). *A diplomacia Pura (2º edição*). Venda Nova: Bertrand Editores.

Magalhães, J. C. (2001). *Manual Diplomático: Direito diplomático, prática diplomática (4ª Edição*). Lisboa: Editorial Bizâncio.

MCDC. (2019). MCDM *Countering Hybrid Warfare Project: Countering Hybrid Warfare A Multinational Capability Development Campaign project*. Shutterstock: Multinational Capability Development Campaign.

MNE-Ministério dos Negócios Estrangeiros. (s.d.). *Comunidades Portuguesas* [Página *online*]. Retirado de https://www.portaldiplomatico.mne.gov.pt/politica-externa/comunidades-portuguesas#salvaguardar-as-pessoas-e-os-bens-a-protecao.

MNE-Ministério dos Negócios Estrangeiros. (2018). *Política Externa* [Página *online*]. Retirado de https://www.portaldiplomatico.mne.gov.pt/politica-externa/politica-externa.

MNE-Ministério dos Negócios Estrangeiros. (2020a). *Diplomacia Pública* [Página *online*]. Retirado de https://www.portaldiplomatico.mne.gov.pt/politica-externa/diplomacia-publica.

MNE-Ministério dos Negócios Estrangeiros. (2020b). *Mapa da Rede Diplomática* [Página *online*]. Retirado de https://www.portaldiplomatico.mne.gov.pt/rede-diplomatica/mapa-da-rede-diplomatica.

Ministério dos Negócios Estrangeiros. (2020c). *Organizações Internacionais* [Página *online*]. Retirado de https://www.portaldiplomatico.mne.gov.pt/relacoesbilaterais/ organizacoes-internacionais.

Moita, L. (2006). Da diplomacia clássica à nova diplomacia. *Nova diplomacia: paradigma, actores, espaços*. Janus 2006.

Moita, L., Pinto, L. V., & Pereira, P. (2019). *Estudo da Estrutura Diplomática Portuguesa*. Lisboa: Observare- Observatório de Relações Exteriores.

NATO. (2014). *Wales Summit Declaration 05 de Setembro de 2014* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO. (2020). *Resilience and Article 3* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_132722.htm.

NATO. (2021). *Search for Hybrid threat* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/search.htm?query=hybrid+threat&submitSearch=.

Observatório da Emigração. (2019). *Emigrantes Portugueses são mais de dois milhoes e meio* [Página *online*]. Retirado de http://observatorioemigracao.pt/np4/7118.html.

Pavlov, N., & Hadjitorov, S. (2019). *Quantifying Resilience: A Case Study on Critical Infrastructure Resilience in the Republic of Bulgaria*. Em: *CMRD COE Proceedings 2019* (77-93). NATO Crisis Management and Disaster Response Center of Excelence.

Pereira, P. S. C. (2018a). *A Política Externa Portuguesa* [Página *online*]. Retirado de https://www.portaldiplomatico.mne.gov.pt/politica-externa/politica-externa.

Pereira, P. S. C. (2018b). Portugal Portuguese Foreign Policy. Em: B. Belli & F. Nasser, *The Road Ahead The 21st Century World Order in the Eyes of Policy Planners*. Brasilia: Fundação Alexandre de Gusmão.

Popper, K. R. (2012). *A Lógica da Pesquisa Cientifica Tradução de Leonidas Hegenberg e Octanny Silveira da Mota (18.ª Edição)*. São Paulo: Editora Cultrix.

Quivy, R., & Campehoudt, L. Van. (2003). *Manual de Investigação em Ciências Sociais (3.ª Ed)*. Lisboa: Gradiva.

Richterová, J. (2015). *Background Report NATO Hybrid Threats*. Bruxelas: NATO.

Rumsfeld, D. (2005). *The National Defence Strategy of the United States of America* [Página *online*]. Retirado de https://archive.defense.gov/news/Mar2005/d20050318nds1.pdf.

Santos, D. M. A. (2019). *O século XXI e a arte da guerra: a defesa da coesão nacional*. *Forte Força Terrestre* [Página *online*]. Retirado de https://www.forte.jor.br/2019/07/11/o-seculo-xxi-e-a-arte-da-guerra-a-defesa-da-coesao-nacional/.

Sarmento, M. (2013). *Metodologia Científica para a Elaboração, Escrita e Apresentação de Teses*. Lisboa: Universidade Lusíada Editora.

Serrão, D. (2019). *Relatório do Simpósio «Cyber Power in Hybrid Warfare»*. Lisboa: Instituto Universitário Militar.

SIEMENS. (2013). *Toolkit for Resilient Cities* [Página *online*]. Retirado de https://www.preventionweb.net/files/36081_toolkitforresilientcitiesnycasestud.pdf.

Sistema de Segurança Interna. (2021). *Relatório Anual de Segurança Interna de 2020*. Lisboa: Autor.

Sousa, M. J., & Baptista, C. S. (2010). *Como Fazer Investigação, Dissertações, Teses e Relatórios segundo Bolonha (5ª Edição)*. Lisboa: Pactor - Edições de Ciências Sociais, Forenses e da Educação.

Tecedeiro, H. (2017). Problema do euro não é técnico, nem económico, é político. *Diário de Notícias, de 06 de maio* [Página *online*]. Retirado de https://www.dn.pt/mundo/problema-do-euro-nao-e-tecnico-nem-economico-e-politico-7330444.html.

U.S. Joint Chiefs of Staff. (2013). Joint Publication 1 Joint Doctrine for the Armed Forces of the United States. Washington: Armed Forces of the United States.

Vilelas, J. (2009). Investigação – *o processo de construção do conhecimento*. Lisboa:Edições Sílabo

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA, VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS. (INFORMACIONAL)

PREVENTION AND TACKLING OF HYBRID THREATS: IDENTIFYING MEASUREMENT INSTRUMENTS, VARIABLES AND NATIONAL RESILIENCE INDICATORS AGAINST HYBRID THREATS (INFORMATIONAL)

Autor
MAJ TM Luís Filipe Xavier Cavaco de Mendonça Dias

Orientador
MAJ TM Tiago Filipe Abreu Moura Guedes

1. INTRODUÇÃO

Na crise da Crimeia de 2014, as Ameaças Híbridas (AH) manifestaram-se com campanhas de desinformação no ciberespaço que visaram o descrédito das Forças Armadas (FFAA) e a desconfiança da sociedade (fracionada cultural e socialmente) em relação às autoridades do Estado, dando à Rússia o pretexto para a invasão militar (Danyk, Maliarchuk & Briggs, 2017; Gunneriusson, 2019). Fazem também parte do ambiente das AH, os ciberataques a infraestruturas críticas ou serviços essenciais, a ciberespionagem, a influência em eleições, a instrumentalização política e desinformação em torno do vírus Covid-19 (Giannopoulos & Smith., 2020; Jakovljevic, Bjedov, Jaksic, & Jakovljevic, 2020; Patel, Moncayo, Conroy, Jordan, & Erickson, 2020).

Após a anexação da Crimeia, a União Europeia (UE) e a Organização do Tratado do Atlântico Norte (OTAN), ficaram alerta para o problema que claramente não é estritamente militar, tendo incrementado a cooperação entre ambas desde então. Na sequência da Cimeira de Varsóvia de 2016, essa cooperação manifestou-se com uma declaração conjunta, da UE e OTAN, visando a cooperação no planeamento civil-militar, ciberdefesa, partilha de informação e comunicação estratégica coordenada (Shea, 2016).

O Centro Europeu de Excelência para o Combate às AH (Hybrid CoE), criado em 2017, foi um primeiro projeto conjunto da UE e da OTAN neste âmbito. Portugal, reconhecendo a dimensão do problema, que é transversal às sociedades

democráticas, aderiu ao Hybrid CoE em dezembro de 2019. Conforme referiu Ana Zacarias à data da adesão, estas ameaças "[...] muitas vezes, são dirigidas ao Estado, aos órgãos políticos, a interferências em processos eleitorais, mas também afetam empresas, serviços financeiros [...]" (LUSA, 2019).

O Hybrid CoE, define AH como uma ação coordenada e sincronizada, conduzida por atores estatais ou não estatais, cujo objetivo é minar ou prejudicar um alvo, influenciando a sua tomada de decisões a nível local, regional, estatal ou institucional (Hybrid CoE, s.d.). Estas ameaças visam deliberadamente as vulnerabilidades dos estados democráticos e das instituições, utilizando uma vasta gama de meios e concebidas para se manterem abaixo do limiar de deteção e imputação, entre o aceitável e inaceitável, o legal e ilegal, na designada "*gray zone*" (Giannopoulos et al., 2020, p. 4).

A cooperação no seio da UE e da OTAN é fundamental, mas "[…] a principal responsabilidade na luta contra as AH cabe aos Estados-Membros […] sendo necessária uma abordagem global da segurança que abranja […] toda a sociedade […]" (Conselho da UE, 2019). O combate às AH não é responsabilidade única de uma entidade específica e é necessário adotar abordagens holísticas, *whole-of-government* e *whole-of-society*, promovendo a aproximação, confiança e partilha de informação regular entre organismos do estado (civis e militares), extensível à sociedade e setor privado, num novo ecossistema de segurança preparado para responder a crises de forma mais eficiente (MCDC, 2019). Quanto ao papel da defesa, o secretário-geral da OTAN referiu que: "[…] our militaries cannot be strong if our societies are weak, so our first line of defence must be strong societies […]" (Stoltenberg, 2020).

A agenda estratégica da UE para 2019-2024, apela ao aumento da resiliência e proteção das sociedades face às AH, salientando a importância da proteção contra os ciberataques e a desinformação (Conselho Europeu, 2019). De acordo com a OTAN (2020b), a resiliência é a capacidade de uma sociedade resistir e recuperar fácil e rapidamente, de choques provocados por AH, entre outras, combinando tanto a preparação civil como a capacidade militar. O conceito de resiliência tem assumido um papel de relevo tanto na OTAN como na UE, pois é o que melhor lida com vulnerabilidades e ameaças que são incertas. Assim, para garantir a dissuasão e resposta face às AH, importa ser resiliente, sendo necessário identificar indicadores que permitam medir a resiliência do Estado face a estas ameaças (Giannopoulos et al., 2020, p. 5).

As AH são impulsionadas pela tecnologia que surge como um elemento multiplicador na dimensão informacional, explorando as vulnerabilidades de uma sociedade em rede, pelo que o objeto de investigação é a resiliência nacional face às AH no domínio informacional.

A investigação foi delimitada no tempo, espaço e conteúdo, sem prejuízo da sua contextualização (Santos & Lima, 2019, p.42). Delimita-se temporalmente desde 2016, ano em que a Comissão Europeia (CE) e a Alta Representante deram um primeiro passo e estabeleceram o Quadro Comum em Matéria de Luta contra as AH (CE, 2016), até ao presente. Quanto ao espaço, é delimitada a Portugal, pois estuda-se a resiliência nacional, e à UE e OTAN, por definirem orientações e recomendações nesta área, relevantes para os Estados-Membros. O conteúdo, foca o estudo das ações e efeitos das técnicas no âmbito das AH no ambiente informacional, bem como as respostas dos visados, à luz da legislação, políticas, ações e quadros de referência.

O objetivo geral (OG) da investigação, bem como os objetivos específicos (OE) necessários para o atingir, estão definidos na Figura 1.

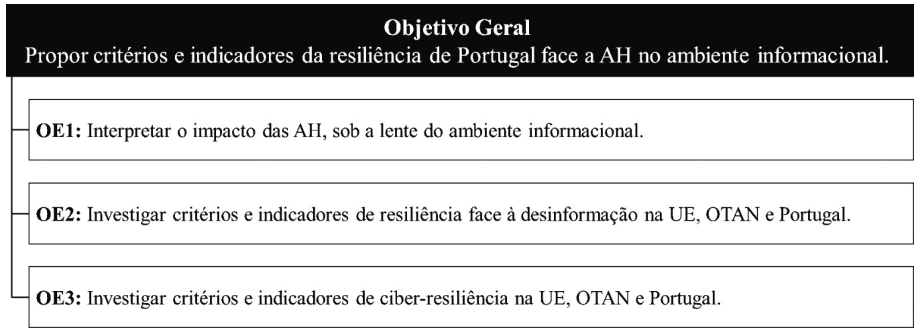


Figura 1 – Objetivos da investigação

A problemática de investigação é formulada pela Questão Central (QC) e pelas Questões Derivadas (QD), definidas na Figura 2.

As QD concorrem diretamente para um OE correspondente, e serviram como elementos orientadores da investigação.

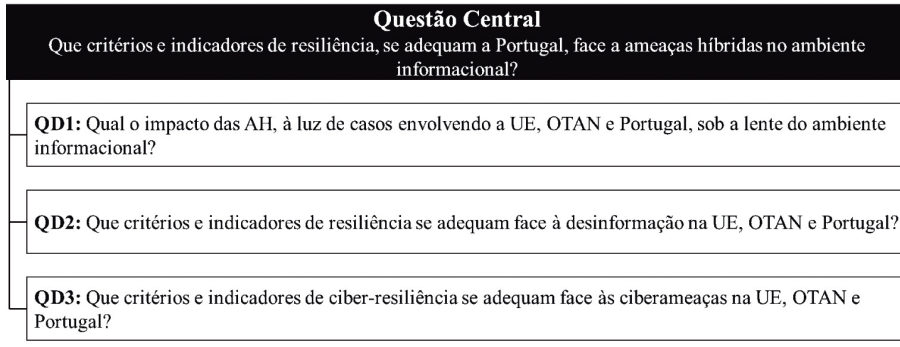


Figura 2 – Questões da investigação

Este estudo está estruturado com esta introdução e mais quatro capítulos, antecedendo as Conclusões. O primeiro capítulo é a introdução e no segundo capítulo, enquadra-se concetualmente o tema. No terceiro, apresenta-se a metodologia. No quarto capítulo apresenta-se e discute-se os resultados da investigação, interpretando o impacto das AH sob a lente do ambiente informacional, analisando os conteúdos sobre a resiliência face à desinformação e às ciberameaças e confirmando os indicadores de resiliência junto de especialistas. Por fim, no quinto capítulo, apresentam-se as conclusões.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

O tema deste Trabalho de Investigação Individual (TII) enquadra-se no ramo do conhecimento das Ciências Militares, reguladas pelo Art.º 5º do Decreto-Lei n.º 249/2015 de 28 de outubro de 2015 (p. 9300), na área de Estudo das Crises e dos Conflitos Armados, no domínio do planeamento estratégico militar.

Neste capítulo apresentam-se os conceitos essenciais e a revisão da literatura focando as AH no domínio informacional, e descreve-se a metodologia adotada.

Importa definir o que são AH e a sua conceptualização, a importância do ambiente informacional e o conceito de resiliência.

2.1. AMBIENTE INFORMACIONAL, CIBERESPAÇO E DESINFORMAÇÃO

A Estratégia Nacional de Segurança no Ciberespaço (ENSC), publicada através da Resolução do Conselho de Ministros (RCM) n.º 92/2019, de 05 de junho, no ponto primeiro, define o *ciberespaço* como "[…] um ambiente complexo, de

valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação.". A ENSC define ainda no mesmo ponto, a *cibersegurança* como o "[…] conjunto de medidas e ações de prevenção, monitorização […]" que visam "[…] garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem […]", e *ciberdefesa* como a "[…] atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço.".

O *ambiente de informação* permeia todos os domínios físicos e consiste num agregado de indivíduos, organizações, e sistemas que recolhem, processam, divulgam, ou atuam sobre a informação (JP3-12, 2018). Segundo a OTAN (2019, p. A-7), as comunicações estratégicas dirigem, coordenam, e sincronizam o esforço global de comunicação, para moldar o ambiente de informação, e integram as operações psicológicas (PsyOps) e operações de informação (InfoOps), com outras atividades militares. As InfoOps criam efeitos sobre a vontade, compreensão e capacidade dos adversários, as PsyOps são dirigidas a audiências alvo aprovadas, para influenciar perceções, atitudes e comportamentos, que afetam a realização de objetivos políticos e militares (OTAN, 2019).

O ciberespaço, totalmente contido no ambiente de informação, permite executar Operações no Ciberespaço (OpCiber) criando efeitos no ambiente de informação, portanto, com uma forte ligação de apoio às operações no ambiente informacional (JP3-12, 2018). As OpCiber podem ser ofensivas, destinadas a projetar poder no e através do ciberespaço, ou defensivas, para defender a rede de defesa nacional ou outras de ameaças ativas.

A *desinformação*, erradamente reduzida a "*fake news*", segundo Humprecht, Esser & Van Aelst (2020) é informação falsa estrategicamente partilhada para obter lucros ou causar danos e prejuízo público (ambiente, segurança, processos democráticos, etc.). Os autores definem ainda *misinformation* como a partilha não intencional de conteúdos falsos ou enganosos, e *malinformation* como informação genuína (e.g., privada), partilhada para causar danos. Os conceitos sobrepõem-se (*cfr*. Figura 3), uma vez que os utilizadores em linha partilham involuntariamente informações falsas.

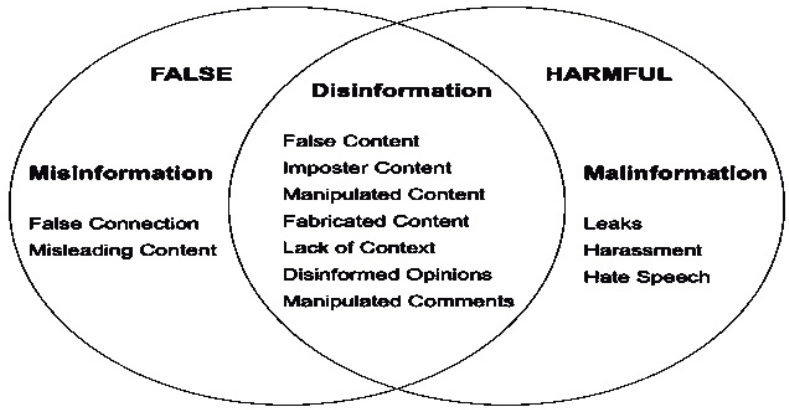


Figura 3 – Tipos de informação no ambiente das redes sociais
Fonte: Humprecht et al. (2020).

Propaganda é a persuasão e influência sobre atitudes e opiniões do público-alvo, com fins ideológicos, políticos ou comerciais, através da divulgação de informação parcial (que pode ou não ser factual) (Nelson, 1996).

2.2. Resiliência

O conceito de *resiliência*, pode ser interpretado como uma filosofia e metodologia que procura uma melhor preparação de sistemas complexos para uma variedade de ameaças, conhecidas ou não (Linkov et al., 2019). Em vez de especificar medidas contra uma ameaça específica, a abordagem de resiliência prepara os sistemas para um amplo universo de possíveis roturas.

A ciber-resiliência visa reduzir o risco das funções da organização (e.g., do Estado) dependerem do ciberespaço, procurando reduzir (ou anular) o impacto e a probabilidade de ocorrência de uma ameaça (ciberataques, falhas e outros perigos) no ciberespaço, e continuar a operar as suas funções essenciais nesse ambiente degradado (Ross, Pillitteri, Graubart, Bodeau & Mcquaid, 2019, p. 78).

2.3. Estado da Arte

Na abordagem clássica da guerra, o instrumento de poder militar é o centro de gravidade, mas hoje, o informacional tem um peso significativo nas novas formas de fazer a guerra (Dodonov, Dodonova & Mozgovoy, 2019). Segundo Nunes (2018, p. 81), a sociedade em rede aumenta as vulnerabilidades e as ameaças. Olhando

à trindade de Clausewitz (1984, p. 89) – povo, governo e militares – as AH têm o foco nas duas primeiras, estimuladas por essa sociedade tecnológica. Os analistas russos Chekinov e Bogdanov (2013), descrevem a "Guerra de Nova Geração" com ênfase no seu formato tecnológico e na superioridade da informação.

As AH fundamentam-se em conceitos antigos (Boot, 2013; Fiott & Parkes, 2019, p. 4; Marcuzzi, 2018; Murray & Mansoor, 2012). Por exemplo, Sun Tzu, no século IX a.C., já referia a utilização de uma abordagem indireta (alimentando a discórdia e desconfiança) (Tzu, 1963, p. 77). Liddell Hart, propôs que o inimigo deve ser desequilibrado atacando as suas ligações cognitivas e as suas componentes mais fracas (Hart, 1941). As novas tecnologias proporcionam simplesmente formas mais eficientes de implementar estas ideias estratégicas. Aludindo a Cohen (1999), poderemos estar perante uma revolução em assuntos militares, aproximando a natureza da guerra à população, fazendo uso das novas tecnologias.

Existem diversos livros e artigos que focam a conflitualidade no ciberespaço (Abaimov & Martellini, 2020; Lino Santos & Guedes, 2015; Schreier, 2015; Steffens, 2020) e outros que focam a guerra de informação (Giles, 2016; Whyte, Thrall & Mazanec, 2020).

No âmbito nacional, Nunes (2020) foca a edificação da capacidade de ciberdefesa, enquanto Alves (2020) propõe linhas de ação para as FFAA portuguesas responderem às AH. Quanto aos desafios da desinformação, destaca-se o relatório da Entidade Reguladora para a Comunicação Social (ERC) (2019).

A UE, a OTAN, outras organizações e académicos, têm publicado diversos conteúdos relativos à resposta face às AH, e que citamos ao longo do trabalho. O Hybrid CoE e o MCDC são as referências internacionais no desenvolvimento conceptual e de recomendações na resposta às AH. No que diz respeito à segurança no ciberespaço, destacam-se o Centro de Excelência em Ciberdefesa Cooperativa (CCDCOE) (acreditado pela OTAN) e a Agência da UE para a Segurança das Redes e da Informação (ENISA). Ao nível da desinformação, releva-se o Centro de Excelência em Comunicações Estratégicas (NATO StratCom COE).

A investigação nesta área é muito recente, pelo que ainda não existem estudos científicos e consolidados que abordem a resiliência nacional contra AH, na perspetiva do ambiente informacional, como este TII se propõe fazer.

3. METODOLOGIA E MÉTODO

3.1 Metodologia

A resiliência do instrumento de poder informacional face as AH, foi o conceito de partida, analisado à luz de duas dimensões: a ciber-resiliência e a resiliência face a campanhas de desinformação. A primeira, porque o ciberespaço é o meio primordial para o funcionamento da sociedade em rede, a segunda, porque a desinformação é uma das principais técnicas das AH. Para cada dimensão, analisaram-se variáveis que correspondem às ações-efeitos que materializaram exemplos de AH, bem como as respostas da OTAN, UE e Portugal, à luz das diferentes funções críticas de um Estado (PMESII), permitindo deduzir indicadores de resiliência.

A escolha e construção de conceitos, bem como a identificação de variáveis e indicadores permitiram a formulação das questões iniciais da investigação (Vilelas, 2009). O modelo de análise, explicitado em dimensões, variáveis e indicadores, foi construído em consonância com os objetivos e questões que esta investigação procura responder, à luz dos conceitos apresentados neste capítulo (Santos & Lima, 2019, pp. 61–62).

Face ao objeto de investigação, adotou-se uma posição ontológica construtivista, segundo a premissa de que o conhecimento é uma construção social (Bryman, 2012, p. 33). Com uma abordagem epistemológica interpretativista, sem recurso a técnicas das ciências naturais, e um raciocínio dedutivo, partiu-se da "[…] lei geral para o particular […]" (Santos & Lima, 2019, pp. 16-18), transpondo as respostas e recomendações da OTAN e da UE para o caso nacional. A estratégia de investigação foi qualitativa, vertida num estudo descritivo, interpretando os fenómenos "[…] a partir de padrões encontrados nos dados […]", sem preocupação com medições e análises estatísticas (Vilelas, 2009, cit. por Santos & Lima, 2019, p. 27). O desenho de pesquisa foi baseado no estudo de casos, num horizonte temporal transversal, pois foram extraídos indicadores observando as recomendações da UE e da OTAN, e adaptados ao contexto nacional.

3.2 Método

Na 1ª fase definiu-se o objeto de estudo, delimitou-se o tema, formulou-se o problema de investigação, definiram-se os objetivos, questões de investigação e ainda o procedimento metodológico descrito. Realizaram-se ainda entrevistas

exploratórias com especialistas que permitiram desenvolver e definir o modelo de análise.

Na 2ª fase (*cfr*. Figura 4) obtiveram-se as respostas às QD através da revisão da literatura e da análise documental (e.g., legislação, políticas, quadros de referência, estruturas organizacionais) da UE, OTAN e Portugal. O esforço de pesquisa, centrou-se na dedução de indicadores que permitem medir a resiliência nacional face às AH (informacional).

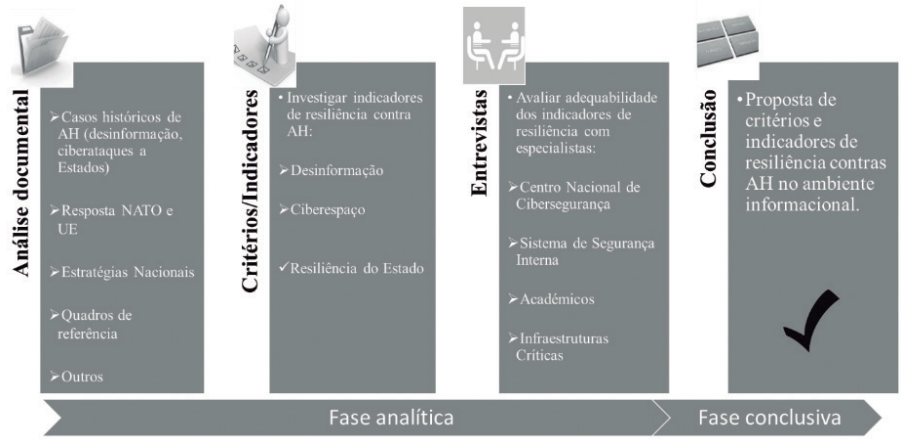


Figura 4 – Esquema síntese da 2.ª fase da investigação

Foram realizadas entrevistas semiestruturadas a seis personalidades relevantes que permitiram incluir novos indicadores e confirmar a adequabilidade e a importância dos indicadores elencados, servindo de suporte para a resposta à QC (Quivy & Campenhoudt, 1998, p. 121). As respostas a quatro das seis questões, foram objeto de tratamento com estatística descritiva, através do *Microsoft Excel*. O conteúdo das entrevistas, foi analisado utilizando o método das relações por coocorrências (Santos & Lima, 2019, p. 120).

4. APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

4.1. O impacto das Ameaças Híbridas

Inicialmente, procura-se neste capítulo, interpretar o impacto das AH, sob a lente do ambiente informacional, e responder à QD1.

4.1.1 O renascer das técnicas da Guerra Fria

Durante a Guerra Fria, os EUA e a União Soviética (URSS) aperfeiçoaram estratégias indiretas (e.g., guerras por procuração, interferências eleitorais, campanhas de desinformação), em que os EUA visavam denegrir e conter o comunismo, e a URSS o enfraquecimento do Ocidente (Santo, 2009). A investigação de Dov Levin (2019) entre diversas outras (Cull, Gatov, Pomerantsev, Applebaum & Shawcross, 2017; Hickman, Weissmann, Nilsson, Bachman, Gunneriusson & Thunholm., 2018; Lucas & Mistry, 2009), ilustra que ambas as superpotências utilizaram a desinformação como tática central para cultivar o apoio ideológico, interna e externamente.

O famoso NSC-68 (1950), um documento estratégico dos EUA, de 1950, refere a utilização da desinformação para combater a expansão comunista. Por outro lado, a doutrina soviética, usava o termo "*Active Measures*", para agrupar técnicas de desinformação, e.g., agentes de influência, histórias falsas, falsificações (e.g., planos ou cartas forjadas), entre outras (AMWG, 1981; Juurvee, 2018).

Um exemplo de desinformação, foi a alegação dos serviços secretos da URSS (KGB), em jornais soviéticos e internacionais, de que os EUA criaram em laboratório o vírus da SIDA, como arma química (Ward, 2019). Para além da imprensa, o artigo científico Segal, & Dehmlow, 1987) do professor alemão e agente do KGB, Jakob Segal, deu outra dimensão à história, provocando a desconfiança nas populações (Cull et al., 2017).

Só na administração de Reagan, a partir de 1980, os EUA conseguiram dar uma resposta forte à desinformação soviética, com a criação do *Active Measures Working Group* (AMWG), um grupo interagências (Romerstein, 2001). As principais contramedidas adotadas, segundo Cull et al. (2017), foram o *descrédito vigoroso* (denúncia de falsidades), a ameaça de *sanções* (e.g., cooperação, económicas), uso dos *media internacionais* para denunciar, os *desertores soviéticos* (testemunhos) e a *coleta de informação* para identificação das campanhas.

4.1.2 Os novos métodos impulsionados no ciberespaço

Devido à descentralização das fontes de informação que a internet veio proporcionar, aumentou o volume de desinformação bem como os atores envolvidos na sua disseminação. Adicionalmente, a crescente dependência da sociedade moderna no ciberespaço, pode levar a ciberataques disruptivos com as mesmas consequências de uma guerra convencional (RCM n.o 92, 2019; Steiger et al., 2018; Stiennon, 2015).

Descrevendo exemplos, em 2007, na Estónia, foi lançado um ataque de *negação de serviço* distribuído (DDoS), alegadamente motivado pela Rússia após deslocalização de um memorial soviético, suspendendo as funções do Estado durante duas semanas Buckland, Schreier & Winkler, 2010). Na Geórgia, em 2008, a Rússia demonstrou, pela primeira vez, a viabilidade de um ciberataque (também DDoS mas não só) em apoio a uma operação militar convencional (Abaimov & Martellini, 2020, p. 70).

Valeriano e Maness (2015) fizeram um estudo sobre ciberconflitos ocorridos entre 2001 e 2011, com 111 incidentes entre Estados, sendo aproximadamente metade relacionados com *ciberespionagem*. Em 2009, a *Information Warfare Monitor* (2009), revelou a existência de uma rede de ciberespionagem (GhostNet), com alcance a 103 Estados diferentes, incluindo Portugal (duas embaixadas e o CEGER[33]). Desde este incidente, aumentou o foco nos grupos de ciberespionagem, e.g., grupo APT1 alegadamente a cargo da unidade 61398 do Exército de Libertação Popular Chinês (Mandiant, 2013). Ainda no âmbito da ciberespionagem, o recente ataque com impacto ainda desconhecido, que explorou a cadeia de distribuição de atualizações do *software* Solarwinds, é tido como um dos mais sofisticados até agora visto (Menn, 2021). A ciberespionagem é uma ameaça crescente que importa destacar, pois o roubo de segredos de estado e comerciais, direitos de propriedade intelectual e informação, têm um impacto estratégico difícil de prever (ENISA, 2020a).

Em 2010, no Irão, as centrais de enriquecimento de Urânio fecharam em resultado de uma cibersabotagem extremamente sofisticada, através de um código malicioso, i.e., malware, designado Stuxnet (Abaimov & Martellini, 2020). Outro ciberataque a infraestruturas críticas, ocorreu na Ucrânia em 2015, provocando um corte de energia para 225.000 pessoas durante 3 horas (Lee et al., 2016).

Em 2017, surgiu o WannaCry, o maior ataque mundial de *ransomware*[34], encriptando a informação e solicitando o resgate em Bitcoins (Chen & Bridges, 2017). Importa realçar que este ataque foi alavancado por um *zero-day* (explora uma vulnerabilidade desconhecida), uma ciberarma designada EternalBlue, do arsenal da *National Security Agency* dos EUA (NSA), divulgada pelo grupo *Shadow Brokers*, relevando os riscos dos arsenais de ciberarmas serem capturados e

[33] Centro de Gestão da Rede Informática do Governo.
[34] O *ransomware* é uma classe de *malware* que se autopropaga, encripta os dados de um computador vítima e solicita o resgate, tendo surgido como uma ciberameaça dominante (ENISA, 2020).

usados de forma indiscriminada por cibercriminosos como no caso do WannaCry e posteriores (Abaimov & Martellini, 2020).

Por fim, importa referir o uso do ciberespaço como ferramenta para *influenciar processos eleitorais* em estados democráticos. Destaca-se o caso da empresa Cambridge Analytica, que alegadamente influenciou diversas eleições, como nos EUA em 2016 ou o referendo do Brexit, traçando o perfil psicológico das pessoas através de dados fornecidos pelo Facebook, influenciando os votos com mensagens direcionadas (Isaak & Hanna, 2018). Este ataque demonstrou vulnerabilidades na legislação da privacidade digital e o poder das grandes empresas tecnológicas. Noutro exemplo, em 2017, apenas dois dias antes das eleições presidenciais francesas, sem tempo de resposta foram divulgados 9 GB de e-mails comprometedores do partido de Emmanuel Macron (Abaimov & Martellini, 2020, p. 14).

4.1.3 O caso da anexação da Crimeia

Na Ucrânia, as consequências das operações de informação e psicológicas através de campanhas de desinformação no ciberespaço, resultaram no descrédito das FFAA e desconfiança da sociedade em relação às principais autoridades do Estado (Danyk et al., 2017). Foram utilizados conteúdos, nas redes sociais e outros recursos da internet, difundidos com autorias credíveis (e.g., antigos militares patrióticos), replicados em reportagens de televisões públicas na Ucrânia, que utilizaram essas fontes não verificadas (Danyk et al., 2017). A atuação da Rússia, minando a confiança em instituições internacionais e nacionais, é o exemplo de AH impulsionadas no ciberespaço (Atkinson, 2018; Chivvis, 2017).

Esta é a doutrina russa de Gerasimov, que atinge objetivos políticos e estratégicos, com a ênfase no uso dos instrumentos de poder informacional, político, económico, com foco em aumentar o protesto social, agredir e influenciar a consciência pública através da tecnologia e de ciberataques (Galeotti, 2019). Do ponto de vista russo, a guerra é agora conduzida por uma proporção aproximada de 4:1 de medidas não-militares e militares (Bartles, 2016). A transição para o uso explícito da força militar, acontece na fase final do conflito, a coberto do pretexto da manutenção da paz (Dodonov et al., 2019).

A doutrina de Gerasimov é baseada no que a Rússia considera que tem sido a atuação dos EUA, ao provocar instabilidade em países com regimes não-democráticos obtendo o pretexto para intervir militarmente (Bartles, 2016).

4.1.4. O impacto em Portugal

As AH são também uma preocupação para Portugal. Vejamos a posição da China, como potência emergente, e a sua relação com Portugal. A China fez investimentos críticos em Portugal, designadamente na EDP, na REN ou através da carteira da Fosun (investidor privado chinês), que "[…] vai da saúde à indústria farmacêutica, dos seguros à banca, passando por imobiliário e telecomunicações […]" (Costa, 2021). A persuasão chinesa é tal que impôs censura (preservando o amor à pátria chinesa) aos jornalistas da Rádio Televisão de Macau, contrariando os acordos bilaterais com Portugal e sem que ninguém consiga evitar. Por outro lado, temos os EUA a pressionar Portugal para "[…] escolher entre os aliados e os chineses […]", referindo-se à tecnologia 5G, tentando condicionar a decisão portuguesa (Jornal SOL, 2020).

O último Relatório Anual de Segurança Interna (RASI 2020), sem atribuir autoria, refere as "[…] ameaças persistentes, tecnologicamente avançadas, de origem estatal […]", especificando a ciberespionagem contra entidades de investigação científica (envolvidas em terapêuticas e vacinas da COVID-19) e "[…] infraestruturas críticas nacionais, com a finalidade de aceder a informação classificada, com valor político e económico […]" (Sistema de Segurança Interna [SSI], 2021, p. 102). Suspeita-se que tanto a China como a Rússia estejam envolvidas nestes ciberataques (Oliveira, 2021).

