ACADEMIA MILITAR

Portugal face às Ameaças Híbridas: o imperativo de adequação a um novo desafio

Autor: Aspirante de Infantaria Diogo Augusto Mesquita Fonte

Orientador: Tenente-Coronel Professor Doutor Proença Garcia
Coorientador: Professor Eurico Rodrigues

Mestrado Integrado de Ciências Militares na Especialidade de Infantaria
Relatório Científico Final do Trabalho de Investigação Aplicada
Lisboa, maio de 2023

ACADEMIA MILITAR

Portugal face às Ameaças Híbridas: o imperativo de adequação a um novo desafio

Autor: Aspirante de Infantaria Diogo Augusto Mesquita Fonte

Orientador: Tenente-Coronel Professor Doutor Proença Garcia
Coorientador: Professor Eurico Rodrigues

Mestrado Integrado de Ciências Militares na Especialidade de Segurança
Relatório Científico Final do Trabalho de Investigação Aplicada
Lisboa, maio de 2023

EPÍGRAFE

“If you want something you’ve never had, you must be willing to do something you’ve never done”

— Thomas Jefferson

DEDICATÓRIA

Aos meus pais,

Por todos os sacrifícios que fizeram por mim.

Às minhas avós,

Que por mais que fosse difícil nunca duvidaram de mim e sempre me apoiaram.

Ao Daniel, ao Francisco, ao Bruno, ao Paulo, ao João e à Barbara,

Por terem feito parte desta longa jornada onde sempre me apoiaram e nunca me deixaram cair. Um enorme obrigado a todos vós.

Ao Filipe, em especial, meu parelha eterno, por todas as memórias, histórias e momentos que nunca esquecerei.

Ao João e ao Fábio, amigos mais antigos,

Que nunca me deixaram de apoiar, independentemente das circunstâncias da vida, estando sempre presentes.

Sou-vos muito grato.

AGRADECIMENTOS

Cinco anos se passaram desde os meus primeiros passos na Academia Militar. Muito aconteceu – dificuldades, sorrisos, tristezas, superações. Em primeiro lugar, quero demonstrar o meu profundo reconhecimento à mui nobre instituição Academia Militar, por estes cinco anos de formação. Estarei eternamente em dívida. Porém, nada disto teria sido possível sem um conjunto de pessoas que se cruzaram no meu caminho tornando-o mais enriquecedor. Desde já uma enorme gratidão a todos vocês.

Ao meu orientador, Tenente-Coronel Professor Doutor Proença Garcia, primeiramente por ter aceite o desafio de me orientar nesta investigação, como também pelo seu exemplo de profissionalismo, disponibilidade, transparência e, acima de tudo, exemplo, pois descobri que o sucesso é uma conquista contínua e emocionante. Não há limites para o que podemos alcançar se estivermos dispostos a dedicarmo-nos de corpo e alma.

Ao meu coorientador, Professor Eurico Rodrigues, pelo nível de conhecimento transmitido e pela confiança depositada, que dentro de todas as suas funções sempre se mostrou disponível em auxiliar-me.

Ao Tenente-Coronel de Artilharia André, o qual posso chamar de amigo. Desde o primeiro dia nesta minha jornada me acompanhou e se disponibilizou para tudo com prontidão imensa.

Aos diretores de curso de Infantaria, pelos ensinamentos e transmissão de disciplina e valores, e a todos os excelentíssimos oficiais que se disponibilizaram e prescindiram do seu valioso tempo para responder às minhas entrevistas contribuindo positivamente para este trabalho.

Ao meu curso, em especial ao curso de Infantaria, por estes cinco anos. Muito me ensinaram, muito vivemos e que mais tarde irei recordar vivamente, todas as nossas histórias perdurarão no tempo.

Filipe, Daniel e Francisco, sem dúvida as pessoas mais importantes para mim nesta jornada, que em tudo me ajudaram e sempre contribuíram positivamente para o meu sucesso. Obrigado, irmãos.

E por último, e nunca menos importante, aos meus pais. A eles lhes devo a vida e tudo o que sou hoje. Um agradecimento sincero e um orgulho eterno em vocês.

A todos, muito obrigado,

Diego Fonte.

RESUMO

A mudança da sociedade para um novo paradigma civilizacional, caracterizado pelo surgimento de ameaças transnacionais e digitais e pelo declínio das guerras interestatais convencionais, realçou a importância das ameaças híbridas como um grande desafio para a segurança e a defesa nacional. Em resposta, é necessária uma abordagem abrangente e integrada para prevenir e combater eficazmente estas ameaças, o que exige a coordenação de vários aspetos da defesa nacional e o envolvimento de toda a sociedade.

Esta investigação tem como objetivo avaliar as capacidades militares de Portugal em relação à guerra híbrida e investigar os pontos fortes e fracos do país neste domínio. Ao examinar as várias dimensões das ameaças híbridas e avaliar a eficácia da resposta de Portugal às mesmas. Este estudo procura contribuir para uma melhor compreensão dos desafios e oportunidades que o país enfrenta neste ambiente em rápida evolução.

Alicerçado ao presente estudo encontram-se quatro objetivos específicos, cada um deles exigindo uma investigação meticulosa e aprofundada. O primeiro objetivo passa por identificar as atuais limitações da defesa nacional contra as ameaças híbridas, identificando assim áreas de melhoria para a capacidade de defesa do país. O segundo objetivo é identificar e avaliar métodos e estratégias que possam aumentar a eficiência dos esforços para prevenir e combater as ameaças híbridas. Quanto ao terceiro objetivo, interessa analisar os conflitos europeus significativos e as suas consequências para compreender melhor o contexto em que as ameaças híbridas podem surgir. Finalmente, o quarto objetivo é examinar o papel das Forças Armadas na defesa nacional contra as ameaças híbridas e identificar formas de aumentar a sua eficácia na salvaguarda do país.

Esta investigação carateriza-se por apresentar uma estratégia de investigação qualitativa, definindo-se como um estudo exploratório-descritivo. Assim, iniciamos esta investigação pelo enquadramento teórico, tendo em conta a imensidão de pesquisa sobre o tema. Como técnica de recolha de dados, recorreu-se à análise documental e elaboração de entrevistas.

Assim sendo, como resultados obteve-se que Portugal necessita de um investimento na consciencialização geral no que diz respeito a esta temática de forma a atingir os níveis idealmente desejáveis, investir em tecnologias avançadas, treino especializado e exercícios realistas.

Palavras-chave: Ameaças Híbridas, Combate, Capacidades, Formação

ABSTRACT

Society's shift to a new civilizational paradigm, characterized by the emergence of transnational and digital threats and the decline of conventional interstate wars, has highlighted the importance of hybrid threats as a major challenge to security and defense. In response, a comprehensive and integrated approach is needed to effectively prevent and counter these threats, which requires the coordination of several aspects of national defense and the involvement of the entire society.

The aim of this research is to assess Portugal's military capabilities regarding hybrid warfare, and to investigate the country's strengths and weaknesses in this domain. By examining the various dimensions of hybrid threats and evaluating the effectiveness of Portugal's response to them. This study seeks to contribute to a better understanding of the challenges and opportunities facing the country in this rapidly evolving environment.

Underpinning this study are four specific objectives, each requiring thorough and in-depth research. The first objective is to identify the current limitations of the national defense against hybrid threats, thereby identifying areas of improvement for the country's defense capability. The second objective is to identify and evaluate methods and strategies that can increase the efficiency of efforts to prevent and counter hybrid threats. The third objective is to analyze significant European conflicts and their consequences to better understand the context in which hybrid threats may arise. Finally, the fourth objective is to examine the role of the Armed Forces in national defense against hybrid threats and identify ways to increase their effectiveness in safeguarding the country.

This research is characterized by a qualitative research strategy, defined as an exploratory-descriptive study, thus we began this research with the theoretical framework, considering the immensity of research on the subject. As data collection techniques, we used document analysis and interviews.

The results obtained were that Portugal needs to invest in a general awareness of this issue in order to reach the ideally desirable levels, invest in advanced technologies, specialized training, and realistic exercises.

Keywords: Hybrid Threats, Combat, Capabilities, Training

ÍNDICE GERAL

EPÍGRAFE i
DEDICATÓRIA ii
AGRADECIMENTOS iii
RESUMO iv
ABSTRACT v
ÍNDICE GERAL vi
ÍNDICE DE FIGURAS viii
LISTA DE APÊNDICES ix
LISTA DE ANEXOS x
LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS xi
INTRODUÇÃO 1
PARTE I – ENQUADRAMENTO TEÓRICO 4
CAPÍTULO 1 - A ORIGEM E EVOLUÇÃO DO CONCEITO DE GUERRA HÍBRIDA . 4
1.1 Guerra Híbrida: Enquadramento Histórico 4
1.2 Ameaças Híbridas: Conceptualização e Multidimensionalidade 8
1.3 Tipologia de Ameaças Híbridas e Modelo Conceptual 11
1.4 CiberWar 12
1.5 Síntese Conclusiva 14
CAPÍTULO 2 - O PAPEL DOS ESTADOS NO COMBATE ÀS AMEAÇAS HÍBRIDAS 15
2.1 Ameaças e Desafios ao Estado de Direito 15
2.2 Portugal e a sua relação com a política externa 15
2.3 Síntese Conclusiva 19
PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO 20
DE CAMPO 20
CAPÍTULO 3 - METODOLOGIA, MÉTODOS E MATERIAIS 20

3.1 Definição dos objetivos de investigação 20
3.2 Tipo de Estudo 20
3.3 Técnicas, procedimentos e meios utilizados 21
3.4 Recolha de dados 22
3.5 Amostragem: composição e justificação 23
3.6 Tratamento dos dados 25
CAPÍTULO 4 - APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS 27
4.1 Resultados 27
4.2 Discussão de Resultados 32
CONCLUSÕES 37
REFERÊNCIAS BIBLIOGRÁFICAS 40
APÊNDICES I
ANEXOS XXI

ÍNDICE DE FIGURAS

Figura nº 1 – Modelo conceptual do Hybrid CoE 12

LISTA DE APÊNDICES

APÊNDICE A – MODELO DE ANÁLISE II

APÊNDICE B – ESTRUTURA BASE DO BLOCO DE ENTREVISTAS III

APÊNDICE C – LISTA E CARATERIZAÇÃO DOS ENTREVISTADOS V

APÊNDICE D – CODIFICAÇÃO ALFANUMÉRICA DAS ENTREVISTAS VI

APÊNDICE E – ANÁLISE DE CONTEÚDO DAS ENTREVISTAS IX

LISTA DE ANEXOS

ANEXOS XXII

ANEXO A – ATIVIDADE HÍBRIDA DA RÚSSIA NA UCRÂNIA XXII

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AH	AMEAÇAS HÍBRIDAS
CEDN	CONCEITO ESTRATÉGICO DE DEFESA NACIONAL
CPLP	COMUNIDADE DOS PAÍSES DE LÍNGUA PORTUGUESA
EP	EXÉRCITO PORTUGUÊS
FFAA	FORÇAS ARMADAS
FND	FORÇAS NACIONAIS DESTACADAS
GH	GUERRA HÍBRIDA
GNR	GUARDA NACIONAL REPUBLICANA
ISIL	ESTADO ISLÂMICO DO IRAQUE E DO LEVANTE
MINUSCA	UNITED NATIONS MULTIDIMENSIONAL INTEGRATED STABILIZATION MISSION IN THE CENTRAL AFRICAN REPUBLIC
MCDC	MULTINATIONAL CAPABILITY DEVELOPMENT CAMPAIGN
MDN	MINISTÉRIO DA DEFESA NACIONAL
NATO	NORTH ATLANTIC TREATY ORGANIZATION
OE	OBJETIVO ESPECÍFICO
OG	OBJETIVO GERAL
ONU	ORGANIZAÇÃO DAS NAÇÕES UNIDAS
PCSD	POLÍTICA COMUM DE SEGURANÇA E DEFESA
PD	PERGUNTA DERIVADA
PP	PERGUNTA DE PARTIDA
TC	TRAINING CIRCULAR
UE	UNIÃO EUROPEIA

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (RCFTIA), intitulado por "*Portugal face às Ameaças Híbridas: o imperativo de adequação a um novo desafio"* foi desenvolvido como parte do ciclo de estudos da Academia Militar, referente ao Mestrado Integrado de Ciências Militares na Especialidade de Infantaria.