Relativamente à desinformação, o RASI 2020 refere que as campanhas sobre a origem da COVID-19 e outras relacionadas, procuraram "[…] enfraquecer a confiança da sociedade portuguesa na resposta à crise […]". Adicionalmente, o efeito do confinamento associou-se à crescente disseminação de conteúdos de propaganda e desinformação de movimentos radicais de extrema-direita (SSI, 2021, p. 102). Segundo o RASI, para responder às AH é prioritário combater a desinformação e proteger os processos eleitorais (SSI, 2021, p. 223).

Apesar de "[…] Portugal não ser um alvo significativo de ataques híbridos cinéticos devido à sua dimensão geopolítica […]", não é imune aos crescentes ataques não cinéticos (Alves, 2020, p. 30). De facto, apesar da pandemia ter aumentado a perceção que estamos sujeitos a este tipo de ameaças, Pathé Duarte (2020) demonstrou que Portugal esteve sujeito a pressões económicas, ciberataques e operações de narrativa nas redes sociais e *media*, perpetrados por agentes estatais (China e Rússia) e não-Estatais, muito antes da pandemia.

Segundo o Centro Nacional de Cibersegurança (CNCS) (2020), os cibercriminosos e agentes estatais agem em colaboração estreita, com ciberataques e desinformação por vezes vendidos como um[35]serviço, dificultando a imputação.

Os incidentes registados pelo CERT.PT têm vindo a aumentar nos últimos anos, não estando imunes setores críticos do Estado.

4.1.5. Desafios futuros

Os EUA sugerem que os esforços globais de influência, com ciberataques e desinformação, irão aumentar (*Office of the Director of National Intelligence*, 2021).

A imputação de um ciberataque é essencial para uma eventual resposta, mas implica saber quem o executou e quais as consequências, algo complexo de responder no ciberespaço, tornando-o no local de eleição das AH (Brenner, 2009; Rid & Buchanan, 2015). Muitas das atribuições ao nível Estado, são feitas com base em suposições e não em provas digitais fiáveis, por serem difíceis de obter, principalmente em ataques que recorrem a criptografia e ocultação e ocorrem em múltiplas fases e por diversos locais geográficos e jurisdições (Clark & Landau, 2011; Wheeler, Larsen & Leader, 2003). Os hackers profissionais encaminham os ataques através de países com os quais a vítima tem más relações diplomáticas dificultando a investigação (Schreier, 2015). As propostas que visam arquiteturas para a internet, que tornem a imputação mais controlável, conduzirá a um controlo e vigilância governamentais indesejados que chocam com a liberdade e privacidade (Buckland et al., 2010). Por exemplo, a Rússia ou a China, mantém enorme censura e restrições nas suas arquiteturas internas (Newman, 2020).

O problema da imputação tem de ser resolvido com capacidades técnicas e diplomacia que garanta colaboração total entre países, empresas e organizações, quer ao nível militar quer civil (Clark & Landau, 2011; Schreier, 2015). Adicionalmente, qualquer pessoa é uma porta de entrada na rede de uma organização (civil ou militar), sendo necessário apostar na educação em cibersegurança e encará-la como uma responsabilidade partilhada (Clarke & Knake, 2010, p. 170).

Os desafios dos sistemas ciber-físicos, e.g., armas autónomas, carros autónomos, internet das coisas (IoT) e o seu uso em *smart cities*, trazem novos desafios na área da cibersegurança e potencial para aumentar as AH (Alguliyev et al., 2018).

---

[35] O CERT.PT é a Equipa de Resposta a Incidentes de Segurança Informática Nacional (Lei n.º 46/2018).

As ferramentas antigas podem ser utilizadas de uma nova forma, ou num contexto diferente do que estamos habituados e podem ser criadas combinações inesperadas (Giannopoulos et al., 2020). Importa realçar o papel disruptivo da inteligência artificial, que é um facilitador dos sistemas ciber-físicos, mas pode também automatizar ciberataques ou criar conteúdos falsos de forma inovadora, e.g., manipulação de imagens ou vídeos (designados *deepfakes*) (Hybrid CoE, 2021). As grandes empresas tecnológicas terão maior influência, passando a ter também um papel cada vez mais relevante para a segurança e defesa, pelo que a regulação e políticas deverão estar sempre a par do desenvolvimento tecnológico (Hybrid CoE, 2021).

No contexto dos desafios elencados, e respondendo à QD1, o uso do instrumento de poder informacional para influenciar o domínio cognitivo (tomada de decisão), é predominante na conflitualidade atual, composta por ameaças permanentes, difíceis de identificar. É necessário criar resiliência não só no domínio tecnológico, mas também no domínio social (dimensão humana, perceção, crenças e raciocínio), pois tal como refere Alex Stamos [36](2020), estas novas ameaças não são apenas um problema tecnológico, mas fundamentalmente um problema humano.

4.2. Resiliência contra AH com foco na desinformação e propaganda

Este subcapítulo visa investigar possíveis indicadores de resiliência face à desinformação, à luz das respostas da UE, OTAN e Portugal, procurando responder à QD2.

4.2.1. A resposta da UE

Em resposta à desinformação russa, na sequência da anexação da Crimeia, a UE cria a *East StratCom Task Force* (*cfr*. Figura 5), integrada no Serviço Europeu para a Ação Externa (SEAE), reforçando a comunicação estratégica de promoção da UE e apoiando a liberdade de imprensa dos países de leste (CE, 2018b). Um projeto pioneiro do *East StratCom*, foi a divulgação de desinformação pró-Kremlin no sítio em linha EUvsDisinfo[37] ou na conta @EUmythbuster do Twitter, já com

[36] Antigo responsável da cibersegurança do Facebook e atualmente membro da equipa de combate a fraudes eleitorais dos EUA.
37 https://euvsdisinfo.eu/

mais de 11.535 exemplares de desinformação. (Pamment, 2020). Numa pesquisa efetuada com o filtro Portugal, obtêm-se duas notícias falsas em que Portugal é implicado, numa tentativa de dividir e enfraquecer a UE.

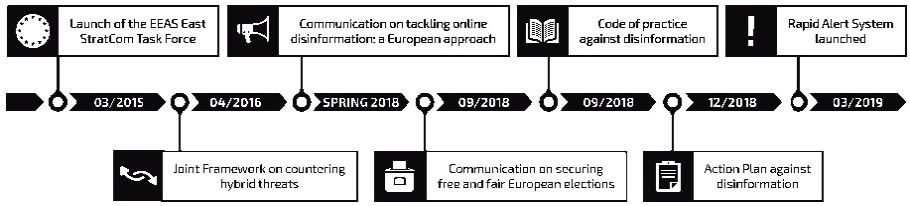


Figura 5 – Ações da UE para combate à desinformação
Fonte: Disponível em *EU* vs *DISINFORMATION* (s.d.).

Num espetro de resposta mais alargado, surge o Quadro Comum em Matéria de Luta contra as AH, onde são propostas 22 ações destinadas a reforçar a resiliência dos Estados-Membros e da UE, com foco no aumento do conhecimento situacional, na comunicação estratégica e na cooperação com a OTAN (CE, 2016). A criação do Hybrid COE a par dos Exercícios Coordenados e Paralelos (PACE)[38], refletiram essa cooperação (CE, 2017). Na sequência do quadro comum é também criada a Célula de Fusão contra as AH integrada na estrutura de informações (INTCEN) do SEAE, contribuindo para o conhecimento situacional (CE, 2020).

Seguiram-se, em 2018, duas comunicações conjuntas: "Combater a desinformação em linha: uma estratégia europeia" (CE, 2018b), e "Aumentar a resiliência e reforçar a capacidade de enfrentar AH" (CE, 2018c). A primeira, entre outras medidas, aprova o apoio e criação de uma rede europeia independente de verificadores de factos. A segunda, foca a necessidade de aumentar o conhecimento situacional, o esforço dos Estados-Membros, a comunicação estratégica e a ciber-resiliência.

Reconhecendo a necessária colaboração com o setor privado, em outubro de 2018, a UE lançou um Código de Conduta contra a Desinformação juntamente com medidas concretas (e.g., deteção de desinformação, funcionalidade de reporte) para implementação voluntária pela indústria tecnológica (alguns signatários foram a Google, Facebook, Twitter, etc.).

[38] Exercício com foco na gestão e resposta a crises num ambiente de ameaças híbridas.

Em dezembro de 2018 foi publicado o Plano de Ação contra a Desinformação, ainda hoje o pilar da abordagem da UE no combate à desinformação (Pamment, 2020). O plano centra-se na cooperação com a OTAN, deteção e exposição da desinformação, literacia mediática, jornalismo de qualidade, comunicação estratégica, sensibilização e resiliência da sociedade. Incentivou ainda as plataformas digitais a aplicarem o Código de Conduta, e estabelece uma abordagem *whole--of-society,* com cooperação entre autoridades públicas, jornalistas, investigadores (meio académico), verificadores de factos, plataformas digitais, setor privado e a sociedade civil em geral. Na sequência do plano, é lançado o Sistema de Alerta Rápido (SAR), para permitir uma consciência situacional comum entre os Estados--Membros, que, no entanto, ainda tem baixos níveis de partilha (Pamment, 2020).

Relativamente à correlação entre segurança interna e externa, deverão ser adotados métodos de trabalho horizontais, numa abordagem *whole-of-government*, com partilha de informações entre as autoridades, formação e exercícios que permitam soluções comuns para combater AH, e particularmente a desinformação (Conselho da UE, 2019).

O recém publicado Plano de Ação para a Democracia Europeia (CE, 2020a), foca-se na promoção de eleições livres, no reforço da liberdade dos *media*, e na luta contra a desinformação. O plano prevê criar instrumentos que permitam impor sanções aos autores de desinformação, e transformar o Código de Conduta num quadro de corregulação, em consonância com a nova *Digital Services Act* (DSA), ou Lei dos Serviços Digitais, que permitirá aplicar multas às tecnológicas que não implementem medidas contra a utilização de técnicas manipuladoras (LUSA, 2020).

4.2.2. A resposta da OTAN

Ao contrário da UE, que vê as AH sem se referir a guerra (e.g., GH), a OTAN, pela sua natureza militar, já em 2010 utilizava ambos os termos mas com a perceção de que a resposta dependia de fatores fora da esfera militar (Uziębło, 2017, p. 14). Assim, a UE tem vindo a liderar o processo na construção de resiliência face a AH, mas a OTAN, um parceiro fundamental, assume-se preparada para apoiar os Estados-Membros a edificarem a sua capacidade de resposta e se necessário dar uma resposta coletiva (OTAN, 2021c).

Os esforços da OTAN para lidar com os métodos híbridos, manifestaram--se no relatório anual de 2015, após a anexação da Crimeia (J. Stoltenberg, 2016). O conceito de resiliência, visto como a melhor forma de lidar com AH, foi central na

Cimeira de Varsóvia (2016), que inclusivamente proporcionou a declaração conjunta entre a UE e a OTAN (renovada em 2018) visando a cooperação no planeamento civil-militar, ciberdefesa, partilha de informação e comunicação estratégica coordenada (Shea, 2016). Após esse acordo, estabeleceu-se uma proximidade e partilha entre organismos de ambas as partes: o NCIRC[39] da OTAN e o CERT da UE, o HybridCOE e outros[40] da OTAN, a Célula de Fusão da UE e a célula do *Joint Intelligence and Security Division* da OTAN (Conselho da UE, 2019).

A OTAN, vê a desinformação como uma ameaça que procura aprofundar as divisões dentro e entre os aliados (OTAN, 2020a). Alguns dos desafios são o alcance do Russia Today (RT) e Sputnik (*media* controlada pelo Estado), ou a fábrica *troll* (desestabilizadores de discussão) de São Petersburgo - oficialmente chamada *Internet Research Agency* – com recurso a contas falsas ou automatizadas, para difusão de notícias que contêm elementos verdadeiros e falsos, dificultando os filtros de deteção naturais das pessoas (OTAN, 2020a).

A OTAN pauta-se por comunicações baseadas em factos, refutando publicamente as principais narrativas de desinformação destinadas à Aliança, através do sítio em linha "NATO-*Russia: Setting the Record Straight*" (OTAN, 2021a), mas também em relatórios e textos em linha (NATO StratCom COE, 2019; OTAN, 2020a). Outras ações concretas são a intensificação da comunicação digital, a tradução de conteúdos em várias línguas (e.g., canal de YouTube da OTAN em russo), informação oportuna aos *media*, ou *brífingues* aos *media* de países de leste, incluindo a Rússia (OTAN, 2020a).

Em suma, a OTAN, em linha com a UE, defende que a cooperação é fundamental para responder às AH, mas cada país tem de avaliar as suas próprias vulnerabilidades e aumentar a sua resiliência com uma abordagem integrada.

4.2.3. A resposta nacional

Sendo as AH um assunto transversal, não existe uma área governativa onde recaia a responsabilidade de resposta, mas todas devem contribuir e tornarem-se resilientes (Alves, 2020). Nesse âmbito, existe uma rede interministerial para as AH, liderada pelo Ministério dos Negócios Estrangeiros, que acompanha e participa no desenvolvimento dos trabalhos sobre as ameaças híbridas.

---

[39] NATO *Computer Incident Response Capability*.
[40] Como exemplo o NATO StratCom COE ou o CCDCOE.

Relativamente à desinformação, a ERC é a entidade nacional que supervisiona a aplicação do Código de Conduta contra a Desinformação pelas plataformas digitais. Segundo Sousa (2021), embaixador para a ciberdiplomacia e ponto de contato nacional do SAR, "[…] Portugal tem um regulador de uma geração muito avançada […] que se ocupa da regulação da liberdade de informação em todos os domínios […]", incluindo os sítios na internet, das televisões e dos jornais, colocando-nos na vanguarda da UE. A ERC preocupa-se com falsos sites de informação de autoria desconhecida e fins que aparentam ir além do lucro da publicidade, mas também com o combate à desinformação (rigor informativo) que possa provir de órgãos de comunicação social (OCS) (ERC, 2019). Os desafios da ERC neste domínio são muitos e estão detalhados no relatório intitulado "A Desinformação – Contexto Europeu e Nacional" (ERC, 2019).

De facto, o trabalho da ERC não se tem re velado fácil, exemplo disso foi a polémica ao ter registado o sítio "Notícias Viriato" como publicação informativa, quando este tinha sido identificado como sítio de propaganda pelo Medialab do ISCTE/Instituto Universitário de Lisboa e não existindo à data qualquer jornalista associado, condição obrigatória para registo (Câncio, 2020). Apesar deste incidente pontual, a listagem de registos na ERC pode ser consultada no seu sítio oficial, e é uma forma de verificar a credibilidade das fontes de informação em linha.

Desde 2018, aquando do lançamento do primeiro verificador de factos, intitulado Polígrafo[41], diversos OCS dedicaram-se à mesma causa.

Ao contrário de diversos países da UE, a legislação nacional não determina imputação e sanção à produção e difusão de conteúdos integrados no conceito de desinformação (ERC, 2019, p. 67). Segundo Sousa (2021), dar ao Estado a possibilidade de ajuizar conteúdos pode ser considerado censura, e a desinformação não deve ser considerada crime, devendo-se sim, apostar numa comunicação estratégica eficaz.

De encontro às recomendações da UE para eleições livres e justas, Portugal criou uma rede eleitoral com diversas autoridades responsáveis pelo acompanhamento e execução das regras relativas às atividades em linha, "[…] sendo a ERC um dos seus membros, bem como o MAI, a CNE, a ANACOM, a CNPD, entre outras […], porém os mecanismos existentes são parcos." (ERC, 2019, p. 70).

[41] https://poligrafo.sapo.pt/

A responsabilidade no combate à desinformação recai no cidadão, que deve ser proativo e verificar a veracidade da informação antes de partilhar, para isso é fundamental promover a literacia mediática (ERC, 2019).

4.2.4 Abordagens de resiliência à desinformação

Na revisão de literatura efetuada, identificámos apenas um trabalho, o de Humprecht et al. (2020), que se adequa a um modelo de resiliência nacional face à desinformação.

Esse modelo identifica indicadores mensuráveis e as métricas que lhes permitiram comparar a resiliência de sociedades de diversos países. Os indicadores são enquadrados nas dimensões política, informação (*media*) e económica. Salienta-se que as fontes de dados usadas são públicas e permitem uma aplicação imediata da abordagem.

Destaca-se que ao considerarem como indicador, a votação em partidos populistas, assumem que o populismo está associado à desinformação, o que poderá ser verdade, mas pode ser um indicador tendencial (R. Aranha, entrevista via *Microsoft Teams*, 19 de março de 2021).

Em resposta à QD2, com base na investigação e contexto da UE, OTAN e Portugal, e na abordagem de Humprecht et al. (2020), deduziram-se 28 indicadores de resiliência nacional face à desinformação.

4.3. Resiliência no Ciberespaço

Este capítulo visa investigar possíveis indicadores de ciber-resiliência, à luz das respostas da UE, OTAN e Portugal, e de abordagens de referência, procurando responder à QD3.

4.3.1. A resposta da UE

Os incidentes na Estónia (2007) deram um impulso, mas só em 2016 a UE assume uma abordagem holística e um papel centralizador na elaboração de políticas e medidas englobando a proteção de infraestruturas-críticas, cibersegurança, ciberdefesa e a resposta às AH (Beláz, 2019).

A Diretiva 2016/1148, de Segurança das Redes e Sistemas de Informação (SRI), obriga os Estados-Membros a adotarem estratégias nacionais e designar autoridades competentes e equipas de resposta a incidentes de segurança

informática (CSIRT), bem como a obrigatoriedade de notificação de incidentes.

O Regulamento Geral sobre a Proteção de Dados (RGPD) (2016/679), impôs obrigações com o objetivo de proteger os dados pessoais dos cidadãos.

Em 2017, a UE instituiu um conjunto de instrumentos de ciberdiplomacia, incluindo sanções, já com efeitos práticos, e.g., resposta ao caso WannaCry (Conselho da UE, 2020).

O Regulamento (2019/881) da Cibersegurança (*Cybersecurity Act*), cria um quadro de certificação europeu e reforça as competências da ENISA, focando a redução de vulnerabilidades na origem através da certificação de produtos (e.g., IoT), serviços e processos digitais.

A recente Estratégia Europeia de Cibersegurança de dezembro de 2020, foca que é necessário ultrapassar a falsa dicotomia existente entre «em linha» e «fora de linha» e quebrar uma abordagem compartimentada (CE, 2020b). A nova estratégia apresenta algumas iniciativas centrais, como a criação de um *Cyber Shield* (rede de centros de operações de segurança) e uma *Joint Cyber Unit* (resposta mais eficaz às ciberameaças).

Na nova estratégia é proposta a SRI 2.0, abrangendo mais setores de atividade e promovendo a gestão do risco das cadeias de fornecimento (e.g., 5G) e as ações de supervisão das autoridades nacionais. É também proposta uma nova Diretiva sobre Resiliência das Entidades Críticas nos setores da energia, transportes, banca, infraestruturas dos mercados financeiros, saúde, água potável, águas residuais, infraestruturas digitais, administração pública e espaço, sujeitando-as a avaliações regulares de risco.

Embora a SRI pretenda "[…] atingir um elevado nível de segurança em toda a UE, centra-se explicitamente em alcançar uma harmonização mínima e não máxima […]" (TCE, 2019, p. 23). A SRI 2.0 deverá reforçar esse nível de segurança.

Relativamente à estrutura, destacamos a ENISA enquanto órgão essencialmente consultivo, o Centro Europeu da Cibercriminalidade da Europol (EC3) reforça a resposta à cibercriminalidade, a CERT-UE dá apoio aos órgãos da UE, o SEAE é responsável pela articulação da ciberdefesa e ciberdiplomacia, e alberga os centros de recolha e análise de informações, e por fim, a Agência Europeia de Defesa (EDA) visa desenvolver as capacidades de ciberdefesa (TCE, 2019). Em Bucareste, será o novo Centro Europeu de Competências em Cibersegurança para coordenar a investigação e inovação (Conselho da UE, 2021).

A UE tem apostado na investigação, desenvolvimento e inovação (I&D&I), com incentivos no quadro da *Permanent Structured Cooperation* (PESCO) e do Fundo Europeu de Defesa (FED). Destaca-se a co-liderança de Portugal na Disciplina de Ciberdefesa da UE e a liderança nacional do Projeto *Cyber Academia and Innovation Hub* (CAIH).

Por fim, realça-se a Bússola Estratégica Europeia, a estratégia em estudo que vigorará a partir de 2022, com enfoque na gestão de crises e resiliência (Presidência Portuguesa do Conselho da UE, 2021).

Em perspetiva, o CNCS refere-se à UE como uma entidade reguladora que impede uma digitalização descontrolada, reorientando-a (CNCS, 2021a).

4.3.2. A resposta da OTAN

O esforço da OTAN nesta matéria começou após os incidentes na Estónia e Geórgia, mas só na cimeira de Varsóvia em 2016, o ciberespaço foi reconhecido como um domínio de operações (OTAN, 2021b). A resiliência foi um conceito central da cimeira, focando a cooperação com a UE e a necessidade de garantir o funcionamento das redes cibernéticas, a capacidade governativa e os serviços críticos, mesmo sob condições de crise (Alves, 2020).

Na sequência da cimeira de 2016, Portugal e outros Estados-Membros ratificaram o *Cyber Defence Pledge*, assumindo o compromisso de melhorar a sua resiliência e a capacidade de responder a ciberataques, incluindo aqueles inseridos em campanhas híbridas (OTAN, 2016).

Em 2018, na cimeira de Bruxelas, foi decidido criar um *Cyberspace Operations Centre* (CyOC) para coordenação da atividade operacional da OTAN no ciberespaço, bem como o acordo dos aliados em disponibilizar as suas capacidades nacionais para as operações (OTAN, 2021b). Tendo em conta a dificuldade de imputação dos ciberataques, entende-se a posição cautelosa da OTAN, ao assumir uma postura maioritariamente defensiva e relegando o caráter ofensivo das OpCiber aos designados *Sovereign Cyber Effects Provided Voluntarily by Allies* (SCEPVA) (AJP-3.20, 2020). Adicionalmente, os membros da OTAN têm diferentes visões sobre as OpCiber violarem ou não a soberania nacional, o que torna muito difícil uma resposta coletiva (Pomerleau, 2019).

A OTAN foca a ciberdefesa na proteção das próprias redes (incluindo operações e missões) e no aumento da resiliência em toda a Aliança. (OTAN, 2021b). Para aumento da resiliência, a OTAN tem incentivado projetos de I&D e

tem aposta clara na educação e treino, aqui, destaca-se o papel de Portugal, na "[…] liderança do projeto NATO *Smart Defense Multinational Cyber Defence Education and Training* (MNCDE&T) […] e na instalação da NATO *Communications and Information Academy* (NCI *Academy*) em Oeiras." (P. Nunes, 2020, p. 17).

4.3.3. A resposta nacional

Apesar dos esforços das organizações internacionais a que Portugal pertence, os Estados-Membros são os principais responsáveis pela sua própria cibersegurança.

Na sequência da RCM n.º 26/2013, "Defesa 2020", de 11 de abril, o Ministro da Defesa Nacional (MDN), determinou a criação do Centro de Ciberdefesa (CCD), que surge em 2015 sob a tutela do Estado-Maior-General das Forças Armadas (EMGFA), (RCM n.o 26, 2013). Na diretiva estratégica do EMGFA 2018-2021 (DEEMGFA), é identificado o objetivo estratégico de dinamizar a edificação da capacidade de ciberdefesa nacional, demonstrando que a capacidade (onde se inclui a ofensiva conforme ENSC 2019-2023) está numa fase embrionária, sendo os recursos humanos uma grave limitação (EMGFA, 2018; P. Nunes, 2020).

Aprovado no Decreto-Lei n.º 69/2014 surge o CNCS, com responsabilidade de coordenação operacional e autoridade nacional em matéria de cibersegurança relativamente ao Estado e operadores de infraestruturas críticas. O CNCS transpôs a Diretiva SRI para a legislação nacional (Lei n.º 46/2018), sendo a entidade que centraliza as notificações de incidentes e comunicação com as demais estruturas nacionais e internacionais. A resposta coordenada aos incidentes de cibersegurança é garantida pelo CERT.PT do CNCS e a rede de CSIRT, bem como o designado "[…] Grupo dos Quatro (G4), composto pelo CNCS, CCD, Unidade Nacional de Combate ao Cibercrime e Criminalidade Tecnológica (UNC3T) e Serviços de Informações de Segurança (SIS)." (P. Nunes, 2020, p. 15). A articulação para a cooperação nacional e internacional está sintetizada na Figura 6.

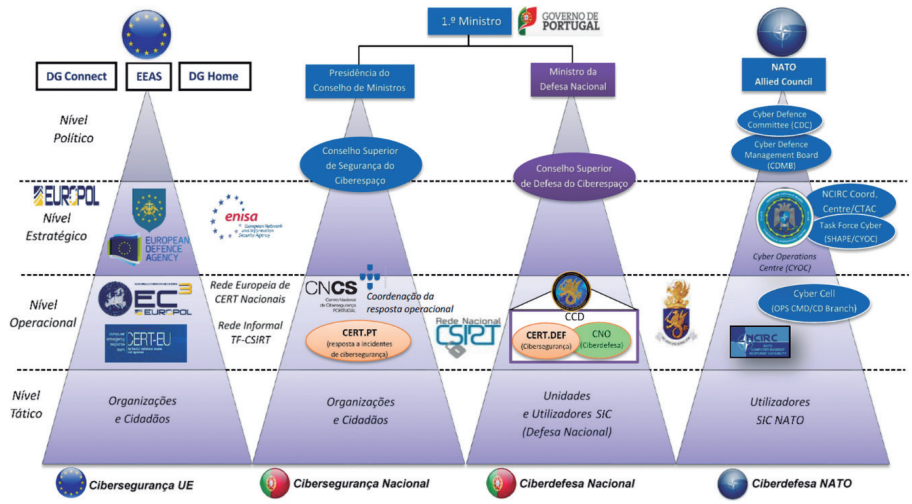


Figura 6 – Articulação da estrutura de ciberdefesa (panorama nacional e internacional)
Fonte: Adaptado a partir de Nunes (2020, p. 33).

No âmbito das atribuições do CNCS, foi proposto em 2019 o Quadro Nacional de Referência para a Cibersegurança (QNRCS), com base em normas internacionais de referência, para que qualquer entidade possa cumprir (voluntariamente) os requisitos mínimos de cibersegurança (CNCS, 2019).

É importante destacar que o QNRCS prevê a gestão de cibersegurança como um processo contínuo focando aspetos humanos, tecnológicos, processuais e físicos (e.g., redundância), abordando a gestão do risco e resiliência. Por exemplo, a organização deve identificar os requisitos de resiliência necessários para suportar a prestação de serviços críticos, deve planear a continuidade do negócio (em níveis aceitáveis pré-definidos) na sequência de um incidente disruptivo, entre outras.

Os objetivos do QNRCS estão organizados por categorias (*cfr.* Figura 7) e subcategorias "[…] onde se explanam medidas técnicas e processuais […] que permitam às organizações melhorar a sua capacidade de proteção […]" (CNCS, 2019, p. 15).

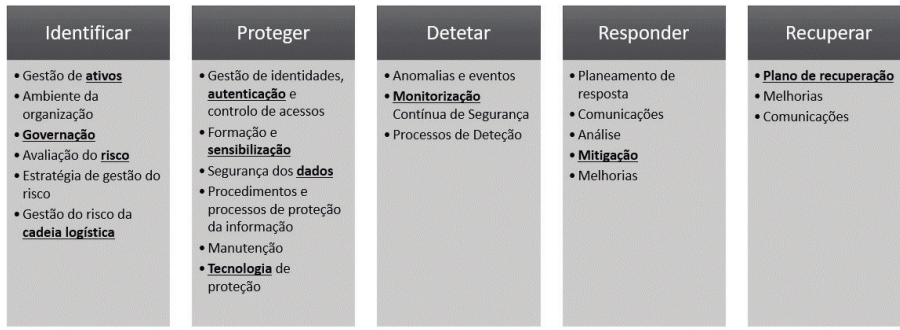


Figura 7 – Objetivos e categorias do QNRCS
Fonte: Adaptado a partir de QRNCS (CNCS, 2019).

Importa referir, de acordo com a Estratégia para a Inovação e Modernização do Estado e da Administração Pública 2020-2023, aprovada na RCM n.º 55/2020, 80 % dos organismos da Administração Pública (AP) deverão ser certificados em conformidade com o QNRCS. Este parece ser um passo, em consonância com aquilo que virá a ser espelhado na SRI2.0, em que o CNCS deverá assumir-se como Autoridade Nacional de Certificação da Cibersegurança (CNCS, 2021b). Contudo, resta perceber quais os requisitos de segurança e medidas aplicáveis, pois o art.º 14 da Lei n.º46/2018, define apenas que devem ser "[…] proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.".

A preparação civil, é vertida no Sistema Nacional de Planeamento Civil de Emergência (SNPCE) (Decreto-Lei n. º 43/2020, de 21 de julho, 2019), liderado pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC), que integra diversas comissões especializadas, relevando-se a Comissão de Planeamento de Emergência (CPE) da Cibersegurança.

Por fim, importa referir que a ENSC 2019-2023, define como objetivo estratégico "maximizar a resiliência". Os eixos de intervenção, incidem no reforço das estruturas de cibersegurança e ciberdefesa, na educação e sensibilização, proteção e resposta às ameaças, investigação, inovação e cooperação. A ENSC, prevê que é necessário antecipar a emergência e a adoção atempada de ações que acrescentem resiliência. A cooperação (nacional e internacional) e uma resposta em rede integrada entre os vários setores (públicos e privados), a par de uma sociedade resiliente com competências digitais, são fatores fundamentais para a resiliência.

4.3.4. Abordagens de ciber-resiliência

O *National Institute of Standards and Technology* (NIST), define ciber-resiliência como a capacidade de *"*[…] *anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."* (Ross et al., 2019). Os objetivos de ciber-resiliência são descritos no Quadro 1.

Quadro 1 – Objetivos da ciber-resiliência

Objetivo	Descrição
Antecipar	Estar informado e preparado para a adversidade
Resistir	Continuar as funções essenciais apesar das adversidades
Recuperar	Restaurar todas as funções durante e após a adversidade
Adaptar	Modificar as funções e/ou a capacidade para prever mudanças no ambiente técnico, opera-cional, ou da ameaça.

Fonte: Adaptado a partir de Ross et al. (2019).

A ciber-resiliência pode aplicar-se a um pequeno aparelho eletrónico, a um sistema complexo de *software* e *hardware*, a uma organização ou a um Estado (Ross et al., 2019, p. 1). Um Estado ciber-resiliente, pode suportar ciberataques ou outros perigos ou falhas no ciberespaço, e continuar a operar nesse ambiente degradado desempenhando as suas funções essenciais.

Ao reduzir o risco das funções da organização (e.g., do Estado) dependerem do ciberespaço, procurando diminuir (ou anular) o impacto e a probabilidade de ocorrência de uma ameaça, aumentamos a ciber-resiliência (Ross et al., 2019, p. 78). As diversas técnicas para aumentar a ciber-resiliência, apesar da maioria se aplicar numa perspetiva de engenharia de sistemas, são detalhadas no documento do NIST da autoria de Ross et al. (2019).

Destacamos também o trabalho de Spidalieri (2015), em que avalia a ciber-resiliência dos EUA, baseado na metodologia *Cyber Readiness Index* (Hathaway, 2015), criada para avaliar a maturidade de um Estado em matéria de cibersegurança.

Outro projeto, do *World Economic Forum* (WEF) por Keys et. al. (2016), propõe uma abordagem baseada no modelo de cibersegurança para infraestruturas críticas do NIST *Cybersecurity Framework* (2014) e no modelo de Linkov (2013). As colunas do Quadro 2 representam os objetivos tradicionais de resiliência a desastres, com a adição do "detect" inspirado na NIST *Cybersecurity Framework* (2014) (Keys et. al., 2016). Nas linhas do ...??? tem-se os domínios da doutrina

Network-Centric Warfare: físico, informação, cognitivo e social. Os indicadores que completam o quadro, são uma combinação dos indicadores propostos no modelo do NIST e de Linkov, e são detalhados no trabalho de Keys et. al. (2016).

Quadro 2 – Estrutura base do quadro de ciber-resiliência do WEF

	Plan & Prepare	*Detect*	*Absorb*	*Recover from*	*Adapt to*
Physical					
Information					
Cognitive					
Social					

Fonte: Disponível em Keys et al. (2016).

Em resposta à QD3, com base na investigação e contexto da UE, OTAN e Portugal, e nas abordagens descritas acima, deduziram-se 58 indicadores de ciber-resiliência nacional (*cfr*. Quadro 3. A maturidade de cibersegurança (e.g., nível de implementação do QNRCS) das entidades críticas, o nível de risco e evolução das AH no ciberespaço em Portugal, a capacidade das FFAA conduzirem OpCiber (ofensivas e defensivas), a agilidade dos canais de cooperação (internos e externos), são alguns dos indicadores de ciber-resiliência elencados.

4.4. Critérios e indicadores de resiliência contra Ameaças Híbridas

Este subcapítulo responde à QC, com um primeiro subcapítulo onde se faz um enquadramento e explicação da abordagem, e um segundo e terceiro onde se propõem os indicadores de resiliência nacional face à desinformação e indicadores da ciber-resiliência nacional, respetivamente.

4.4.1. Enquadramento e abordagem sobre a Resiliência e sua relação com o modelo conceptual das Ameaças Híbridas

Os modelos conceituais do HybridCoE (2020) e do MCDC (2019), referem que as AH não são responsabilidade única de uma entidade especifica e é necessário adotar uma abordagem *whole-of-government*, que promove a aproximação, confiança e partilha de informação regular entre organismos do estado (civis e militares), e uma abordagem holística *whole-of-society* (extensível à sociedade e

setor privado), reunindo atores civis, militares e políticos num novo ecossistema de segurança preparado para responder a crises de forma mais eficiente. O MCDC (2019) dá como exemplo as abordagens *whole-of-society* espelhada nas estratégias da Suécia ("*Total Defence*"), Noruega ("'*Support and Cooperation*"), Finlândia ("*Comprehensive Security*"), entre outros.

Quanto ao papel da defesa, conforme referiu o secretário-geral da OTAN (2020), "*our militaries cannot be strong if our societies are weak, so our first line of defence must be strong societies*", realçando, por exemplo, a dependência dos militares nas infraestruturas civis ou cadeias de abastecimento, quer para comunicações quer para transporte.

Em Portugal, está sob proposta a criação de um "[…] sistema de resiliência nacional […]" associado a um novo "[…] sistema nacional de gestão de crises […]" que responderá não só a AH como a qualquer outra ameaça ou risco (e.g., sismo), pretendendo-se uma abordagem *whole-of-government*, apoiada em tecnologias de *BigData* e Inteligência Artificial para apoio à decisão e partilha de informação (N.L. Pires, entrevista via *Microsoft Teams,* 09 de março de 2021).

Nesta linha de pensamento, *whole-of-government* e *whole-of-society,* a abordagem de resiliência proposta neste TII, subdivide-se em variáveis que representam as funções críticas de um Estado (PMESII), inspirada no modelo conceptual do MCDC.

4.4.2. Abordagem para a resiliência nacional

A abordagem conceptual relativa à resiliência social dos Estados-Membros da UE, desenvolvida por Manca, Benczur & Giovannini (2017), propõe um processo genérico que compreende a obtenção de indicadores, o processo analítico (métricas e processamento) e a visualização (e.g., *dashboard*), para que se possa monitorizar a resiliência e identificar pontos de melhoria. Num processo continuo de lições aprendidas, devemos perceber quais os indicadores que mais contribuem ou quais devem ser removidos e substituídos por outros, para melhor aferir a resiliência (Manca et al., 2017).

No presente TII, focou-se a identificação de indicadores. O processo analítico e a visualização, não sendo objeto deste estudo, terão que ser analisadas em trabalhos futuros para materializar a abordagem numa ferramenta prática que permita monitorizar e melhorar a resiliência nacional.

Por dedução, através da análise das ações e respostas face a AH (descritas

nos subcapítulos 3.2 e 3.3) da UE, OTAN e Portugal, foram obtidos os indicadores inicialmente propostos. Os indicadores, inspirados na revisão de literatura e adequados ao contexto nacional, têm como requisito serem mensuráveis (e.g. uma percentagem, variação, sim/não).

Através das entrevistas a seis especialistas, confirmaram-se alguns dos indicadores propostos e incluíram-se outros após análise do conteúdo das entrevistas, utilizando o método das relações por ocorrências Santos & Lima, 2019, p. 120). Assim, considerou-se um indicador válido (i.e., indicador selecionado) desde que tivesse duas ou mais ocorrências, com avaliação média igual ou superior a 3,5 (numa escala de 1 - pouco importante a 5 - muito importante). A decisão de optar pelo valor 3.5, surge na sequência do contributo de Miguel Correia (entrevista via correio eletrónico, 09 de março de 2021) que sugeriu priorizar indicadores, potenciando a aplicabilidade prática dos mesmos. No caso da resiliência nacional face à desinformação selecionaram-se 23 de um total de 52 indicadores. No caso da ciber-resiliência selecionaram-se 54 de um total de 114 indicadores.

4.4.3. Indicadores de resiliência nacional contra a desinformação

Conforme referido, optou-se por identificar indicadores associados a cada uma das funções críticas do Estado (PMESII). No entanto, importa salientar a importância do domínio Social, pois as campanhas de desinformação e outros métodos híbridos interligados, procuram afetar a homogeneidade da cultura e da sociedade do Estado alvo. Contudo, existe uma clara ligação entre domínios, por exemplo, a ciberespionagem pode ser o primeiro passo para obter *Informação* para influenciar a opinião pública (*Social*), as perceções e o discurso, minando a discussão e o processo *Político* no Estado alvo.

Importa também realçar, que o combate à desinformação é um tema sensível devido ao direito à liberdade de expressão, ou seja, é necessário evitar que os mecanismos se tornem em censura ou controle da opinião pública (O. Rocha, entrevista via correio eletrónico, 10 de março de 2021).

Os indicadores selecionados, estão espelhados naquilo que designamos de matriz de resiliência nacional face à desinformação (cfr. Quadro 3). O farol dos indicadores propostos, são os quatro pilares do plano de ação da UE para combate à desinformação (CE, 2018a): melhorar a deteção e denúncia, reforçar a coordenação, mobilizar o setor privado e sensibilizar as pessoas.

Quadro 3 - Proposta de matriz da resiliência nacional face à desinformação (AH)

	Indicadores de resiliência nacional face à desinformação no âmbito das ameaças híbridas
Ações / Domínios	Melhorar (detetar, analisar, denunciar); Reforçar coordenação; Mobilizar o setor privado; Sensibilizar as pessoas
Político	**P.1.** Está definida a coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração? **P.2.** Existe uma estratégia nacional que contemple resposta à desinformação no âmbito das AH? **P.3.** Existe uma estratégia de comunicação para preparar a população ou contrariar narrativas de desinformação? **P.4.** Existem mecanismos de cooperação internacional no domínio político-diplomático para responder à desinformação no âmbito das AH?
Militar	**M.1.** Agilidade na partilha, cooperação e coordenação com as autoridades civis **M.2.** Capacidades para detetar, analisar e denunciar desinformação ao nível militar **M.3.** Exercícios militares que contemplem o combate à desinformação (que vise denegrir a instituição ou liderança militar) **M.4.** Existe um plano de comunicação estratégico que reforce a união e prestígio da instituição militar e vise anular efeitos de desinformação?
Económico	**E.1.** Investimento em I&D para criação de mecanismos de combate à desinformação
Social	**S.1.** Nível de polarização da sociedade (e.g. V-Dem https://www.v-dem.net/) **S.2.** Nível de confiança nos media (e.g. digitalnewsreport.org/interactive/) **S.3.** Percentagem de cidadãos que usa redes sociais como fonte de notícias (e.g. digitalnewsreport.org/interactive/) **S.4.** Existem mecanismos para identificação de audiências alvo mais vulneráveis às campanhas de desinformação?
Informação	**I.1.** Quantidade de mecanismos (e.g. *fact checks*), por OCS, para detetar, analisar e denunciar as fontes de desinformação? **I.2.** Existe um sistema de informação comum para conhecimento situacional da desinformação aos diferentes níveis e entre as diferentes instituições? **I.3.** Nível de risco e registos da evolução da desinformação em Portugal **I.4.** Existe uma plataforma pública centralizada para difundir campanhas de desinformação (e.g. https://euvsdisinfo.eu/)? **I.5.** Existem mecanismos para certificação de órgãos de comunicação social na internet? **I.6.** Variação do volume de ações de sensibilização - comunicação estratégica e educação (literacia mediática) **I.7.** Ações de formação para jornalistas
Infraestruturas	**II.1.** Existe um gabinete de comunicação estratégica? **II.2.** Existe uma Célula de Fusão Nacional para aumentar o conhecimento situacional? **II.3.** Existem recursos e infraestruturas dedicadas à deteção de campanhas de desinformação no ciberespaço (inclui deteção de redes de distribuição com *bots* ou *trolls*)?

4.4.4. Indicadores de ciber-resiliência nacional

No Quadro 4 está esquematizada a matriz de ciber-resiliência com os indicadores selecionados e adequados ao contexto nacional, inspirada nos modelos propostos por Keys et al. (2016) e Spidalieri (Spidalieri, 2015), apresentados anteriormente. Pretende-se que a matriz proposta, possa vir a contribuir para uma visão da ciber-resiliência nacional face a AH (ou outras) no ciberespaço, num processo dinâmico de adaptação da mesma.

Na matriz, o domínio Infraestruturas integra o conjunto de entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, embora estas sejam transversais aos outros domínios (e.g., autarquias são também do domínio Político).

Quadro 4 - Proposta de matriz da ciber-resiliência nacional face a AH

		Indicadores de ciber-resiliência face a ameaças híbridas					
Objetivos resiliência ->		**Antecipar**			**Resistir**	**Recuperar**	**Adaptar**
Objetivos cibersegurança / **Domínios**		**1. Identificar/Planear**	**2. Proteger**	**3. Detetar**	**4. Responder**	**5. Recuperar**	**6. Adaptar**
CS	**Infraestruturas** Operadores Infraestruturas críticas e Svc. essenciais; Administração Pública; Prestadores de Serviços Digitais	**CS.1.1.** Maturidade QNRCS (Identificar) **CS.1.2.** Foco em ativos críticos **CS.1.3.** Assume ataques com sucesso no planeamento **CS.1.4.** Certifica ativos críticos **CS.1.5.** Exercícios e treinos	**CS.2.1.** Maturidade QNRCS (Proteger) **CS.2.2.** Foco em ativos críticos	**CS.3.1.** Maturidade QNRCS (Detetar) **CS.3.2.** Agilidade na partilha e colaboração **CS.3.3.** Deteção de redes de distribuição de desinformação	**CS.4.1.** Maturidade QNRCS (Responder) **CS.4.2.** Capacidade de coordenação da resposta **CS.4.3.** Colaboração	**CS.5.1.** Maturidade QNRCS (Recup.) **CS.5.2.** Foco nos ativos críticos **CS.5.3.** Agilidade	**CSD.6.1.** Rever e corrigir configurações/ procedimentos **CSD.6.2.** Melhorar partilha de informação
CD	**Militar** (Forças Armadas)	**CD.1.x=CS.1.x** **CD.1.6.** Garante diversidade (fornecedores, arquitetura) **CD.1.7.** Projeção de poder	**CD.2.x=CS2.x** **CD.2.3.**Projeção de poder e Dissuasão	**CD.3.x.=CS.3.x.**	**CD.4.x.=CS.4.x.** **CD.4.4.** Capacidade de OpCiber (ofensivas e defensivas)	**CD.5.x.=CS.5.x**	
S	**Social**	**S.1.** Oferta formativa em cibersegurança **S.2.** Níveis de ensino onde se ministram conteúdos de cibersegurança **S.3.** Observação de atitudes e comportamentos (e.g., fonte observatório do CNCS) **S.4.** Campanhas de sensibilização para a cibersegurança nacional					
E	**Económico**	**E.1.** Investimento privado e público em cibersegurança incluindo I&D&I (e.g., fonte observatório do CNCS) **E.2.** Mercado de trabalho de cibersegurança (e.g., fonte observatório do CNCS)					
P	**Político**	**P.1.** Existe uma estratégia de segurança no ciberespaço que contemple resposta a AH? **P.2.** Existe atribuição de competências na resposta a AH? **P.3.** Políticas de investimento em cibersegurança e ciberdefesa **P.4.** O regime jurídico da segurança do ciberespaço impõe obrigatoriedade de certificação ou requisitos de segurança suficientes (e.g., requisitos QNRCS pelo CNCS)? **P.5.** Existe um planeamento civil de emergência para fazer face a AH no ciberespaço? **P.6.** Existem autoridades nacionais competentes em matéria eleitoral com recursos adequados para responder a AH no ciberespaço?					
I	**Informação** (partilha)	**I.1.** Existe uma Célula de Fusão para AH ao nível nacional e interoperável com o da UE? **I.2.** Existe coordenação entre instituições e uma definição clara dos fluxos de partilha de informação e colaboração? **I.3.** Existe um sistema de informação comum para conhecimento situacional de AH aos diferentes níveis e entre as diferentes instituições? **I.4.** Nível de risco e registos da evolução das AH no ciberespaço em Portugal					

Nos domínios Infraestruturas e Militar, propõe-se como indicadores de resiliência, os níveis de maturidade das organizações em matéria de cibersegurança, de acordo com o QNRCS. Assim, para obter uma visão mais granular, optou-se por subdividir a matriz, para esses dois domínios, de acordo com os objetivos de segurança do QNRCS (identificar, proteger, detetar, responder e recuperar), aninhados dentro dos objetivos da *framework* de sistemas ciber-resilientes do NIST, que pressupõe ataques com sucesso (antecipar, resistir, recuperar e adaptar) (CNCS, 2019; Ross et al., 2019).

No âmbito Militar, acrescem aos indicadores de cibersegurança, os indicadores específicos que evidenciem a maturidade da capacidade de ciberdefesa, conforme salientado por Paulo Nunes (entrevista via mail, 08 de março de 2021).

As restantes dimensões PMESII, para além da Infraestruturas e Militar já referidas, são analisadas à luz da influência que possam ter na ciber-resiliência.

Por fim, importa referir que se assume o pressuposto que é ou será possível aferir a maturidade de cibersegurança das diferentes organizações, por exemplo, através de auditorias, reporte, questionários, ou exigência de eventuais certificações QNRCS ou equivalentes (e.g., ISO 27001), caso contrário, a medição da ciber-resiliência será sempre falaciosa e só será efetivamente aferida após um ciberataque.

Não será certamente simples verificar ou exigir a todas as entidades críticas que sejam certificadas de acordo com o QNRCS na sua plenitude, mas será possível mapear os controlos e processos de cibersegurança através de vários níveis de maturidade, a atingir de acordo com a dimensão, função, ou análise de risco de cada entidade ou setor. Por exemplo, o departamento de defesa dos EUA requer certificação de cibersegurança às empresas privadas que façam contratos de defesa, de acordo com um *Cybersecurity Maturity Model Certification* (CMMC) que se subdivide em 5 níveis de maturidade, sendo que o mais básico é tão simples como perguntar se a empresa tem software de antivírus, faz *updates* ao software de antivírus, ou se tem política de passwords (Lopez, 2020). A framework de segurança do NIST também prevê diferentes níveis de maturidade (*tiers*) que refletem uma progressão de respostas (NIST, 2018). O QNRCS sugere que o "[…] documento seja interiorizado com espírito crítico […]" e cada organização deve adaptar o QNRCS face às suas especificidades (CNCS, 2019, p. 10). Contudo, seria muito útil haver a predefinição de um *perfil* de maturidade (i.e., controlos ou medidas técnicas e processuais a implementar) desejável para as organizações dos vários setores, em sintonia com regras emanadas pelos reguladores setoriais (e.g., Entidade Reguladora dos Serviços Energéticos).

A tendência será que a certificação em cibersegurança seja um processo natural no futuro, tal como é a higiene e segurança do trabalho atualmente (G. Marques, entrevista via *Microsoft Teams*, 11 de março de 2021).

Um tópico de discussão interessante seria a "[…] obrigatoriedade de as empresas realizarem ações de formação de cibersegurança (e.g., *e-learning*) utilizando, por exemplo, os cursos disponibilizados pelo CNCS." (R. Aranha, entrevista via *Microsoft Teams*, 19 de março de 2021).

5. CONCLUSÕES

As novas tecnologias vieram alavancar e potenciar as AH, um conceito antigo com nova designação. Por um lado, temos o problema da dependência tecnológica que aumenta as vulnerabilidades exploradas através de ciberataques. Por outro lado, temos as redes sociais e outros meios de comunicação, que permitem a comunicação em massa e a qualquer indivíduo ser uma fonte de notícias, potenciando a propaganda e a desinformação fácil.

As AH permitem atingir objetivos estratégicos sem ultrapassar o limiar da guerra convencional, quer seja porque os efeitos gerados não justificam uma resposta militar convencional, quer porque há ambiguidade em aspetos legais ou é impossível provar a imputação. Contudo, o assunto continua a ser também do foro militar, não só porque as AH podem combinar as técnicas do instrumento militar, mas também porque colocam em causa a soberania das nações.

A UE e a NATO despertaram para o problema após a anexação da Crimeia, onde a Rússia demonstrou como acentuar fracionamentos culturais e sociais com recurso a campanhas de desinformação. A pandemia veio acentuar as AH, com a ciberespionagem em torno de entidades que investigam terapêuticas, ou com a desinformação em torno das vacinas ou da origem do vírus COVID-19, criando a desconfiança em torno da eficácia das instituições e organizações.

Neste contexto, a resiliência surge como a melhor resposta para fazer face a vulnerabilidades e ameaças que são incertas. Assim, torna-se basilar propor critérios e indicadores da resiliência de Portugal face a AH no ambiente informacional.

O Hybrid CoE e a UE referem que as campanhas de desinformação e os ciberataques fazem frequentemente parte do ambiente das AH. O ciberespaço é um meio privilegiado para as AH (permite alcance, velocidade, ocultação, e a imputação é difícil) e sendo o próprio ciberespaço um domínio contido no ambiente informacional, optou-se por analisar duas dimensões: (i) ciber-resiliência; e (ii) a resiliência face à desinformação.

Face ao objeto de investigação, adotou-se um raciocínio dedutivo, assente numa estratégia de investigação qualitativa, consubstanciada num desenho de pesquisa baseado no estudo de casos, transpondo e contextualizando as respostas e recomendações da OTAN e da UE, bem como de outras abordagens de referência, para o caso nacional.

Através da revisão da literatura e da análise documental, para resposta às QD, o esforço de pesquisa centrou-se em perceber o fenómeno das AH e em deduzir

indicadores que permitissem medir a resiliência nacional face a AH (informacional). Para resposta à QC, foram realizadas entrevistas semiestruturadas a especialistas reconhecidos, que permitiram confirmar a adequabilidade e a importância dos indicadores deduzidos previamente.

Relativamente ao impacto das AH sob a lente do ambiente informacional, foi possível observar o seu uso desde a Guerra Fria aos novos métodos alavancados no ciberespaço. Portugal não é imune e está sujeito a ciberataques e desinformação. Os esforços globais de influência tendem a aumentar e é necessário criar resiliência não só no domínio tecnológico, mas também no domínio social. A dificuldade de imputação persiste como a grande dificuldade na resposta. Esse problema, só pode ser resolvido com a regulação, o reforço de competências, tecnologia, diplomacia, colaboração total (externa e interna, civil e militar), e com a aposta na educação e consciencialização, fomentando a cibersegurança como uma responsabilidade partilhada.

Relativamente aos critérios e indicadores de resiliência nacional face à desinformação, deduziram-se 28 indicadores. Como exemplo de alguns dos indicadores elencados temos a existência de um gabinete de comunicação estratégica, o nível de polarização da sociedade, o nível de confiança nos *media*, a existência de uma plataforma pública para difundir campanhas de desinformação, ou a existência de uma célula de fusão nacional (e.g., integrada nos serviços de informações).

Quanto aos critérios e indicadores de ciber-resiliência nacional, deduziram-se 58 indicadores. Alguns exemplos dos indicadores elencados são a maturidade de cibersegurança (e.g., nível de implementação do QNRCS) das entidades críticas, a certificação de ativos críticos, o nível de investimento privado e público em cibersegurança, a existência de uma definição clara dos fluxos de partilha de informação e colaboração ente instituições, ou a capacidade das FFAA conduzirem OpCiber (ofensivas e defensivas).

A resposta às AH não são responsabilidade única de uma entidade especifica e torna-se necessário adotar abordagens holísticas. Assim, os indicadores deduzidos nas respostas às QD2 e QD3, refletem uma perspetiva *whole-of-government* em que se deve promover a partilha de informações, a formação e exercícios de forma integrada (organismos do Estado), permitindo soluções comuns para obter resiliência face às AH, e uma perspetiva *whole-of-society*, que estende a cooperação ao setor privado, jornalistas, investigadores (meio académico), verificadores

de factos, plataformas digitais, e a sociedade civil em geral. Neste sentido, os indicadores forma subdivididos em variáveis que representam as funções críticas de um Estado (PMESII).

Os indicadores deduzidos nas respostas à QD2 e QD3, foram submetidos à apreciação dos entrevistados. As entrevistas permitiram também que os entrevistados sugerissem novos indicadores. Como resultado, aplicando o critério de seleção descrito no sexto capítulo, no caso da resiliência nacional face à desinformação selecionaram-se 23 de um total de 52 indicadores, e no caso da ciber-resiliência selecionaram-se 54 de um total de 114 indicadores. Os indicadores selecionados (i.e., adequados ao contexto nacional) constituem a resposta à QC e a materialização do OG (*Propor critérios e indicadores da resiliência de Portugal face a AH no ambiente informacional*).

Como principais contributos para o conhecimento, este TII propõe um conjunto de indicadores de resiliência nacional face a AH, no ambiente informacional, enquadrados por uma abordagem alinhada com as recomendações da UE e da OTAN, colhendo o melhor de outras abordagens relacionadas com resiliência (ainda que noutros âmbitos).

Elenca-se como possível limitação da investigação, o facto de não existir um leque mais alargado de especialistas entrevistados, para complementar a validação e adição de novos indicadores. Do total de entrevistas planeadas (e.g., a membros da rede interministerial para AH) só seis corresponderam. Salienta-se que sendo as AH um tópico recente, o conhecimento nesta área ainda não está consolidado de forma transversal, em especial quando restrito ao ambiente informacional.

Quanto a estudos futuros, sugere-se o desenvolvimento das métricas para o processo analítico e a visualização, para materializar a abordagem proposta numa ferramenta prática que permita monitorizar e melhorar a resiliência nacional.

REFERÊNCIAS BIBLIOGRÁFICAS

Abaimov, S., & Martellini, M. (2020). Cyber *Arms - Security in Cyberspace*. Boca Raton: CRC Press.

AJP-3.20. (2020). Allied Joint Doctrine for Cyberspace Operations. Bruxelas: NATO Standardization Office.

Alves, A. J. F. M. (2020). *A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas*. Trabalho de Investigação Individual do CPOG 2019/2020. Lisboa: Instituto Universitário Militar.

AMWG. (1981). Forgery, Disinformation, Political Operations. *United States Department of State Bureau of Public Affairs, 88*, 4.

Atkinson, C. (2018). Hybrid Warfare and Societal Resilience: Implications for Democratic Governance. *Information & Security: An International Journal, 39*(1), 63–76.

Bartles, C. K. (2016). Getting Gerasimov Right. *Military Review*, (February), 30–38.

Beláz, A. (2019). The changing role of the EU in Cybersecurity. *Biztonságtudományi Szemle, 1*(1-2.), 17–30.

Boot, M. (2013). *Invisible Armies: An Epic History of Guerrilla Warfare from Ancient Times to the Present*. New York, NY: Liveright Publishing.

Brenner, S. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Nova Iorque: Oxford University Press.

Brianna Keys, Aashish Chhajer, Zilong Liu, Daniel Horner, & Stuart Shapiro. (2016). *A framework for assessing cyber resilience*. Retirado de http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf

Bryman, A. (2012). *Social Research Methods (4th ed.)*. Oxford: Oxford University Press.

Buckland, B. S., Schreier, F., & Winkler, T. H. (2010). *Democratic governance challenges of cyber security*. Génova: DCAF.

Câncio, F. (2020). ERC regista como "informativo" site de desinformação e propaganda. [Página *online*]. Retirado de https://www.dn.pt/edicao-do-dia/27-jan-2020/erc-regista-como-informativo-site-de-desinformacao-e-propaganda-11751353.html

Centro Nacional de Cibersegurança. (2020). *Relatório de Cibersegurança em Portugal - Riscos & Conflitos*.

Chekinov, S. G., & Bogdanov, S. A. (2013). The Nature and Content of a New-Generation War. *Military Thought, 4*, 12–23.

Chen, Q., & Bridges, R. A. (2017). Automated behavioral analysis of malware: A case study of wannacry ransomware. *Proceedings - 16th IEEE International Conference on Machine Learning and Applications, ICMLA 2017, 2017-Decem*, 454–460.

Chivvis, C. (2017). Understanding Russian "Hybrid Warfare": And What Can Be Done About It. *Rand Corporation*.

Clark, D., & Landau, S. (2011). Untangling attribution. *Harvard National Security Journal, 2*(February 2010), 323-352.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: the next threat to national security and what to do about it*. Nova Iorque: HarperCollins e-books.

Clausewitz, C. Von, Howard, M., & Paret, P. (1984). *On War*. Princeton, N.J: Princeton University Press.

CNCS. (2019). *Quadro Nacional de Referência para Cibersegurança*. Lisboa: Autor.

CNCS. (2021a). *Boletim no1/2021 do Observatório Nacional de Cibersegurança*. Lisboa: Autor.

CNCS. (2021b). *Projeto de decreto-lei regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança*. [Página *online*]. Retirado de https://www.cncs.gov.pt/recursos/noticias/projeto-de-decreto-lei-regulamenta-o-regime-juridico-da-seguranca-do-ciberespaco.

Comissão Europeia. (2016). *Comunicação conjunta - Quadro comum em matéria de luta contras as ameaças híbridas - uma resposta da UE*. [Página *online*]. Retirado de https://eur-lex.europa.eu/legalcontent/PT/TXT/PDF

Comissão Europeia. (2017). *Relatório Conjunto relativo à aplicação do Quadro em matéria das ameaças híbridas - uma resposta da UE*. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0030&from=PT

Comissão Europeia. (2018a). *Action Plan against Disinformation*. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri

Comissão Europeia. (2018b). *Comunicação - Combater a desinformação em linha: uma estratégia europeia*. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0236&from=PT

Comissão Europeia. (2018c). *Comunicação - Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas*. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018JC0016&from=PT

Comissão Europeia. (2020a). *Comunicação sobre o plano de ação para a democracia europeia*. [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0790&from=PT

Comissão Europeia. (2020b). *Nova Estratégia da UE para a Cibersegurança e novas regras para aumentar a resiliência das entidades críticas físicas e digitais*.

[Página *online*]. Retirado de https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391. https://ec.europa.eu/commission/presscorner/detail/pt/IP_20_2391

Conselho da UE. (2019). *Conclusões do Conselho sobre aumentar a resiliência*. [Página *online*]. Retirado de https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/pt/pdf

Conselho da UE. (2020). *UE impõe primeiras sanções contra ciberataques*. [Página *online*]. Retirado de https://www.consilium.europa.eu/pt/press/press-releases/2020/07/30/eu-imposes-the-first-ever-sanctions-against-cyber-attacks/.

Conselho da UE. (2021). *Conselho dá luz verde - Consilium*. [Página *online*]. Retirado de https://www.consilium.europa.eu/pt/press/press-releases/2021/04/20/bucharest-based-cybersecurity-competence-centre-gets-green-light-from-council/.

Conselho Europeu. (2019). *A New Strategic Agenda 2019-2024*. [Página *online*]. Retirado de https://www.consilium.europa.eu/media/39914/a-new-strategic-agenda-2019-2024.pdf

Costa, F. S. (2021). *A "guerra fria" com a China está a aquecer*. [Página *online*]. Retirado de https://eco.sapo.pt/especiais/a-guerra-fria-com-a-china-esta-a-aquecer/. https://eco.sapo.pt/especiais/a-guerra-fria-com-a-china-esta-a-aquecer/

Cull, N. J., Gatov, V., Pomerantsev, P., Applebaum, A., & Shawcross, A. (2017). *Soviet Subversion, Disinformation and Propaganda: How the West Fought Against it: An Analytic History, with Lessons for the Present*. [Página *online*]. Retirado de https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf

Danyk, Y., Maliarchuk, T., & Briggs, C. (2017). *Hybrid War: High-tech, Information and Cyber Conflicts. Connections: The Quarterly Journal, 16*(2), 5–24.

Dodonov, R., Dodonova, V., & Mozgovoy, L. (2019). *Polemological Paradigm of Comprehension of Essence of Hybrid War*. 7–17. doi: 10.31865/2520-684292018157445.

Estado-Maior-General das Forças Armadas. (2018). *Diretiva Estratégica do EMGFA 2018-2021, de 18 abril de 2018*. Lisboa: CEMGFA.

ENISA. (2020). ENISA *Threat Landscape 2020 - Main Incidents in the EU and Worldwide*. Retirado de https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents/at_download/fullReport

Entidade Reguladora Para a Comunicação Social. (2019). *A Desinformação - Contexto Europeu e Nacional*. Retirado de https://www.parlamento.pt/Documents/2019/abril/ desinformacao_contextoeuroeunacional-ERC-abril2019.pdf

EU vs *DISINFORMATION*. (n.d.). [Página *online*]. Retirado de https://euvsdisinfo.eu/

Fiott, D., & Parkes, R. (2019). Protecting Europe: The EU's response to hybrid threats. *Chaillot Paper, 151*(April). Retirado de https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_151.pdf

Galeotti, M. (2019). The mythical 'Gerasimov Doctrine' and the language of threat. *Critical Studies on Security, 7*(2), 157–161. doi: 10.1080/21624887.2018.1441623

Giannopoulos, G., & Smith, H. (2019). *The Landscape of Hybrid Threats: A conceptual model*. Brussels: European Commission.

Giles, K. (2016). *Handbook of Russian Information Warfare*. (Fellowship Monograph). NATO Defence College, Roma.

Gunneriusson, H. (2019). Hybrid Warfare and Deniability as Understood by the Military. *Polish Political Science Yearbook, 48*(2).

Hart, B. H. L. (1941). *The strategy of indirect approach*. Londres: Faber and Faber Limited.

Hathaway, M. (2015). *Cyber Readiness Index 2.0*. [Página *online*]. Retirado de https://www.belfercenter.org/publication/cyber-readiness-index-20

Hickman, K., Weissmann, M., Nilsson, N., Bachman, S., Gunneriusson, H. & Thunholm, P. (2018). Hybrid Threats and Asymmetric Warfare: What to do? Em: Swedish Defence University. *Conference proceeding (February)*.

Humprecht, E., Esser, F., & Van Aelst, P. (2020). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. *The International Journal of Press/Politics, 25*(3), 493–516. doi:10.1177/1940161219900126

Hybrid CoE. (2017). *Hybrid threats as a concept - Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats* [Página *online*]. Retirado de https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Hybrid CoE. (2021). *The future of cyberspace and and hybrid threats*. [Página *online*]. Retirado de https://www.hybridcoe.fi/wp-content/uploads/2021/04/20210407_Hybrid_CoE_Trend_Report_6_The_future_of_cyberspace_WEB.pdf

Isaak, J., & Hanna, M. J. (2018). User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection. *Computer, 51*(8), 56–59.

Jakovljevic, M., Bjedov, S., Jaksic, N., & Jakovljevic, I. (2020). Covid-19 pandemia and public and global mental health from the perspective of global health security. *Psychiatria Danubina, 32*(1), 6–14.

Jens Stoltenberg. (2020). *Keynote speech by NATO Secretary General Jens Stoltenberg at the Global Security 2020 (GLOBSEC) Bratislava Forum, 07-Oct.-2020*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/opinions_178605.htm

Jornal SOL. (2020). *Marcelo responde a "ameaça" do embaixador dos EUA*. [Página *online*]. Retirado de https://sol.sapo.pt/artigo/710015/marcelo-responde-a-ameaca-do-embaixador-dos-eua

JP3-12. (2018). *Joint Publication 3-12 - Cyberspace Operations*. Washington: Joint Chiefs of Staff.

Juurvee, I. (2018). *The resurrection of ' active measures ': Intelligence services as a part of Russia ' s influencing toolbox*. [Página *online*]. Retirado de https://www.hybridcoe.fi/wp-content/uploads/2020/07/Strategic-analysis-7-April.pdf

Lee, R. M., Assante, M. J., & Conway, T. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid*. *White Paper*. Retirado de https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2016/05/20081514/E-ISAC_SANS_Ukraine_DUC_5.pdf

Levin, D. H. (2019). Partisan electoral interventions by the great powers: Introducing the PEIG Dataset. *Data Feature Conflict Management and Peace Science, 36,* 88–106.

Linkov, I., Baiardi, F., Florin, M. V., Greer, S., Lambert, J. H., Pollock, M., Rickli, J. M., Roslycky, L., Seager, T., Thorisson, H., & Trump, B. D. (2019). Applying Resilience to Hybrid Threats. *IEEE Security and Privacy, 17*(5), 78–83.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions, 33*(4), 471–476. doi:10.1007/s10669-013-9485-y

Lucas, S., & Mistry, K. (2009). Illusions of Coherence: George F. Kennan, U.S. Strategy and Political Warfare in the Early Cold War, 1946–1950. *Diplomatic History, 33*(1), 39–66.

LUSA. (2019). *Governo quer plano nacional para combater desinformação e ciberataques - Combate às Fake News, uma questão democrática*. [Página *online*]. Retirado de https://combatefakenews.lusa.pt/fake-news-governo-quer-plano-nacional-para-combater-desinformacao-e-ciberataques-c-audio/

LUSA. (2020). *Fake News*. [Página *online*]. Retirado de https://www.dinheirovivo.pt/empresas/fake-news-ue-vai-dizer-as-plataformas-como-devem-eliminar-desinformacao-e-pode-multa-las-13101588.html

Manca, A. R., Benczur, P., & Giovannini, E. (2017). *Building a Scientific Narrative Towards a More Resilient EU Society - Part 1: A Conceptual Framework*. Luxembourg: União Europeia, Joint Research Centre.

Mandiant. (2013). APT1 *Exposing One of China's Cyber Espionage Units*. Retirado de https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

Marcuzzi, S. (2018). Hybrid Warfare in Historical Perspectives. *Max Weber International Workshop*. Retirado de http://www.natofoundation.org/wp-content/uploads/2018/06/NDCF_StefanoMarcuzzi_Paper.pdf

Menn, J. (2021). *U.S. intelligence agencies say Russia likely behind hacking of government agencies*. [Página *online*]. Retirado de https://www.reuters.com/world/us/us-intelligence-agencies-say-russia-likely-behind-hacking-government -2021-01-05/

Monitor, I. W. (2009). Tracking GhostNet: Investigating a Cyber Espionage Network. *Think Tank White Paper, March 29*, 1–53.

Multinational Capability Development Campaign (2019). *Countering Hybrid Warfare Project*. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/concepts_mcdc_countering_hybrid_warfare.pdf

Murray, W., & Mansoor, P. R. (2012). *Fighting Complex Opponents from the Ancient World*. New York: Cambridge University Press.

NATO StratCom COE. (2019). Hybrid Threats - A Strategic Communications Perspective. *Encyclopedia of Creativity, Invention, Innovation and Entrepreneurship*. doi.org: 10.1007/978-3-319-15347-6_300702

Nelson, R. A. (1996). *A Chronology and Glossary of Propaganda in the United States*. Londres: Greenwood.

Newman, L. H. (2020). *Russia Takes a Big Step Toward Internet Isolation*. [Página *online*]. Retirado de https://www.wired.com/story/russia-internet-control-disconnect-censorship/.

NIST. (2018). *Cybersecurity Framework*. [Página *online*]. Retirado de https://www.nist.gov/cyberframework/framework.

NSC-68. (1950). National Security Council Report: United States Objectives and Programs for National Security. *History and Public Policy Program Digital Archive*.

Nunes, P. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional*. Trabalho de Investigação Individual do CPOG 2019/2020. Lisboa: Instituto Universitário Militar.

Nunes, P. V., Mendes, C. P., Santos, J. R. L., Santos, L. C. dos, Moniz, P., & Casimiro, S. V. (2018). *Contributos para uma Estratégia Nacional de Ciber Defesa*.

Office of the Director of National Intelligence. (2021). *Annual Threat Assessment of the US Intelligence Community*. Retirado de https://www.dni.gov/files/ODNI/ documents/ assessments/ATA-2021 -Unclassified-Report.pdf

Oliveira, M. (2021). *China e Rússia suspeitas de fazerem ciberespionagem a Portugal*. [Página *online*]. Retirado de https://www.publico.pt/2021/04/06/ sociedade/noticia/china-russia-suspeitas-fazerem-ciberespionagem-portugal-1957275

Organização do Tratado do Atlântico Norte. (2016). *Cyber Defence Pledge*. [Página *online*] Retirado de https://www.nato.int/cps/en/natohq/official_texts_133177.htm

Organização do Tratado do Atlântico Norte. (2020a). *NATO's approach to countering disinformation*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq.htm.

Organização do Tratado do Atlântico Norte. (2020b). *Resilience and Article 3*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_132722.htm. https://www.nato.int/cps/en/natohq/topics_132722.htm

Organização do Tratado do Atlântico Norte. (2021a). *NATO-Russia: setting the record straight*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/115204.htm.

Organização do Tratado do Atlântico Norte. (2021b). *NATO - Cyber defence*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_78170.htm. https://www.nato.int/cps/en/natohq/topics_78170.htm

Organização do Tratado do Atlântico Norte. (2021c). *NATO - Topic: NATO's response to hybrid threats*. [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm

Pamment, J. (2020). *The EU's Role in Fighting Disinformation: Taking Back the Initiative*. [Página *online*]. Retirado de https://carnegieendowment.org/2020/07/15/eu-s-role-in-fighting-disinformation-taking-back-initiative-pub-82286

Patel, S. S., Moncayo, O. E., Conroy, K. M., Jordan, D., & Erickson, T. B. (2020). *The landscape of disinformation on health crisis communication during the COVID-19 pandemic in Ukraine*. *Journal of Science Communication 19(05) (2020)A02*.

Pathe Duarte, F. (2020). *Non-kinetic hybrid threats in Europe – the Portuguese case study (2017-18)*. *Transforming Government: People, Process and Policy, 14*(3), 433–451. doi: 10.1108/TG-01-2020-0011

Pomerleau, M. (2019). *When do cyberattacks deserve a response from NATO?* [Página *online*]. Retirado de https://www.fifthdomain.com/international/2019/12/03/when-do-cyberattacks-deserve-a-response-from-nato/

Presidência Portuguesa do Conselho da UE. (2021). *Workshop de Ministros da Defesa da UE sobre a Bússola Estratégica*. [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/comunicacao/noticias_fa/Paginas.aspx

Quivy, R., & Campenhoudt, L. Van. (1998). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.