A crescente complexidade do cenário internacional e o surgimento de novas formas de ameaças têm exigido aos países uma reavaliação constante das suas estratégias de defesa. Nesse contexto, a Guerra Híbrida (GH) tem-se revelado uma preocupação cada vez mais relevante, pois combina diferentes métodos e táticas para alcançar objetivos políticos e militares, desafiando as estruturas tradicionais de segurança (Bilal, 2021). No caso de Portugal, é essencial analisar as mudanças necessárias para atingir um nível de defesa ótimo contra a GH e, por isso, objetivamos identificar as mudanças a serem realizadas em Portugal visando um nível de defesa contra a GH mais eficaz.

Em linha de pensamento de Bachmann (2015), a GH representa um desafio multifacetado que vai além dos confrontos militares convencionais, envolvendo estratégias de desinformação, ciberataques, sabotagens, influência política e social, entre outros. A fim de garantir que um país se defenda eficazmente contra este tipo de guerra, é exigida uma abordagem holística, que integre os diversos setores governamentais e sociais.

Nesse contexto, é importante destacar o papel das Forças Armadas (FFAA), que desempenham um papel crucial na defesa do país (Drab, 2018). No entanto, diante das mudanças na natureza das ameaças, é necessário adaptar as estratégias, capacidades e treinos para enfrentar os desafios da GH de forma mais eficiente (Fernandes, 2016).

Ao identificar as limitações existentes, como lacunas na capacidade de informações, deficiências na segurança cibernética ou falta de coordenação interinstitucional, será possível direcionar esforços para superar esses obstáculos. Além disso, é fundamental analisar métodos eficientes utilizados por outros países e organizações, adaptando-os à realidade portuguesa e considerando as especificidades do país.

A compreensão dos conflitos em curso e das ameaças à Europa é essencial para contextualizar a GH e suas repercussões para Portugal. Através dessa análise, será possível identificar tendências, padrões e possíveis cenários futuros, permitindo a elaboração de estratégias de defesa efetivas e idóneas.

Por fim, é necessário avaliar o impacto dessas mudanças e desafios para as FFAA Portuguesas, o que envolve a revisão das políticas de recrutamento, treino e capacitação dos militares, bem como o desenvolvimento de capacidades e recursos necessários para enfrentar as ameaças da GH de forma competente.

Ao cumprir os objetivos propostos e responder às perguntas que se ergueram, este estudo procura contribuir para a promoção de uma defesa mais robusta face à GH em Portugal. A análise cuidadosa dessas questões permitirá identificar as mudanças necessárias, fortalecer as capacidades de defesa e garantir a segurança e a soberania do país no atual contexto internacional.

Assim, este trabalho, com base numa investigação exploratória-descritiva de natureza qualitativa, contribuirá para, em primeiro lugar, compreender as lacunas presentes na Defesa Nacional bem como perceber quais as mudanças a realizar para aumentar as suas capacidades nesta luta tão vigente.

Após realizado um enquadramento explicação do motivo da investigação, formulou-se a pergunta de partida (PP): **"Quais são as mudanças a realizar em Portugal para atingir um adequado nível de defesa contra as Ameaças Híbridas?"**.

A PP acima enunciada visa alcançar o objetivo geral (OG): "Analisar a evolução teórico-prática das AH, com enfoque no posicionamento de Portugal"

De maneira a compreender mais detalhadamente o OG do trabalho estabeleceram-se objetivos específicos (OE), de caráter mais prático e instrumental. Estes objetivos têm por finalidade dividir e analisar em partes menores o objetivo geral, de acordo com a abordagem de Walliman (2011). Para a seguinte investigação identificaram-se os OE a seguir:

- OE1: Identificar as limitações da defesa contra a Guerra Híbrida;

- OE2: Identificar métodos para alcançar eficiência neste âmbito;

- OE3: Identificar os conflitos europeus e as suas repercussões;

- OE4: Compreender qual a tarefa das Forças Armadas;

Para a prossecução dos objetivos definidos, o presente trabalho de investigação divide-se em duas partes. A Parte I expõe aquilo que diz respeito ao enquadramento teórico, dividindo-se em dois capítulos (1); A origem da evolução do conceito de Guerra Híbrida e (2) O papel dos Estado no combate às Ameaças Híbridas. Já no que concerne à Parte II, esta contempla os seguintes capítulos: (3) Metodologia, métodos e materiais; (4) Apresentação, análise e discussão de resultados e, por fim, as conclusões.

Surge ainda uma parte pós-textual, constituída por apêndices e anexos que em tudo contribuem para uma melhor investigação e compreensão da matéria a ser estudada.

PARTE I – ENQUADRAMENTO TEÓRICO

CAPÍTULO 1 - A ORIGEM E EVOLUÇÃO DO CONCEITO DE GUERRA HÍBRIDA

1.1 Guerra Híbrida: Enquadramento Histórico

Com o términus da Guerra Fria, novos conceitos surgiram no debate sobre a natureza mutável da guerra e as diferenças entre guerras passadas, presentes e futuras. Olhando para a evolução da dinâmica dos conflitos nas últimas décadas, podemos observar diferentes realidades e fenómenos num contexto cada vez mais complexo. Contudo, nas guerras modernas, os atores estatais enfrentam ou competem com novos atores num ambiente de ameaça amplo e diversificado motivado por fatores étnicos, económicos, sociais e religiosos, citando apenas alguns. Este é o caso de alguns conflitos contemporâneos, as chamadas guerras híbridas, em que potenciais adversários – estados, grupos patrocinados pelo estado ou atores autofinanciados – exploram a disponibilidade de capacidades militares sofisticadas (Fernandes, 2017).

A emergência de conceitos e temas de GH nos últimos anos não expressa o fim da guerra convencional ou da própria agressão convencional. Levanta, contudo, novas questões de tomada de decisão e coordenação de respostas que vão além das puramente militares em termos de competência e responsabilidade.

Andersson et al. (2015) consideram ser importante que os Estados e as organizações internacionais de segurança e defesa, em cooperação com os seus parceiros, desenvolvam um entendimento comum, explorem e aperfeiçoem os possíveis elementos da GH para refletir a natureza mutável e "híbrida" da guerra, e desenvolvam novas formas de pensar para responder eficazmente a estas ameaças.

Estes novos conflitos são caracterizados pela necessidade de reduzir a violência face ao aumento da capacidade destrutiva das armas, pela diminuição da probabilidade de conflitos em larga escala entre as grandes potências, pela emergência de conflitos intraestatais, pela tendência para a fragmentação e enfraquecimento do poder estatal e pela propagação de ameaças sob a forma de atos de violência não convencionais. Onde se incluem ameaças político-estratégicas e sociopolíticas, bem como AH que consistem em elementos

táticos, irregulares e criminosos trabalhando em conjunto para alcançar os mesmos objetivos estatais (Lousada et al., 2010).

Tais ameaças não se limitam aos atores não estatais, e os Estados podem transformar as suas forças tradicionais em forças irregulares e adotar novas táticas. Exemplos incluem a *fedayeen* (organização paramilitar) no Iraque, em 2003, e o recente destacamento de tropas sem uniformes estatais – chamados pequenos homens verdes – na campanha de 2014 na Ucrânia. O desafio consiste em identificá-los, compreendê-los e combatê-los.

Estes novos conflitos tendem a envolver intervenções extraterritoriais e multilaterais, como foi o caso no Iraque, onde se sucederam tanto intervenções pró-governamentais como pró-insurgência. Os objetivos prosseguidos são diversos e sobrepostos (não apenas a aquisição e retenção de poder), o controlo da informação tornou-se muito importante nos conflitos, e a propaganda tornou-se um objetivo-chave de muitas operações para influenciar a opinião pública (Dourado et al., 2020).

A "cor" da guerra está a assumir proporções alarmantes. Os conflitos armados têm mudado drasticamente. Mais atores não estatais e menos Estados estão envolvidos em "novas guerras" com ameaças difusas, onde os conflitos muitas vezes não têm objetivos políticos. Os Estados já não têm um monopólio exclusivo sobre o uso da força, porém esta continua a basear-se em considerações políticas.

Uma análise da história recente dos conflitos armados mostra muitos exemplos em que as partes que detinham os meios melhores e mais eficazes ganharam, são exemplos a guerra no Kosovo causada pelas diferenças tecnológicas entre as forças aliadas e jugoslavas, ou a Guerra do Golfo de 1991 (Jerónimo et al., 2003).

Nos conflitos modernos, o sucesso já não depende da capacidade de destruir o inimigo, mas sim da capacidade de lhe negar o apoio da população e de o isolar do apoio que necessita. Só assim podemos compreender porque é que a superioridade militar tradicional é ineficaz nas guerras civis ou de contrainsurgência (Schurman, 2011).

A maioria dos proponentes da "nova guerra" acredita que, ao contrário do modelo de Clausewitz, as características fundamentais da guerra estão a mudar. Os argumentos apresentados dizem respeito à inconsistência entre o conceito trinitário de guerra e a utilização da guerra como instrumento político.

Smith (2020), debruçou-se sobre o tema e considerou que a guerra não assumirá mais o papel principal enquanto facto definidor dos conflitos internacionais, perde essência, e as novas guerras sofrerão uma mudança de paradigma no sentido da guerra industrial entre Estados para conflito estratégico entre as partes.

Contudo, notamos que ainda existem guerras em que ambos os paradigmas – ou uma fusão evolutiva entre eles – podem ser observados, tais como o conflito israelo-árabe, que inclui tanto a guerra industrial como a guerra étnica; a guerra do Iraque de 2003, que evoluiu de uma clássica guerra industrial clausewitziana para um conflito complexo característico de "novas guerras"; e o conflito de 2014 entre a Rússia e a Ucrânia, caracterizado como uma GH.