RCM n.o 26, 11 de abril. (2013). *Aprova a reforma "Defesa 2020."* Diário da República, 1.a Série, 77, 2285–2289. Lisboa: Presidência do Conselho de Ministros.

RCM n.o 92. (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1.a Série, 108.

Rid, T., & Buchanan, B. (2015). *Attributing Cyber Attacks*. *Journal of Strategic Studies, 38*(January 2015), 4–37.

Romerstein, H. (2001). Disinformation as a KGB Weapon in the Cold War. *Journal of Intelligence History, 1*(1), 54–67. doi: 10.1080/16161262.2001.10555046

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & Mcquaid, R. (2019). Developing Cyber Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication 800-160 Volume 2, 2*, 224. Retirado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf

Santo, G. E. (2009). A NATO numa Perspectiva Militar: entre o Sonho e as Realidades. *Nação e Defesa, 123,* Lisboa: IDN, 31–39.

Santos, Lino, & Guedes, A. M. (2015). Breves reflexões sobre o poder e o ciberespaço. *RDeS – Revista de Direito e Segurança, III*(6), 189–209.

Santos, Lúcio, & Lima, J. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2ª ed.). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Schreier, F. (2015). On Cyberwarfare. *DCAF HORIZON, 7*.

Segal, J., Segal, L., & Dehmlow, R. (1987). AIDS: Its nature and origin. *Bertrand Russell Peace Foundation, Australian Branch*.

Shea, J. (2016). Resilience: a core element of collective defence. [Página *online*]. Retirado de https://www.nato.int/docu/review/articles/2016/03/30/resilience-a-core-element-of-collective-defence/index.html

Sistema de Segurança Interna. (2021). *Relatório Anual de Segurança Interna 2020*. Lisboa: Sistema de Segurança Interna. Retirado de http://www.ansr.pt/InstrumentosDeGestao/Documents/Relatório Anual de Segurança Interna (RASI)/RASI 2016.pdf

Sousa, L. B. (2021). *Portugal nunca foi alvo de uma campanha de desinformação externa*. [Página *online*]. Retirado de https://www.dn.pt/edicao-do-dia/05-mar-2021/portugal-nunca-foi-alvo-de-uma-campanha-de-desinformacao-13420138.html

Spidalieri, F. (2015). State of the States on Cybersecurity. *Pell Center for International Relations and Public Policy, November*. doi: 10.1016/j.jacc.2018.01.032

Stamos, A. (2020). *Realistic Threats and Realistic Users: Lessons from the Election*. [Página *online*]. Retirado de https://www.sigsac.org/ccs/CCS2020/keynotes.html.

Steffens, T. (2020). *Attribution of Advanced Persistent Threats*. Berlim: Springer Vieweg.

Steiger, S., Harnisch, S., Zettl, K., & Lohmann, J. (2018). Conceptualising conflicts in cyberspace. *Journal of Cyber Policy, 3*(1), 77–95.

Stiennon, R. (2015). *There Will Be Cyberwar: How the Move to Network-centric Warfighting Set the Stage for Cyberwar*. Birmingham: IT-Harvest Press.

Stoltenberg, J. (2016). *The Secretary General's Annual Report 2015*. Bruxelas: NATO. doi: 10.1353/bmc.2015.0008

Lopez, Todd. (2020). *DOD to Require Cybersecurity Certification in Some Contract Bids*. [Página *online*]. Retirado de https://www.defense.gov/Explore/ News/ Article/ Article/2071434/dod-to-require-cybersecurity-certification-in-some-contract-bids/

Tribunal de Contas Europeu. (2019). *Desafios à eficácia da política de cibersegurança da UE*. Luxemburgo: Autor.

Tzu, S. (1963). The Art of War. In *Sun Tzu On The Art Of War*. Traduzido por Samuel B. Griffith. Oxford: Oxford University Press. doi: 10.4324/9781315030081

Uziębło, J. J. (2017). United in ambiguity? EU and NATO approaches to hybrid warfare and hybrid threats. *EU Diplomacy Papers, 5,* 38. Retirado de https://www.coleurope.eu/research-paper/united-ambiguity-eu-and-nato-approaches-hybrid-warfare-and-hybrid-threats

Valeriano, B., & Maness, R. C. (2015). *Cyber War versus Cyber Realities, Cyber Conflict in the International System*. Oxford: Oxford University Press.

Vilelas, J. (2009). *Investigação – o processo de construção do conhecimento*. Lisboa: Edições Sílabo.

Ward, M. (2019). *Formative Battles: Cold War Disinformation Campaigns and Mitigation Strategies*. Washington: Wilson Center.

Wheeler, D. A. D. A., Larsen, G. N., & Leader, T. (2003). *Techniques for cyber attack attribution* (Issue October). IDA Paper P-3792. Institute for Defense Analysis.

Whyte, C., Thrall, A. T., & Mazanec, B. M. (2020). *Information warfare in the age of cyber conflict*. Oxfordshire: Routledge.

William Sebastian Cohen. (1999). *Annual Report to the President and the Congress*. Washington, DC: US Government Printing Office.

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA, VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS. (MILITAR)

PREVENTION AND TACKLING OF HYBRID THREATS: IDENTIFYING MEASUREMENT INSTRUMENTS, VARIABLES AND NATIONAL RESILIENCE INDICATORS AGAINST HYBRID THREATS (MILITARY)

Autor
MAJ ART Aires Almeida Carqueijo

Orientador
TCOR ENG António Carlos dos Santos Ferreira

1. INTRODUÇÃO

As ameaças à estabilidade e segurança ocorrem cada vez mais na "*gray zone*", onde atores estatais e não estatais empregam táticas híbridas, tornando o ambiente de segurança atual cada vez mais complexo e ambíguo, caraterizado pela combinação "híbrida" de instrumentos militares e não militares, dificultando a consciência situacional e a tomada de decisão rápida e consensual (Rühle & Roberts, 2021).

Na verdade, já Creveld (1991) apontava que a forma de fazer a guerra estava a ser transformada, o que implicaria também alterações estratégicas. De facto, as mudanças no modo de fazer a guerra têm sido uma constante ao longo da história, com mudanças ao nível das estratégias, táticas, ameaças e ferramentas tecnológicas empregues (Cordesman, 2003; Greene, 2006; Jomini, 1879; Mallin, 1970; Tzu, 2010). Neste contexto, "a guerra híbrida […] encontrou na componente cibernética um instrumento de ação de elevado potencial em função do custo reduzido, rapidez de atuação, sensação de anonimato e leque crescente de possíveis alvos" (Nunes, Santos, Ralo, & Mendes, 2018, p. 35). A máxima de Tzu (2010) relativa a subjugar o inimigo sem lutar ser o ápice da habilidade, continua atual.

Apesar da terminologia não ser nova (Hoffman, 2009, 2010), com a anexação da Crimeia, em 2014, as Ameaças Híbridas (AH), pela rutura que representavam, passaram a fazer parte do léxico do contexto político, originando, desde essa data, a implementação de medidas ao nível estatal e internacional (Giannopoulos, Smith, & Theocharidou, 2021).

Não obstante os desenvolvimentos e discussões de 2015 (North Atlantic Treaty Organization [NATO], 2015), em julho de 2016, na Cimeira de Varsóvia, os Chefes de Estado e de Governo dos países membros da Organização do Tratado do Atlântico Norte (OTAN), afirmavam que a responsabilidade primária para responder às AH residia na nação-alvo, devendo a Aliança e os Aliados estarem preparados para as contrariar, comprometendo-se a OTAN a cooperar ativamente com os seus parceiros e Organizações Internacionais (OI), nomeadamente a União Europeia (UE) (NATO, 2016b). Nesta Cimeira, os Aliados reiteravam talqualmente o compromisso de continuar a incrementar a resiliência, convenção inclusive já presente no artigo terceiro do *Tratado do Atlântico Norte* (NATO, 1949, 2016b, 2021a). Neste seguimento, em dezembro de 2016, o Presidente do Conselho Europeu, o Presidente da Comissão Europeia e o Secretário-Geral da OTAN assinaram uma declaração conjunta, onde reconheciam que a OTAN e a UE enfrentavam desafios sem precedentes, afirmando o reforço da parceria estratégica em diversas áreas, incluindo o sincronismo no combate às AH, estabelecendo a criação do *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE)[42] e o reforço da partilha de informações críticas entre a *European Union* (EU) *Hybrid Fusion Cell*[43] (HFC) e a OTAN (NATO, 2016a).

Paralelamente e sinergicamente com os desenvolvimentos ao nível da OTAN, a UE mostrou uma atitude ativa nesta área, almejando incrementar a resiliência, promover a comunicação estratégica e combater a desinformação (European Commission, 2016, 2018, 2020; European Council, 2019a, 2019b). Esta temática é de tal modo relevante e atual, que no *Programa da Presidência Portuguesa do Conselho da União Europeia*, a efetivar no primeiro semestre de 2021, uma "Europa resiliente" se constitui numa das cinco linhas de ação, sendo salientada uma "especial atenção" aos domínios das AH (UE, 2021, p. 36).

Portugal não está alheio a esta temática, pois, nas palavras da Secretária de Estado dos Assuntos Europeus, Ana Paula Zacarias, impera "fazer a identificação dos nossos pontos de vulnerabilidade para podermos fazer um plano nacional de luta" contra as AH (Lusa, 2019) e nas do Diretor de Serviços para os Assuntos de Segurança e Defesa, Jorge Aranda, "a resposta às AH requer uma abordagem

[42] O *Hybrid CoE* é uma OI independente que promove uma abordagem *whole-of-government* e *whole-of-society* para combater as AH (Hybrid CoE, 2021).
[43] O EU HFC, criado dentro do EU *Intelligence and Situation Centre*, tem um papel central na coordenação relativamente ao aviso prévio e à consciência situacional atinente às AH (European Commission, 2020).

whole of government, se não mesmo *whole of society*" (Presidência Portuguesa do Conselho da União Europeia 2021, 2021).

Assim Portugal adere ao Hybrid CoE em dezembro de 2019 (Hybrid CoE, 2019), encontrando-se a ser redigido um documento de enquadramento nacional das AH, orientado segundo uma abordagem *all of government*.

Neste seguimento, e considerando que a resposta às AH "passa por incrementar a resiliência" (Curso de Promoção a Oficial General [CPOG] 2019-2020, 2020, p. 235), importa considerar como objeto de estudo do presente trabalho a resiliência do instrumento de poder militar nacional às AH. Constitui-se assim como Objetivo Geral (OG) da investigação propor variáveis e indicadores de resiliência nacional face às AH, no Domínio Militar (DM). Estas variáveis e indicadores constituem um primeiro passo com destino à mensuração da resiliência do DM, para o consequente colmatar de vulnerabilidades. Afinal, é às Forças Armadas (FFAA) que "incumbe a defesa militar da República" (Decreto de aprovação da Constituição, 1976).

Dada a extensão da temática, esta terá que ser inevitavelmente delimitada temporal, espacial e concetualmente (Santos et al., 2019). Em termos temporais, iniciar-se-á em 2014, até à atualidade, dado ter sido após a implementação efetiva de táticas híbridas pela Rússia na Crimeia e no leste da Ucrânia que foi dada especial atenção a este fenómeno pela comunidade científica (Bajarūnas, 2020, p. 62), desenvolvendo estudos e conceitos essenciais à presente investigação. No concernente ao espaço, cingir-se-á ao território nacional, no âmbito da inserção de Portugal na OTAN e na UE, dado que estas duas organizações têm vindo a harmonizar esforços para delinear uma estratégia comum na resposta a estas ameaças (Caliskan, 2019; Mälksoo, 2018; Pereira, 2018). Relativamente ao conteúdo, será analisada a implementação da capacidade de resiliência nacional às AH ao nível das FFAA, dado que "a credibilidade da instituição militar e a sua capacidade para desempenhar as missões essenciais da defesa nacional" são indispensáveis, importando desenvolver "capacidade para enfrentar as ameaças e riscos mais prováveis e para cumprir os compromissos internacionais" (Governo de Portugal, 2013, pp. 22–28), sendo as FFAA "fundamentais na resiliência e gestão de crises" (N. C. B. L. Pires, entrevista por videoconferência, 16 de abril de 2021).

Contribuindo diretamente para o OG, identificam-se os seguintes Objetivos Específicos (OE):

– OE1 – Identificar as ferramentas das AH que podem afetar o DM nacional;

– OE2 – Analisar a resiliência do DM nacional face às AH;

– OE3 – Debater indicadores de resiliência nacional face às AH, no DM.

Com o intuito de se atingir a observância do OG apresenta-se como Questão Central (QC): Quais as variáveis e indicadores de resiliência nacional face às AH, no DM? A resposta a esta questão é de primordial importância pois permitirá, por exemplo, em estudos futuros, quantificar o nível de resiliência, face a estas ameaças, bem como detetar vulnerabilidades que ao serem colmatadas originarão um incremento na resiliência nacional.

Com o intuito de chegar à resposta à QC, e intrínsecas aos OE, foram identificadas três Questões Derivadas (QD):

– QD1 (OE1) – Quais as ferramentas das AH que podem afetar o DM nacional?

– QD2 (OE2) – Qual o estado da implementação da resiliência face às AH no DM nacional?

– QD3 (OE3) – Quais os indicadores de resiliência face às AH, no DM, aplicáveis à realidade nacional?

O presente estudo encontra-se organizado em cinco capítulos. O primeiro remete para a introdução e o segundo, a investigação é enquadrada teórico-conceptualmente, alumiando-se o estado da arte e a revisão da literatura, espelhando as teorias e conceitos estruturantes, culminado com a apresentação do modelo de análise. No terceiro é abordada a metodologia e o método seguidos na presente investigação, aclarando raciocínio, estratégia de investigação, desenho de pesquisa, participantes e procedimento, talqualmente como instrumento e técnicas de recolha de dados. No quarto é dado enfoque à investigação propriamente dita, apresentando-se os dados e discutindo-se os resultados, pretendendo-se atingir os OE através da resposta às QD, permitindo, com a resposta à QC, atingir o OG. No quinto e último capítulo são traçadas as conclusões que derivam do explanado nos capítulos anteriores, almejando-se efetuar a súmula dos resultados obtidos, aditar contributos para o conhecimento, traçar recomendações e propor estudos futuros, apresentando-se concomitantemente as limitações da investigação.

2. ENQUADRAMENTO TEÓRICO E CONCETUAL

No presente capítulo é efetuado o enquadramento teórico e conceptual, onde se alumia o estado da arte e a revisão da literatura, espelhando as teorias e conceitos estruturantes, com particular ênfase para a resiliência e o DM. O capítulo culmina com a apresentação do modelo de análise.

2.1. Estado da arte/revisão da literatura

2.1.1. A resiliência

Os estudos sobre resiliência espelham o facto de as definições de resiliência variarem de acordo com a abordagem, disciplina ou assunto em que estas se alicerçam (Balmer, Pooley, & Cohen, 2014; Bourbeau, 2015; Community & Regional Resilience Institute [CAPRI], 2013; Folke et al., 2002; Southwick et al., 2014), podendo inclusive encontrar-se diferentes definições dentro da mesma disciplina (CAPRI, 2013). Esta multiplicidade de definições e as discrepâncias entre elas tornam difícil avaliar, operacionalizar ou comparar os resultados das pesquisas sobre resiliência e, assim, aglutinar o conhecimento acumulado sobre resiliência com base nelas (Davydov, Stewart, Ritchie, & Chaudieu, 2010).

Não obstante as inúmeras definições que aparecem na literatura, é possível destacar três caraterísticas principais que aparecem na sua maioria:

- A resiliência é percecionada como uma habilidade, ou capacidade (mas não como uma reação, resposta, traço ou processo), de um indivíduo, grupo, comunidade ou sociedade (Ajdukovic, Kimhi, & Lahad, 2015; Bonanno, 2004; Egeland, Carlson, & Sroufe, 1993; Parsons et al., 2016);
- A resiliência envolve uma mudança dinâmica ou transformação no comportamento (Adger, 2000; Berkes & Ross, 2013; Gaillard, 2010);
- A resiliência é tipificada por uma capacidade adaptativa e dinâmica de um sistema para se ajustar a uma determinada situação em evolução (Fletcher & Sarkar, 2013; Padan & Elran, 2019).

Como requisito para a existência de comportamento resiliente deve ocorrer uma rutura. Esta pré-condição decorre da necessidade de resiliência surgir apenas num estado em que o equilíbrio de um sistema é interrompido, independentemente desta interrupção ter origem humana (guerras, violência ou acidentes) ou na natureza (por exemplo catástrofes naturais), desde que cause uma perturbação significativa na rotina (Elran, 2006).

Nesta envolvente, Padan e Gal (2020, p. 36) apresentam a resiliência como sendo a capacidade de um sistema (indivíduo/comunidade/estado) se comportar, durante uma crise ou após uma rutura, de forma adaptativa, para retornar a um nível anterior ou mesmo aperfeiçoado de funcionamento. Estes autores dividem a resiliência nos domínios social, político, económico e securitário/militar, afirmando que as capacidades de resiliência podem ser díspares nos diferentes domínios. De facto, e numa perspetiva ontológica, cada domínio representa uma categoria distinta (Fjäder, 2014).

Colocando o foco no DM, e apesar de no AAP-06 NATO *Glossary of Terms and Definitions* não existir referência à definição de resiliência (NSO, 2020a), se regressarmos a 2006, a OTAN define resiliência como a capacidade de uma unidade funcional continuar a desempenhar uma função fundamental na presença de falhas ou erros (NSO, 2020b). Esta definição viria a ter uma abrangência colaborativa, na definição proposta pelo *Allied Command Transformation* (ACT), que carateriza a resiliência como a capacidade de resistir e recuperar fácil e rapidamente de choques e tensões, combinando fatores civis, económicos, comerciais e militares, sendo alcançada através do aumento da preparação nos setores público e privado, apoiada e ampliada pela capacidade militar, tendo o seu ciclo (Figura 1) as fases de preparação, absorção, recuperação e adaptação (ACT, 2018, p. 1).

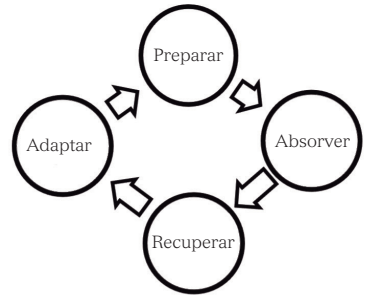


Figura 1 – Ciclo da resiliência
Fonte: Adaptado de ACT (2018, p. 1).

A preparação representa o trabalho que as entidades produzem para se tornarem mais capazes de lidar com futuras perturbações, a absorção é a capacidade de uma entidade para suportar uma perturbação ou incidente, a recuperação enfatiza a capacidade de restaurar a funcionalidade após uma perturbação ou incidente, e a adaptação alude à capacidade de mudança com base nas lições aprendidas (DeGuzman, 2021; United States [US] Army Corps of Engineers, 2020).

O conceito de resiliência e inerente ciclo pode assim ser representado graficamente (Figura 2) como um processo adaptativo, no qual a resiliência é medida pela absorção de choques com um impacto mínimo (Cgap), ao mesmo tempo em que mantém as funções essenciais num nível aceitável e, em seguida, recupera a funcionalidade num tempo razoável (t1) e a um custo razoável. Logo, um sistema bem integrado foca-se especificamente em gerir as consequências de um ataque e isolar o evento da função geral do sistema. Em seguida, o sistema adapta-se

e aumenta sua capacidade (Cf) para suportar choques futuros, reduzindo as suas vulnerabilidades e aumentando a velocidade de recuperação (ACT, 2019; Hodicky et al., 2020).

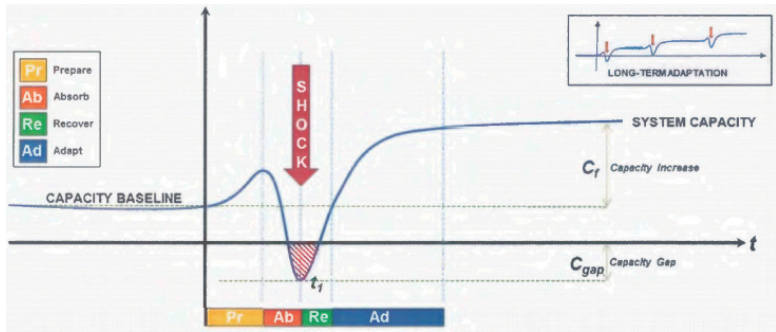


Figura 2 – Representação gráfica do ciclo da resiliência
Fonte: ACT (2019).

Tendo em conta que a OTAN depende de recursos civis e de infraestruturas, como caminhos-de-ferro, portos, aeroportos e redes de energia, para apoiar o movimento rápido e eficaz, bem como a sustentação de suas forças militares, e que esses ativos são vulneráveis a ataques externos e a interrupções internas, a *Civil Preparedness* (CP) pressupõe que as funções básicas do governo podem continuar durante emergências ou desastres, em tempos de paz ou em períodos de crise, garantindo que o setor civil, nas nações aliadas, está pronto para fornecer apoio a uma operação militar da OTAN (NATO, 2021a). A CP está intrínseca ao conceito militar de resiliência colaborativa, consubstanciado na capacidade da OTAN para conduzir e sustentar operações, preparando-se, absorvendo, recuperando e adaptando-se à surpresa ou choque estratégico (de ataques híbridos e/ou terroristas) por meio de estruturas, sistemas e processos harmonizados e resilientes, possibilitados pela cooperação persistente entre as vertentes pública, militar e partes interessadas privadas (NATO, 2019). Assim, na Cimeira de Varsóvia, foi estabelecido o compromisso de incrementar a resiliência individual e coletiva, sendo a CP considerada como um pilar central da resiliência, integrando sete requisitos chave (NATO, 2016b):

– Assegurar a governabilidade e serviços críticos governamentais;
– Resiliência do setor energético;
– Capacidade para lidar com fluxos migratórios não controlados;

– Resiliência dos recursos alimentares e água;
– Capacidade para lidar com catástrofes com baixas numerosas;
– Resiliência dos sistemas de comunicações;
– Resiliência do setor de transportes.

No que concerne à CP nacional, importa destacar o estudo *Collaborative resilience: A new military capability of the Portuguese Armed Forces*, que transpõe o conceito da resiliência colaborativa da OTAN para as FFAA Portuguesas (Serôdio & Rodrigues, 2020), que também será utilizado como base para a presente investigação, dado ser único na profundidade dada à temática.

Ao nível da cooperação, importa também referir a cooperação internacional, entre OI, Estados e outras entidades, como o Hybrid CoE ou outros centros de excelência (Figura 3), para garantir a partilha de informações e possibilitar a realização de exercícios conjuntos, vertentes essenciais para o incremento da resiliência (European Commission, 2020; NATO, 2016a, 2016b; Hybrid CoE, 2021; Weissmann et al., 2021).

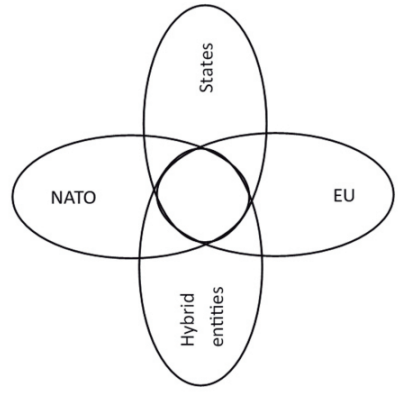


Figura 3 – Cooperação internacional
Fonte: Weissmann, Nilsson e Palmertz (2021, p. 271).

2.1.2. O domínio militar

Mantendo presente que um "investigador de Relações Internacionais é aquele que pretende ter alguma capacidade em lidar com as questões que surgem nas relações entre nações" (Tiickner, 2009. cit. por Rigueira, 2012, p. 23), é relevante perceber como o instrumento de poder militar se enquadra na estratégia de um Estado, bem como definir a sua abrangência. Neste âmbito, importa referir que no

Sistema Internacional, e inerentes relações, operam atores estatais e não-estatais, como sejam OI governamentais ou não governamentais e entidades privadas (Atama, 2003; Ikenberry, 2011; Reynolds, 1979).

O instrumento de poder militar é o uso da força ou a ameaça de usar a força para atingir objetivos nacionais, sendo o poder militar a "capacidade de um Estado utilizar uma força militar para materializar a sua soberania" (Tomé, 2002, p. 39), ou seja, a soma dos sistemas de armas e equipamentos de uma nação, mão de obra treinada, organizações, doutrinas, base industrial e capacidade de sustentação, podendo o instrumento militar ser empregue aquém do combate, como por exemplo em exercícios com aliados ou demonstrações de força (Mastapeter, 2008; US Marine Corps, 1997). O poder militar é assim a forma como os Estados geram violência organizada para uso no campo de batalha ou como parte de estratégias coercitivas (Horowitz, 2010; Smith, 2006), sendo que a capacidade de projetar poder militar no exterior tem permitido, historicamente, às nações influenciar os eventos internacionais em seu favor e encerrar conflitos e disputas, militares ou não, em termos favoráveis aos interesses nacionais (Earle, Craig, & Gilbert, 1943). Considera-se assim que o poder militar é decisivo para as Relações Internacionais e para o equilíbrio global de poder, sendo a difusão do poder militar imperativa para a segurança dos Estados e impulsionada pelas suas perceções das ameaças (Posen, 1984; Sloan, 2002, 2008).

O instrumento de poder militar está diretamente relacionado com a estratégia, definida por Ribeiro (2009, p. 22) como "a ciência e a arte de edificar, dispor e empregar meios de coação num dado meio e tempo, para se materializarem objetivos fixados pela política, superando problemas e explorando eventualidades em ambiente de desacordo", e por Couto (2020, p. 227) como a "ciência e arte de desenvolver e utilizar as 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". Esta estratégia, ou grande estratégia, é assim, igualmente, a arte e ciência de desenvolver, aplicar e coordenar os instrumentos do poder nacional (Diplomático, Informacional, Militar e Económico – DIME) para atingir esses objetivos (US Department of Defense, 2016).

Ao nível das AH, existe a sincronização de múltiplos instrumentos de poder *(smart power*), aproveitando vulnerabilidades, fragilidades e dependências específicas nos vários domínios PMESII (Figura 4), para obter sinergia nos efeitos (MCDC, 2019, p. 15).

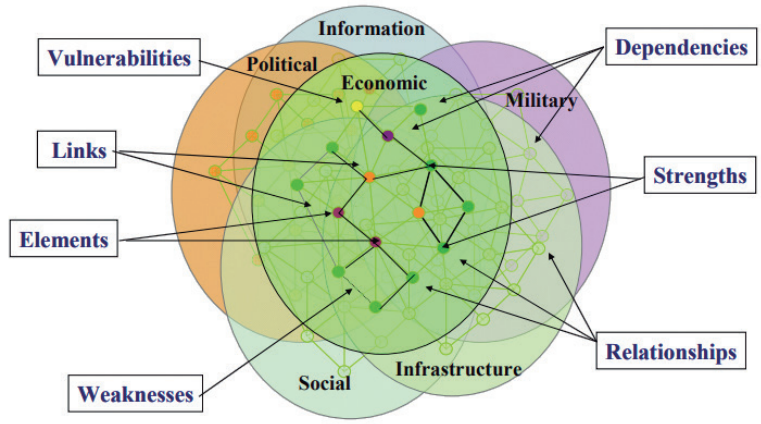


Figura 4 – Perspetiva gráfica dos domínios PMESII
Fonte: NATO (2007).

Especificamente ao nível do DM, consubstanciado nas FFAA e conjunto de capacidades militares (Martin, Dan-Suteu, & Vella, 2019, p. 11), a resiliência às AH deve ser incrementada mormente em duas áreas. A primeira é a contribuição para a resiliência nacional, que deve evoluir para enfrentar ameaças cada vez mais intensas (Benbow, Bird, & Thornton, 2019; Monaghan, 2019), e a segunda é a sua própria resiliência (área estudada nesta investigação), contra ameaças que possam impedir a sua projeção ou sustentação (Haaster & Roorda, 2016; Monaghan, 2019). Devem ainda ser aplicados dois princípios: o da cooperação mais estreita entre domínios e o da cooperação mais estreita com aliados e parceiros (Monaghan, 2019).

Tendo em conta que estamos a tratar o DM, e respetivas capacidades, importa aludir ao conceito de capacidade militar, que se consubstancia em "elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais ou efeito que é necessário atingir, englobando componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade [DOTMLPII]" (Conselho de Chefes de Estado-Maior, 2014).

3. METODOLOGIA E MÉTODO

Materializando a relevância que a metodologia tem na investigação científica (Bryman, 2012; Freixo, 2018; Sarmento, 2013; Vilelas, 2009; Yin, 2018), no presente capítulo é espelhada a metodologia e método empregues.

3.1 Metodologia

A metodologia aplicada à investigação (Quadro 1), e estrutura a seguir no presente trabalho, baseiam-se nas normas em vigor no IUM, a que se aditam obras de referência ao nível da metodologia de investigação científica (Bryman, 2012; Freixo, 2018; Sarmento, 2013; Vilelas, 2009; Yin, 2018).

Quadro 1 – Metodologia da investigação

Orientação ontológica	Construtivismo
Orientação epistemológica	Interpretativa
Raciocínio	Dedutivo
Estratégia de investigação	Qualitativa
Desenho de pesquisa	Estudo de caso
Horizonte temporal	Transversal

Tendo em conta que a problemática das AH envolve atores estatais e não-estatais, bem como as respetivas interações, adotou-se uma orientação ontológica construtivista e epistemológica interpretativa, dado que os fenómenos sociais e respetivos significados estão permanentemente em constante revisão, competindo ao investigador verificar e compreender esses fenómenos e processos inerentes (Bryman, 2012).

O raciocínio utilizado é tendencialmente dedutivo, na medida em que se "parte do geral para o particular" (L. A. B. Santos et al., 2019, p. 19), nomeadamente de estudos, teorias e conceitos gerais do Hybrid CoE, MCDC, OTAN, UE e investigadores diversos, particularizados para o caso nacional. Neste processo garantiu-se a veracidade das premissas, relacionadas com raciocínio válido, para que as conclusões fossem igualmente verdadeiras (Freixo, 2018; Santos & Lima, 2019).

A estratégia utilizada é qualitativa dado existir uma "relação indissociável entre o mundo real e a subjetividade do sujeito que não é passível de ser traduzida em números" (Sousa & Baptista, 2011, p. 55), motivo pelo que a investigação se baseia em pesquisa documental e entrevistas, sendo a análise efetuada a partir dos padrões encontrados e tendo por base as experiências dos indivíduos estudados (Vilelas, 2009), nomeadamente os especialistas entrevistados.

O desenho de pesquisa consubstancia-se num estudo de caso, pela sua eficiência na investigação exaustiva de processos organizacionais (Yin, 2018),

recolhendo-se informação detalhada sobre o objeto de estudo, cujo comportamento a estudar, a resiliência, foi previamente selecionado.

3.2. Método

3.2.1. Participantes e Procedimento

O percurso metodológico decorreu em duas fases, tendo a primeira sido destinada ao esclarecimento do estado da arte e à elaboração do projeto de investigação, e a segunda à elaboração de entrevistas, resposta às QD e QC, bem como à redação do presente TII.

Com o objetivo de ampliar os conhecimentos do investigador ao máximo, na primeira fase foram contactadas diversas entidades, realizando-se diversas entrevistas exploratórias e reuniões, merecendo destaque o contacto com o Conselheiro de Embaixada Jorge Eduardo Ferreira Silva Aranda, Diretor de Serviços para os Assuntos de Segurança e Defesa, da Direção-Geral de Política Externa, e responsável pelo grupo de trabalho interministerial incumbido da redação de um documento de enquadramento nacional das AH. Foram talqualmente contactados Oficiais das FFAA integrantes da Portuguese Military Representation to NATO *and EU Military Committees* com o objetivo de esclarecer a visão destas organizações relativamente a esta temática, bem como para a obtenção de documentação. Concomitantemente foi efetuada a leitura de uma extensa bibliografia, assistindo-se ainda aos webinars, virtual events e seminários *Hybrid Threats and the use of the Cyber Domain, High Level Event on Hybrid Threats Virtual Event, The future of European Defence and the priorities of the Portuguese Presidency* e *O impacto das tecnologias disruptivas na defesa*.

No concernente à segunda fase da investigação, constituiu-se uma amostra não-probabilística intencional (Pardal & Correia, 1995, p. 34), convidando-se 15 especialistas (militares e civis), dos quais dez aceitaram participar no estudo e foram entrevistados.

3.2.2. Instrumentos de recolha de dados

Na presente investigação utilizaram-se como instrumentos de recolha de dados a entrevista e a análise documental:

– Foi efetuada uma entrevista não estruturada dirigida (L. A. B. Santos et al., 2019, pp. 83–86), com duas questões abertas centradas num assunto cada,

para aprofundar o conhecimento relativamente ao contributo das FFAA para a resiliência nacional às AH e para a sua prevenção e combate.

– Foram efetuadas nove entrevistas semiestruturadas (L. A. B. Santos et al., 2019, pp. 83–86; Sarmento, 2013, p. 34), constituídas por cinco questões. A primeira direcionada para a QD1, as segunda, terceira e quarta para a QD2, e a quinta para a QD3. Foram escolhidas entrevistas semiestruturadas de modo a permitir aos entrevistados exprimirem mais facilmente as suas opiniões, acautelando a possibilidade de o entrevistador poder solicitar esclarecimentos adicionais.
– A análise documental, baseada mormente em legislação, literatura científica e documentos oficiais do Hybrid CoE, MCDC, OTAN e UE, permitiu não só servir de base para a realização das entrevistas, mas também para efetuar cruzamento e complementaridade de dados.

3.2.3. Técnicas de tratamento de dados

A análise das entrevistas foi efetuada de acordo com a metodologia proposta por Sarmento (2013, pp. 29–63), pretendendo-se não só "descrever as situações, mas também interpretar o sentido em que foi dito" (Guerra, 2006, p. 69). À entrevista não estruturada foi efetuada uma análise qualitativa e às semiestruturadas análise categorial. A análise categorial foi efetuada seguindo os seguintes passos para cada uma das questões:

– Constituição das unidades de contexto;

– Determinação das unidades de registo;

– Elaboração do quadro matriz das unidades de contexto e de registo;

– Elaboração do quadro de análise de conteúdo, por categorias e subcategorias, com a quantificação das unidades de registo, de acordo com as unidades de enumeração;

– Produção de conclusões, "evidenciando os resultados superiores a 50% e enfatizando os resultados maiores ou iguais a 80%" (Sarmento, 2013, p. 66).

Foram utilizados os programas *Microsoft Excel*, *Microsoft Power Business Intelligence* e *Microsoft Word*, para apoio à organização e estruturação das unidades de contexto, determinação e quantificação das unidades de registo, e apresentação gráfica dos resultados.

4. APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

No presente capítulo é efetuada a apresentação dos dados e a discussão dos resultados da investigação, estando dividida em quatro pontos. No primeiro são abordadas as ferramentas das AH que afetam o DM, dando-se resposta à primeira QD. No segundo alude-se à resiliência do DM nacional face às AH, respondendo-se à segunda QD. No terceiro efetua-se a discussão dos indicadores de resiliência face às AH, para dar resposta à terceira QD. Como apogeu do capítulo, é efetuada uma síntese conclusiva onde se responde à QC da presente investigação.