Na guerra moderna, ao contrário dos paradigmas anteriores, os indivíduos combatem Estados-nação fora da estrutura do Estado-nação (por exemplo, o terrorismo) (Smith, 2020). Ainda que a realidade da guerra continue a mudar, as mudanças que ocorrem são devidas a fatores contextuais e não fundamentais – nomeadamente os combatentes, os seus objetivos e as armas que utilizam. Schurman (2011) observa de igual forma que nenhum elemento de conflito armado, passado ou presente, escapa à influência clausewitziana do acaso e do destino, e de que cada guerra, independentemente da forma que a caracterize, é moldada pela interação dos elementos eternos da tríade paradoxal.

Assim, o termo GH surgiu no início do século XXI, quando os exércitos ocidentais se encontravam em ambientes operacionais complexos e desafiantes como o Afeganistão e o Iraque, e os teóricos da guerra procuravam compreender melhor a sua evolução, incluindo a natureza da guerra nestes conflitos. Contudo, com a anexação da Crimeia e a intervenção militar russa na Ucrânia oriental, esta questão assumiu uma nova interpretação, levando a NATO a classificá-la como GH e a enfatizar a sua importância, a fim de se preparar para futuras ameaças à aliança atlântica (Santiáñez, 2018).

Este conceito refletiu-se na declaração final da Cimeira do País de Gales de 2014, onde os líderes reafirmaram que a Aliança deve estar efetivamente preparada para enfrentar os desafios únicos da GH, que utiliza uma série de atividades militares, paramilitares e políticas encobertas num contexto altamente integrado (NATO, 2015).

O termo GH tem sido utilizado desde pelo menos 2005 e foi usado na Segunda Guerra do Líbano em 2006 para qualificar a estratégia do Hezbollah que consistia em combinar táticas e capacidades de guerra convencionais com atividades criminosas de guerrilha para contrariar a superioridade tecnológica das Forças de Defesa de Israel. Hodiernamente, desde 2013, tais operações têm sido associadas ao Estado Islâmico do Iraque e do Levante (ISIL), que combina operações militares convencionais com o terrorismo, crime organizado, guerra cibernética entre outras atividades.

O termo “híbrido” na guerra pode ser amplamente definido como uma combinação de meios e métodos convencionais e/ou não convencionais, envolvendo forças táticas e não convencionais.

Embora haja algum consenso sobre as características da GH, não há consenso relativamente à ideia de que esta forma de conflito seja nova (Fernandes, 2017). Muitos teóricos argumentam que não se trata de um fenómeno novo. Existem inclusive inúmeros exemplos da utilização de estratégias características deste tipo de guerra em guerras anteriores: A Guerra da Independência Americana (1775-1783) e a Guerra do Vietname, envolvendo o exército regular do Vietname do Norte – principalmente capacidades convencionais – e as forças vietcongues irregulares – táticas irregulares – que combateram um conflito coordenado e contínuo contra as forças convencionais dominadas pela França e pelos Estados Unidos (Dourado et al., 2020).

A combinação de meios táticos e irregulares foi igualmente comum na guerra do Iraque de 2003, mais uma vez refletindo a natureza adaptativa da ameaça. No entanto, a utilização e exploração do conceito de GH é mais recente. Os acontecimentos de 11 de setembro de 2001 e a guerra Israel-Líbano de 2006 estimularam a investigação nesta área, particularmente no que diz respeito à dimensão assimétrica do fenómeno.

Frank Hoffman, um investigador e analista militar americano, desempenhou um papel de liderança no desenvolvimento da teoria da GH. Hoffman (2007) salienta que a GH engloba várias formas de guerra, incluindo capacidades convencionais, táticas e formações não organizadas, atos terroristas, incluindo violência em massa e coerciva, e arrastão.

Enquanto no passado as componentes táticas e organizadas de um conflito ocorriam em diferentes locais e formações, no atual conceito de GH estas forças são indistinguíveis dentro de uma única força e campo de batalha e a componente desorganizada determina frequentemente o equilíbrio das operações.

A GH é entendida como o uso centralmente planeado e dirigido de uma variedade de táticas encobertas e evidentes, desde operações de inteligência e ciberoperações até à pressão económica e força convencional, tanto por atores militares como civis (European External Action Service, 2015), sendo que um dos principais objetivos da GH é desestabilizar governos e instituições inimigas, criando caos e um vácuo de poder (Blum et al., 2015).

Embora estes conceitos não sejam nem homogéneos, nem novos, e enfrentem desafios cada vez mais distintos, combinam-se para criar uma nova forma de guerra. Combinando ainda conflitos de estado mortíferos com o fervor fanático e sustentado da guerra irregular.

1.2 Ameaças Híbridas: Conceptualização e Multidimensionalidade

O termo GH enfatiza a aparente complexidade da guerra, a multiplicidade de atores e o esbatimento das categorias de conflitos tradicionais, incluindo, necessariamente AH. Para melhor entendimento, As AH são definidas como ameaças de adversários existentes ou potenciais, incluindo Estados, atores não estatais e terroristas, que tenham demonstrado ou possam demonstrar a capacidade de utilizar meios convencionais e não convencionais para alcançar os seus objetivos (U.S. Government Accountability Office, 2010).

A avaliação da NATO e o relatório de agosto de 2010 "*Military Contributions to Countering Hybrid Threats*" estabeleceu uma abordagem comum para enfrentar as AH e um quadro que permita às organizações desenvolver respostas eficazes a estes desafios. As AH permitem que os adversários – incluindo Estados, atores não estatais ou organizações terroristas – possam utilizar operações combinadas para alcançar os seus objetivos num ambiente operacional cada vez mais ilimitado (NATO, 2010).

De acordo com o quadro da aliança atlântica, as AH caracterizam-se por "indivíduos e grupos interligados", com as seguintes características:

- Utilização eficiente das novas tecnologias de comunicação para a partilha e cooperação de informação;
- Reconhecimento da importância estratégica da circulação internacional dos meios de comunicação social e utilizando-a para alcançar os seus objetivos específicos;
- Utilização de ferramentas que incluem tanto meios não letais como uma combinação de métodos letais e criminosos apoiados por agências de informações legítimas e organizações comerciais;
- Exploração hábil de diferentes interpretações nacionais e limitações do direito internacional e das leis da guerra para sobressair sobre estratégica e tacitamente os seus opositores (NATO, 2010).

A U.S. Army Training Circular (TC) 7-100 (U.S. Army, 2010) estabelece uma ameaça híbrida como uma combinação dinâmica de forças táticas, irregulares e imprevisíveis, que podem incluir elementos criminosos, cooperando com estas forças para atingir um objetivo comum. Como resultado, estas ameaças utilizam diferentes tipos de guerra e táticas frequentemente irregulares, contrariamente às guerras anteriores onde estas táticas complementavam componentes convencionais.

Estas AH podem ser criadas por adversários, tais como estados-nação que utilizam formas prolongadas de guerra ou que utilizam terceiros (*proxy forces*) para coação e intimidação, ou atores não estatais que utilizam conceitos operacionais e recursos disponíveis para os mesmos estados-nação (U.S. Army, 2011).

A presença destes elementos pode ser vista no conflito de Israel com a organização política paramilitar Hezbollah, a Segunda Guerra do Líbano em 2006, a anexação da Crimeia pela Rússia e o conflito na Ucrânia Oriental em 2014, bem como as recentes operações do chamado ISIL na Síria e no Iraque, que utilizam operações, armas e táticas convencionais em sinergia com o uso do terrorismo, crime organizado, propaganda, ataques informáticos e outros meios.

Em 2006, as Forças de Defesa de Israel realizaram uma mudança organizacional e doutrinal, de uma abordagem simétrica da guerra para uma abordagem assimétrica centrada no conflito de baixa intensidade e no terrorismo. No início da Segunda Guerra do Líbano, as Forças de Defesa de Israel enfrentaram terrenos difíceis no Líbano e forças Hezbollah bem equipadas e treinadas utilizando armas convencionais tais como mísseis antitanque, armas antiaéreas avançadas, mísseis terra-ar, e mísseis de curto e médio alcance. As forças do Hezbollah passaram por um treino extensivo no Líbano, Síria e Irão, desenvolvendo unidades para conduzir operações descentralizadas e aprendendo a combinar táticas de guerrilha com táticas militares convencionais, guerra psicológica, terrorismo, crime e armas para criar conceitos inovadores para a defesa do sul do Líbano contra a agressão israelita (Rogers, 2012).

O Hezbollah demonstrou uma gama de capacidades militares estatais e um protótipo daquilo a que Frank Hoffman (2009) chama GH, um prenúncio de como a GH pode testar as fundações de uma força superior e explorar as suas fraquezas. O Hezbollah conseguiu explorar as consequências políticas das suas limitadas operações táticas, que foram reforçadas pelos meios de comunicação social.

Israel subestima frequentemente a capacidade do Hezbollah para lutar e adaptar-se a um ambiente operacional em mudança e, assim, acaba por perder a perceção da guerra estratégica. O Hezbollah, consciente da sua dimensão, emprega uma estratégia coerciva a nível e utiliza uma abordagem operacional que combina táticas convencionais e irregulares, destacando as suas forças para moldar o ambiente operacional e impedir uma vitória israelita clara e decisiva (Davis Jr., 2013).

Do mesmo modo, o ISIL é visto como uma poderosa força não estatal capaz de confiscar território e de utilizar meios convencionais e não convencionais, o que se enquadra

na nossa definição de uma ameaça híbrida. É capaz de utilizar o terrorismo, táticas irregulares e guerra de informação para conceber, planear, utilizar e sustentar meios e ações convencionais específicas das forças convencionais, trabalhando em conjunto para explorar as vulnerabilidades de um adversário. Estas capacidades foram demonstradas em operações no Iraque, onde conseguiram ganhar força e atingir objetivos através de manobras e armas caracterizadas por um forte poder de fogo convencional (NATO, 2015).

Tais operações são típicas de AH, que procuram explorar simultaneamente as melhores capacidades das forças táticas e irregulares e são capazes de mudar rapidamente entre operações e táticas em todo o espectro de operações. Como John Davis (2014) salienta na sua definição de pensamento híbrido, uma das principais características das AH é a adaptação contínua a ambientes operacionais em mudança através da flexibilidade e da utilização simultânea de recursos e de diferentes modos de guerra.

As ameaças são inovadoras, adaptáveis, globalmente ligadas e operam a nível local em ambientes operacionais onde as populações lutam para enfrentar o caos. As ameaças têm mesmo acesso a uma gama de tecnologias avançadas, incluindo a capacidade de utilizar armas de destruição maciça (U.S. Army, 2010).

A natureza letal e complexa dos atores não estatais e a sua capacidade de sustentar, prolongar o conflito e desafiar o estado moderno é um novo fator no nosso tempo. Com base nesta análise, a GH combina meios convencionais, irregulares e assimétricos, incluindo a manipulação política e ideológica de conflitos, como se viu no conflito entre a Rússia e a Geórgia, em 2008, e no conflito no leste da Ucrânia, em 2014, e em última análise pode combinar operações especiais e forças convencionais, agentes de informações, agitadores políticos, manipulação dos media e guerra de informação, coerção económica, ciberataques, uso de forças de representação, forças paramilitares, terrorismo e o destacamento de atores militares e políticos.