4.1. Afetação das ferramentas das ameaças híbridas ao domínio militar

Partindo da lista de 40 ferramentas das AH, elencadas por Giannopoulos et al. (2021, pp. 33–35) no relatório *The landscape of hybrid threats: A conceptual model*, elaborado no seio dos *Joint Research Centre*, serviço de conhecimento e ciência da Comissão Europeia e Hybrid CoE, foram apresentadas aos entrevistados as 17 identificadas como afetando diretamente o DM, cumprindo enfatizar que todos os especialistas concordaram que estas podem afetar o DM de um Estado, independentemente da origem ser do domínio dos atores estatais ou não estatais. É, no entanto, importante salvaguardar que estas ferramentas apenas se tornam efetivamente AH "quando se efetiva mais do que uma ao mesmo tempo […] em mais do que um domínio" (N. C. B. L. Pires, *op. cit.*), tornando-se ações coordenadas e sincronizadas.

4.1.1. Afetação ao domínio militar nacional

Passando especificamente para o caso nacional, e questionados os entrevistados relativamente à concordância da possibilidade de afetação destas ferramentas das AH ao DM nacional, evidencia-se que obtiveram mais de 50% de concordância:

– Investimento estrangeiro direto;
– Proliferação de armamento;
– Operações convencionais e não convencionais das FFAA;
– Organizações paramilitares (*proxies*);
– Explorar limites, lacunas e incertezas na legislação;

– Aproveitamento das regras legais, de processos, instituições e argumentos;
– Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite).

Das respostas enfatizam-se com grau de concordância superior a 80 %:

– Operações físicas contra infraestruturas;
– Criação e exploração da dependência de infraestruturas (incluindo dependência civil-militar);
– Espionagem *cyber*;
– Operações *cyber*;
– Violação do espaço aéreo;
– Violação do espaço marítimo;
– Exercícios militares;
– Recolha de informações;
– Operações clandestinas;
– Infiltração.

Importa anotar que as AH descartadas por alguns dos entrevistados, foram-no principalmente pela baixa probabilidade de Portugal ser afetado por estas, dada a sua posição, o que está em sintonia com o referido por Duarte (2020, cit. por Alves, 2020, p. 29) relativamente a que "Portugal não tem sido alvo significativo de ataques híbridos cinéticos devido à sua dimensão geopolítica".

A verificação relativamente a se no período da abrangência do estudo o DM nacional foi afetado por alguma destas ferramentas não foi possível, dada a não disponibilização dos dados por motivos de classificação de segurança, tendo apenas sido possível consultar através de estudos e fontes abertas a afetação parcial destas a Portugal, fundamentalmente ao nível da espionagem/operações cyber (Duarte, 2020; Público, 2021) e violação do espaço aéreo (Diário de Notícias, 2014).

Das respostas dos especialistas foram ainda elencadas outras possíveis ferramentas, ainda que com baixo nível de concordância, nomeadamente: (i) Operações de informação que sustentam as *Narrative Led Operations* e *Weaponizing* dos Órgãos de Comunicação Social (OCS); (ii) Criação ou exploração de dependências económicas; (iii) Explorar vulnerabilidades da Administração Pública; (iv) Minar a economia e (v) Promover e explorar a corrupção.

Relativamente às operações de informação que sustentam as *Narrative Led Operations* e *Weaponizing* dos OCS, esta é uma ferramenta ao alcance de muitos atores (Nissen, 2015) e de facto são identificadas por Duarte (2020) como tendo

estado presentes em Portugal em 2017/2018. Não obstante e dado que Giannopoulos et al. (2021) apresentam os domínios político, social e informacional como os diretamente afetados, não fica provado que afetem diretamente o DM podendo, no entanto, afetar indiretamente através de outro domínio. O anteriormente exposto é talqualmente válido para a criação ou exploração de dependências económicas e minar a economia que são identificadas por Duarte (2020, p. 446) como tendo estado presentes em Portugal em 2017/2018 mas são apresentadas por Giannopoulos et al. (2021) como afetando diretamente os domínios político e económico. No que concerne à exploração das vulnerabilidades da administração pública, afetam diretamente os domínios político e social, e a promoção e exploração da corrupção primariamente os domínios económico e social. A afetação indireta de um domínio pode ser visualizada na Figura 5.

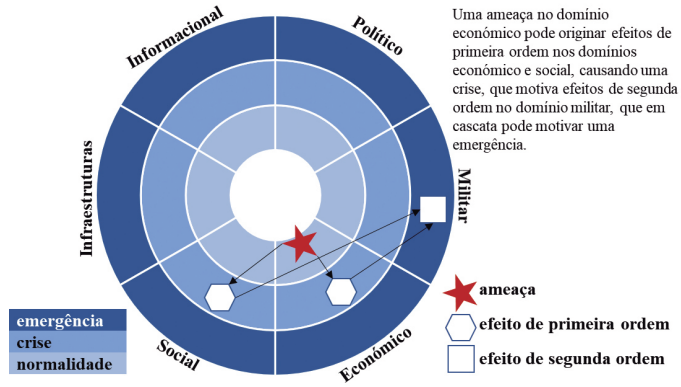


Figura 5 – Visualização da afetação indireta das AH
Fonte: Adaptado de MCDC (2017, p. 14).

4.1.2. Resposta à primeira questão derivada

Destarte, e em resposta à QD "Quais as ferramentas das AH que podem afetar o DM nacional?", identificam-se como passíveis de afetarem diretamente as seguintes:

– Operações físicas contra infraestruturas;
– Criação e exploração da dependência de infraestruturas (incluindo dependência civil-militar);
– Investimento estrangeiro direto;
– Espionagem *cyber*;

– Operações *cyber*;
– Violação do espaço aéreo;
– Violação do espaço marítimo;
– Proliferação de armamento;
– Operações convencionais e não convencionais das FFAA;
– Organizações paramilitares (*proxies*);
– Exercícios militares;
– Explorar limites, lacunas e incertezas na legislação;
– Aproveitamento das regras legais, de processos, instituições e argumentos;
– Recolha de informações;
– Operações clandestinas;
– Infiltração;
– Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite).

4.2. Resiliência do domínio militar nacional face às ameaças híbridas

Partindo da conjetura que a resiliência do DM nacional não se encerra em si mesmo, em virtude de este estar diretamente condicionado pela inserção nas OI, OTAN e UE, bem como pela garantia do setor civil estar pronto para fornecer apoio a uma operação militar, tanto em tempo de paz como no decorrer de crises (CP), será analisada a resiliência do DM nas variáveis da cooperação internacional, da CP e das capacidades militares, a que se seguirá a resposta à segunda QD.

4.2.1. Cooperação internacional

Na questão da cooperação internacional, pretendia-se analisar a partilha de informação, bem como a participação em exercícios. Neste âmbito, cumpre enfatizar que 89% dos entrevistados consideram existir partilha de informações com organismos internacionais relativamente às AH e/ou às suas ferramentas. Cumpre talqualmente evidenciar que 78% consideram a existência de participação em exercícios internacionais com presença da temática das AH e/ou suas ferramentas.

No que à troca de informações, a OTAN reconhece que construir uma rede robusta de partilha de informações é crítica para rastrear e superar estratégias híbridas, dado que o conhecimento local e regional de cada Estado contribui não apenas para melhorar a compreensão da política geoestratégica regional,

mas também das atividades da vida real no terreno (Meyer, 2017, pp. 15–16). Neste seguimento, os entrevistados realçam que enquanto membro da OTAN e UE, Portugal por inerência já faz parte de uma rede de partilha de informação, nomeadamente no DM. Neste âmbito, e apesar da referência à necessidade de incremento, é referida troca de informações com as seguintes entidades: (i) Grupo de Amigos da Presidência para Combate às AH[44]; HFC; Hybrid CoE e NATO *Intelligence Fusion Center* (NIFC)[45].

Relativamente à participação em exercícios conjuntos e combinados, cuja troca de experiências é considerada valiosa, há a considerar que os exercícios começam e tendem a integrar cenários híbridos, sendo considerado que a participação nacional logrará em ser incrementada para além dos militares que atendem por inerência de estarem em cargos na estrutura das OI, naquele momento.

4.2.2 *Civil Preparedness*

No contexto nacional, e de acordo com o Decreto-Lei n.o 45/2019, de 01 de abril, a CP integra-se no Planeamento Civil de Emergência (PCE), que se encontra à responsabilidade da Autoridade Nacional de Emergência e Proteção Civil (ANEPC), em fase de desenvolvimento e como tal pouco definido (Oliveira, 2020, cit. por Serôdio & Rodrigues, 2020, p. 145). A ANEPC absorve assim as competências do extinto Conselho Nacional de Planeamento Civil de Emergência.

Derivado do facto explanado, evidencia-se que 56% dos entrevistados apenas refere que esta temática se encontra à responsabilidade da ANEPC, não tecendo comentários relativamente aos sete requisitos chave da OTAN para a CP, considerada para a Aliança Atlântica como um pilar central da resiliência. Relativamente a esta temática, três entrevistados exaltam a importância do PCE e um revela que se encontra em desenvolvimento o levantamento das infraestruturas críticas.

Considerando que o PCE é transversal às diversas áreas governativas do Estado, através do Decreto-Lei n.o 43/2020, de 21 de julho, é estabelecido o Sistema Nacional de Planeamento Civil de Emergência (SNPCE), que "visa garantir a organização e preparação dos setores estratégicos do Estado para fazer face a

[44] Grupo de análise e reflexão relativamente às AH.
[45] O NIFC tem como missão fornecer ao *Supreme Allied Commander Europe e Allied Command Operations* informações oportunas, relevantes e precisas para apoiar o planeamento e a execução das operações da OTAN e permitir a dissuasão e defesa da área euro-atlântica (NIFC, 2021).

situações de crise". De acordo com este Decreto-Lei, o PCE coordena capacidades não pertencentes às FFAA, podendo as FFAA participar nas ações do SNPCE.

Relativamente ao estado de desenvolvimento dos sete requisitos chave da OTAN relativos à CP, não foi possível obter esclarecimentos substanciais por parte da ANEPC ou outras entidades, dado tratar-se de matéria classificada.

4.2.3. Resiliência das capacidades militares

No DM importa investir em capacidades (Jaeski, 2017, p. 12), o que motivou o propósito de analisar o estado de implementação da resiliência às AH nas capacidades militares, tendo os entrevistados sido questionados relativamente ao contributo das componentes DOTMLPII para a supramencionada resiliência.

Relativamente à componente doutrina, evidencia-se que 56% dos entrevistados consideram que a doutrina existente contribui para a resiliência às AH, sendo de enfatizar que 89% consideram que esta doutrina existe apenas parcialmente para algumas das ferramentas das AH. Considera-se que a doutrina existente, apesar de contribuir para esta resiliência, não se encontra agregada, nem foi encontrada doutrina específica para as AH, podendo esta matéria ser incorporada, nomeadamente ao nível da coordenação com entidades civis.

No que concerne à componente organização, a maioria dos entrevistados referiu desconhecer a existência de órgãos/elementos com responsabilidades específicas relativamente às AH e à resiliência a estas, tendo 22% atestado a sua inexistência. De facto, não foi encontrado nenhum órgão que no descritivo das suas incumbências tivesse a temática das AH, existindo no entanto elementos que investigam a temática e participam em grupos de trabalho, bem como órgãos, como por exemplo o Centro de Informações e Segurança Militares (CISMIL)[46] (R. J. R. P. Santos, 2012), que por inerência têm incumbências ao nível das AH.

Aludindo ao treino, cumpre evidenciar que 67% dos entrevistados consideram que o treino efetuado contribui indiretamente para a resiliência às AH, na medida em que o treino militar por inerência potencia a resiliência, aludindo os entrevistados a algumas áreas do treino que estão vocacionadas para ferramentas das AH, como por exemplo ao nível da ciberdefesa, cibersegurança e contrainformação. Consideram ainda que existe dificuldade ao nível das FFAA em

[46] O CISMIL "tem por missão assegurar a produção de informações necessárias ao cumprimento das missões das [FFAA] e à garantia da segurança militar" (Decreto-Lei n.o 184/2014, de 29 de dezembro).

criar exercícios com a abrangência necessária para o treino relativo às AH.

No que se refere ao material, importava perceber da existência de equipamentos destinados a laborar com estas ameaças, tendo 56% atestado a sua inexistência e os restantes manifestado desconhecimento ou que apenas contribuiriam indiretamente, não sendo esse o seu propósito.

No concernente à liderança, importa evidenciar que 78% dos entrevistados atestam a inexistência de uma estratégia militar relativa às AH, sendo um dos motivos apontados a inexistência dessa estratégia a nível nacional. Não obstante, é referido que existe consciencialização e preocupação ao nível das chefias relativamente a este assunto.

Passando para a componente do pessoal, e assumindo a formação um peso substancial nesta componente, 67% dos entrevistados evidenciam que é reduzida, começando a existir a preocupação de abordar as AH em cursos de formação inicial e de progressão na carreira, coexistindo a participação em seminários e *webinars*.

No que alude às infraestruturas (sistemas de energia, sistemas de comunicações, sistemas de transporte, abastecimentos, etc.) e à resiliência destas, por exemplo através da existência de sistemas de reserva, 67% dos entrevistados evidenciam a sua reduzida resiliência, referindo inclusive a existência de uma cascata de interdependências a este nível. A resiliência existente é apontada mais para boas práticas, que se constituem como apanágio nas FFAA, do que para uma efetiva preparação desta área.

Relativamente à interoperabilidade, tanto de procedimentos, como de sistemas, é de enfatizar que a totalidade dos entrevistados consideram que internamente nas FFAA é limitada, estando a ser trilhado o caminho no sentido de a aumentar. Já no caso da interoperabilidade das FFAA com organismos civis, o cenário é mencionado como sendo mais preocupante.

4.2.4 Resposta à segunda questão derivada

No seguimento do aclarado e respondendo à QD "Qual o estado da implementação da resiliência face às AH no DM nacional?", importa referir que:

– Ao nível da cooperação internacional existe partilha de informações com organismos internacionais, nomeadamente com o Grupo de Amigos da Presidência para Combate às AH, HFC, Hybrid CoE e NIFC, bem como a participação, ainda que reduzida, em exercícios internacionais. Estes factos contribuem para a resiliência face às AH, havendo espaço para incremento e melhoria.

– Relativamente à CP, o PCE encontra-se à responsabilidade da ANEPC, tendo sido criado em 2020 o SNPCE. Apesar da importância desta área, não foi possível averiguar o real estado de desenvolvimento relativamente à implementação dos sete requisitos chave da OTAN, nem o seu atual contributo para a resiliência face às AH.
– No que alude às capacidades militares e às suas componentes DOTMLPII, estas contribuem na sua maioria para a resiliência às AH, ainda que indiretamente, dada a inexistência de uma estratégia militar para esta área e/ou órgãos/elementos especificamente responsáveis por ela.

4.3 Indicadores de resiliência face às ameaças híbridas

4.3.1 Cooperação internacional

Das entrevistas e debate realizados, e relativamente à cooperação internacional, evidenciam-se como indicadores:

– Partilha de informações com organismos internacionais relativamente às AH e às suas ferramentas, com 78% de concordância, sendo que atentando à teorização de Weissmann et al. (2021, p. 271) importa dividir este indicador em três, especificando OTAN, UE e organismos internacionais específicos para as AH.
– Participação em exercícios internacionais com presença da temática das AH e/ou suas ferramentas, com 56% de concordância.

4.3.2 *Civil Preparedness*

No que concerne à CP, ficou claro que os indicadores devem surgir dos sete requisitos chave da OTAN, que receberam entre 78 e 89% de concordância. Ainda assim, considera-se que estes requisitos são demasiado abrangentes para se constituíram como indicadores, pelo que deve ser consultado o *Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria* (North Atlantic Council [NAC], 2020) para se obterem os indicadores[47].

[47] Tendo em conta a quantidade de indicadores, não é praticável que sejam introduzidos no presente TII.

4.3.3 Capacidades militares

Relativamente às componentes das capacidades militares, evidenciam-se como indicadores (com grau de concordância entre 67 e 78%):

- Existência de doutrina relativa às AH e suas ferramentas;
- Existência de órgãos/elementos com responsabilidades específicas no âmbito das AH e suas ferramentas – tendo em conta a adaptação do ciclo da resiliência, considera-se que deve ser adicionada a existência de órgãos/elementos com responsabilidades específicas no âmbito das lições aprendidas;
- Existência de treino relativamente às AH e suas ferramentas;
- Existência de equipamentos adequados para lidar com as AH e suas ferramentas;
- Existência de estratégia militar relativa às AH e suas ferramentas;
- Existência de formação relativa às AH e suas ferramentas;
- Resiliência das infraestruturas às AH e suas ferramentas – considera-se que esta resiliência deve ser garantida através de um plano de resiliência das infraestruturas críticas e da existência de sistemas de *backup*;
- Existência de interoperabilidade nos sistemas das FFAA e com organismos civis.

No referente às componentes das capacidades militares, não foi possível especificar mais os indicadores, através de documentação específica, dado que "este assunto é classificado, o que limita o que pode ser partilhado" (R. M. C. Guerreiro, *email*, 05 de maio de 2021).

Surge ainda como indicador, de dimensão nacional e com concordância de 78%, a existência de uma estratégia nacional relativa às AH. Esta estratégia é considerada importante para que sejam delineadas as estratégias e documentação dos vários domínios.

4.3.4 Resposta à terceira questão derivada

No seguimento do referido e respondendo à QD "Quais os indicadores de resiliência face às AH, no DM, aplicáveis à realidade nacional?", espelham-se os seguintes:

- Partilha de informações relativas às AH com a OTAN;
- Partilha de informações relativas às AH com a UE;

– Partilha de informações relativas às AH com organismos internacionais específicos;
– Participação em exercícios internacionais com cenário de AH;
– Existência de uma estratégia nacional relativa às AH;
– Indicadores do *Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria* (NAC, 2020) relativamente ao PCE (CP);
– Existência de doutrina relativa às AH;
– Existência de doutrina que abranja as ferramentas das AH;
– Existência de órgãos/elementos com responsabilidades específicas no âmbito das AH;
– Existência de órgãos/elementos com responsabilidades específicas no âmbito das lições aprendidas;
– Existência de treino relativamente às AH e suas ferramentas;
– Existência de equipamentos adequados para lidar com as AH e suas ferramentas;
– Existência de estratégia militar relativa às AH e suas ferramentas;
– Existência de formação relativa às AH e suas ferramentas;
– Existência de um plano de resiliência das infraestruturas críticas;
– Existência de sistemas de *backup* nas infraestruturas;
– Existência de interoperabilidade nos sistemas das FFAA;
– Existência de interoperabilidade entre os sistemas das FFAA e os dos organismos civis.

4.4 Síntese conclusiva

No seguimento da resposta às QD, cumpre responder à QC "Quais as variáveis e indicadores de resiliência nacional face às AH, no DM?", tendo para isso sido elaborado o Quadro 2.

Quadro 2 – Variáveis e indicadores de resiliência nacional face às AH, no DM

Variáveis	Indicadores
Cooperação internacional (dimensão OTAN e UE)	
Partilha de informação	Partilha de informações relativas às AH com a OTAN
	Partilha de informações relativas às AH com a UE
	Partilha de informações relativas às AH com organismos internacionais específicos
Participação em exercícios	Participação em exercícios internacionais com cenário de AH
Estratégia global (dimensão nacional)	
Estratégia	Existência de uma estratégia nacional relativa às AH
PCE (dimensão nacional)	
Continuidade da capacidade governativa	Indicadores no Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria (NAC, 2020)
Resiliência do setor energético	
Fluxos migratórios não controlados	
Resiliência dos recursos alimentares e água	
Lidar com catástrofes com baixas numerosas	
Resiliência dos sistemas de comunicações	
Resiliência do setor de transportes	
Capacidades militares (dimensão FFAA)	
Doutrina	Existência de doutrina relativa às AH
	Existência de doutrina que abranja as ferramentas das AH
Organização	Existência de órgãos/elementos com responsabilidades específicas no âmbito das AH
	Existência de órgãos/elementos com responsabilidades específicas no âmbito das lições aprendidas
Treino	Existência de treino relativamente às AH e suas ferramentas
Material	Existência de equipamentos adequados para lidar com as AH e suas ferramentas
Liderança	Existência de estratégia militar relativa às AH e suas ferramentas
Pessoal	Existência de formação relativa às AH e suas ferramentas
Infraestruturas	Existência de um plano de resiliência das infraestruturas críticas
	Existência de sistemas de backup
Interoperabilidade	Existência de interoperabilidade nos sistemas das FFAA
	Existência de interoperabilidade entre os sistemas das FFAA e os dos organismos civis

5. CONCLUSÕES

Não obstante as mudanças no modo de fazer a guerra terem sido uma constante ao longo da história, com mudanças ao nível das estratégias, táticas, ameaças e ferramentas tecnológicas empregues, na atualidade os atores estatais e não estatais empregam táticas híbridas, tornando o ambiente de segurança atual cada vez mais complexo e ambíguo. As ameaças atuam assim na "*gray zone*", pela combinação "híbrida" de instrumentos militares e não militares, dificultando a consciência situacional e a tomada de decisão, e aproveitando vulnerabilidades, fragilidades e dependências específicas nos vários domínios PMESII.

Com a anexação da Crimeia, em 2014, as AH passaram a fazer parte do léxico do contexto político, asseverando a premência dos Estados estarem prontos para as contrariar, com implicações na inerente necessidade de incremento da resiliência. As AH reforçariam talqualmente a ligação entre a OTAN e a UE, que enfrentavam desafios sem precedentes, firmando uma parceria estratégica no combate às AH, criando o Hybrid CoE e reforçando a partilha de informações. A atitude ativa nesta área almejava incrementar a resiliência, promover a comunicação estratégica e combater a desinformação.

Portugal, ciente da importância desta temática, adere ao Hybrid CoE, em dezembro de 2019, estando presentemente a ser diligenciada no Ministério dos Negócios Estrangeiros a elaboração de um documento de enquadramento nacional das AH, orientado segundo uma abordagem *all of governmen*t.

Neste seguimento, e considerando que a resposta às AH passa por incrementar a resiliência, em termos metodológicos e com o objetivo de propor variáveis e indicadores de resiliência nacional face às AH, no DM, o investigador efetuou um estudo de caso, colocando-se sob uma orientação ontológica construtivista e epistemológica interpretativa, utilizando raciocínio tendencialmente dedutivo, numa estratégia qualitativa.

Com o objetivo de ampliar os conhecimentos do investigador ao máximo, foram contactadas diversas entidades, realizando-se diversas entrevistas exploratórias e reuniões. Concomitantemente, foi efetuada a leitura de uma extensa bibliografia, assistindo-se ainda a *webinars, virtual events* e seminários. Posteriormente constituiu-se uma amostra não-probabilística intencional, com dez especialistas aglutinadores de conhecimentos profundos na temática em apreço, dado o cargo em que estão colocados, as suas qualificações académicas e os trabalhos de investigação realizados. A um dos especialistas foi efetuada

uma entrevista não estruturada, para aprofundar o conhecimento relativamente ao contributo das FFAA para a resiliência nacional às ameaças híbridas, sendo analisada qualitativamente. Aos restantes nove foram efetuadas entrevistas semiestruturadas que através de uma análise categorial contribuíram para a resposta às QD. A análise documental, baseada mormente em legislação, literatura científica e documentos oficiais do Hybrid CoE, MCDC, OTAN e UE, permitiu não só servir de base para a realização das entrevistas, mas também para efetuar cruzamento e complementaridade de dados.

Como principais conclusões, foram identificadas as ferramentas das AH passíveis de afetar o DM nacional, foi analisado o estado da implementação da resiliência face às AH no DM nacional e foram propostas variáveis e indicadores de resiliência nacional face às AH, no DM.

Identificam-se como passíveis de afetarem o DM nacional as seguintes ferramentas das AH:

- Operações físicas contra infraestruturas;
- Criação e exploração da dependência de infraestruturas (incluindo dependência civil-militar);
- Investimento estrangeiro direto;
- Espionagem *cyber*;
- Operações *cyber*;
- Violação do espaço aéreo;
- Violação do espaço marítimo;
- Proliferação de armamento;
- Operações convencionais e não convencionais das FFAA;
- Organizações paramilitares (*proxies*);
- Exercícios militares;
- Explorar limites, lacunas e incertezas na legislação;
- Aproveitamento das regras legais, de processos, instituições e argumentos;
- Recolha de informações;
- Operações clandestinas;
- Infiltração;
- Operações eletrónicas (interferência e falsificação de sistemas de navegação por satélite).

No que alude ao estado de implementação da resiliência face às AH no DM nacional, ao nível da cooperação internacional existe partilha de informações com

organismos internacionais, nomeadamente com o Grupo de Amigos da Presidência para Combate às AH, HFC, Hybrid CoE e NIFC, bem como a participação, ainda que reduzida, em exercícios internacionais. Estes factos contribuem para a resiliência face às AH, havendo espaço para incremento e melhoria. Relativamente à CP, o PCE encontra-se à responsabilidade da ANEPC, tendo sido criado em 2020 o SNPCE. Apesar da importância desta área, não foi possível averiguar o real estado de desenvolvimento relativamente à implementação dos sete requisitos chave da OTAN, nem o seu atual contributo para a resiliência face às AH. No que alude às capacidades militares e às suas componentes DOTMLPII, estas contribuem na sua maioria para a resiliência às AH, ainda que indiretamente, dada a inexistência de uma estratégia militar para esta área e/ou órgãos/elementos especificamente responsáveis por ela.

Como contributo principal, a investigação permitiu propor variáveis e indicadores de resiliência nacional face às AH, no DM, no âmbito da cooperação internacional, da estratégia global, do PCE (relativo à CP) e das capacidades militares.

No âmbito da cooperação internacional há a considerar as variáveis da partilha da informação e da participação em exercícios. Relativamente à partilha de informação, consideram-se os seguintes indicadores: partilha de informações relativas às AH com a OTAN; partilha de informações relativas às AH com a UE; e partilha de informações relativas às AH com organismos internacionais específicos. No que alude à participação em exercícios, propõe-se o indicador participação em exercícios internacionais com cenário de AH.

No âmbito da estratégia global, considera-se a variável estratégia, para a qual se propõe como indicador a existência de uma estratégia nacional relativa às AH.

No âmbito do PCE, propõe-se a utilização dos indicadores presentes no *Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria*, publicação do NAC, para as variáveis: continuidade da capacidade governativa; resiliência do setor energético; fluxos migratórios não controlados; resiliência dos recursos alimentares e água; lidar com catástrofes com baixas numerosas; resiliência dos sistemas de comunicações; e resiliência do setor de transportes. Por serem demasiado extensos, não era viável a sua transcrição para o presente TII.

No âmbito das capacidades militares, foram consideradas como variáveis as componentes DOTMLPII. Relativamente à variável doutrina, propõem-se os indicadores existência de doutrina relativa às AH e existência de doutrina que abranja

as ferramentas das AH. No que se refere à variável organização, propõem-se como indicadores: existência de órgãos/elementos com responsabilidades específicas no âmbito das AH; e existência de órgãos/elementos com responsabilidades específicas no âmbito das lições aprendidas. No concernente à variável treino, considera-se o indicador existência de treino relativamente às AH e suas ferramentas. No que alude à variável material, propõe-se o indicador existência de equipamentos adequados para lidar com as AH e suas ferramentas. Relativamente à variável liderança, indica-se o indicador existência de estratégia militar relativa às AH e às suas ferramentas. No que concerne à variável pessoal, considera-se o indicador existência de formação relativa às AH e suas ferramentas. Relativamente à variável infraestruturas, prevêem-se os indicadores: existência de um plano de resiliência das infraestruturas críticas; e existência de sistemas de *backup*. Para a variável interoperabilidade propõem-se como indicadores: existência de interoperabilidade nos sistemas das FFAA; e existência de interoperabilidade entre os sistemas das FFAA e os dos organismos civis.

Não obstante os resultados alcançados, considera-se que a presente investigação teve duas limitações. A primeira consubstancia-se na inexistência de documentação nacional enquadrante relativamente às ameaças híbridas, como por exemplo uma estratégia nacional de combate às AH, o que permitiria ter um alinhamento do estudo com os objetivos estratégicos nacionais. A segunda prende-se com a decisão de efetuar um estudo não classificado, de modo que não perdesse abrangência de divulgação e, com isso, interesse académico, o que acabou por repetidamente impedir o acesso a informação classificada que detalharia áreas como a CP, alumiaria a visão da OTAN e da UE relativamente à temática e permitiria confirmar a real afetação das ferramentas das AH ao domínio militar nacional.

Vislumbra-se a importância de efetuar estudos futuros relativamente a esta temática, nomeadamente aumentar a abrangência para todos os domínios e instrumentos de poder, para se atingirem as variáveis e os indicadores de resiliência nacional às AH, que devem ser mensurados e integrados numa fórmula de resiliência nacional às AH. No seguimento das limitações apresentadas, considera-se talqualmente importante efetuar este estudo com matérias classificadas de modo que, embora perca abrangência de divulgação, ganhe plenitude de análise.

Em termos práticos e considerando não só a importância manifestada pela OTAN relativamente à CP, mas também pela transversalidade do PCE nas diversas áreas governativas do Estado, é importante que as FFAA mantenham um papel ativo no SNPCE, em estreita ligação com a ANEPC.

REFERÊNCIAS BIBLIOGRÁFICAS

Adger, N. W. (2000). Social and Ecological Resilience: Are They Related? *Progress in Human Geography, 24*(3), 347–364.

Ajdukovic, D., Kimhi, S., & Lahad, M. (2015). *Resiliency: Enhancing Coping with Crisis and Terrorism*. Amsterdam: IOS Press.

Allied Command Transformation. (2018). *Collaborative Resilience (CoRe) Concept Proposal*. Retirado de https://www.cimic-coe.org/resources/coic-2018/tt-180439-collaborative-resilience-concept-workshop-20-22-mar-18-summary-of-outcomes-nu0259.pdf.

Allied Command Transformation. (2019). *ACO Interim Direction and Guidance for Resilience through Civil Preparedness*. Merchtem: Autor.

Alves, A. J. F. M. (2020). *A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas*. (Trabalho de Investigação Individual, Curso de Promoção a Oficial General 2019-2020). Instituto Universitário Militar [IUM], Lisboa.

Atama, M. (2003). The Impact of Non-State Actors on World Politics: A Challenge to Nation-States. *Turkish Journal of International Relations, 2*(1), 42–66.

Bajarūnas, E. (2020). Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond. *European View, 19*(1), 62–70.

Balmer, G. M., Pooley, J.-A., & Cohen, L. (2014). Psychological Resilience of Western Australian Police Officers: Relationship between Resilience, Coping Style, Psychological Functioning and Demographics. *Police Practice and Research: An International Journal, 15*(4), 270–282.

Benbow, T., Bird, T., & Thornton, R. (2019). *A review of UK Defence's contribution to homeland resilience and security in light of the changing global context*. London: Defence Studies Department.

Berkes, F., & Ross, H. (2013). Community Resilience: Toward an Integrated Approach. *Society & Natural Resources, 26*(1), 5–20.

Bonanno, G. A. (2004). Loss, Trauma, and Human Resilience: Have We Underestimated the Human Capacity to Thrive After Extremely Aversive Events? *American Psychologist, 59*(1), 20–28.

Bourbeau, P. (2015). Resilience and International Politics: Premises, Debates, Agenda. *International Studies Review, 17*(3), 374–395.

Bryman, A. (2012). *Social Research Methods* (4.ª Ed.). Oxford: Oxford University Press.

Caliskan, M. (2019). Hybrid warfare through the lens of strategic theory. *Defense & Security Analysis, 35*(2), 40–58.

Community & Regional Resilience Institute. (2013). *Definitions of Community Resilience: An Analysis*. Meridian Institute. Retirado de: https://s31207.pcdn.co/wp-content/uploads/2019/08/Definitions-of-community-resilience.pdf.

Cordesman, A. H. (2003). *The Iraq War: Strategy, Tactics, and Military Lessons*. Washington, D.C.: The Center for Strategic and International Studies Press.

Couto, A. C. (2020). *Elementos de Estratégia - Apontamentos para um curso*. Volume 1. (Reedição 2020). Alfragide: LEYA.

Creveld, M. V. (1991). *The Transformation of War*. New York: The Free Press.

Curso de Promoção a Oficial General 2019-2020. (2020). *Desafios Estratégicos para Portugal no Pós-Covid-19*. Cadernos do IUM, 43. Lisboa: Instituto Universitário Militar.

Davydov, D., Stewart, R., Ritchie, K., & Chaudieu, I. (2010). Resilience and mental health. *Clinical Psychology Review, Elsevier, 30*(5), 479–495.

Decreto-Lei n.o 43/2020, de 21 de julho. (2020). *Estabelece o Sistema Nacional de Planeamento Civil de Emergência*. Diário da República, 1.a Serie, 140, 17-24. Lisboa: Presidência do Conselho de Ministros.

Decreto-Lei n.o 45/2019, de 01 de abril. (2019). *Aprova a orgânica da Autoridade Nacional de Emergência e Proteção Civil*. Diário da República, 1.a Serie, 64, 1798-1808. Lisboa: Presidência do Conselho de Ministros.

Decreto de aprovação da Constituição. (1976). *Constituição da República Portuguesa*. Diário da República, 1.a Série, 86, 738-775. Lisboa: Presidência da República.

DeGuzman, R. (2021, 15 de abril). *Resilience: Challenges Old and New* [Página *online*]. Retirado de https://www.mbpce.com/blog/resilience-challenges-old-and-new/.

Diário de Notícias. (2014, 29 de outubro). *Aviões russos intercetados junto a espaço aéreo português por F-16 da Força Aérea* [Página *online*]. Retirado de https://www.dn.pt/portugal/avioes-russos-intercetados-junto-a-espaco-aereo-portugues-por-f-16-da-forca-aerea-4209073.html.

Duarte, F. P. (2020). Non-kinetic hybrid threats in Europe – the Portuguese case study (2017-18). *Transforming Government: People, Process and Policy, 14*(3), 433–451.

Earle, E. M., Craig, G. A., & Gilbert, F. (Eds.). (1943). *Makers of Modern Strategy: Military Thought from Machiavelli to Hitler*. Princeton: Princeton University Press.

Egeland, B., Carlson, E., & Sroufe, L. A. (1993). *Resilience as Process*. *Development and Psychopathology, 5*(4), 517–528.

Elran, M. (2006). I*srael's National Resilience: The Influence of the Second Intifada on*

Israeli Society. (Memorandum no. 81). Tel Aviv: Jaffee Center for Strategic Studies.

Estado-Maior do Exército. (2015). *Normas de Gestão de Projetos no Exército*. Lisboa: Exército Português.

European Commission. (2016). *Joint Framework on countering hybrid threats a European Union response*. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=EN.

European Commission. (2018). *Joint Communication on Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats*. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0016&from=GA.

European Commission. (2020). *Report on the implementation of the 2016 Joint Framework on countering hybrid threats*. Brussels: Autor.

European Council. (2019a, 21 de junho). *A new strategic agenda for the EU 2019-2024* [Página *online*]. Retirado de https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/.

European Council. (2019b). *European Council meeting (20 June 2019) – Conclusions*. Retirado de https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf.

Fjäder, C. (2014). "The Nation-state, National Security and Resilience in the Age of Globalization. *Resilience: International Policies, Practices and Discourses, 2*(2), 114–129.

Fletcher, D., & Sarkar, M. (2013). Psychological Resilience: A Review and Critique of Definitions, Concepts, and Theory. *European Psychologist, 18*(1), 12–23.