Na atual GH, as forças táticas e irregulares já não são destacadas separadamente em diferentes zonas de conflito, mas sim combinadas numa só área. Os adversários híbridos, por outro lado, procuram a vitória utilizando uma combinação de táticas irregulares e os meios mais difíceis de atacar e alcançar os seus objetivos políticos (Hoffman, 2007).

Atualmente, a complexidade do ambiente operacional manifesta-se não só na complexidade do controlo geográfico sobre as áreas urbanas, mas igualmente na relevância do controlo sobre novos territórios não geográficos, tais como o ciberespaço – "o ciberespaço constitui a nova área operacional de intervenção por parte das FFAA dos diferentes países e das próprias organizações internacionais, como a NATO, sendo

claramente dominador ao nível das preocupações com o futuro da Segurança e Defesa…" (Telo, Borges & Pires, 2018, p.47). Tal evidencia-se pelos ciberataques russos ao governo e sistema bancário da Estónia em 2008, Geórgia em 2008 e Ucrânia em 2014 (Huovinen, 2011).

A vantagem procurada pela ameaça híbrida sobre um adversário convencional não se limita aos seus meios de força militar, mas procura sinergias entre todos os outros elementos do poder de um adversário – diplomático, informativo e económico. Procura explorar e saturar o ambiente operacional, alcançando resultados coerentes com as suas intenções, forçando o adversário a responder em múltiplas frentes e em múltiplas direções, paralisando-o (U.S. Army, 2010).

A condução de uma campanha contra tal adversário requer paciência e o máximo controlo da população. Numerosos exemplos podem ser encontrados no passado, onde atores tecnologicamente mais avançados não conseguiram alcançar uma vitória clara e decisiva.

Frank Hoffman (2009) salienta que a evolução dos conflitos modernos é caracterizada por uma "convergência" entre formas de guerra, que por sua vez inclui ações físicas e psicológicas, cinéticas e não cinéticas, bélicas e não bélicas. Não estamos a combater uma multiplicidade de desafios diferentes, mas sim a sua convergência na GH.

1.3 Tipologia de Ameaças Híbridas e Modelo Conceptual

A necessidade de compreender as AH requer quatro pilares:

i. Os atores e propósitos estratégicos;
ii. Instrumentos utilizados;
iii. Áreas envolvidas;
iv. Etapas da campanha híbrida.

Os intervenientes realizam os seus propósitos estratégicos ao selecionarem uma conjugação de instrumentos que cada um explora oportunidades, alavanca ou gera fraquezas num ou mais setores, criando efeitos diretos ou de arrastamento. As campanhas híbridas envolvem geralmente intervenções – por exemplo, no domínio cognitivo ou psicológico – e influências para configurar condutas (fase preparatória) e podem (mas nem sempre) transformar-se em medidas coercivas (Giannopoulos et al., 2020).

O HybridCoE apresenta o seguinte modelo e sugere que ele pode ser adaptado a cenários específicos para aumentar a capacidade de resistência.

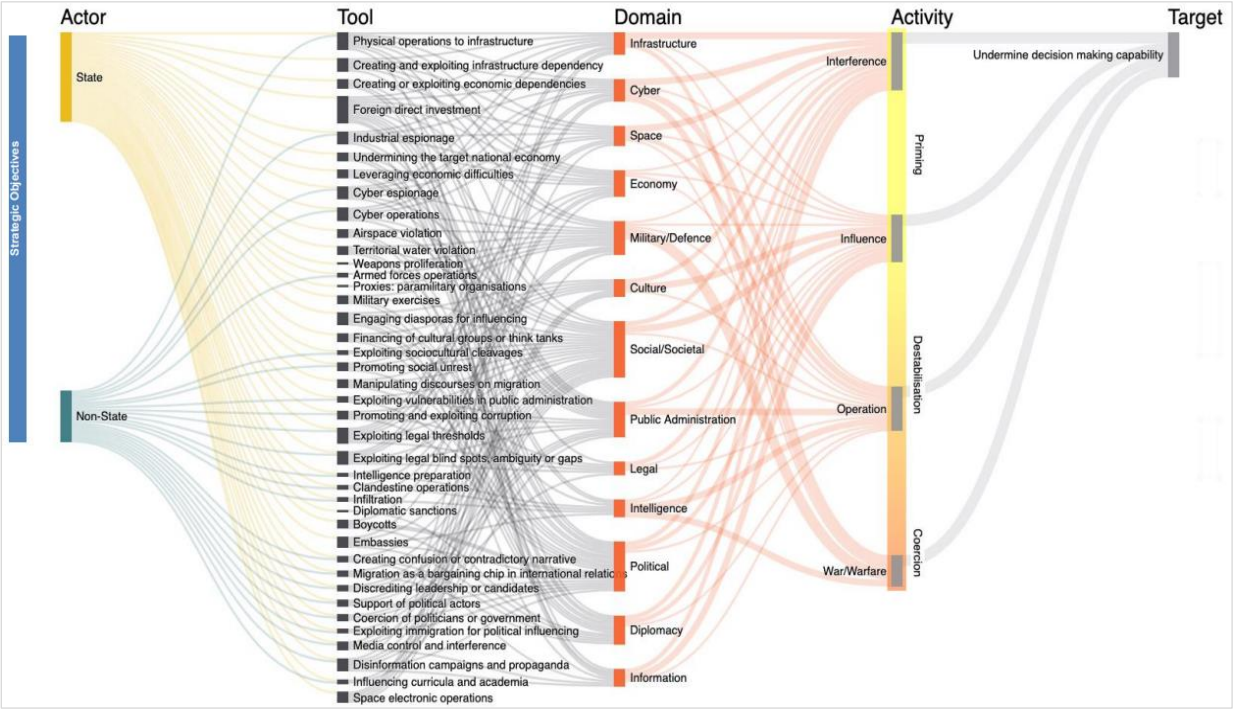


Figura 1 – Modelo conceptual do Hybrid CoE

Fonte: Giannopoulos et al. (2020)

Existe ainda outro modelo apresentado pela *Multinational Capability Development Campaign* (MCDC) (2019) que proporciona uma representação dos ataques híbridos e foca:

i. A vulnerabilidade inerente às funcionalidades essenciais;
ii. A habilidade do atacante de sincronizar diferentes recursos energéticos;
iii. As consequências de tais ações.

1.4 CiberWar

O objetivo de uma ameaça híbrida é atacar um alvo de um ou mais domínios, utilizando uma combinação de meios e explorando vulnerabilidades ou capacidades. Dada a natureza de tais ações, é essencial identificar áreas de concentração ou funções críticas onde o Estado deve assegurar a sua resiliência contra tais ameaças, uma vez que estas estão intimamente ligadas à segurança nacional e às capacidades de tomada de decisão. Militar e defesa, aeroespacial, governação, infraestruturas, economia, inteligência, informação, cibersegurança, diplomacia, política, cultura, sociedade e direito são áreas-chave onde emergem AH (Hybrid CoE, 2022).

O domínio da informação é de particular interesse devido ao seu papel na agenda internacional. A desinformação, frequentemente utilizada como instrumento de política externa, visa principalmente criar confusão e desacordo entre alvos específicos e contribui

para uma tentativa geral de influenciar as decisões de outros governos. Este campo tem-se tornado cada vez mais complexo com a expansão para o ciberespaço, incluindo ciberataques, *hacking* e outras atividades subversivas intimamente ligadas ao conceito de GH.

A modernização tecnológica mudou a forma como este domínio funciona, uma vez que os sistemas informáticos são a forma mais eficiente de os atores facilitarem e automatizarem a disseminação de informação utilizando *hackers*, *trolls*, *honeypots*, *bots* e falsas contas de utilizadores como atores digitais (Gerrits, 2018).

Segundo Pinto (2022), o domínio da informação é reconhecido como uma dimensão imensamente importante na GH, onde a desinformação é um instrumento de guerra assimétrica, tal como a guerra económica, deve ser considerada quando os agressores procuram alcançar os seus objetivos através de meios não militares. Neste caso, são tomadas medidas restritivas contra o Estado alvo para perturbar sectores como a economia e o comércio através de sanções, embargos, penalidades e disputas comerciais.

O conceito de guerra cibernética é baseado em duas teorias militares fundamentais. A primeira refere-se à capacidade deste tipo de conflito de forçar um adversário a render-se causando uma "paralisia" estratégica para atingir os objetivos desejados, e a segunda refere-se à capacidade de atingir esses objetivos sem recorrer à força física (Limnell, 2015).

A cibersegurança e a ciberdefesa, por outro lado, referem-se a uma série de questões relacionadas com os sistemas de informação que são cada vez mais importantes para a segurança interna dos Estados. Estruturas críticas tais como centrais hidroelétricas, reatores nucleares, sistemas bancários, sistemas de transporte e outros requerem inteligência cibernética avançada para compreender como os computadores estão comprometidos e infetados com *malware*.

Neste novo cenário, as partes beligerantes mudaram. Os peritos em desenvolvimento de *software* tornaram-se os novos engenheiros de combate, as marionetas tornaram-se atacantes de redes e os computadores armados com *malware* tornaram-se armas (Geers, 2015).

Os ciberataques alargam o alcance da guerra, perturbam as redes de comando e controlo do inimigo e são cada vez mais úteis ao Estado. A simbiose entre *hackers* e FFAA pode assim conduzir a estratégias de invasão mais rápidas e mais eficazes. É importante reconhecer que o sector de infraestruturas críticas é vulnerável a ataques cibernéticos. O problema assenta no facto dos sistemas críticos para a sobrevivência de um país, tais como energia, finanças, indústria e transportes, que estão agora interligados e controlados pela Internet, foram desenvolvidos antes de a Internet se tornar ubíqua. Isto mostra como as

defesas idealizadas destes sistemas são vulneráveis a novas ameaças (Comissão Europeia, 2018).

As preocupações sobre o desenvolvimento da guerra cibernética e o futuro da era digital tornaram-se uma grande preocupação para os Estados. À luz destas preocupações, a elevada sofisticação do conflito cibernético na era da informática é novamente realçada. Ao avaliar as capacidades militares no ciberespaço – olhando para objetivos estratégicos, tecnológicos e políticos – estas doutrinas explicam a atribuição de recursos e como a organização da economia de investimento de um Estado evolui em relação às suas capacidades cibernéticas.

Embora seja uma indicação clara de crescimento e apoio à guerra cibernética, os dados sobre os motores económicos de um país são geralmente pouco claros e difíceis de obter. Isto significa que, mesmo quando existem dados sobre o financiamento público de tecnologias de cibersegurança, é pouco provável que estes sejam significativos e transparentes. No entanto, alguns países anunciaram que estão a criar unidades de defesa cibernética nas suas FFAA, o que por si só pode ser encarado como parte de uma tendência para o reforço das capacidades e medidas de defesa cibernética. Outros indicadores mensuráveis da atividade cibernética incluem o recrutamento de peritos cibernéticos, a atualização de estratégias militares cibernéticas e o desenvolvimento de parcerias público-privadas entre Estados (Comissão Europeia, 2020).