Folke, C., Carpenter, S., Elmqvist, T., Gunderson, L. H., Holling, C. S., & Walker, B. (2002). *Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations*. *AMBIO A Journal of the Human Environment, 31*(5), 437–440.

Freixo, M. J. V. (2018). *Metodologia Científica Fundamentos Métodos e Técnicas*. 5.ª Ed. Lisboa: Instituto Piaget.

Gaillard, J.-C. (2010). Vulnerability, Capacity and Resilience: Perspectives for Climate and Development Policy. *Journal of International Development, 22*(2), 218–232.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The Landscape of Hybrid Threats: A conceptual model*. Luxembourg: Publications Office of the European Union.

Governo de Portugal. (2013). *Conceito Estratégico de Defesa Nacional*. Retirado de https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_

DocumentoLookupList/10_Conceito-Estrategico-de-Defesa-Nacional.pdf.

Greene, R. (2006). *The 33 Strategies Of War*. London: Profile Books.

Guerra, I. (2006). *Pesquisa Qualitativa e Análise de Conteúdo. Sentidos e formas de uso*. Lisboa: Princípia.

Haaster, J., & Roorda, M. (2016). The Impact of Hybrid Warfare on Traditional Operational Rationale - D-Day's Demise. *Militaire Spectator, 185*(4), 175–185.

Hodicky, J., Özkan, G., Özdemir, H., Stodola, P., Drozd, J., & Buck, W. (2020). Dynamic Modeling for Resilience Measurement: NATO Resilience Decision Support Model. *Applied Sciences, 10*(2639), 1–10.

Hoffman, F. G. (2009). Hybrid Threats: Reconceptualizing the Evolving Character of Modern Conflict. *Strategic Forum, 240*, 1–8.

Horowitz, M. C. (2010). *The Diffusion of Military Power: Causes and Consequences for International Politics*. New Jersey: Princeton University Press.

Ikenberry, G. J. (2011). The Future of the Liberal World Order: Internationalism After America. *Foreign Affairs, 90*(3), 56–68.

Jaeski, A. (2017). What to do with hostile information campaign/propaganda? Em *Hybrid Threats: Overcoming Ambiguity, Building Resilience* 9–12. NATO Energy Security CoE Retirado de https://enseccoe.org/data/public/uploads/2017/03/ zurnalas_no11_sp_176x250mm_3mm_2.pdf.

Jomini, A. H. B. (1879). *The Art of War*. Philadelphia: J. B. Lippincott & Co.

Lusa. (2019). *Governo quer plano nacional para combater desinformação e ciberataques*. Retirado de https://www.publico.pt/2019/08/30/tecnologia/noticia/governo-quer-plano-nacional-combater-desinformacao-ciberataques-1885035.

Mälksoo, M. (2018). Countering hybrid warfare as ontological security management: the emerging practices of the EU and NATO. *European Security, 27*(3), 374–392.

Mallin, J. (1970). *Strategy for Conquest: Communist Documents on Guerrilla Warfare*. Lorida: University of Miami Press.

Martin, I., Dan-Suteu, S.-A., & Vella, G. (2019). Strategy, foresight and the military instrument of power. Em G. Calopareanu, I. Martin, I. Enache, C. Popescu, D. Ghiba, & N.-T. Lehaci (Eds.), *Technologies - Military Applications, Simulation and Resources* 9–16. Bucharest: «CAROL I» National Defence University.

Mastapeter, C. W. (2008). *The instruments of national power: achieving the strategic advantage in a changing world*. (Master's Thesis in Security Studies). Naval Postgraduate School, Monterey.

Meyer, H. (2017). A NATO Land Domain Perspective. *Em Hybrid Threats:*

Overcoming Ambiguity, Building Resilience 13–17. NATO Energy Security CoE. Retirado de https://enseccoe.org/data/public/uploads/2017/03/zurnalas_no11_sp_176x250mm_3mm_2.pdf.

Monaghan, S. (2019). Countering Hybrid Warfare So What for the Future Joint Force? *PRISM, 8*(2), 82–98.

Multinational Capability Development Campaign. (2019). *Countering Hybrid Warfare*. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf.

Nissen, T. E. (2015). *The Weaponization of Social Media – Characteristics of Contemporary Conflicts*. Copenhagen : Royal Danish Defence College.

North Atlantic Council. (2020). *Updated Baseline Requirements, Resilience Guidelines and Evaluation Criteria*. Brussels: Autor.

North Atlantic Treaty Organization. (1949). *The North Atlantic Treaty*. Washington D. C.: Autor. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf.

North Atlantic Treaty Organization. (2015, 25 de junho). *Statement by NATO Defence Ministers* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/news_121133.htm?selectedLocale=en.

North Atlantic Treaty Organization. (2016a, 06 de dezembro). *Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_138829.htm.

North Atlantic Treaty Organization. (2016b, 09 de julho). *Warsaw Summit Communiqué* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_133169.htm#hybrid.

North Atlantic Treaty Organization. (2021a, 23 de março). *Civil preparedness* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_49158.htm.

North Atlantic Treaty Organization. (2021b, 16 de março). *NATO's response to hybrid threats* [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm.

North Atlantic Treaty Organization Intelligence Fusion Center. (2021, 03 de maio). *NATO Intelligence Fusion Center* [Página *online*]. Retirado de https://web.ifc.bices.org/.

North Atlantic Treaty Organization Standardization Office. (2020a). AAP-06 *NATO Glossary of Terms and Definitions*. Brussels: Autor. Retirado de http://nso.

nato.int/nso/ZPUBLIC/_BRANCHINFO/TERMINOLOGY_PUBLIC/NON-CLASSIFIED%20NATO%20GLOSSARIES/AAP-6.PDF.

North Atlantic Treaty Organization Standardization Office. (2020b, 17 de novembro). *NATO Term The Official NATO Terminology Database* [Página *online*]. Retirado de https://nso.nato.int/natoterm/Web.mvc.

Nunes, P. V., Santos, L. C., Ralo, J., & Mendes, C. P. (2018). Defesa do Ciberespaço. Em *Contributos para uma Estratégia Nacional de Ciberdefesa* 33–46. Lisboa: Instituto de Defesa NAcional.

Padan, C., & Elran, M. (2019). *The "Gaza Envelope" Communities: A Case Study of Societal Resilience in Israel (2006–2016)*. (Memorandum No. 188). Tel Aviv: Tel Aviv University Institute for National Security Studies.

Padan, C., & Gal, R. (2020). A Multi-dimensional Matrix for Better Defining and Conceptualizing Resilience. *Connections: The Quarterly Journal, 19*(3), 33–46.

Pardal, L. A., & Correia, E. (1995). *Métodos e técnicas de investigação social*. Porto:Areal.

Parsons, M., Glavac, S., Hastings, P., Marshall, G., McGregor, J., McNeill, J., Morley, P., Reeve, I., & Stayner, R. (2016). Top-down assessment of disaster resilience: A conceptual framework using coping and adaptive capacities. *International Journal of Disaster Risk Reduction, 19*, 1–11.

Pereira, J. (2018). As ameaças híbridas - Uma abordagem conceptual no quadro da OTAN e da UE. *CEDIS Working Papers Direito, Segurança e Democracia, 60*, 1–28.

Posen, B. P. (1984). *The Sources of Military Doctrine: France, Britain, and Germany Between the World Wars*. New York: Cornell University Press.

Presidência Portuguesa do Conselho da União Europeia 2021. (2021, 16 de março). *A importância das "ameaças híbridas" à segurança, na vizinhança sul da Europa* [Página *online*]. Retirado de https://www.2021portugal.eu/pt/noticias/a-importancia-das-ameacas-hibridas-a-seguranca-na-vizinhanca-sul-da-europa/.

Público. (2021, 06 de abril). *China e Rússia suspeitas de fazerem ciberespionagem a Portugal* [Página *online*]. Retirado de https://www.publico.pt/2021/04/06/sociedade/noticia/china-russia-suspeitas-fazerem-ciberespionagem-portugal-1957275.

Reynolds, P. A. (1979). NonState Actors and International Outcomes. *British Journal of International Studies, 5*(2), 91–111.

Ribeiro, A. S. (2009). *Teoria Geral da Estratégia*. Coimbra: Edições Almedina.

Rigueira, P. (2012). Relações internacionais como disciplina. *Relações Internacionais*

(R:I), 36, 23–46.

Rühle, M., & Roberts, C. (2021). *Enlarging NATO's toolbox to counter hybrid threats*. Retirado de https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html.

Santos, R. J. R. P. (2012). *A partilha de informações em Portugal: contributo para o aperfeiçoamento do sistema*. (Trabalho de Investigação Individual, Curso de Estado-Maior Conjunto 2011/2012). Instituto de Estudos Superiores Militares [IESM], Lisboa.

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.

Serôdio, L. M. N., & Rodrigues, T. M. V. (2020). Colaborative resilience: A new military capability of the Portuguese Armed Forces. *Revista de Ciências Militares, VIII*(2), 141–167.

Sloan, E. C. (2002). *The Revolution in Military Affairs*. Canada: McGill-Queen's University Press.

Sloan, E. C. (2008). *Military Transformation and Modern Warfare*. London: Praeger Security International.

Smith, R. (2006). *The Utility of Force: The Art of War in the Modern World*. Virginia: Penguin Books.

Sousa, M. J., & Baptista, C. S. (2011). *Como fazer investigação, dissertações, teses e relatórios segundo Bolonha*. Lisboa: Lidel.

Southwick, S. M., Bonanno, G. A., Masten, A. S., Panter-Brick, C., & Yehuda, R. (2014). Resilience definitions, theory, and challenges: interdisciplinary perspectives. *European Journal of Psychotraumatology, 5*(1).

The European Centre of Excellence for Countering Hybrid Threats. (2019, 17 de dezembro). *Portugal becomes a participating state of the Hybrid CoE* [Página *online*]. Retirado de https://www.hybridcoe.fi/news/portugal-becomes-a-participating-state-of-the-hybrid-coe/.

The European Centre of Excellence for Countering Hybrid Threats. (2020, 16 de novembro). *Hybrid threats as a concept* [Página *online*]. Retirado de https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/.

The European Centre of Excellence for Countering Hybrid Threats. (2021, 13 de março). *What is Hybrid CoE* [Página *online*]. Retirado de https://www.hybridcoe.fi/who-what-and-how/.

Tomé, A. A. (2002). Poder e estratégia em ambiente de Globalização. *Mais Alto: Revista da Força Aérea Portuguesa, 336*, 36–41.

União Europeia. (2021). *Programa da Presidência Portuguesa do Conselho da União*

Europeia. Retirado de https://infoeuropa.eurocid.pt/registo/000085448/documento/0001/.

United States Army Corps of Engineers. (2020). Implementation of Resilience Principles in the Engineering & Construction Community of Practice. *Engineering and Construction Bulletin, 6*, 1–3.

United States Department of Defense. (2016). *Department of Defense Dictionary of Military and Associated Terms*. Retirado de https://fas.org/irp/doddir/dod/jp1_02.pdf.

United States Marine Corps. (1997). *MCDP 1-1 Strategy*. Washington, D.C.: Department of the Navy.

Vilelas, J. (2009). *Investigação: o Processo de Construção do Conhecimento*. Lisboa: Edições Sílabo.

Weissmann, M., Nilsson, N., & Palmertz, B. (2021). Moving out of the blizzard: Towards a comprehensive approach to hybrid threats and hybrid warfare. Em M. Weissmann, N. Nilsson, B. Palmertz, & P. Thunholm (Eds.), *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. London: I.B. Tauris.

Yin, R. K. (2018). *Case study research and applications design and methods*. (6.ª Ed.). Los Angeles: SAGE Publications Ltd.

A PREVENÇÃO E O COMBATE DE AMEAÇAS HÍBRIDAS: IDENTIFICAR INSTRUMENTOS DE MEDIDA, VARIÁVEIS E INDICADORES DE RESILIÊNCIA NACIONAIS FACE ÀS AMEAÇAS HÍBRIDAS. (ECONÓMICO)

PREVENTION AND TACKLING OF HYBRID THREATS: IDENTIFYING MEASUREMENT INSTRUMENTS, VARIABLES AND NATIONAL RESILIENCE INDICATORS AGAINST HYBRID THREATS (ECONOMOMICS)

Autor
MAJ ENG Nuno Fernando Ramos Hingá Fernandes

Orientador
TCOR ADM Domingos Manuel Lameira Lopes

1. INTRODUÇÃO

O presente Trabalho de Investigação Individual (TII) foi elaborado no âmbito da Unidade Curricular Trabalho Final de Curso do Curso de Estado-Maior Conjunto (CEMC), estando enquadrado no domínio de investigação dos Elementos Nucleares das Ciências Militares, na área do Estudo das Crises e dos Conflitos Armados e subárea do Planeamento Estratégico Militar (Centro de Investigação e Desenvolvimento do Instituto Universitário Militar [CIDIUM], 2019).

O mesmo faz parte de um conjunto de quatro TII, que se debruçam sobre a temática das Ameaças Híbridas (AH), mas que têm como foco, os diferentes instrumentos de poder, designadamente o instrumento de poder militar, diplomático, informacional e económico.

Quando se pensa em Guerra, pensamos em armas, operações militares, perdas, e revoluções políticas, mas estes são apenas os aspetos visíveis da Guerra. O início do século XXI marcou a mudança na configuração dos conflitos, para uma forma muito menos violenta, menos convencional, mais seletiva e com características que não podem ser diretamente observadas.

Nesse contexto, a União Europeia (UE) e a Organização do Tratado do Atlântico Norte (OTAN) têm vindo a ser confrontadas com um número significativo de novas ameaças que designam por AH.

Em oposição ao conceito de Guerra Híbrida (GH), que se concentra no instrumento de poder militar, as AH consistem num orquestrar de ações

sincronizadas usando múltiplas ferramentas, para atingir as vulnerabilidades das sociedades e dos Estados, nos diversos instrumentos de poder[48]. Deliberadamente exploram a ambiguidade e a não-linearidade para evitar a deteção, sendo apenas detetadas quando já estão perfeitamente inveteradas e capazes de infligir danos (Cullen & Reichborn-Kjennerud, 2017, p. 10).

A UE e a OTAN estão por isso envolvidas como parte de uma abordagem abrangente à segurança, trabalhando de forma estratégica, coordenada e coerente em todos os campos de ação relevantes para prevenir os efeitos dessas ameaças. Além disso, para enfrentar esses desafios, os Estados-Membros são incentivados a concentrarem-se na preparação do setor civil, para fazer face aos ataques conduzidos por ameaças desta tipologia (Comissão Europeia [CE], 2020).

Tendo as AH capacidade para residir no anonimato e perpetrar ações simultâneas nos diferentes instrumentos de poder, é difícil controlar a grande amplitude de vulnerabilidades intrínsecas de cada Estado. Assim, como defendem Linkov, Baiardi, Florin, Greer, Lambert e Trump (2019), o foco do combate às AH deve ser a resiliência dos diversos instrumentos de poder, prevalecendo a necessidade de aptidão para recuperar, regressando ao seu estado inicial.

Levando isso em consideração, num processo liderado pela CE, os Estados-Membros foram convidados a considerar a criação de um Centro de Excelência para a luta contra as AH (Hybrid CoE), que se concentraria no desenvolvimento da resiliência e na construção de capacidades para combater as AH através de pesquisa, treino e exercícios com participantes intersectoriais. O centro também fortaleceria o alinhamento entre os setores privado e público, civil e militar, bem como académico (CE, 2016).

A adesão portuguesa ao Hybrid CoE e a presente redação do documento de enquadramento nacional das AH, orientado segundo uma abordagem global de segurança que abrange todas as administrações públicas e toda a sociedade, são evidências da procura de uma estratégia nacional capaz, eficiente e, desejavelmente, dissuasora.

Geralmente os efeitos de uma ação que ocorre num domínio acabam por se propagar em cascata, desestabilizando outros instrumentos de poder. Atendendo

[48] Cullen e Reichborn-Kjennerud (2017) classificam as vulnerabilidades de um Estado segundo os instrumentos de poder político, militar, económico, social, informacional e de infraestruturas (PMESII). Giannopoulos, Smith e Theocharidou (2021) classificam-nas em 13 domínios diferentes. Para efeitos do presente trabalho considera-se que os dois termos são sinónimos, dizendo respeito aos setores de um país onde existem vulnerabilidades.

a isso e à sua centralidade, o sistema económico dos Estados-Membros da UE é um dos domínios mais atrativos para a atuação das AH. Subverter a credibilidade do setor económico ou perturbar as suas dinâmicas, pode criar o caos dentro do próprio Estado ou mesmo no seio da UE, devido às interdependências financeiras, monetárias e de mercado único (Aho, Midões, & Šnore, 2020).

Neste contexto, julga-se pertinente quantificar a capacidade de resiliência da economia nacional face a estas ameaças, oferecendo aos decisores políticos e partes interessadas um instrumento prático e inovador, que possa ser usado de forma proativa, para edificar a resiliência do sistema económico, em oposição à abordagem geralmente reativa de limitação de danos, quando a agressão já se verificou.

Resulta assim, como objeto de estudo do presente trabalho a resiliência da economia nacional face a AH. Não obstante, a abrangência e a importância da temática, a natureza do presente trabalho e a dimensão que lhe foi imposta obrigam à delimitação da pesquisa na dimensão espacial, de conteúdo e temporal (Sampieri, 2003, cit. por Santos & Lima, 2019). Segundo a dimensão espacial, a pesquisa incide sobre Portugal, uma vez que o objeto de investigação é a resiliência da economia do país, e sobre os restantes países membros da UE, uma vez que esta se trata de uma organização internacional de cooperação económica, e como tal as economias dos Estados são, em certa medida, indissociáveis umas das outras. Em termos de conteúdo, a pesquisa está circunscrita aos aspetos que contribuem para a resiliência da economia nacional, face às potenciais alterações induzidas por AH provenientes exclusivamente de atores Estado. Na dimensão temporal está delimitada à atualidade.

O objetivo geral (OG) do presente trabalho é avaliar a resiliência do domínio económico nacional face as AH, para apoiar a tomada de decisão na criação de condições de resposta efetiva a estas ameaças. Para a concretização do OG, concorreram os seguintes objetivos específicos (OE):

– OE1: Classificar as ameaças passiveis de afetar a economia de um Estado;

– OE2: Selecionar indicadores de resiliência no instrumento de poder económico;

– OE3: Criar um modelo analítico para avaliar a resiliência da componente económica nacional.

Quanto ao problema da investigação, que se constitui o elemento central deste trabalho, dele derivando todos os outros elementos do processo, o mesmo assentará na seguinte questão central: Como é avaliada a resiliência do instrumento de poder económico nacional?

Este trabalho encontra-se organizado em cinco capítulos. No que diz respeito ao corpo do trabalho, após a introdução, no segundo capítulo são apresentados os resultados da revisão da literatura alusiva à temática e apresentada, no terceiro, a metodologia e o método seguidos na investigação. No quarto capítulo é efetuada (i) uma classificação das AH, identificando ferramentas utilizadas para conduzir os ataques; os principais atores e os seus objetivos; (ii) as vulnerabilidades do domínio económico que podem ser exploradas; (iii) e projetam-se as variáveis e os indicadores, para a conceção de um modelo de avaliação do domínio económico. Por fim, no último capítulo, reservado às conclusões, é feita uma revisão do procedimento metodológico, uma sumula dos resultados obtidos, descritas as limitações da investigação e são propostos estudos futuros no âmbito da mesma temática.

2. ENQUADRAMENTO TEÓRICO CONCEPTUAL

No presente capítulo é apresentada a informação que decorre do processo de revisão da literatura e é detalhada a metodologia seguida na investigação.

Os termos GH e AH são por vezes usados indistintamente, sendo essa uma das razões pelas quais os conceitos podem parecer confusos. Assim, para estabelecer uma base conceptual consistente, é importante dissipar qualquer ambiguidade entre os dois conceitos, bem distintos, ainda que relacionados, fazendo o seu enquadramento e explicação.

2.1. Guerra Híbrida

Frank Hoffman (2007) atribui os créditos da utilização do termo GH pela primeira vez ao Tenente Robert Walker, que na sua tese de doutoramento não publicada, na *Naval Post Graduate School*, definiu GH como sendo "aquela que se situa entre a Guerra não Convencional e a Guerra Convencional" (Walker, 1998, pp. 4–5).

Em 2002, o Major William Nemeth também usou a expressão para idealizar uma forma de contrariar as ações das sociedades híbridas e mistas na Tchetchénia. Definiu então GH como "[…] a guerra de guerrilha contemporânea […] que se tornou mais eficaz porque emprega tecnologia moderna e métodos modernos de mobilização" (Nemeth, 2002, p. 29).

O termo de GH apareceu posteriormente, em novembro de 2005, num artigo publicado por dois oficiais do *US Marine Corps,* o General James Mattis e o próprio Coronel Frank Hoffman (Mattis & Hoffman, 2005). O seu principal

objetivo era influenciar o debate em torno da *Quadrennial Defense Review* (QDR) de 2006, que se encontrava em preparação, e apelar à necessidade de quebrar a tendência transformacional imposta pela anterior QDR, de 2001, que estava a causar dificuldades às forças no Iraque (Durand, 2003).

O projeto de transformação pretendia dar mais enfase às novas tecnologias e à redução de forças no terreno, no entanto, a contrainsurgência estava a reganhar preponderância e a persistir nas qualidades humanas, ao invés das qualidades técnicas, o que deu uma nova voz aos adeptos das *boot on the ground* (Ucko, 2009).

Hoffman e Mattis reconheceram esse aspeto, enfatizando a nova complexidade da Guerra Moderna, que apelidaram de GH. Segundo eles, os EUA estariam, nos próximos anos, propensos a ser confrontados "simultaneamente com o colapso de um Estado falido que perdeu o controle de certas armas biológicas e balísticas, ao mesmo tempo que tinha que enfrentar uma violência gerada pelas divisões étnicas e por grupos terroristas radicais" (Mattis & Hoffman, 2005, p. 19).

O conceito permaneceu teórico até agosto de 2006, quando a campanha israelita contra o *Hezbollah* começou a tomar forma. As capacidades sofisticadas do movimento xiita libanês, sobrepunham-se às forças israelitas, divididas entre uma Força Aérea extremamente confiante na eficácia dos bombardeamentos estratégicos, e um Exército dimensionado para um conflito de baixa intensidade nos territórios da Palestina. Neste contexto, constatou-se que o espectro intermédio da conflitualidade havia sido negligenciado, a favor dos dois extremos, e que existiam atores irregulares cujas capacidades no domínio militar se equiparavam à de atores convencionais, enquanto continuavam a beneficiar das vantagens tradicionais da Guerra Irregular (Johnson, 2011).

Em resultado disso, embora do conceito de GH fosse tendencialmente encarado como potenciador da doutrina irregular, a sua interpretação rumou no sentido oposto e passou a servir de base para a defesa das capacidades mais tradicionais, que alguns temiam ver desaparecer, a favor da contrainsurgência (Russel, 2014).

Um novo conjunto de artigos sobre o tema surgiu entre 2008 e 2009, da autoria do General Hoffman, para mais uma vez influenciar o debate sobre a QDR 2010, cujo relatório final se refere pela primeira vez a GH (US Department of Defense, 2010, p. 8).

Enquanto isso, o conceito surgiu no seio da OTAN, por intermédio do *Allied Command Transformation* (ACT), um comando criado em 2003, cuja missão era pensar nas novas formas dos conflitos. Foi precisamente o General Mattis, coautor

do artigo de 2005, quem assumiu o comando do ACT em 2007 e introduziu o conceito na doutrina da OTAN (ACT, 2009).

Segundo Monaghan (2019) o termo GH representa uma mudança do carácter da Guerra contra adversários violentos, durante um conflito armado, enquanto que o termo AH descreve um desafio diferente, traduzindo a utilização de diversos meios ambíguos, para explorar as vulnerabilidades de uma sociedade, sem desencadear reações. Embora esteja sempre subjacente o propósito de neutralizar a capacidade do oponente prosseguir os seus objetivos, a estratégia utilizada para tal, é conceptualmente diferente. A GH visa neutralizar o instrumento militar e a sua eficiência na conduta de operações, ao passo que o alvo principal das AH é a população e a capacidade de decisão do governo (Monaghan, 2019).

A Figura 1 elucida visualmente onde cada um dos conceitos se localiza dentro do espetro da conflitualidade.

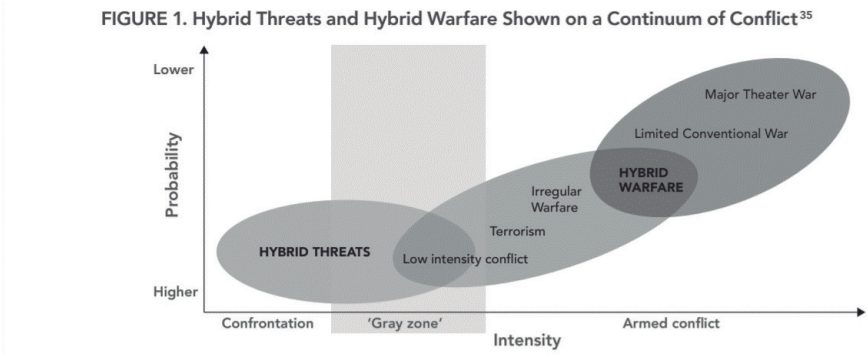


Figura 1 – Ameaças Híbridas e Guerra Híbrida no espetro da conflitualidade
Fonte: Monaghan (2019).

2.2. Resiliência do instrumento do Poder Económico

A Comunicação Conjunta da CE (2018) faz uma abordagem estratégica do assunto, enfatizando que a estratégia para contrariar os efeitos das AH passa, entre outros, pelo investimento na resiliência da administração pública e de toda a sociedade, aumentando a sua capacidade para superar crises internas, bem como crises externas, na medida em que as interdependências são cada vez mais. O Hybrid COE (s.d.) também considera que estabelecer um sistema resiliente deve ser uma das principais apostas para neutralizar as AH, uma vez que permite "justapor a normalidade ao caos em que tais ameaças prosperam".

Para perceber o significado de resiliência no domínio da economia, importa primeiro compreender que a produção de bens e serviços é cada vez mais global e envolve uma multiplicidade de organizações especializadas, ligadas através de cadeias de abastecimento transnacionais. Esta grande interconetividade fomenta a propagação de perturbações e pode gerar oscilações intensas e frequentes no preço dos ativos. Estes fenómenos económicos podem, por sua vez, ser dilatados pelo aumento da amplitude, extensão espaço-temporal ou frequência de eventos desestabilizadores (Colon, 2016, p. 12).

Para Christopherson, Michie e Tyler (2010), os efeitos de um choque numa economia dependem da suposição subjacente ao equilíbrio económico. Numa primeira abordagem, pode-se assumir que existe uma trajetória de crescimento única para a qual a economia eventualmente retornará após o choque, na medida que a interferência apenas adiou o crescimento. Portanto, a resiliência reside na velocidade e na eficiência da recuperação. Numa segunda abordagem, considera-se que existem múltiplas forças impulsionadoras, e que uma alteração da trajetória fará a economia reorganizar-se e transitar para outra região diferente, que pode ter uma maior ou menor taxa de crescimento, conforme esta seja mais ou menos resiliente.

Na Figura 2 encontram-se representadas as trajetórias que a economia descreve segundo cada uma das abordagens. No primeiro gráfico assume-se que existe apenas um estado de equilíbrio, logo a economia retoma a sua taxa de crescimento anterior, depois de um choque de recessão. No segundo e terceiro gráfico, o choque leva a uma alteração de trajetória, indicando que a economia se reorganiza num novo estado de equilíbrio.

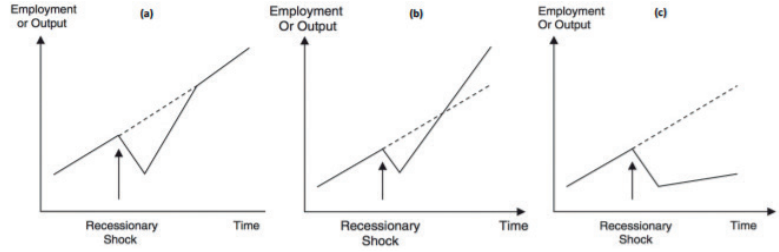


Figura 2 – Trajetórias hipotéticas de resposta a um choque de recessão
Fonte: Martin (2012).

Alguns autores consideram mais verosimilhante o comportamento económico da segunda abordagem, pois um choque não só desvia a economia da sua trajetória de crescimento, como também desencadeia profundas mudanças, gerando novas rotas de desenvolvimento (Simmie & Martin, 2010).

As novas rotas de desenvolvimento serão definidas pelo nível de resiliência económica e não pelas vulnerabilidades que a economia compreende, pois como defende Briguglio (2003), existe uma aparente contradição de que um país pode estar altamente exposto a choques exógenos, tornando-o economicamente vulnerável, e ainda assim, conseguir atingir níveis elevados de Produto Interno Bruto (PIB) per capita.

Briguglio (2003) explica o fenómeno, que designa por "Paradoxo de Singapura", em termos da justaposição da vulnerabilidade e da resiliência económica e propõe uma abordagem metodológica a este respeito. Nessa abordagem, a vulnerabilidade económica é atribuída a características permanentes (ou quase permanentes) sobre as quais um país não consegue exercer praticamente nenhum controlo, ou seja, as vulnerabilidades não são fruto de políticas inadequadas, que expõem o país a choques exógenos. Por outro lado, a resiliência económica, essa sim, está associada a ações empreendidas pelos decisores políticos e agentes económicos privados, que permitem a um país resistir ou recuperar dos efeitos negativos dos choques, contrabalançando as suas vulnerabilidades inerentes.

Portanto, a nova configuração da economia (segundo e terceiro gráfico da Figura 2) depois desta ser adversamente afetada por choques externos, resulta da combinação dos dois elementos, conforme apresentado na Figura 3. O sinal positivo à frente do elemento resiliência indica que a nova trajetória é tão melhor quanto maior a resiliência acumulada.

Figura 3 – Efeitos adversos de choques exógenos
Fonte: Adaptado de Briguglio (2004).

A possibilidade de construir resiliência económica significa que os Estados vulneráveis não devem ser complacentes com a suas vulnerabilidades económicas, devendo adotar medidas políticas que lhes permitam melhorar a sua capacidade de lidar ou recuperar de choques externos.

3. METODOLOGIA E MÉTODO

A metodologia seguida na elaboração do presente TII baseia-se numa orientação ontológica construtivista e epistemológica interpretivista, uma vez que considera que os fenómenos sociais e os seus significados estão constantemente a ser executados pelos atores sociais (Bryman, 2012, cit. por Santos & Lima, 2019, p. 16).

A investigação segue um raciocínio indutivo assente no conhecimento base existente sobre os conceitos e as dimensões em análise e dos quais resulta, através de uma estratégia de investigação qualitativa, a construção de um modelo teórico para apoio à decisão.

Quanto ao desenho de pesquisa entende-se que a temática se enquadrava num estudo de caso, uma vez que a investigação incidiu sobre uma única unidade de estudo – neste caso a resiliência da economia de um Estado – o que está alinhado com a estratégia de investigação qualitativa. Este aspeto está também relacionado com o horizonte temporal transversal, na medida em que o estudo foi realizado com base nos dados recolhidos num determinado instante de tempo.

A recolha de dados foi efetuada através da observação não participante e não estruturada, recorrendo a uma revisão e análise exaustiva da literatura reunida, por forma a alcançar o mais alto grau de precisão e viabilizar uma pesquisa consistente com o objetivo da investigação, especialmente porque o autor se encontrava em território desconhecido.

No que respeita às fases do percurso de investigação, este trabalho foi dividido em duas fases. A primeira fase - fase exploratória - englobou, entre outros, a identificação do objeto de estudo, a definição do problema de investigação e o enquadramento e contextualização geral. Para identificação do objeto de estudo, dentro das hipóteses disponíveis, foram seguidos os critérios da familiaridade, da afetividade e da disponibilidade de recursos necessários à investigação. Para a identificação do problema e subsequentemente definição do objetivo fundamental da investigação, foram examinados vários estudos subordinados ao tema das AH. Em resultado dessa investigação preliminar foi desenvolvida uma base conceptual, por forma a enquadrar o trabalho e estabelecer o modelo de análise a adotar. Como resultado da fase exploratória foi também concebido um quadro cronológico e uma articulação inicial.

Na fase seguinte do processo metodológico – fase analítica e conclusiva – foi efetuada a recolha e tratamento de dados resultantes de uma análise documental criteriosa, para dar resposta às questões formuladas com dados objetivos.

As principais fontes bibliográficas incluíram documentação estruturante da UE, estudos desenvolvidos pelo Hybrid CoE, estudos desenvolvidos ao abrigo do *Countering Hybrid Warfare Project* e literatura da especialidade. Para a quantificação dos indicadores e aplicação do modelo analítico concebido, foi utilizada a base de dados do Gabinete de Estatísticas da UE - Eurostat (s.d) - e a base de dados do Banco Mundial - *World Governance Indicators* (WGI) - desenvolvida por Kaufmann e Kraay (s.d.).

Por fim, foi feita uma síntese dos elementos recolhidos no decorrer da investigação e a consequente redação do trabalho de investigação, com a apresentação das conclusões do estudo, identificação das limitações, recomendações e eventuais sugestões para futuros trabalhos de investigação.

4. APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

4.1. Caracterização das Ameaças Híbridas

As AH visam um Estado através de diversos domínios, aplicando combinações de ferramentas. Cada ferramenta pode atuar num único, em múltiplos domínios, ou na interface entre eles, criando ou explorando vulnerabilidades ou tomando vantagem de uma oportunidade.

O presente capítulo classifica as AH passíveis de afetar a economia de um Estado, começando por identificar as diversas ferramentas utilizadas, elencando de seguida os principais atores e os seus objetivos, e as principais vulnerabilidades do instrumento de poder económico.

4.1.1. Ferramentas das Ameaças Híbridas

À exceção do domínio cibernético, que trouxe novas ferramentas e novas oportunidades para maximizar os efeitos, as ferramentas utilizadas para perpetuar um ataque com AH já são antigas. Como refere o Major-General Mažeikis (2015), é possível elencar um sem número de exemplos na história da humanidade: o Cavalo de Troia, construído pelos gregos para entrar na cidade de Troia; o início da II Guerra Mundial, quando os nazis organizaram um ataque à sua própria estação de rádio com um grupo de pessoas vestidas com uniformes polacos; ou quando a URSS organizou o bombardeamento dos seus próprios postos de guarda na fronteira com a Finlândia, culpando mais tarde os finlandeses.

O que constitui uma novidade do século XXI é a utilização simultânea e complementar desses instrumentos, para atingir um objetivo comum (Treverton, Thvedt, Chen, Lee, & McCue, 2018). Para além da simultaneidade, a outra característica que define uma AH é a utilização estratégica de ferramentas ou instrumentos de poder, tanto na vertical como na horizontal. Isso significa que as AH atingem e exploram vulnerabilidades de outro Estado, aumentando a intensidade de uma ou várias ferramentas e/ou fazendo escalada horizontal através do emprego de múltiplas ferramentas, para amplificar os efeitos[49] (Cullen & Reichborn-Kjennerud, 2017).