Contudo, é iminente o aumento dos ataques cibernéticos patrocinados pelo Estado e acompanhado pela perceção de que não há um preço significativo a pagar por estes ataques devido à falta de legislação que regulamente os ataques cibernéticos, uma vez que ainda não existem protocolos claros para responder aos ataques cibernéticos patrocinados pelo Estado que ameaçam a segurança nacional (Costa, 2021a).

1.5 Síntese Conclusiva

O capítulo ostentado faz uma abordagem sobre aquilo que é o conceito de GH. Referenciando que os surgimentos de novos conceitos se deram após o fim da Guerra Fria e que atualmente se enfrenta uma multiplicidade de atores e ameaças motivados por razões étnicas, económicas, sociais e religiosas. As GH apresentam caraterísticas como a diminuição de conflitos de larga escala, enfraquecimento do poder estatal e a desenvolvimento de ameaças não convencionais. A hegemonia militar tradicional já não assegura a prosperidade nas guerras da atualidade.

CAPÍTULO 2 - O PAPEL DOS ESTADOS NO COMBATE ÀS AMEAÇAS HÍBRIDAS

2.1 Ameaças e Desafios ao Estado de Direito

As recentes tentativas de definir AH tornam possível falar sobre o uso da lei como parte de uma campanha híbrida. Tal ocorre quando os adversários combinam e coordenam deliberadamente ações no campo jurídico com ações nos demais campos para atacar maliciosamente as deficiências sistémicas das sociedades democráticas, geralmente utilizando métodos extraídos da caixa de ferramentas estratégicas de regimes autoritários, forças revisionistas e Estados malfeitores.

É fundamental esclarecer alguns elementos deste modelo conceptual. Em geral, os Estados que apoiam uma ordem internacional baseada em regras devem reconhecer que o Estado de direito tem um valor que vai além do seu expediente político. Este valor deriva do carácter formal do direito como um sistema de raciocínio e prática, baseado em certos princípios do que constitui um argumento válido. Isto é o que distingue o direito dos argumentos quase jurídicos e o direito da pura política.

Na prática, indica que os Estados que desejam defender o Estado de direito devem defendê-lo contra AH que o mina, não só quando os seus interesses estratégicos num caso particular estão em jogo, mas também de uma forma geral. Várias táticas híbridas são particularmente preocupantes, tais como ignorar a lei, explorar fronteiras legais e zonas cinzentas, evitar e depreciar a lei, e fazer falsas alegações legais. Tais táticas devem ser desencorajadas e os atores hostis devem ser tratados em conformidade, caso contrário arriscam-se a ser acusados de duplicidade de critérios (Giannopoulos et al., 2020).

Os Estados dependem da lei para alcançar resultados noutras áreas, tal como dependem de atos ilegais para alcançar resultados na esfera jurídica. Esta combinação justifica que se identifique a lei como uma potencial AH.

2.2 Portugal e a sua relação com a política externa

A participação de Portugal em missões internacionais tem sido um pilar estratégico da política externa portuguesa desde os anos 90 (Teixeira, 2010). Neste sentido, a presença de Portugal em missões de manutenção da paz é uma forma conveniente de demonstrar a capacidade do Estado em contribuir em rede para a segurança coletiva e promover os interesses nacionais, e é entendida como uma forma de reforçar a presença de Portugal no

mundo através de uma rede de alianças e organizações que possam aumentar o seu prestígio externo e ajudar a promover a paz e segurança internacionais (Presidência do Conselho de Ministros, 2013).

A importância da questão é evidenciada não só pela tendência para uma maior participação portuguesa em missões internacionais (Cravinho, 2021), mas também pela crescente literatura sobre o tema e questões estratégicas, tais como as origens e fundamentos da estratégia portuguesa (Duarte, 2013) ou a definição da cultura estratégica portuguesa (Reis, 2013; Reis et al., 2013).

Da mesma forma se destacam os estudos de política externa que identificam a mudança de prioridades após 25 de Abril de 1974, incluindo a participação de Portugal na arquitetura de segurança internacional como uma das quatro linhas principais da política externa portuguesa após o fim da Guerra Fria (Freire & Brito, 2010).

Vários autores refletiram do mesmo modo sobre as dinâmicas de segurança regional e global em relação à posição de Portugal nas organizações e alianças das quais é membro, incluindo a ONU (Organização das Nações Unidas), NATO e UE (Cravinho, 2010). Finalmente, pode-se apontar importantes estudos sobre as missões/operações em que Portugal participa e a identificação do contexto internacional em que estas surgem e se desenvolvem (Reis et al, 2020).

Atualmente, a política externa portuguesa, e em particular as relações externas das FFAA portuguesas, encontram-se centradas no internacionalismo e procura promover os valores democráticos, os direitos humanos e o direito internacional através de estratégias de construção de pontes e da participação ativa em diferentes plataformas internacionais. O que conduz inevitavelmente a uma abordagem diferente da geopolítica e geoestratégia, agora baseada na proximidade e interesses comuns em alianças e organizações internacionais das quais Portugal é membro (PRONE, 2021).

Em 2003, a UE tinha-se tornado um ator imprescindível. Portugal só participou em missões internacionais da ONU e da NATO, sendo esta última de maior relevância que a primeira (Estado-Maior General das Forças Armadas, 2021), uma vez que a UE ainda não dispunha de uma política de segurança e defesa claramente definida. Neste ponto é pertinente notar a diferença entre a participação em missões da UE e da NATO – sendo esta última mais importante – principalmente devido aos esforços feitos para assegurar a presença de Portugal em todas as operações militares da UE.

De igual modo, na sequência da participação de Portugal na MINUSCA (United Nations Multidimensional Integrated Stabilization Mission in the Central African Republic),

é claramente reconhecida a importância estratégica de assegurar uma presença equilibrada em todas as missões das organizações de defesa e segurança de que Portugal é membro (Ministério da Defesa, 2018).

Pode assim argumentar-se que os progressos doutrinais e práticos nesta área contribuíram para uma maior coerência na participação das Forças Nacionais Destacadas (FND) nestas organizações, embora isto não garanta necessariamente uma participação equilibrada nas missões da NATO, UE e ONU. Esta tendência parece estar relacionada com a abordagem inicial da coprodução da segurança internacional, que foi principalmente reativa e centrada no cumprimento de obrigações para com a NATO e, mais tarde, para com a UE.

O empenho de Portugal numa abordagem mais proactiva e a adoção pelo Ministério da Defesa da Garantia de Participação Equilibrada como orientação política para o envolvimento (Ministério da Defesa, 2018) ajudam a criar condições favoráveis para uma política mais coerente de envolvimento neste triângulo multilateral. As relações com outros eixos da política externa e a reputação internacional de Portugal como país amigo e pacífico contribuíram grandemente para esta consolidação, dando ao país uma vantagem comparativa sobre os países médios e grandes cuja política externa pode ser interpretada como mais empenhada e intervencionista.

Esta dimensão torna-se particularmente determinante em situações de crise complexas, pois os aliados tendem a esperar que Portugal contribua para a segurança de uma forma mais "neutra", através de um modelo simples e integrado de relações com outras potências. Isto sublinha a credibilidade do país como parceiro e participante nos esforços multilaterais de segurança compatíveis com os objetivos e interesses nacionais. Promove uma dimensão de participação em missões internacionais que contrasta com a dimensão geográfica do país e é reforçada por muitos anos de experiência na acumulação de conhecimentos e aplicação de lições aprendidas (Brito, 2005).

O movimento para uma participação interdependente na dinâmica de segurança internacional, abordando interesses relacionados e problemas comuns, coincidindo com o desenvolvimento do Conceito Estratégico de Defesa Nacional (CEDN), significa que o critério de proximidade geográfica desempenha um papel limitado no planeamento estratégico e na tomada de decisões das operações da FND.

Neste contexto, embora existam algumas áreas de particular preocupação uma vez que a posição de Portugal se sobrepõe à da ONU, NATO e UE, se acrescentarmos o papel fundamental desempenhado pela Comunidade dos Países de Língua Portuguesa (CPLP) na

política externa de Portugal e o facto de os fluxos de insegurança não dependerem de fronteiras políticas, podemos concluir que a posição geopolítica e geoestratégica de Portugal está a crescer (Giannopoulos et al., 2020).

De acordo com a Estratégia de Segurança Cibernética Europa 2020, reforçaremos a posição da UE no ciberespaço e melhoraremos a nossa capacidade de prevenção de ataques cibernéticos através do reforço e desenvolvimento de capacidades, formação, exercícios, construção de resiliência e todos os instrumentos à disposição da UE para responder decisivamente a ataques cibernéticos contra a UE, as suas instituições e os seus Estados Membros.

Isto reforça o compromisso estratégico operacional e estrutural das FFAA, de responder imediata e sustentadamente às ameaças que visam negar à UE e aos seus parceiros o acesso seguro e aberto ao ciberespaço. Igualmente incorporado nesta estratégia, apoia-se os parceiros a reforçar a sua resiliência cibernética e a mobilizar peritos da UE e dos Estados-Membros para ajudar na eventualidade de uma crise cibernética, mas também com o reforço da solidariedade e o apoio mútuo através de uma formação cibernética regular (Giannopoulos et al., 2020).

A estratégia genética das FFAA portuguesas, passa por reforçar as capacidades de inteligência cibernética para melhorar a resiliência cibernética, incluindo o apoio efetivo a missões e operações civis e militares da Política Comum de Segurança e Defesa (PCSD). Neste sentido, melhora-se a interoperabilidade e a partilha de informação através de equipas militares de resposta cibernética (CERT miles) e operações de defesa cibernética.

Reconhece-se que o reforço da cibersegurança das FFAA é uma forma de melhorar a eficácia e segurança das operações em terra, no ar, no mar e no espaço, sendo que a liberdade de ação depende do acesso seguro e autónomo ao espaço, obrigando a uma adaptação a um ambiente espacial mais competitivo e exigente.

O aumento da dependência dos sistemas e serviços espaciais torna as FFAA mais vulneráveis a ações irresponsáveis e ameaçadoras por parte de concorrentes estratégicos. O número crescente de objetos em órbita e detritos espaciais também aumenta os riscos e as tensões. Os programas espaciais da UE e outras infraestruturas espaciais na UE e nos seus Estados Membros contribuem para a resiliência organizacional.

Estes sistemas fornecem serviços essenciais que substituem ou complementam as infraestruturas de observação da Terra, navegação por satélite e telecomunicações. O sistema espacial da UE deveria fornecer conectividade global aos atores de segurança e defesa. Para este fim, serão desenvolvidas propostas para um sistema espacial global da UE para

comunicações seguras, em particular no âmbito do Programa de Conectividade Segura da União para 2023-2027 (Pinto, 2022).