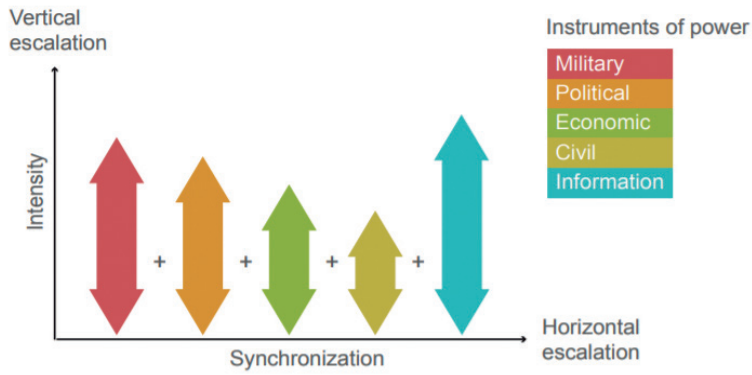


Figura 4 – Escalada vertical e horizontal de ferramentas
Fonte: Cullen & Reichborn-Kjennerud (2017).

No contexto das AH, o domínio da economia está intimamente relacionado com outros domínios, resultando as ligações, em grande parte, do facto da economia ser sustentada pelas empresas, que desenvolvem as suas atividades segundo uma rede multidominio (Giannopoulos et al., 2021).

Os instrumentos de política económica são as principais ferramentas utilizadas pelas AH, para alcançar os seus objetivos, afetando o domínio económico (Fabre, 2018; Norris, 2016). Por exemplo, as medidas ou políticas económicas

[49] Cullen e Reichborn-Kjennerud (2017) consideram que os instrumentos de poder utilizados pelos agressores são o militar, político, económico, civil e informacional (MPECI). Giannopoulos et al. (2021) são mais específicos considerando que os atores podem utilizar 40 ferramentas diferentes para atingir o seu oponente.

podem ser utilizadas para aumentar a pressão política, ou a coerção económica pode procurar modificar a posição de política externa de um Estado, ou ainda enfraquecer a sua economia, sociedade ou segurança (Blackwill & Harris, 2016; Iancu et al., 2016). No entanto, cada manifestação de um instrumento não constitui necessariamente uma atividade das AH. Por exemplo, uma operação cibernética pode ou não fazer parte de uma atividade das AH (Giannopoulos et al., 2021). Apresenta-se na Figura 5 uma lista indicativa das ferramentas utilizadas pelas AH no domínio económico.

Figura 5 – Ferramentas utilizadas pelas AH no domínio económico
Fonte: Giannopoulos et al. (2021).

4.1.2. Principais Atores

A atividade subjacente às AH é empreendida particularmente por atores com uma visão autoritária ou totalitária do poder. O objetivo é visar as vulnerabilidades sistémicas das democracias, utilizando todos os instrumentos que um Estado autoritário tem à sua disposição (Giannopoulos et al., 2021).

A utilização de AH como mecanismo de apoio às diferentes políticas, para assegurar os seus interesses estratégicos tem sido atribuída a Estados como a

Rússia, China, Irão e Coreia do Norte, e a atores não estatais como o Hezbollah, a Al-Qaeda, ao Daesh, vários grupos intermediários, sindicatos transnacionais do crime organizado, movimentos ideológicos ou atores independentes com fins lucrativos (Giannopoulos et al., 2021).

Uma revisão da literatura existente sobre a temática revela que a caracterização dos atores não estatais não tem sido o foco central dos investigadores, embora o conceito tenha sido originado pela sua forma de atuar, como referido anteriormente. Com efeito, no presente trabalho serão apenas tratados os atores Estado.

A Rússia é o Estado que mais emprega AH, pois tem uma grande experiência na sua utilização, se considerarmos que é o principal sucessor da União Soviética, que utilizava recorrentemente instrumentos não-militares para perseguir os seus interesses (Mažeikis, 2015). Os interesses centrais que orientam a política externa russa são: dominar o *near abroad* e ver a Rússia reconhecida como uma grande potência global (Radin & Reach, 2017).

A Rússia considera os EUA e a OTAN os principais desafios aos seus interesses e à sua segurança, especialmente depois da crise política de 2011 (Treverton et al., 2018). No entanto, procurará sempre evitar uma confrontação militar, pois sabe que perderá no confronto com a OTAN (Fisher, 2015) e também não se encontra capaz de ganhar uma competição económica, pois o PIB real da Rússia caiu drasticamente durante a crise de 2008-2009 e tem vindo a sofrer uma desaceleração acentuada desde então (Giles et al., 2015). A par disso, a Comunidade Económica da Eurásia também tem revelado fragilidades, demonstrando diferenças entre os objetivos declarados da organização e os objetivos dos Estados-membros (Golam & Monowar, 2018). Assim, para a Rússia, a estratégia passa pelo recurso a AH, criando confusão, caos e incerteza nas instituições dos seus adversários (Treverton et al., 2018).

Uma análise da *Alliance for Securing Democracy* (German Marshall Fund, s.d.) concluiu que, desde 2004, o governo russo tem utilizado ciberataques, ações de desinformação e campanhas de influência financeira para interferir nos assuntos internos de pelo menos 27 países da Europa e da América do Norte (Dorrel, 2017).

Segundo Galeotti (2017, p. 1), os métodos do governo russo para prosseguir os seus objetivos no estrangeiro são "largamente determinados pela correlação entre a força das instituições nacionais dos países e a sua vulnerabilidade à influência russa".

Nos países que a Rússia considera o seu *near abroad*, o objetivo é exercer controlo sobre os governos facilmente influenciáveis ou enfraquecer os líderes pró-ocidentais. No resto da Europa, procura principalmente criar fissuras nas organizações coletivas, designadamente na OTAN e na UE, amplificando a discórdia política e social (Polyakova et al., 2016). Os factos indicam que a Rússia atua com mais ousadia no seu *near abroad* do que nos Estados da OTAN e da UE, mas não se coíbe de aplicar toda a gama de instrumentos de poder no resto do continente europeu e para além-fronteiras (US Senate, 2018).

Quanto aos outros Estados conhecidos como sendo utilizadores de AH, os seus principais objetivos são menos claros, e provavelmente mais de oportunidade (Treverton et al., 2018). Um estudo conduzido por Ross Babbage (2019) observou que a utilização chinesa de AH é declaradamente apoiada pelo Partido Comunista Chinês (PCC) e pelas Forças Armadas chinesas, e que a sua estratégia de atuação tem procurado alcançar vitórias rápidas e decisivas.

A China é o maior credor do mundo com empréstimos e investimentos que ascendem a quase 10% do PIB global. A origem dos empréstimos é obscura, uma vez que nem o Fundo Monetário Internacional, nem o Banco Mundial, nem as agências de notação de crédito conseguem ter uma cobertura de dados válida. Além disso, o governo chinês também não divulga os dados sobre as suas atividades de empréstimo no estrangeiro e não é membro de nenhuma organização credora proeminente, como o Clube de Paris ou a Organização para a Cooperação e Desenvolvimento Económico (OCDE) (Massa, 2011).

A grande quantidade de investimentos num país em particular permite à China utilizar a ameaça de desinvestimento como instrumento de influência para exercer pressão económica sobre o próprio país ou sobre outros países que usufruam do mesmo mercado (Aho et al., 2020).

A fim de controlar as cadeias de abastecimento globais e de expandir o poder e a influência do PCC, a China tornou a *Belt and Road Initiative* no maior projeto de infraestruturas do mundo moderno (Greeven, 2020). Para alcançar esse objetivo, o envolvimento de setores estratégicos importantes, como são os portos europeus, é essencial, pois permitem controlar algumas das principais cadeias de valor acrescentado. Nesse sentido, os investimentos chineses nos portos marítimos europeus têm vindo a aumentar nos últimos anos (Putten, Hong, & Blécourt, 2018).

Na mesma medida têm aumentado as críticas provenientes de vários grupos de reflexão, meios de comunicação e governos ocidentais, que apontam

os investimentos chineses nos portos como uma ferramenta, para tornar um país beneficiário economicamente dependente e usar essa dependência como uma fonte indireta de influência política (Putten, 2019).

Um resultado desta mudança de perceção é o novo regulamento da UE para rastreio dos investimentos diretos estrangeiros. O regulamento insta os Estados-Membros a considerarem cuidadosamente os potenciais efeitos de "segurança ou de ordem pública" dos investimentos diretos estrangeiros em infraestruturas críticas, tecnologias ou fatores de produção essenciais (UE, 2019, pp. 79 I/1-I/2). Este regulamento não se destine explicitamente a nenhuma nação em particular, no entanto, presume-se que as preocupações com os investimentos da China são suscetíveis de ter desempenhado um papel por detrás desta iniciativa (Putten et al., 2018).

4.1.3. Vulnerabilidades do Estados

Numa sociedade globalizada as relações económicas são suscetíveis à manipulação estatal, e por isso são recorrentemente exploradas como meio de alcançar fins estratégicos de vários países (Blackwill & Harris, 2016; Iancu et al., 2016).

A economia, como domínio das AH, é definida pela OTAN (2013, pp. I–8) como "a soma total da produção, distribuição e consumo de todos os bens e serviços" de um país, e inclui o seu desenvolvimento económico e distribuição de riqueza.

A exploração do domínio económico não tem os mesmos objetivos que uma campanha militar declarada. O objetivo de uma AH, quando atua no domínio económico, é enfraquecer de forma abrangente o Estado alvo, afetando a confiança da população na democracia e no governo (Giannopoulos et al., 2021).

Uma das principais vulnerabilidades do domínio económico é a dependência energética ou dependências de infraestruturas que por sua vez podem gerar dependências económicas ou tornar-se num instrumento para exercer pressão económica. Por exemplo, a Rússia tem vindo a alavancar a sua posição como exportadora de gás natural, não só na Ucrânia, mas também na UE que se encontra muito vulnerável aos choques energéticos exteriores, apesar de ter vindo a realizar esforços para fortalecer a sua infraestrutura energética e a diversificar dos seus fornecedores (Rocha, 2016).

As vulnerabilidades dos Estados nesse domínio, podem também advir do desenvolvimento de infraestruturas onerosas que impliquem projetos de capital para atrair investimento estrangeiro direto (IED), pois além de afetar negativamente a balança comercial e de pagamentos, também leva a que o país recetor do investimento fique com um elevado grau de dependência de investidores oportunistas, cujas intensões nem sempre são claras (Teixeira & Lehmann, 2007, cit. por Pereira, 2017).

Também as dificuldades económicas e/ou desigualdades podem ser facilmente exploradas com ataques cibernéticos e campanhas de desinformação, para influenciar os resultados eleitorais ou exercer pressão indireta sobre o governo (Tennis, 2020). Os estratos sociais mais desfavorecidos, que não têm meios financeiros, e para os quais as oportunidades de trabalho são escassas ou inexistentes, tendem a ter a reação psicológica de culpar o *status quo* e condenar as trajetórias de democratização. Também existe uma significativa correlação entre os níveis de riqueza e a educação, sendo, por conseguinte, os setores mais pobres da sociedade os mais vulneráveis a notícias falsas e a campanhas de propaganda (Popescu & Zamfir, 2018).

Assumir obrigações financeiras além das capacidades dos Estados soberanos, pode degenerar no aumento descontrolado da dívida soberana ou da balança comercial e de pagamentos e criar sérios riscos de choques sistemáticos na segurança financeira e no próprio sistema de segurança nacional, pois um colapso financeiro pode ser utilizado como narrativa para corroer a legitimidade de um governo, ou mesmo para justificar as ações ou posições geopolíticas (Yordanova, 2018).

O poder económico, obtido através da lavagem de dinheiro e através de corrupção, pode amplificar ganhos na influência política, estabelecendo um "ciclo desvirtuoso de corrupção", no qual o aumento do poder político permite um aumento do poder económico (Cullen & Wegge, 2019, p. 2). Na forma mais tradicional, a corrupção pode permitir que redes ilícitas façam tráfico através das fronteiras, enquanto empresas de fachada e intermediários agem ostensivamente na aquisição de influência económica e política, para ocultar as verdadeiras origens e motivações da atividade.

4.1.4. Síntese Conclusiva

O presente capítulo classificou as AH passiveis de afetar a economia de um Estado. concluindo-se que as AH atingem e exploram as vulnerabilidades de um

Estado, aumentando a intensidade de uma ou várias ferramentas e/ou fazendo escalada horizontal através do emprego de múltiplas ferramentas, para amplificar os efeitos. Os instrumentos de política económica são as principais ferramentas utilizadas pelas AH, para alcançar os seus objetivos, afetando o domínio económico.

A Rússia é o Estado que mais emprega AH, pois não está em posição de ganhar uma confrontação militar ou uma competição económica com a OTAN e os EUA, que representam os principais desafios aos seus interesses e à sua segurança. A mesma tem utilizado ciberataques, ações de desinformação e campanhas de influência financeira para interferir nos assuntos internos em diversos países da Europa e da América do Norte. Nos países que considera o seu *near abroad*, o objetivo é exercer controlo sobre os governos facilmente influenciável ou enfraquecer os líderes pró-ocidentais. Nos restantes países, a intensão é criar fissuras nas organizações coletivas, designadamente a OTAN e a UE, amplificando a discórdia política e social.

A utilização de AH também é declaradamente apoiada pelo PCC e pelas Forças Armadas chinesas, no entanto, em contraste com a prática russa de lutar para alcançar vitórias rápidas e decisivas, os chineses concentram-se mais na posição de vantagem a longo prazo, sustentando a campanha durante um período prolongado. Como maior credor a nível global, a China utiliza a ameaça de desinvestimento como instrumento de influência, para exercer pressão económica sobre os países economicamente mais dependentes. Alguns dos maiores investimentos têm recaído em infraestruturas, tecnologias e fatores de produção essenciais dos países europeus, o que tem deixado a UE preocupada quanto aos potenciais efeitos de segurança ou ordem pública.

As principais vulnerabilidades que as AH procuram explorar são: a dependência energética ou dependências de infraestruturas, que por sua vez podem gerar dependências económicas ou tornar-se num instrumento para exercer pressão económica; a dependência de IED, pois coloca o país recetor do investimento à mercê de investidores oportunistas; as dificuldades económicas e/ou desigualdades, que podem ser facilmente exploradas com ataques cibernéticos e campanhas de desinformação para influenciar os resultados eleitorais ou exercer pressão indireta sobre o governo; o aumento descontrolado da dívida soberana ou da balança comercial e de pagamentos, que trás riscos para a segurança financeira e para o próprio sistema de segurança nacional; a corrupção, que pode amplificar ganhos na influência política, estabelecendo um ciclo desvirtuoso de corrupção, no qual o aumento do poder político permite um aumento do poder económico.

4.2. Modelo de análise de Resiliência

A proatividade e a tomada de decisões eficientes, para atenuação das potenciais perdas, resultantes de ações conduzidas por AH, dependem muito da possibilidade de haver indicadores relativos à resiliência (Mažeikis, 2015).

No presente capítulo são selecionadas as variáveis e os indicadores, para a conceção de um modelo de avaliação do domínio económico.

4.2.1. Variáveis

Os diversos modelos de análise de resiliência consultados partilham alguma subjetividade na sua conceção, em particular no que diz respeito à escolha das variáveis. Esta é uma questão difícil de resolver, contudo, como defende Farrugia (2007) o problema pode ser minimizado se o objetivo do índice for muito bem definido.

No caso do presente índice, de acordo com o seu objetivo, foi tomada especial atenção para incluir variáveis que reflitam a propensão a danos provocados por forças externas, e não variáveis que reflitam condições ou vulnerabilidades inerentes, em consonância com o modelo apresentado por Briguglio (2003). É importante notar também que existiu um cuidado de basear a escolha num conjunto de critérios relacionados com uma cobertura adequada, simplicidade e facilidade de compreensão, adequação para comparações e acessibilidade de dados.

Como defende Briguglio (2003), um papel importante dos decisores políticos é a monitorização das vulnerabilidades potenciais da economia do Estado a choques económicos, não no sentido de serem capazes de prever choques específicos, mas sim a capacidade da economia absorver os efeitos de choques potenciais, através de resiliência.

Tendo isso em consideração, as vulnerabilidades atrás identificadas foram agregadas em dois grupos, a que correspondem duas variáveis diretamente influenciáveis pelas ações empreendidas pelos decisores políticos e agentes económicos privados, conforme apresentado no quadro seguinte.

Quadro 1 – Variáveis de resiliência

	Vulnerabilidades	Variáveis
Domínio económico	IED	Estabilidade macroeconómica
	Balança comercial e de pagamentos	
	Divida soberana	
	Dificuldades económicas e/ou desigualdades	
	Nível tecnológico	
	Corrupção	Boa governação
	Plano legal	
	Dependência de infraestruturas críticas e de recursos essenciais	

A estabilidade macroeconómica está relacionada com a interação entre a procura e a oferta de uma economia. Se a procura se mover em harmonia com a oferta, a economia está em equilíbrio. Esse equilíbrio manifesta-se internamente, tendo uma posição orçamental sustentável, baixa inflação de preços e uma taxa de desemprego próxima da taxa natural. Externamente, reflete-se na posição da conta corrente internacional ou pelo nível da dívida externa (Briguglio, 2003).

A boa governação é essencial para que um sistema económico funcione corretamente e, por conseguinte, para ser resiliente. A boa governação é definida pelo Banco Mundial como "a maneira pela qual o poder é exercido na administração dos recursos sociais e económicos de um país visando o desenvolvimento" e também "a capacidade dos governos de planear, formular e programar políticas e cumprir funções" (The World Bank, 1992, p. 1).

4.2.2. Indicadores

Grande parte dos modelos de análise utiliza indicadores macroeconómicos clássicos, como o PIB *per capita*, rendimento das famílias, Valor Acrescentado Bruto, importações, exportações e taxas de emprego/desemprego, para medir a resiliência. São exemplo disso os trabalhos desenvolvidos por Drobniak (2017), Wink (2014) ou o programa *European Spatial Planning Observation Network* (ESPON) adotado pela CE. Estes modelos procuram identificar o bem-estar económico de um Estado de forma abrangente. Para além disso, utilizam dados facilmente disponíveis para facilitar a comparação entre países e regiões.

Modelos mais recentes procuram incluir indicadores que permitam uma compreensão mais vasta da resiliência económica a longo prazo. Assim, os dados

baseados nas características das empresas e dos trabalhadores, tais como o número global de empresas, a presença de empresas internacionais e o nível de qualificação da mão-de-obra, têm ganho relevância (Hill et al., 2012).

No presente trabalho, para avaliar as características estruturais da estabilidade macroeconómica, serão seguidos os conceitos do ESPON (2014), que utilizando a evolução do PIB e da taxa de emprego, demonstra que as seguintes áreas políticas requerem ações para fomentar a resiliência macroeconómica: diversidade, competência e inovação.

A diversidade torna os países menos dependentes de empresas ou sectores específicos. Vários países caracterizam-se pela cobertura de múltiplos segmentos de mercado, também conhecida como diferenciação horizontal (Sorensen & Sorenson, 2007). As economias mais diversificadas tendem a ser mais resilientes, uma vez que são mais capazes de se adaptar a novas circunstâncias após qualquer choque (ESPON, 2014).

Os países e regiões com trabalhadores mais qualificados demonstram ser mais resistentes aos choques (ESPON, 2014). Os trabalhadores mais qualificados tendem também a ocupar empregos mais resistentes a crises e a ser menos substituíveis por novas tecnologias (Hirsch-Kreinsen, 2016).

As regiões com níveis mais elevados de atividades ligadas à inovação, o que é evidenciado sob a forma de patentes ou investimento em investigação e desenvolvimento, tendem a responder a choques mais positivamente do que outras (ESPON, 2014).

A qualidade da governação, geralmente traduzida pelos baixos níveis de corrupção, Estado de direito imparcial, eficácia e responsabilização governamental, é também um fator chave para a resiliência das economias de um país (Charron, Apuente, & Dijkstra, 2012). De facto, como demonstra o programa de investigação ESPON (2014), existe uma forte correlação positiva entre a qualidade do governo e a capacidade de resistência da economia, durante e após os choques económicos.

A análise de diversos estudos permitiu concluir que a base de dados WGI é uma fonte apropriada para obter os indicadores de boa governação. Desde logo porque não se concentra apenas num único conceito de boa governação, comportando seis indicadores inter-relacionados, que se consideram pertinentes:

voice and accountability[50]; estabilidade política e ausência de terrorismo e violência; eficácia governamental; qualidade regulamentar; Estado de Direito; controlo da corrupção. Depois, porque a WGI abrange todos os Estados-membros da UE, desde meados dos anos 90, e é atualizado anualmente, sendo transparente na forma como é construído, publicando livremente a fonte dos dados subjacentes sobre os quais é construído, juntamente com uma descrição relativamente clara do significado conceptual de cada conceito.

Na Quadro 2 são apresentados os indicadores identificados para cada uma das variáveis, bem como a sua proveniência.

Quadro 2 – Indicadores de resiliência do domínio económico

	Variáveis	Indicadores de resiliência	Modelo de análise
Domínio económico	Estabilidade macroeconómica	Diversidade	ESPON
		Competência	
		Inovação	
	Boa governação	*Voice and accountability*	WGI
		Estabilidade política e ausência de terrorismo e violência	
		Eficácia governamental	
		Qualidade regulamentar	
		Estado de Direito	
		Controlo da corrupção	

4.2.3. Síntese Conclusiva

No presente capítulo foram selecionadas as variáveis e os indicadores para a conceção de um modelo de avaliação do domínio económico. Para tal, as vulnerabilidades atrás identificadas foram agregadas em dois grupos, a que correspondem duas variáveis, diretamente influenciáveis pelas ações empreendidas pelos decisores políticos e agentes económicos privados: a estabilidade macroeconómica e a boa governação.

[50] *Voice and accountability* capta a perceção de que os cidadãos de um país têm a possibilidade de participar na seleção dos seus governantes, bem como a liberdade de expressão, a liberdade de associação e a liberdade dos meios de comunicação social (Kaufmann & Kraay, s.d.).

Para avaliar as características estruturais da estabilidade macroeconómica, foram seguidos os conceitos do projeto de investigação ESPON, que demonstram que as áreas políticas que requerem ações para fomentar a resiliência macroeconómica são: a diversidade, a competência e a inovação.

Para obter os indicadores de boa governação foi seguida a base de dados WGI, que abrange todos os Estados-membros da UE e comporta seis indicadores inter-relacionados: *voice and accountability;* estabilidade política e ausência de terrorismo e violência; eficácia governamental; qualidade regulamentar; Estado de Direito; controlo da corrupção.

4.3. Modelo de análise da resiliência do domínio económico face às ameaças híbridas

No presente capítulo as variáveis e os indicadores identificados no ponto anterior são integrados num modelo analítico, que permite avaliar a resiliência do instrumento de poder económico nacional face a AH.

4.3.1. Quantificação de indicadores

Existem inúmeros estudos que desenvolvem medidas de diversidade económica e testam, estatisticamente, como as mudanças na estrutura industrial de uma região afetam a sua estabilidade macroeconómica e desempenho. Para medir a diversidade económica, um dos índices mais comuns é o *Índice Ogiva* (Rodgers, 1957), que mede os rácios de concentração dos sectores laborais de um país ou região (Siegel, Johnson, & Alwang, 1995). A fórmula de cálculo é a seguinte:

$$\text{Índice Ogiva} = \sum_{i=1}^{N} \frac{(Si\text{-}1/N)^2}{1/N} \quad (1)$$

Em que N é o número de sectores da economia e S_i é a quota-parte sectorial da atividade económica para o sector i. Quanto mais equitativa for a distribuição da atividade económica pelos seus sectores, maior será a diversidade (Rodgers, 1957). Com N sectores, uma distribuição equitativa implica que Si seja igual a $1/N$, a quota ideal para cada sector, e o *Índice Ogiva* seja igual a zero, o que significa uma diversidade perfeita. Uma distribuição mais desigual da atividade económica pelos diversos setores resulta num valor mais elevado do índice.

Para o presente estudo, a atividade económica dos países é dividida em dez setores chave, de acordo com a nomenclatura de atividades económicas NACE-rev2,

instituída como referência na UE para efeitos estatísticos, e a quota setorial é representada pela quota de emprego no respetivo setor. Os dados utilizados são da base de dados *Eurostat* (s.d.).

Na fórmula apresentada pode-se observar a concentração sectorial da atividade económica dos 27 países da UE resultante do procedimento matemático.

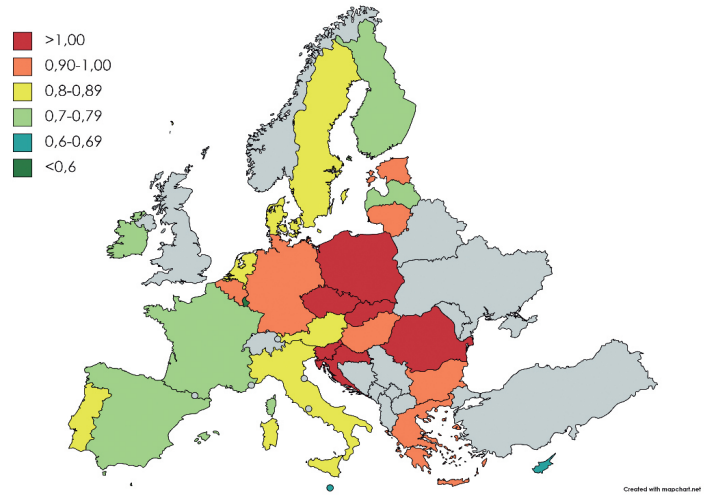


Figura 6 – Concentração sectorial da atividade económica
Fonte: Elaborado com base nos dados do *Eurostat* (dados de 2020).

Os níveis de competências são medidos pela quota de emprego nos setores de tecnologia e de conhecimento intensivo. Na Figura 7 pode-se observar que as elevadas competências parecem estar concentradas nos países nórdicos e nos países vizinhos. Pode-se deduzir que, de acordo com a teoria explanada anteriormente, estes países terão maior capacidade de recuperar de eventuais choques exógenos.

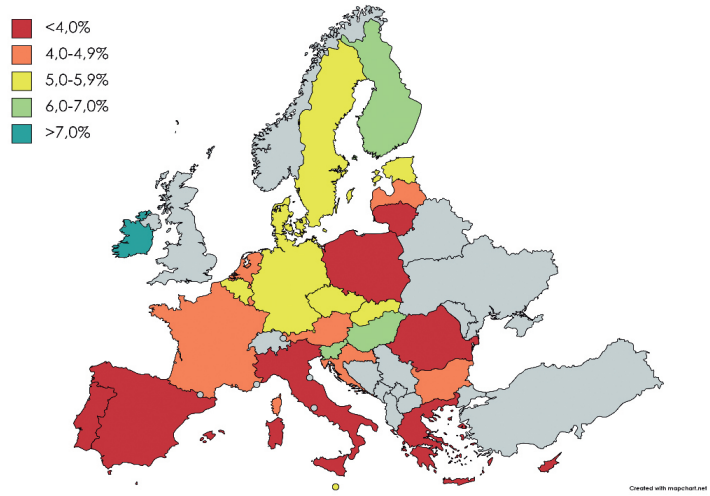


Figura 7 – Percentagem do emprego total nos sectores de conhecimento intensivo
Fonte: Elaborado com base nos dados do *Eurostat* (dados de 2020).

Os níveis de inovação são diretamente medidos pela percentagem do PIB que corresponde ao investimento em inovação e desenvolvimento (vide Figura 8).

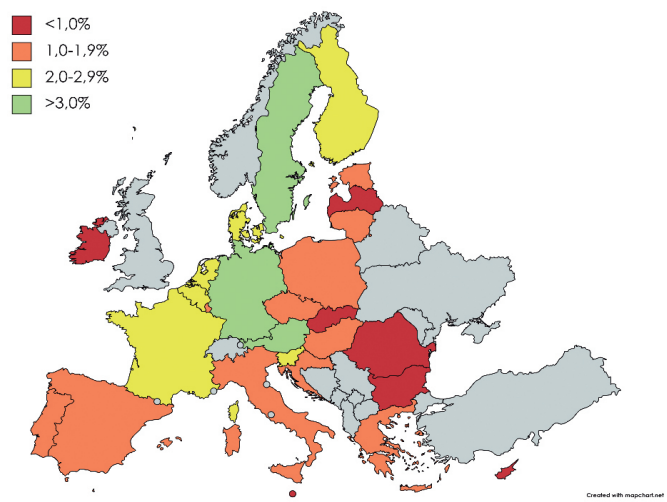


Figura 8 – Percentagem do PIB gasta em inovação e desenvolvimento
Fonte: Elaborado com base nos dados do *Eurostat* (dados de 2020).

A medição dos indicadores de boa governação é diretamente extraída do modelo de análise WGI, numa escala que vai de -2,5 (pior prestação) a +2,5 (melhor prestação.

4.3.2. Normalização de indicadores

O modelo de análise aqui apresentado incorpora cada um dos nove indicadores de resiliência do domínio económico, considerando que cada um contribui com igual peso. Para acomodar as diferentes escalas e métricas de indicadores, os seus valores são reportados como z-scores, o que quantifica quantos desvios padrão - numa direção positiva ou negativa - o desempenho de um país num indicador diverge da média europeia. Os z-scores seguem a fórmula (2), em que x corresponde ao valor registado para o país em análise, μ corresponde à média da UE e σ ao desvio padrão:

$$Z = \frac{X-\mu}{\sigma} \quad (2)$$

No caso do indicador diversidade, uma vez que o aumento do seu valor corresponde a uma perda na capacidade de resiliência, procede-se à inversão de sinal, multiplicando os respetivos valores por -1. Deste modo, todos os indicadores estão normalizados ao racional de quanto mais elevado o valor, mais o indicador contribui para a resiliência do país em causa.

A soma dos nove z-scores de cada país equivale a um *totalscore*, que reflete a sua prestação no conjunto de indicadores. O modelo de análise utiliza a pontuação do *totalscore* para classificar os 27 países da UE, estratificando a ordenação em 3 níveis de resiliência: alto, médio, baixo. Apresenta-se na Figura 9 o nível de resiliência no domínio económico de cada um dos países da UE.

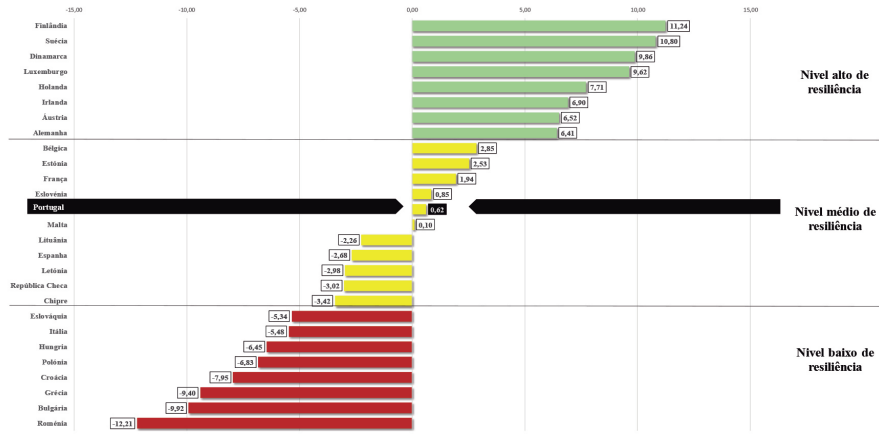


Figura 9 – Níveis de resiliência no domínio económico
Fonte: Elaborado com base nos dados obtidos através do procedimento matemático.

4.3.3. Avaliação dos resultados

Segundo o modelo de análise apresentado, que se baseia num método comparativo entre os diversos países da UE, o domínio económico português apresenta um nível médio de resiliência face a AH. O facto de países como a Finlândia, Suécia ou Dinamarca terem uma capacidade de resiliência muito superior, significa que têm outros fatores e outras condições para um desempenho eficaz na recuperação pós-perturbação. Contudo, ter um bom nível de resiliência não garante, que, perante um choque, estes países respondam eficazmente e recuperem da perturbação, pois podem desperdiçar a sua capacidade de resiliência, atuando sob a expetativa de um bom desempenho. Por outro lado, o facto de Portugal ter um nível inferior de resiliência, não é uma sentença de que o país vacilará perante um choque. Ter uma capacidade inferior implica, contudo, que o país carece de condições para um desempenho eficiente, perante um choque exógeno desencadeado por AH.

Embora os indicadores não devam ser analisados de forma isolada, estes são mecanismos importantes de comparação entre países. Os indicadores que mais contribuem para afastar Portugal do nível superior de resiliência são: a competência (Portugal=3,6%; μ=4,83%); o investimento em inovação e desenvolvimento (1,4% do PIB; μ=1,65%); a qualidade regulamentar (índice WGI=0,97; μ=1,19); e o controlo da corrupção (índice WGI=0,76; μ=0,95). Se estes indicadores fossem equivalentes à média da UE, Portugal obteria um *totalscore* de 2,53, o que não seria suficiente para

atingir o nível mais alto de resiliência, mas que colocaria o país bem posicionado para atingir esse determinado nível.

Para perceber como a melhoria destes indicadores pode aumentar a resiliência económica, é necessário notar que Portugal foi um dos países mais afetados pela crise da dívida pública da Zona Euro, em 2011 (European Central Bank, s.d.). Após a crise, fruto da queda dos níveis de confiança na economia portuguesa, a comunidade internacional cortou drasticamente o investimento em Portugal (Eurostat, s.d.). No entanto, como refere o Presidente da República Portuguesa "[…] as empresas chinesas investiram em Portugal num momento de crise, que era um momento muito difícil para a economia portuguesa […] estiveram presentes quando outros que teriam podido estar, não estiveram" (Sousa, 2019, cit. por Barros & Sol, 2019).

Com efeito, estabeleceram-se em Portugal grandes empresas controladas pelo Estado chinês, com intervenção em sectores estratégicos como a energia, banca, água, saúde e seguros (Duarte, 2020), ocupando o país, até 2017, o décimo lugar da lista de países onde a China mais tinha investido e o segundo lugar dos países europeus, atrás da Suíça (Tartar, Rojanasakul & Diamond, 2018).

A aceitação do investimento chinês tornou-se inevitável e praticamente uma questão de sobrevivência nacional. Essa dependência criou naturalmente vulnerabilidades no instrumento de poder económico. Significa isso que, fruto das circunstâncias, a China encontra-se atualmente em posição de exercer pressão económica sobre o Estado português, para atingir os seus objetivos estratégicos. Um exemplo claro dessa capacidade está subjacente nas recentes declarações do embaixador Zhang Ming, chefe da missão da China para a UE, ao referir-se ao acordo de investimento entre Pequim e Bruxelas:

> Esperamos que Portugal, enquanto assume a presidência rotativa da UE, possa dar um 'empurrão' ao processo e, idealmente, esperamos que na primeira metade deste ano possamos assinar estes documentos. O acordo vai facilitar o acesso de investidores pelo que haverá mais investimento europeu na China e também mais investimento chinês na UE, incluindo em Portugal (Ming, 2021, cit. por Agência Lusa, 2021).

Para contrabalançar as vulnerabilidades inerentes da dependência do investimento chinês, Portugal deve procurar expandir os setores intensivos de tecnologia e conhecimento, por forma a atrair outros investimentos externos para o país. A Irlanda, à semelhança de Portugal, foi um dos países europeus mais

afetado pela crise da dívida pública da Zona Euro, no entanto, recebeu muitos investimentos no setor da tecnologia, sobressaindo atualmente no cenário europeu como um centro de inovação e tecnologia (Irlanda=9,2%; μ=4,83%), onde as empresas jovens podem colocar em prática as suas ideias inovadoras. Muito disso foi fruto do trabalho do Estado irlandês, que através de sua agência de promoção e desenvolvimento de investimentos estrangeiros, criou programas de atração de investimentos externos para o país.

O investimento em inovação e desenvolvimento também é um aspeto que influência cada vez mais os resultados económicos dos países. Contudo, a UE está a perder a sua relevância nessa matéria, em benefício do mercado chinês[51] (OCDE, s.d.). Num relatório produzido pela *BusinessEurope* (2020), o grupo empresarial mais influente da UE, é destacado que o investimento público e privado em inovação e desenvolvimento deve ser uma prioridade, por forma a melhorar os processos, produtos e serviços das empresas, e assim potencializar a sua competitividade, alavancar a economia e reequilibrar o relacionamento com a China.