Dada a importância do controlo civil dos bens espaciais da UE e dos programas espaciais da UE, há uma necessidade urgente de complementar as estratégias espaciais existentes e reforçar a dimensão espacial da UE na área da segurança e defesa.

Uma nova estratégia espacial da UE para a segurança e defesa ajudar-nos-á a compreender coletivamente os riscos e ameaças espaciais desenvolver respostas e capacidades adequadas para responder melhor e mais rapidamente a crises, reforçar a nossa resiliência e explorar plenamente os benefícios e oportunidades do espaço. Tal estratégia deverá incluir, por exemplo, dimensões políticas, operacionais, diplomáticas e de governação.

2.3 Síntese Conclusiva

Neste capítulo são abordas as ameaças e os desafios ao Estado de direito e ainda a política externa relativamente a Portugal. No que concerne às ameaças de Estado de direito é salientado a atualização da lei como componente de AH, em que adversários regulam ações jurídicas com ações em diferentes campos com o intuito de atacar deficiências das sociedades democráticas. Relativamente à política externa, é destacável a participação de Portugal em missões internacionais por forma a viabilizar interesses nacionais arquitetando alianças e organizações de maneira a contribuir para a segurança coletiva. É salientada a evolução da estratégia de participação Portugal, sendo esta considerada mais proativa.

Relativamente à segurança cibernética e no que concerne a este aspeto é reconhecido o reforço das capacidades e Portugal a nível da inteligência e resiliência cibernética. Propõe-se um aprimoramento de um sistema global de comunicações seguras da UE.

PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

CAPÍTULO 3 - METODOLOGIA, MÉTODOS E MATERIAIS

3.1 Definição dos objetivos de investigação

Este estudo tem como objetivo principal analisar as mudanças necessárias em Portugal para alcançar um nível de defesa contra a GH mais eficaz. Para cumprir esse objetivo, foram estabelecidos os seguintes objetivos específicos:

OE1: Identificar as limitações da defesa contra a Guerra Híbrida;

OE2: Identificar métodos para alcançar eficiência neste âmbito;

OE3: Identificar os conflitos europeus e as suas repercussões;

OE4: Compreender qual a tarefa das Forças Armadas;

Além disso, serão abordadas perguntas direcionadas que auxiliarão no cumprimento dos objetivos propostos:

PD1: Quais são os conflitos em curso e ameaças à Europa?

PD2: Qual a capacidade de resposta de Portugal?

PD3: Que impacto tem para as Forças Armadas Portuguesas?

A pergunta de partida deste estudo, "Quais são as mudanças a realizar em Portugal para atingir um adequado nível de defesa contra as Ameaças Híbridas?", será respondida através da análise dos objetivos e perguntas direcionadas apresentados neste subcapítulo. A procura por respostas e soluções contribuirá para fortalecer a capacidade de defesa de Portugal contra a GH e garantir a segurança e a soberania do país no atual.

3.2 Tipo de Estudo

O presente estudo é de natureza qualitativa, e podemos definir o estudo como exploratório-descritivo.

Na investigação qualitativa, o investigador procura aprofundar o seu entendimento dos fenómenos estudados, interpretando-os a partir da perspetiva dos próprios participantes. Nesse tipo de estudo, não há preocupação com números representativos, generalizações

estatísticas ou relações lineares de causa e efeito. Este tipo de investigação concentra-se na observação, interpretação e descrição do problema conforme ele é vivenciado na realidade. Os estudos descritivos têm como objetivo observar, descrever e documentar os diferentes aspetos de uma situação. Já os estudos exploratórios têm o propósito de oferecer uma descrição e classificação de um determinado fenómeno. Com base nos resultados, é possível formular hipóteses na maioria das vezes (Fortin, 2009).

Quanto ao tipo de dados, primários ou secundários, optou-se pela recolha de dados primários uma vez que estes são recolhidos de forma direta na realidade.

A utilização de várias fontes para a recolha de informação relevante auxilia assim o investigador não apenas na recolha de informação mais abrangente, assim como permite a verificação da sua consistência para o aumento da robustez dos resultados (Wahyuni, 2012). A este método de recolha de dados sob várias fontes de análise, denomina-se de triangulação de dados (Santos et al., 2020).

No nosso estudo, foram recolhidos e analisados dados, como mostra a tabela no Anexo A.

É necessário salientar que a investigação se situou num contexto de descoberta e não de prova, tratando-se de uma abordagem de caráter indutiva exploratória descritiva, ou seja, o objetivo dessa tese não teve como proposta confirmar ou inferir hipóteses construídas previamente. Baseia-se assim em Bogdan e Biklen (1994, p. 16) no qual descrevem que "ainda que se possam vir a selecionar questões específicas à medida que se recolhem os dados, a abordagem à investigação não é feita com o objetivo (…) de testar hipóteses".

Consideramos aqui que o método indutivo é um método científico que obtém conclusões gerais a partir de premissas individuais. Na visão dos autores "não se trata de montar um quebra-cabeça cuja forma final conhecemos de antemão. Está-se a construir um quadro que vai ganhando forma à medida que se recolhem e examinam as partes" (Bogdan & Bliken, 1994, p. 50) e que logo após há a possibilidade de se generalizar.

3.3 Técnicas, procedimentos e meios utilizados

Como parte da elaboração desta tese, partiu-se primeiramente de uma profunda pesquisa bibliográfica sobre o tema e os objetivos do trabalho. O objetivo principal desta pesquisa bibliográfica não se restringe unicamente a explanar as citações e os pontos de vistas dos principais autores do contexto do trabalho, mas levantar questões e cruzar informações que serviram de pressupostos para as análises qualitativas (Lima & Newell-McLymont, 2021).

Depois recorreu-se à entrevista. Os métodos de entrevista permitem ao investigador obter dados muito ricos considerando a interação e comunicação que se estabelece entre o entrevistador e entrevistado. Uma vez que se estabelece um contacto direto, o investigador tem uma maior liberdade para controlar a condução do estudo. No caso de entrevistas semiestruturadas, por exemplo, o investigador apresenta uma série de questões que servirão de guião, podendo, contudo, ser adaptadas no decorrer da entrevista de forma a garantir os objetivos da mesma (Quivy & Campenhoudt, 2008).

A principal vantagem deste método resulta da profundidade dos elementos da análise recolhidos e a respetiva flexibilidade que o método proporciona (Quivy & Campenhoudt, 2008). O propósito de um investigador quando elege como método de investigação as entrevistas é essencialmente obter informações únicas; recolher uma agregação numérica de informações de muitas pessoas e descobrir "uma coisa" que os pesquisadores não conseguiram observar (Lima & Newell-McLymont, 2021).

Este método é frequentemente utilizado em estudos exploratório-descritivos e assume três objetivos: "servir de método exploratório para examinar conceitos, relações entre variáveis e conceber hipóteses; servir de principal instrumento de medida de uma investigação; servir de complemento a outros métodos" (Fortin, 2009, p. 245). As entrevistas variam em função do grau de liberdade deixado aos interlocutores e do grau de profundidade da investigação.

As vantagens da utilização deste método resultam de poder ser utilizado em quase todos os setores da população; taxas de respostas mais elevadas; erros de interpretação são mais facilmente detetáveis; maior eficácia na descoberta de informações sobre temas complexos e carregados de emoção. Contudo, este método pode apresentar elevados custos financeiros e temporais, gerando por isso amostras mais pequenas. Dada a intensidade na obtenção de respostas, outro problema surge na dificuldade de codificar e analisar os dados que por vezes pode surgir (DeJonckheere & Vaughn, 2019).

3.4 Recolha de dados

Relativamente à análise documental, a recolha de dados foi feita através da consulta de diversos recursos, tais como livros, artigos académicos, relatórios governamentais, publicações de instituições especializadas, periódicos científicos e outros materiais relevantes. Foram utilizadas bases de dados académicas, bibliotecas virtuais, repositórios online e fontes confiáveis para garantir a abrangência e a representatividade da revisão bibliográfica.

O processo de recolha de dados envolveu a seleção criteriosa das fontes, levando em consideração a pertinência, a atualidade e a qualidade dos materiais encontrados. A leitura crítica dos materiais foi realizada de forma a extrair informações pertinentes à evolução teórico-prática das AH e ao posicionamento de Portugal em relação a esse fenómeno.

Os dados recolhidos na análise documental foram, depois, sintetizados permitindo uma compreensão aprofundada da evolução teórica e prática das AH, bem como o contexto específico do posicionamento de Portugal diante dessas ameaças. A revisão da literatura serviu como base teórica sólida para o estudo, fornecendo um embasamento conceitual e teórico consistente para a análise empírica.

É importante ressaltar que a pesquisa de bibliografia desempenha um papel crucial na investigação científica, permitindo uma compreensão abrangente do estado atual do conhecimento sobre o tema, identificando lacunas e contribuindo para a fundamentação teórica e a contextualização do estudo (Snyder, 2019).

Depois, na técnica da entrevista, a recolha de dados foi realizada por meio de perguntas e respostas diretas com os participantes. Durante a entrevista, o investigador procurou obter informações relevantes e aprofundadas sobre o tema em estudo, consultando um guião de entrevista. O guião estruturado continha uma lista de perguntas a serem abordadas durante a entrevista. Esse roteiro auxilia o investigador a manter o foco e garantir a abordagem dos principais aspetos da pesquisa (Young et al., 2018).

Considera-se, portanto, que é fundamental que os instrumentos de medida sejam adequados aos objetivos da pesquisa e às características dos participantes.

3.5 Amostragem: composição e justificação

Prodanov e Freitas (2013) apresentam os conceitos de população alvo. Nesse sentido, cabe lembrar que, segundo os autores, uma população é um conjunto de elementos com características comuns.

De acordo com Carmo e Ferreira (2008, p. 209), a população corresponde a um "conjunto de elementos abrangidos por uma mesma definição. Esses elementos têm, uma ou mais características comuns a todos eles, características que os diferenciam de outros conjuntos de elementos". Ou, conforme Fortin (1999), trata-se de um conjunto de elementos ou sujeitos que partilham características comuns, as quais são definidas pelo investigador à luz de um conjunto de critérios, de acordo com o estudo que pretende efetuar. A amostra corresponde a "um subconjunto de uma população" ou grupo de sujeitos que fazem parte de uma mesma população" (Fortin, 1999, p. 202).

A amostra pode ser definida como sendo a fração da população sobre a qual se está a realizar o estudo, o que faz com que ela seja representativa, tendo em conta que reflete as características da população em estudo (Prodanov & Freitas, 2013).

Esta deve ter a dimensão adequada para obter a precisão que se pretende, não deve ser superior uma vez que à medida que cresce a dimensão da amostra os custos do processo aumentam e os ganhos de precisão são mínimos. Uma amostra representativa da população é aquela que reflete os aspetos típicos dessa população (Almeida & Freire, 2000).

A amostragem designa o processo pelo qual se obtém uma ou mais amostras de uma população de interesse. Na amostragem seleciona-se parte de uma população e observa-se esta com o objetivo de estimar parâmetros populacionais – características populacionais. Os diferentes procedimentos amostrais devem respeitar os seguintes critérios:

1) As amostras devem ser representativas da população;

2) As amostras devem fornecer estimativas precisas das características da população, podendo medir a sua fiabilidade;

3) Os custos para seleção da amostra devem ser pequenos.

Face ao referido, para a realização deste estudo foi adotada uma amostragem composta por cinco entrevistas a oficiais do Exército Português (EP), e uma a um oficial da Guarda Nacional Republicana (GNR). A seleção desses participantes deu-se com base em critérios específicos, como o seu conhecimento na área, as funções que desempenham ou já desempenharam, além da sua participação em diversos trabalhos similares. Assim, a escolha desses oficiais militares como participantes da investigação foi fundamentada com base na sua experiência e conhecimento profundo no campo de estudo. As suas competências e envolvimento em trabalhos anteriores do mesmo género tornam-nos fontes valiosas de informações e insights relevantes para a investigação em questão.

Cabe ressaltar que duas das entrevistas foram realizadas de forma remota, utilizando meios telemáticos, enquanto as demais foram conduzidas de forma presencial. Essa abordagem permitiu uma maior flexibilidade na obtenção dos dados, considerando as disponibilidades e logísticas dos participantes (Neris et al., 2023). A realização de entrevistas presenciais proporcionou um ambiente mais intimista e facilitou a observação de expressões faciais e linguagem corporal, enquanto as entrevistas remotas oferecem comodidade e facilidade de acesso, reduzindo possíveis barreiras geográficas (Jennings, 2005; Neris et al., 2023).

Essa composição de amostragem, com oficiais do Exército e um oficial da GNR, juntamente com a combinação de entrevistas presenciais e remotas, visa garantir uma

perspetiva abrangente e diversificada sobre o tema em estudo. Essa abordagem permite explorar diferentes visões e experiências, contribuindo para uma análise mais completa e precisa dos dados recolhidos.

3.6 Tratamento dos dados

A análise de conteúdo é uma abordagem utilizada na investigação qualitativa para analisar e interpretar o conteúdo dos dados recolhidos, como entrevistas, textos, documentos ou outras formas de comunicação. Essa técnica envolve a identificação de temas, padrões, categorias ou significados subjacentes no material analisado. O objetivo é extrair e compreender os aspetos relevantes e significativos presentes no conteúdo, permitindo uma compreensão mais profunda dos fenómenos estudados. A análise de conteúdo pode envolver diferentes etapas, como a codificação dos dados, a categorização dos temas e a interpretação dos resultados. Essa abordagem é amplamente utilizada em diversas áreas de investigação, contribuindo para a compreensão e a geração de novos conhecimentos (Kyngäs, 2019; Selvi, 2019).

Na análise de conteúdo, são utilizados diferentes métodos e técnicas, dependendo do objetivo da investigação e do tipo de dados recolhidos. Alguns exemplos incluem:

(i) Codificação: É o processo de atribuir rótulos ou categorias aos segmentos de dados relevantes. Pode ser feito de forma aberta, na qual categorias emergem diretamente dos dados, ou de forma pré-determinada, utilizando um sistema de categorias pré-estabelecido (Sun, 2017);

(ii) Categorização: Envolve agrupar as unidades de análise em categorias ou temas com base em semelhanças ou características partilhadas. Isso permite a organização e a compreensão dos dados de forma mais sistemática (Kleinheksel et al., 2020);

(iii) Análise temática: Consiste em identificar e explorar os padrões, tópicos ou temas recorrentes no conteúdo analisado. Esses temas podem ser identificados através da codificação e categorização dos dados, permitindo uma compreensão mais aprofundada das questões abordadas (Vaismoradi & Snelgrove, 2019);

(iv) Análise de discurso: Concentra-se na análise das formas de linguagem, discursos e significados presentes no conteúdo. Isso envolve a identificação de discursos dominantes, estruturas de poder, metáforas e outras estratégias linguísticas utilizadas (Johnson & McLean, 2020);

(v) Triangulação: É a prática de utilizar múltiplos métodos ou fontes de dados na análise de conteúdo, procurando maior validade e confiabilidade dos resultados. Isso pode

envolver a combinação de entrevistas, análise documental e observação, por exemplo (Campbell et al., 2018).

É importante ressaltar que a análise de conteúdo é um processo iterativo e interpretativo, no qual o investigador constantemente revê, refina e interpreta os dados, procurando compreender as nuances e os significados subjacentes.

CAPÍTULO 4 - APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

4.1 Resultados

Através da análise de conteúdo, as unidades de significado foram distribuídas em torno de 13 categorias e 39 subcategorias (Apêndice E).

Relativamente à primeira questão, "*durante o conflito híbrido da Rússia/Ucrânia, quais foram as modalidades de ação, os domínios e as ferramentas usadas pela Rússia nas funções críticas da Ucrânia de forma a explorarem as respetivas vulnerabilidades e alcançarem os seus objetivos políticos?",* o E1 salientou que a Rússia empregou um conjunto de ações não militares, estruturadas no modelo de Guerra não linear de Asimov. Salientou que "*a ação de 24 de fevereiro de 2022 foi o culminar da Operação Decisiva Militar*", que incluiu ações económicas, diplomáticas, guerra da informação e ataques cibernéticos, sendo que a Rússia tinha como objetivo "*garantir politicamente que a Ucrânia é um estado na área de influência da Rússia* "*Um estado pró-russo*".

Depois, E2 refere que a Rússia utilizou diversas ferramentas e modalidades no domínio cibernético, incluindo intromissões, recolha de informação sensível, negação de serviços básicos e uma extensa campanha de desinformação nas redes sociais. No domínio da informação, houve uma "*campanha de desinformação*" para associar a Ucrânia "*à nazificação do país e à perseguição das minorias russófonas*". A Rússia visava influenciar a população em prol da causa russa e desacreditar o governo ucraniano.

O E3 salienta que a Rússia utilizou instrumentos "*de poder diplomático e informacional*", criando narrativas e enviando agentes para criar indignação nas pessoas. As ferramentas utilizadas incluíram forças militares, espionagem, violação de águas territoriais, operações clandestinas e exercícios militares.

E4 refere que o conceito de AH ainda não está definido a nível da NATO, o que dificulta uma resposta militar. Reconhece que a Rússia utilizou operações de informação, desinformação, ciberataques e explorou diversas vertentes da informação para influenciar decisões políticas.

O E5 salientou que a Rússia utilizou "*vários instrumentos de coação*", não exclusivamente militares, para atingir os seus objetivos políticos. O entrevistado identificou as componentes cibernética, política e de desinformação como parte da estratégia russa. A

guerra multi-domínio foi destacada, com a utilização de todos os domínios, como ar, terra, ciberespaço e espaço.

Por fim, o E6 destaca que não se limita apenas a estes dois países e que tem um alcance a nível global através de campanhas de desinformação e informação, fazendo uma comparação de similaridade com a ações em África. Faz atenção ainda ao facto de que a GH efetuada pela Rússia é conduzida por empresas militares privadas que abrangem diversas atividades.

Com a 2.ª questão, *Relativamente à cooperação internacional e no âmbito da inserção de Portugal na NATO e na UE, existe uma partilha de informações estratégicas com organismos internacionais relativamente às ameaças híbridas e às suas ferramentas bem como a participação em exercícios internacionais?,* verificou-se que E1 considera que Portugal participa em organizações e partilha informações no Sistema de Informações para a República Portuguesa (SIRP) e na área de informações militares na SigMil.

A "*partilha de informações é genérica*" e não distingue se a ameaça é híbrida ou não. Existem "*exercícios para testar e certificar forças*", mas não são especificamente direcionados para a AH devido à falta de um conceito oficializado pela NATO.

O E2 salienta que Portugal coopera com organizações internacionais, como a NATO e a União Europeia, na partilha de informações estratégicas sobre ameaças híbridas e na participação em exercícios internacionais. Na NATO, Portugal colabora no estudo, preparação, prevenção, mitigação, combate e recuperação em relação a estas ameaças. Na União Europeia, Portugal participa em grupos de trabalho e células de fusão híbrida, onde ocorre o intercâmbio de informação estratégica e são realizados exercícios. Portugal também está ativamente envolvido no Centro Europeu de Excelência para Combate às Ameaças Híbridas (Hybrid CoE), realizando estudos, análises, treinos e combate às ameaças híbridas.

No mesmo sentido, E3 reforça que existe cooperação entre a União Europeia e a NATO. Salienta que foram criadas medidas de prontidão, ação e adaptação na NATO para lidar com as AH e contrabalançar a influência russa, bem como foram criadas "*células de estudo*" para entender e combater a GH. Refere que existe partilha de informações, mas depende da vontade dos países. Portugal participa em exercícios internacionais, mas a partilha de informações pode sofrer atrasos.

Depois, E4 diz que tanto a NATO quanto a UE tem trabalhado na doutrina e conscientização sobre as ameaças, mas mostraram vulnerabilidades na prática. As organizações ocidentais estão expostas às AH e têm sido reativas. O problema está identificado, mas as ações práticas ainda não são suficientes para enfrentar as AH. A luta

global envolve diferentes ideologias e modelos políticos, sendo a possibilidade de alterar sistemas políticos autoritários uma preocupação.

O E5 salienta que a entrada da Finlândia na NATO promoveu o combate às AH e que este país criou um centro de comando para lidar com as AH. Foram desenvolvidos diplomas e orientações gerais para a GH.

Por último, E6 confirma que Portugal faz parte de várias organizações, incluindo a NATO e a EU, onde a compartilha de informações estratégicas existe. Faz destaque à resposta à AH com o recurso ao princípio de defesa comum entre estados membros.

Na questão *Tendo por base as orientações estratégicas da UE e da NATO para o CAH e os pilares em que a mesma se suporta, quais são as principais ameaças e oportunidades para o CAH ao nível das FFAA Portuguesas?,* verificou-se que E1 reconhece que a NATO e a União Europeia não possuem "uma estratégia de Conflito de Ameaça Híbrida (CAH)", mas reconhecem a necessidade de criar resiliência nacional e enfrentar AH. O entrevistado destaca a importância da defesa cibernética e da capacidade de dissuasão militar para combater AH. Acredita que é necessário ter domínio cibernético e capacidade de defesa mínima em outros domínios, além de resistência para permitir a ajuda dos aliados.

Já E2 identifica as principais ameaças para as FFAA portuguesas como provenientes "*de estados que se opõem à NATO e à UE*", com possíveis acessos privilegiados através de Portugal. Destaca as vulnerabilidades de cibersegurança, a resiliência deficiente de empresas relevantes para a indústria de defesa e a permeabilidade a campanhas de desinformação como principais ameaças. Menciona as oportunidades decorrentes da participação em organizações como a NATO e a UE, incluindo a adoção "*de uma doutrina comum*", mecanismos avançados de deteção e prevenção, treino internacional e acesso a fundos para combater AH.