No caso concreto de Portugal, o atraso relativo nesta matéria é estrutural, pois não tem permitido, entre outros, colmatar a dependência energética e tecnológica de terceiros, deixando o país numa posição fragilizada. Um exemplo de como a insuficiência tecnológica pode ser critica, encontra-se refletido no memorando assinado recentemente entre a Altice Portugal, a Huawei e a ZTE, para a utilização do equipamento e do software das companhias chinesas, no desenvolvimento da rede de telecomunicações e serviços 5G. Embora o relatório do Centro Nacional de Cibersegurança, que avalia os riscos nesta matéria, tenha sido classificado com a marca reservado, e por isso não tenha sido divulgado, vários países excluíram essas empresas (p.e. Republica Checa, Suécia, Estónia, Dinamarca), por considerarem que a sua inclusão permitiria às autoridades chinesas monitorizar as comunicações e o tráfego de dados.

Em matéria de energia, embora a taxa de dependência energética tenha vindo a diminuir, Portugal continua a ser um dos países da UE mais dependentes de terceiros. Em 2018, Portugal era o sétimo país com a maior dependência energética, cerca de 20% acima da média da UE. A prestação portuguesa também não foi das melhores no que respeita à eficiência energética da economia, tendo sido, no

[51] Desde 2014 que o investimento da UE em inovação e desenvolvimento fica aquém do investimento da China. Em 2019, a diferença foi de 124.000 milhões de dólares americanos (OCDE, s.d.).

mesmo ano, o 15º país com maior quantidade de energia primária despendida, para produzir uma unidade do PIB, cerca de 10% acima da média da UE (Observatório da Energia, Direção Geral de Energia e Geologia, & Agência para a Energia, 2020). Os mercados dos recursos fósseis (gás, petróleo e carvão) constituem a grande fatia das importações, tornando a eficiência energética da economia muito dependente da volatilidade desses mercados. À semelhança do que tem vindo a acontecer nos países nórdicos, a dependência externa portuguesa pode ser compensada com investimento nas atividades de investigação e desenvolvimento, que apoiem a conceção e aplicação de políticas públicas, na área das energias renováveis, para ampliar a diversificação energética e aumentar a segurança de abastecimento, perante uma perturbação de natureza física, que interrompa a produção de forma temporária ou permanente.

Também a qualidade regulamentar pode ter um papel importante no aumento da resiliência da economia nacional face as AH. Em abril de 2019, o Sindicato Nacional de Motoristas de Matérias Perigosas (SNMMP), atuando dentro da lei, teve o poder de paralisar o país, convocando uma greve de vários dias. A paralisação teve repercussões negativas não só nas empresas exportadoras e no turismo, que viram a sua reputação afetada, mas também em toda a economia do país. Não é claro que o SNMMP tenha atuado como intermediário de uma AH, no entanto o caso demonstra que existem lacunas no quadro legal, que podem ser exploradas por este tipo de atores, para afetarem o domínio económico.

A legislação desapropriada também propicia o aumento da corrupção, que pode, por exemplo, permitir o acesso a informação sensível ou alavancar vantagens económicas a empresas através de influência política. De acordo com um estudo da organização *Transparency Internacional* (Kowalczyk-Hoyer, 2016) sobre a transparência, as empresas chinesas estão entre as menos transparentes. Por seu lado, segundo o Índice de Perceção da Corrupção (CPI), uma ferramenta de medição dos níveis de corrupção do sector público de vários países, Portugal tem vindo a descer lugares, registando em 2020, a pontuação mais baixa de sempre. Quanto a isso, Susana Coroado, presidente da organização Transparency Internacional Portugal, é categórica na avaliação que faz:

> Ao longo dos últimos dez anos pouco ou nada tem sido feito pelo combate à corrupção em Portugal e os resultados do CPI são expressão dessa deriva. Os sucessivos governos e a classe política no geral olham para este flagelo como uma coisa menor, sem cuidar de perceber que

> o desenho e implementação de uma estratégia capaz de prevenir e combater eficazmente a corrupção é determinante para o presente e o futuro do nosso país […] (Coroado, 2021, cit. por Transparency Internacional Portugal, 2021).

Como fazem saber Esteves, Brito, Botelho e Sapage (2018) e Duarte (2020), é de notar a presença de ex-políticos nos quadros de empresas detidas pelo Estado chinês, bem como as boas relações entre estas empresas e os grandes escritórios de advocacia, desconhecendo-se as razões pelas quais isso acontece. Quer isto apenas dizer que, para garantir que não sejam veiculadas ações híbridas por via da corrupção, o Estado português deve exigir que as autoridades chinesas e as suas empresas melhorem os padrões de transparência. Deve, em simultâneo, avaliar de uma forma bastante cuidadosa os perigos de abordagens de investimento opacas, sobretudo quando se tratam de investimentos em infraestruturas estratégicas.

4.3.4. Síntese Conclusiva

No presente capítulo as variáveis e os indicadores identificados no ponto anterior foram integrados num modelo analítico, que indica que o domínio económico português apresenta um nível médio de resiliência. Não significa isso, contudo, que Portugal vacilará perante um choque exterior, mas sim que o país carece de condições para um desempenho eficiente.

Os indicadores que mais contribuem para afastar Portugal do nível superior de resiliência são: a competência; o investimento em inovação e desenvolvimento; a qualidade regulamentar; e o controlo da corrupção.

Com efeito, uma forma de melhorar a resiliência e contrabalançar as vulnerabilidades do domínio económico, sobretudo relacionadas com a dependência do investimento chinês, é expandir os setores intensivos de tecnologia e conhecimento, representados pelo indicador competência, por forma a atrair outros investimentos externos para o país, à semelhança do que fez a Irlanda, que se encontrava na mesma situação que Portugal após a crise da Zona Euro, em 2011.

O aumento do investimento em inovação e desenvolvimento também pode tornar Portugal mais resiliente, ao reduzir a dependência energética de terceiros, designadamente através da conceção e aplicação de políticas públicas, na área das energias renováveis, que permitam ampliar a diversificação energética e aumentar a segurança de abastecimento perante uma perturbação de natureza física, que interrompa a produção de forma temporária ou permanentemente. O

mesmo é válido para a dependência tecnológica de terceiros, que ficou evidente na necessidade recente de utilizar equipamento e software de companhias chinesas, no desenvolvimento da rede de telecomunicações e serviços 5G, permitindo às autoridades chinesas monitorizar as comunicações e o tráfego de dados.

Também a qualidade regulamentar tem um papel importante no aumento da resiliência da economia nacional face a AH. Não é claro que o SNMMP, quando teve o poder de paralisar o país, convocando uma greve de vários dias, em abril de 2019, tivesse atuado como intermediário de uma AH, no entanto o caso demonstra que existem lacunas no quadro legal, que podem ser exploradas por este tipo de atores, para afetarem o domínio económico.

Por fim, um maior controlo da corrupção tornará a economia do país mais resiliente, ao garantir que não são veiculadas ações híbridas por essa via. Para materializar esse controlo o Estado português deve, antes de mais, exigir que as autoridades chinesas e as suas empresas melhorem os padrões de transparência e, em simultâneo, avaliar com grande cuidado os perigos de abordagens de investimento opacas, sobretudo quando se trata de investimentos em infraestruturas estratégicas.

5. CONCLUSÕES

A UE e a OTAN têm vindo a ser confrontadas com um número significativo de novas ameaças que designam por AH. Em oposição ao conceito de GH, que se concentra no instrumento de poder militar, as AH consistem num orquestrar de ações sincronizadas, para atingir as vulnerabilidades das sociedades e dos Estados, nos diversos domínios.

Geralmente, os efeitos das ações que ocorrem num domínio acabam por se propagar em cascata e desestabilizar outros instrumentos de poder, sendo o sistema económico dos Estados-membros da UE um dos mais atrativos, devido à sua centralidade.

Tendo isso em consideração, o presente trabalho teve como OG avaliar o nível de resiliência da economia nacional face a AH. Para alcançar o objetivo delineado, foi adotado um raciocínio indutivo, assente no conhecimento base existente sobre os conceitos e as dimensões em análise, e seguida uma estratégia de investigação qualitativa, consubstanciada num estudo de caso, como desenho de pesquisa. A recolha de dados foi efetuada através da observação não participante e não estruturada, recorrendo a uma revisão e análise exaustiva da literatura reunida

de uma vasta gama de fontes bibliográficas, para alcançar o mais alto grau de precisão.

Em resultado da investigação, no terceiro capítulo concluiu-se que as AH atingem e exploram vulnerabilidades de um Estado, aumentando a intensidade de uma ou várias ferramentas e/ou fazendo escalada horizontal através do emprego de múltiplas ferramentas, para amplificar os efeitos. Os instrumentos de política económica são as principais ferramentas utilizadas pelas AH para afetar o domínio económico.

A Rússia é o Estado que mais emprega AH, pois não está em posição de ganhar uma confrontação militar ou uma competição económica contra a OTAN e os EUA, que representam os principais desafios aos seus interesses e à sua segurança. A mesma tem utilizado ciberataques, ações de desinformação e campanhas de influência financeira para interferir nos assuntos internos em diversos países da Europa e da América do Norte. Nos países que considera o seu *near abroad*, a estratégia passa por exercer controlo sobre os governos facilmente influenciável ou enfraquecer os líderes pró-ocidentais. Nos restantes países, a intensão é criar fissuras nas organizações coletivas, designadamente na OTAN e na UE, amplificando a discórdia política e social.

A utilização de AH também é declaradamente apoiada pelo PCC e pelas Forças Armadas chinesas, no entanto, em contraste com a prática russa de lutar para alcançar vitórias rápidas e decisivas, os chineses concentram-se mais na posição de vantagem a longo prazo, sustentando a campanha durante um período prolongado. Como maior credor a nível global, a China utiliza a ameaça de desinvestimento como instrumento de influência, para exercer pressão económica sobre os países economicamente mais dependentes. Alguns dos maiores investimentos têm recaído em infraestruturas, tecnologias e fatores de produção essenciais dos países europeus, o que tem deixado a UE preocupada quanto aos potenciais efeitos de segurança ou ordem pública.

As principais vulnerabilidades que as AH procuram explorar no domínio económico são: a dependência energética ou dependências de infraestruturas, que por sua vez podem gerar dependências económicas ou tornar-se num instrumento para exercer pressão económica; a dependência de IED, pois coloca o país recetor do investimento à mercê de investidores oportunistas; as dificuldades económicas e/ou desigualdades, que podem ser facilmente exploradas com ataques cibernéticos e campanhas de desinformação para influenciar os resultados eleitorais ou exercer

pressão indireta sobre o governo; o aumento descontrolado da dívida soberana ou da balança comercial e de pagamentos, que trás riscos para a segurança financeira e para o próprio sistema de segurança nacional; a corrupção, que pode amplificar ganhos na influência política, estabelecendo um ciclo desvirtuoso de corrupção, no qual o aumento do poder político permite um aumento do poder económico.

Para selecionar as variáveis e os indicadores para a conceção de um modelo de avaliação do domínio económico, as vulnerabilidades do domínio económico foram agregadas em dois grupos, a que correspondem duas variáveis, diretamente influenciáveis pelas ações empreendidas pelos decisores políticos e agentes económicos privados: a estabilidade macroeconómica e a boa governação.

Para avaliar as características estruturais da estabilidade macroeconómica, foram seguidos os conceitos do projeto de investigação ESPON, que demonstram que as áreas políticas que requerem ações para fomentar a resiliência macroeconómica são: a diversidade, a competência e a inovação.

Para quantificar a boa governação, foi seguida a base de dados WGI que abrange todos os Estados-membros da UE e comporta seis indicadores inter-relacionados: *voice and accountability*; estabilidade política e ausência de terrorismo e violência; eficácia governamental; qualidade regulamentar; Estado de Direito; controlo da corrupção.

No quarto capítulo foi criado um modelo analítico para avaliar a resiliência da componente económica nacional. Em resultado da aplicação desse modelo analítico, foi obtida a resposta à QC do presente estudo, concluindo-se que o domínio económico português apresenta um nível médio de resiliência face a AH, não significando, no entanto, que Portugal vacilará perante um choque exterior, mas sim que o país carece de condições para um desempenho eficiente.

Através do modelo analítico desenvolvido, verificou-se que Portugal se encontra num nível intermédio de resiliência, sendo os indicadores que mais contribuem para afastar o país do nível superior a competência, o investimento em inovação e desenvolvimento, a qualidade regulamentar, e o controlo da corrupção.

As vulnerabilidades do domínio económico estão sobretudo relacionadas com a dependência do investimento chinês. Com efeito, uma forma de as contrabalançar passa por ampliar os setores intensivos de tecnologia e conhecimento, por forma a atrair outros investimentos externos para o país.

A construção de resiliência também passa pelo aumento do investimento em inovação e desenvolvimento, para reduzir a dependência energética de terceiros,

designadamente através da conceção e aplicação de políticas públicas na área das energias renováveis, que permitam ampliar a diversificação energética e aumentar a segurança de abastecimento. O mesmo racional também se aplica à dependência tecnológica de terceiros, que se evidenciou recentemente na necessidade de utilizar equipamento e software de companhias chinesas no desenvolvimento da rede de telecomunicações e serviços 5G.

Outro indicador que necessita de ser melhorado está relacionado com a melhoria da qualidade regulamentar. As paralisações provocadas pelo SNMMP, em abril de 2019, demonstram que existem lacunas no quadro legal que podem ser exploradas por este tipo de atores, para afetarem o domínio económico.

Por último, um maior controlo da corrupção também tornará a economia do país mais resiliente, dificultando a veiculação de ações híbridas por essa via. Para melhorar esse controlo, o Estado português deve intimar as autoridades chinesas e às suas empresas a melhorarem os padrões de transparência e avaliar com grande cuidado os perigos de investimentos em infraestruturas estratégicas.

O instrumento de poder económico é uma das principais infraestruturas da sociedade, sendo por isso importante assegurar a sua resiliência. Neste contexto, como resultado do presente estudo e principal contributo para o conhecimento, releva-se o modelo analítico criado, que oferece aos interessados um instrumento prático e inovador, que pode ser usado como ferramenta de medição da resiliência da economia nacional e, consequentemente, pode apoiar a classe dirigente a decidir.

A investigação levada a cabo foi influenciada por duas limitações de grandeza maior. A primeira das quais foi imposta pela atual situação pandémica, obrigando a que a análise bibliográfica se cingisse, em grande parte, a documentos em suporte eletrónico. A segunda, prende-se com o facto da temática ainda não ter sido devidamente debatida nos fóruns nacionais, pelo que a recolha de dados foi realizada, sobretudo, em estudos internacionais.

Para estudos futuros, considera-se pertinente a realização de estudo comparativo dos resultados aqui alcançados com as medidas idealizadas no Plano de Recuperação e Resiliência, a implementar em Portugal até 2030, de forma a compreender em que direção evoluirá a resiliência do instrumento de poder económico face a AH.

REFERÊNCIAS BIBLIOGRÁFICAS

ACT. (2009). *Multiple futures project – Navigating towards 2030* (Final Report). Norfolk: OTAN. Disponível em https://www.act.nato.int/images/stories/events/ 2009/mfp /20090503_MFP.pdf

Agência Lusa. (2021, 30 de janeiro). *China "espera empurrão" de Portugal para acordo de investimento, diz Zhang Ming* [Página *online*]. Disponível em: https://eco.sapo.pt/2021/01/30/china-espera-empurrao-de-portugal-para-acordo-de-investimento-diz-zhang-ming/

Aho, A., Midões, C., & Šnore, A. (2020). *Hybrid threats in the financial system*. Manuscrito em preparação. Disponível em: https://www.hybridcoe.fi/wp-content/uploads/2020/07/20200630_Working-Paper-8_Web-1.pdf

Babbage, R. (2019). *Stealing a march: Chinese hybrid warfare in the Indo-Pacific; Issues and options for allied defence planners: case studies - volume II* [versão PDF]. Disponível em: https://csbaonline.org/research/publications/stealing-a-march-chinese-hybrid-warfare-in-the-indo-pacific-issues- /publication/2

Barros, R., & Sol, C. P. (2019, 27 de abril). *Quem são os 10 milionários chineses com quem Marcelo jantou?* [Página *online*]. Disponível em: https://rr.sapo.pt/2019/04/27/mundo/quem-sao-os-10-milionarios-chineses-com-quem-marcelo-jantou/especial/149445/

Blackwill, R. D., & Harris, J. M. (2016). The lost art of economic statecraft. *Foreign Affairs, 95*(2), 99–110. Disponível em: https://www.foreignaffairs.com/articles/2016-02-16/lost-art-economic-statecraft

Briguglio, L. (2003). *The vulnerability index and small island developing states: a review of conceptual and methodological*. Disponível em: https://www.um.edu.mt/__data/assets/pdf_file/0019/44137/vulnerability_paper_sep03.pdf

Briguglio, L. (2004). *Economic vulnerability and resilience: concepts and measurements. Em: L. Briguglio, & E. J. Kisanga (Ed.), Economic vulnerability and resilience of small states* 43–53. Malta: Islands and Small States Institute & The Commonwealth Secretariat.

BusinessEurope. (2020). *The EU and China. Adressing the systemic challenge* [versão PDF]. Disponível em: https://www.businesseurope.eu/sites/buseur/files/media/reports_and_studies/ the_eu_and_china_full_february_2020_version_for_screen.pdf

CE. (2016). *Quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*. Bruxelas: Autor. Disponível em: https://eur-lex.

europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016JC0018

CE. (2018). *Comunicação conjunta ao Parlamento Europeu e ao Conselho - Aumentar a resiliência*. Bruxelas: Autor. Disponível em: https://op.europa.eu/pt/publication-detail/-/publication/99d9f4ce-6ef9-11e8-9483-01aa75ed71a1

CE. (2020). *Guidance to Member States: recovery and resilience plans*. Bruxelas: Autor. Disponível em: https://ec.europa.eu/info/sites/default/files/document_travail_ service_part1_v2_en.pdf

Charron, N., Apuente, V., & Dijkstra, L. (2012). *Regional governance matters: A study on regional variation in quality of government within the EU*. Manuscrito em preparação. Disponível em: https://ec.europa.eu/regional_policy/sources/docgener/work/2012 _02_governance.pdf

Christopherson, S., Michie, J., & Tyler, P. (2010). Regional resilience: theoretical and empirical perspectives. *Cambridge Journal of Regions, Economy and Society, 3*(1), 3–10. Disponível em: https://www.researchgate.net/profile/Jonathan-Michie/ publication/227464573_ Regional-resilience-Theoretical-and-empirical-perspectives.pdf

CIDIUM. (2019). *Domínios e Áreas de Investigação* [Página *online*]. Disponível em: https://cidium.ium.pt/site/index.php/pt/investiga/dominios-areas- de-investigacao

Colon, C. (2016). *Modeling economic resilience* (Tese de Doutoramento em Economia). Université Paris-Saclay, Paris. Disponível em: https://pastel.archives-ouvertes.fr/tel-01495705/file/58245_COLON_2016_archivage.pdf

Cullen, P., & Reichborn-Kjennerud, E. (2017). *Countering hybrid warfare* [versão PDF]. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/ uploads/attachment_data/file/647776 /dar_mcdc_hybrid_warfare.pdf

Cullen, P., & Wegge, N. (2019). *'A deadlier peril': The role of corruption in hybrid warfare*. Norfolk: ACT, Multinational Capability Development Campaign.

Dorrel, O. (2017, 7 de setembro). *Alleged Russian political meddling documented in 27 countries since 2004* [Página *online*]. Disponível em: https://eu.usatoday.com/story/news/world/2017/09/07/alleged-russian-political-meddling-documented-27-countries-since-2004/619056001/

Drobniak, A. (2017). Economic resilience and hybridization of development – a case of the Central European Regions. *Regional Statistics, 7,* 43–62. Disponível em: https://www.researchgate.net/profile/Adam-Drobniak/

publication/320448239_Economic_resilience_and_hybridization_of_development.

Duarte, F. P. (2020). Non-kinetic hybrid threats in Europe – the Portuguese case study (2017-18). *Transforming Government: People, Process and Policy, 14*(3), 433-451. doi: 10.1108/TG-01-2020-0011

Durand, E. (2003). *Les transformations de l'US Army*. Paris: Institut Français des Relations Internationales. Disponível em: https://www.ifri.org/sites/default/files/atoms/files/ etudes1dedurand1.pdf

ESPON. (2014). *Territorial Dynamics in Europe - Economic Crisis and the Resilience of Regions* (Territorial Observation No. 12). Disponível em: https://www.espon.eu/sites/default/files/attachments/ESPON_Territorial-Observation_12-Crisis-Resilience.pdf

Esteves, P. F., Brito, A., Botelho, L., & Sapage, S. (2018, 5 de dezembro). *Os amigos da China* [Página *online*]. Disponível em: https://www.publico.pt/2018/12/05.

European Central Bank. (s.d.). *Long-term interest rate statistics for EU Member States* [Página *online*]. Disponível em: https://www.ecb.europa.eu/ stats/financial_markets_and_interest_rates/ /html/index.en.html

Eurostat. (s.d.). *European statistical recovery dashboard* [Página *online*]. Disponível em: https://ec.europa.eu/eurostat/web/main/data/database

Fabre, C. (2018). *Economic Statecraft: Human Rights, Sanctions, and Conditionality*. Cambridge: Harvard University Press.

Farrugia, N. (2007). *Conceptual issues in constructing composite indices*. Msida: Malta University. Disponível em: https://core.ac.uk/download/pdf/187769075.pdf

Fisher. M. (2015, 28 de junho). *How World War III became possible. A nuclear conflict with Russia is likelier than you think* [Página *online*]. Disponível em: https://www.vox.com/2015/6/29/8845913/russia-war

Galeotti, M. (2017). *Controlling chaos: how Russia manages its political war in Europe*. Londres: European Council on Foreign Relations. Disponível em: https://ecfr.eu/wp-content/uploads/ECFR228_-_CONTROLLING_CHAOS1.pdf

Giannopoulos, G., Smith, H., & Theocharidou, M. (2021). *The landscape of hybrid threats: A conceptual model*. Luxembourg: Publications Office of the European Union. doi: 10.2760/44985, JRC123305

Giles, K., Hanson, P. H., Nixey, J., Sherr, J., Wood, A., & Lyne, R. (2015). *The russian challenge* [versão PDF]. Disponível em: https://www.chathamhouse.org/2015/06/russian-challenge

German Marshall Fund. (s.d.). Authoritarian Interference Tracker [Página *online*]. Disponível em: https://securingdemocracy.gmfus.org/

Golam, M., & Monowar, M. (2018). Eurasian Economic Union: Evolution, challenges, and possible future directions. *Journal of Eurasian Studies, 9*(2), 163–172. doi: 10.1016/j.euras.2018.05.001

Greeven, M. J. (2020). Globalizing innovation ecosystem, entrepreneurs, and the digital Silk Road. Em: D. Cremer, B. McKern, & J. McGuire (Ed.), *The Belt and Road Initiative – opportunities and challenges of a Chinese economic ambition,* 236–258. New Delhi: Sage Publications.

Hill, E., Clair, T. S., Wial, H., Wolman, H., Atkins, P., Blumenthal, P., Ficenec, S., & Friedhoff, A. (2012). Economic shocks and regional economic resilience. Em: M. Weir, N. Pindus, H. Wial, & H. Wolman (Ed.), *Urban and regional policy and its effects: Building resilient regions* 193–274. Washington, D.C.: Brookings Institution Press.

Hirsch-Kreinsen, H. (2016). *Digitalisation and low-skilled work* [versão PDF]. Disponível em: https://library.fes.de/pdf-files/wiso/12864.pdf

Hoffman. (2007). *Conflict in the 21st Century: The Rise of Hybrid* [versão PDF]. Disponível em: https:/ /potomacinstitute.org/images/stories/publications_0108.pdf

Hybrid CeO, (s.d.). Hybrid threats as a concept [Página *online*]. Disponível em: https://www.hybridcoe.fi/hybrid-threats

Iancu, N., Fortuna, A., Barna, C., & Teodor, M. (2016). *Countering hybrid threats: lessons learned from Ukraine*. Washington, D.C.: IOS Press.

Johnson, D. E. (2011). *Hard fighting: Israel in Lebanon and Gaza* [versão PDF]. Disponível em: https://www.rand.org/pubs/monographs/MG1085.html

Kaufmann, D., & Kraay, A. (s.d.). Worldwide Governance Indicators [Página *online*]. Disponível em: http://info.worldbank.org/governance/wgi/Home/Reports

Kowalczyk-Hoyer, B. (2016). *Transparência em relatórios corporativos - avaliando multinacionais de mercados emergentes* [versão PDF]. Disponível em: https://images.transparencycdn.org/images/2016_TransparencyInCorporateReporting_EMMs_PT.pdf

Linkov, I., Baiardi, F., Florin, M. V., Greer, S., Lambert, M. J. H., & Trump, B. D. (2019). Applying Resilience to Hybrid Threats. *IEEE Security and Privacy Magazine, 17*(5).

Martin, R. (2012). Regional economic resilience, hysteresis and recessionary shocks. (1), 1–32.

Massa, I. (2011). *Export finance activities by the Chinese government* [versão PDF]. Disponível em: https:/ /www.europarl.europa.eu/RegData/etudes/note/join/2011/433862/EXPO-INTA_NT(2011)433862_EN.pdf

Mattis, J. N., & Hoffman, F. (2005). Future warfare: The rise of hybrid wars. *Proceedings*, 131(11), 18–19. Disponível em: http://milnewstbay.pbworks.com/f/MattisFourBlock WarUSNINov2005.pdf

Mazarr, M. J. (2015). *Mastering the gray zone: understanding a changing era of conflit* [versão PDF]. Disponível em: https://www.globalsecurity.org/military/library /report/2015/ssi_mazarr_151202.pdf

Mažeikis, E. (2015, setembro). Keynote speech. Em: Institute of International Relations and Political Science of the Vilnius University and the Ministry of Foreign Affairs of Lithuania, *Hybrid Threats: Overcoming Ambiguity, Building Resilience*. *Workshop* organizado pelo NATO Energy Centre of Excellence, Vilnius.

Monaghan. (2019). Countering Hybrid Warfare. So, what for the future Joint Force? *PRISM, 8*(2), 82–98. Disponível em: https:/ /ndupress.ndu.edu /Portals/68/Documents/prism/prism_8-2/PRISM_8-2_Monaghan.pdf

Nemeth, W. J. M. (2002). *Future war and Chechnya: a case for hybrid warfare* (Tese de Dissertação de Mestrado em *National Security Affairs*). Naval Postgraduate School, Monterey. Disponível em: http://hdl.handle.net/10945/5865

Norris, W. J. (2016). *Chinese economic statecraft: commercial actors, Grand Strategy, and State Control*. Ithaca: University Press.

Observatório da Energia, Direção Geral de Energia e Geologia, & Agência para a Energia. (2020). *Energia e Números*. Lisboa: Agência para a Energia. Disponível em: https://www.dgeg.gov.pt/media/43zf5nvd/energia-em-números-edição-2020.pdf

OCDE. (s.d.). *Gross domestic spending on R&D* [Página *online*]. Disponível em: https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm

OTAN. (2013). Comprehensive Operations Planning Directive. Mons: Autor. Disponível em: https://www.cmdrcoe.org/download.cgf.php?id=9

Pereira, P. I. M. (2017). *O impacto do investimento direto estrangeiro e do capital humano em Portugal* (Tese de Dissertação de Mestrado em Contabilidade). Universidade de Aveiro, Aveiro. Disponível em: https://ria.ua.pt/bitstream/10773/22913/1.pdf

Polyakova, A., Hansen, F. S., Noordaa, R., Bogen, Ø., & Sundbom, H. (2016). *The Kremlin's trojan horses 3*. Washington, D.C.: Atlantic Council. Disponível em: https://www.atlanticcouncil.org/wp-content/uploads/2021/02/The-Kremlins.pdf

Popescu, O., & Zamfir, R. (2018). *Propaganda made to measure: how our vulnerabilities facilitate Russian influence*. Bucharest: Global Focus. Disponível em: https://www.global-focus.eu/wp-content/uploads/2018/03.pdf

Putten, F. P. (2019). *The relevance of the Maritime Silk Road for the Netherlands*. Haia: Netherlands Institute of International Relations. Disponível em: https://www.clingendael.org/sites/default/files/2019.pdf

Putten, F. P., Hong, T., & Blécourt, J. (2018). Chinese investment in the port of Piraeus, Greece: the relevance for the EU and the Netherlands. Em: M. Ferchen, F. N. Pieke, F. P. Putten (Ed.), *Assessing China's Influence in Europe through Investments in Technology and Infrastructure*. *Four Cases* 14–23. Leiden: LeidenAsiaCentre.

Radin, A., & Reach, C. (2017). *Russian views of the international order*. Santa Monica: RAND Corporation.

Rocha, V. A. L. A. (2016). Análise da vulnerabilidade energética da Comunidade Europeia (Tese de Mestrado em Engenharia Eletrotécnica e de Computadores). Universidade do Porto, Porto. Disponível em: https://core.ac.uk/download/pdf/159366773.pdf

Rodgers, A. (1957). Some aspects of industrial diversification in the United States. *Economic Geography, 33*, 16–30. doi: 10.2307/142564

Russel, J. A. (2014). *Counterinsurgency american style: Considering David Petraeus and twenty-first century irregular war*. Small Wars & Insurgencies, 25(1), 69–90. Disponível em: https://www.tandfonline.com/doi/full/10.1080/09592318.2014.893956.

Santos, L. A. B., & Lima, J. M. M. (Coords.) (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.ª ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Siegel, P. B., Johnson, T. G., & Alwang, J. (1995). Regional economic diversity and diversification. *Growth and Change, 26*(2), 261–284. Disponível em: https://www.academia.edu/11370007/Regional_economic_diversity

Simmie, J., & Martin, R. (2010). The economic resilience of regions. *Cambridge Journal of Regions, Economy and Society, 3*(1), 27–43. Disponível em: https://

academic.oup.com/cjres/article-pdf/3/1/27/970612/rsp029.pdf

Sorensen, J. B., & Sorenson, O. (2007). *Corporate demography and income inequality*. *American Sociological Review, 72*(5), 766–783. Disponível em: https://www.jstor.org/stable/25472491

Tartar, A., Rojanasakul, M., & Diamond, J. S. (2018, 23 de abril). *How China is buying its way into Europe* [Página *online*]. Disponível em: https://www.bloomberg.com/graphics/2018-china-business-in-europe/

Tennis. (2020, 20 de julho). *Russia ramps up global elections interference: lessons for the United States* [Página *online*]. Disponível em: https://www.csis.org/blogs/technology-policy-blog/russia-ramps-global-elections-interference-lessons-united-states

The World Bank. (1992). *Governance and development* [versão PDF]. Disponível em: http://documents1.worldbank.org/curated/en/604951468739447676/pdf/multi-page.pdf

Transparency Internacional Portugal. (2021, 28 de janeiro). *Índice de perceção da corrupção 2020* [Página *online*]. Disponível em: https://transparencia.pt/corruption-perception-index/

Treverton, G. F., Thvedt, A., Chen, A. R., Lee, K., & McCue, M. (2018). *Adressing hybrid threats*. Estocolmo: Swedish Defence University. Disponível em: https:// www.hybridcoe.fi/wp-content/uploads/2020/07/Treverton-AddressingHybridThreats.pdf

Ucko, D. H. (2009). *The New Counterinsurgency Era*. Washington, D.C.: Georgetown University Press. Disponível em: http://www.jstor.org/stable/j.ctt2tt63s

UE. (2019). *Regime de análise dos investimentos diretos estrangeiros na União* (Regulamento (UE) 2019/452). Bruxelas: Autor.

US Senate. (2018). *Putin's asymmetric assault on democracy in Russia and Europe: implications for US national security* (Minority staff report prepared for the use of the Committee on Foreign Relations). Washington, D.C.: Autor. Disponível em: https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf

US DoD. (2010). *Quadrennial Defense Review Report*. Virgínia: Autor. Disponível em: https://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf

Walker, R. G. (1998). *The US Marine Corps and Special Operations* (Tese de Dissertação de Mestrado em *Defense Analysis*). Naval Postgraduate School, Monterey. Disponível em: https://apps.dtic.mil/dtic/tr/fulltext/u2/a359694.pdf

Wink, R. (2014). Regional Economic Resilience: Policy Experiences and Issues in Europe. *Raumforschung Und Raumordnung | Spatial Research and Planning, 72*(2), 83–84. Disponível em: https://doi.org/https://doi.org/10.1007/s13147-014-0283-x

Yordanova, G. D. (2018). *Sovereign debt as emerging challenge of hybrid warfare*. Sofia: New Bulgarian University. Disponível em: https://www.researchgate.net/313675600_Sovereign_Debt_as_Emerging_Challenge_of_Hybrid_Warfare.pdf

POSFÁCIO DO COORDENADOR

Diogo Lourenço Serrão é Tenente-coronel do Exército Português.

É mestre em Ciências Militares (especialidade Artilharia) pela Academia Militar; pós-graduado em Ciências Militares – Segurança e Defesa (Curso de Estado-Maior Conjunto) pelo Instituto Universitário Militar e em Seleção de Recursos Humanos pela Universidade Lusófona. Como formação complementar na área das ameaças híbridas, destaque para o NATO *Countering Hybrid Threat Course* na NATO *Special Operations School* em Chièvres, Bélgica.

Ao longo da sua carreira, desempenhou funções:

- De Comando: no Regimento de Artilharia n.º 4, como Comandante da Bateria de Tiro e da 2ª Bateria de Bocas de Fogo da Brigada de Reação Rápida entre 2005 e 2006, no Centro de Tropas de Operações Especiais, como Comandante do Grupo de Operações CHARLIE e DELTA entre 2008 e 2010 e na Academia Militar, como Comandante da 3ª Companhia de Alunos, entre 2011 e 2013.

- De Estado-Maior: no Regimento de Artilharia nº 4, como Chefe da Secção de Pessoal, entre 2015 e 2016 e Chefe da Secção de Operações, Informações e Segurança, em 2017.

- De Docência: na Área de Ensino Específico do Exército, como professor dos Cursos de Promoção a Oficial Superior e dos Cursos Avançados de Planeamento Militar Terrestre, a partir de 2019.

Da sua experiência profissional faz ainda parte, a participação como Comandante do Destacamento de Operações Especiais em 2008 no Teatro de Operações do Kosovo; *Advisor* do Sp*ecial Operations Directorate* no Teatro de Operações do Afeganistão em 2017, Assessor Técnico Permanente e Diretor Técnico do Projeto nº 5 da Cooperação Militar entre Portugal e Angola em 2022.

Tem participado em seminários e conferências, de âmbito nacional e internacional, no quadro da NATO e do Centro de Excelência para o Combate a Ameaças Híbridas em Helsínquia, Finlândia; e é Investigador Integrado do Centro de Investigação e Desenvolvimento do IUM. Foi, no quadro das ameaças híbridas, representante do Ministério de Defesa Nacional no Grupo de Redação do Documento Nacional para o combate a ameaças híbridas e tem participado como conferencista na Pós-Graduação em Conflitos Armados e Direitos Humanos Centro de Direitos Humanos, uma parceria entre o Instituto Universitário Militar (IUM) e o Ius Gentium Conimbrigae/Centro de Direitos Humanos (IGC/CDH). Tem alguns artigos publicados. Presentemente, é professor da área de ensino específico do Exército.