Depois, E3 lista as principais ameaças, incluindo operações físicas contra infraestruturas militares, espionagem, violação de espaço aéreo e territorial, elementos desestabilizadores e disseminação de narrativas contraditórias nos meios de comunicação e redes sociais. Destaca, ainda, a oportunidade de criação de estratégias nacionais de combate às AH envolvendo diferentes instrumentos de poder, bem como o desenvolvimento da capacidade de ciberdefesa.

O E4 sugere que Portugal está pouco acostumado a esse tipo de guerras, mas está a ser afetado pelos instrumentos da GH devido à sua inserção no espaço político. Identifica a falta de doutrina e de capacidade desenvolvida nas operações de informação e cibersegurança das FFAA como principais vulnerabilidades.

O E5 destaca a atuação das FFAA portuguesas no âmbito da NATO, incluindo operações de vigilância e deteção de comunicações em território nacional e participação em exercícios internacionais. Menciona ações de formação, preparação e eventos relacionados à GH e ao multi-domínio. Cita as dificuldades enfrentadas pela Rússia em Donbass como exemplo de falhas na operação de multi-domínio e coordenação.

Por último, o E6 enfatiza que as FFAA portuguesas são apenas um pilar daquilo que é a ação do estado no CAH e ressalva que a abordagem mais eficiente requer uma coordenação de ações de todos os elementos do governo. Faz o reparo que as AH vão mais além das ações das FFAA uma vez que exige uma compreensão dos princípios de "*multi-domain operations*" e estes englobam terra, mar, ar, espaço eletromagnético e ciberespaço. Realça que já existe uma arquitetura multi-domínio em progresso no CEDN.

A análise à 4.ª questão, *Quais as vulnerabilidades e potencialidades no ambiente interno que identifica para Portugal, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH*?, permitiu-nos verificar que os entrevistados enfatizaram as vulnerabilidades em áreas como economia, cibersegurança, coordenação entre autoridades, falta de estratégias e legislação adequadas. Também mencionaram potencialidades, como a participação em alianças e a capacidade de adaptação a novas realidades. Recomendaram ações integradas, como a criação de órgãos de coordenação e uma estratégia nacional para combater as AH.

E1 salientou que as democracias são mais suscetíveis a AH devido à sua abertura a ações não militares. Assim, Portugal é vulnerável a manipulações económicas e manobras informacionais. Em termos militares, o país "*é suscetível a uma ação decisiva de uma potência maior*" e depende de alianças como a UE e a NATO para sua defesa autónoma.

E2 refere que Portugal é permeável ao investimento estrangeiro de origem desconhecida, o que representa uma vulnerabilidade. Os níveis de cibersegurança são reduzidos, tanto no governo quanto nas empresas. A resiliência das entidades críticas, como empresas e infraestruturas, é relativamente baixa e a literacia informacional da população é baixa, facilitando a manipulação através de desinformação.

Depois, o E3 aponta que, no domínio político, há ausência "*de uma cultura política*" e estratégia dissuasora, além da localização periférica em relação à Europa. Reconhece que na economia, existem dependências de cadeias de abastecimento exterior e capital estrangeiro, fraco tecido empresarial e dificuldade em impor instrumentos de política económica. Em termos militares, Portugal possui recursos limitados de resposta a

emergências, coordenação entre autoridades civis e militares, e integração nos mecanismos de resposta da UE e da NATO.

O E4 refere que "*a separação entre segurança interna e externa*" cria vulnerabilidades, e a falta de cooperação entre forças de segurança e FFAA dificulta a coordenação efetiva. Há pouca compreensão política e militar sobre AH e falta de capacidade para a guerra de informação; a capacidade de "desenrascar" pode ser uma potencialidade, mas não é ideal.

O E5, refere que falta uma atuação integrada de todas as potencialidades do Estado no combate às AH. A legislação portuguesa não está adaptada a esse tipo de ameaças, mas existem potencialidades que incluem a ciberdefesa e exercícios de defesa. Sugere a criação de um secretariado em coordenação com o Chefe de Estado-Maior General e a formação de um Conselho de Segurança Nacional e um Centro de Gestão de Crises.

O E6, por fim, destaca que Portugal no que diz respeito às vulnerabilidades e potencialidades compartilha caraterísticas comuns com outros estados Europeus. Considera que Portugal tem uma democracia resiliente, o que aponta como uma vantagem, mas por outro lado uma desvantagem pois não existe uma entidade superior que faça garantir condições de segurança no que toca a interferências, ingerências que podem vir a resultar em manipulação de informação por atores maliciosos. A enfatiza que a educação e o sistema político português, se sustenta em bons valores e princípios que permitem que a população seja mais resiliente.

Quanto à última questão, "*De que forma pode a Defesa Nacional e as FA adaptar-se temporalmente às AH e combate-las eficazmente*?", o E1 destaca a necessidade de Portugal "*criar um sistema integrado*" de defesa nacional para se adaptar e se proteger contra AH. Enfatiza a importância de olhar para a defesa nacional como um todo, desenvolver mecanismos de proteção e resiliência em áreas não militares e estabelecer sistemas de informações para detetar ameaças. Além disso, menciona a importância de desenvolver capacidades autónomas em termos militares para resistir às primeiras ações cinéticas antes de invocar o apoio dos aliados. Ele destaca a necessidade de uma abordagem abrangente, incluindo a educação da cidadania sobre os riscos das AH e o desenvolvimento de capacidades robustas de cibersegurança.

O E2 destaca a dificuldade em determinar os agentes, meios e objetivos das AH assim como a diversidade de vetores de ameaça. Ele enfatiza a importância de adaptar a legislação e as capacidades das FFAA para lidar com essas ameaças. Menciona a necessidade de investimento em recursos materiais, financeiros, tecnológicos e humanos para capacidades

efetivas de ciberdefesa e ciberataque, bem como a cooperação com entidades públicas e privadas, nacionais e estrangeiras.

Depois, o E3 fala da importância de desenvolver uma estratégia nacional de combate às AH, que esteja alinhada com as organizações da NATO e da União Europeia. Ele menciona a necessidade de criar uma célula de resposta específica no Ministério da Defesa Nacional ou nas FFAA, voltada para o combate às AH. Destaca a importância de aumentar a cooperação internacional e tomar medidas em todos os níveis hierárquicos, em todos os ramos das FFAA.

O E4 destaca a necessidade de estruturar a resposta e não apenas desenvolver uma estratégia. Ele menciona a importância de ter um mecanismo de inteligência para lidar com as AH e sugere "*a criação de um conceito nacional*" e um "*centro de gestão de crises*". Aborda a importância de disseminar uma cultura de conscientização sobre as AH em todos os níveis e a necessidade de ter uma estratégia genética, estrutural e operacional.

Por fim, E5 fala da importância da educação, formação e treino das FFAA para lidar com as AH. Menciona a necessidade de adaptar a mentalidade dos militares e criar manuais e doutrinas específicas para combater as AH. Identicamente se destaca a importância de aprender com exemplos de outros países, como a Finlândia, que já possuem doutrina e oferecem treino nesse contexto.

4.2 Discussão de Resultados

Face aos dados apresentados, verificou-se que relativamente ao OE1, *identificar as limitações da defesa contra a GH,* uma dificuldade é a deteção e atribuição de agentes. As AH são caracterizadas pela sua natureza multifacetada e pela utilização de táticas não convencionais (Costa, 2021). Isso dificulta a identificação dos agentes responsáveis e a atribuição clara das ações, tornando desafiador definir a melhor resposta. Outra limitação tem a ver com a integração entre setores. Tal como referido por Cullen e Reichborn-Kjennerud (2017), a GH envolve uma ampla gama de ameaças que podem afetar diferentes setores da sociedade, como militar, civil, político e económico. A coordenação efetiva entre esses setores e a criação de mecanismos de colaboração podem ser complexas, exigindo uma abordagem integrada para enfrentar essas ameaças de forma abrangente.

Outra limitação identificada relaciona-se com a capacidade de ciberdefesa. A cibersegurança desempenha um papel fundamental na defesa contra a GH, pois muitos ataques híbridos envolvem o uso de tecnologias digitais e ataques cibernéticos. No entanto,

a construção e manutenção de capacidades efetivas de ciberdefesa podem ser um desafio, especialmente devido à constante evolução das ameaças e à falta de recursos especializados.

A compreensão adequada das AH e a capacidade de identificá-las exigem um alto nível de conscientização e treino em todos os níveis hierárquicos. Garantir que os militares, as forças de segurança e os tomadores de decisão tenham o conhecimento e as habilidades necessárias para reconhecer e responder a essas ameaças é crucial, mas pode ser um desafio em termos de educação e formação.

Posteriormente, relativamente ao OE2, *identificar métodos para alcançar eficiência neste âmbito*, foi apontado que é essencial investir em capacidades de inteligência robustas e sistemas de monitorização contínuos para identificar precocemente possíveis AH. Isso envolve a recolha, análise e partilha de informações de várias fontes, incluindo agência de inteligência, setores público e privado, e parcerias internacionais.

A GH abrange diversos setores, portanto, é crucial promover a cooperação e colaboração entre as instituições militares, de segurança, políticas, económicas e civis. Isso inclui a criação de mecanismos de comunicação eficazes, partilha de informações e planeamento conjunto para responder de maneira coordenada e abrangente às AH.

Dada a importância da cibersegurança na GH, é essencial investir em capacidades cibernéticas avançadas. Isso inclui, tal como citado por Fernandes (2021), o desenvolvimento de tecnologias de deteção e prevenção de ataques cibernéticos, a formação de especialistas em cibersegurança e a promoção de boas práticas de segurança cibernética em todos os setores.

É fundamental aumentar a conscientização e o conhecimento sobre as AH em todos os níveis da sociedade, desde os cidadãos comuns até aos tomadores de decisão. Isso pode ser alcançado através de campanhas de conscientização, programas de treino e educação em segurança nacional, além de exercícios regulares de simulação para melhorar a preparação e a prontidão para enfrentar a GH.

A GH frequentemente transcende as fronteiras nacionais, portanto, a cooperação internacional é essencial.

Ao recolher dados que dessem resposta ao OE3, *identificar os conflitos europeus e as suas repercussões*, verificou-se que apenas foi referida a atual guerra entre e Rússia e a Ucrânia.

De seguida, sobre o OE4, *compreender qual a tarefa das FFAA*, entendeu-se que as FFAA são responsáveis pela defesa do território nacional contra agressões externas. Isso pode envolver a preparação e a prontidão para combater ameaças convencionais, como

invasões militares, bem como ameaças não convencionais, como ataques cibernéticos ou terroristas, tal como citado no estudo de Grilo (2021).

Do mesmo modo podem ser implantadas para fins de manutenção da paz, em cooperação com organizações internacionais, como as Nações Unidas. Nesse papel, as FFAA trabalham para estabilizar áreas de conflito, implementar acordos de paz, proteger civis e ajudar na reconstrução pós-conflito.

As FFAA também têm o papel de dissuadir potenciais agressores por meio da demonstração de capacidade militar e da prontidão para a defesa. A existência de FFAA fortes e bem equipadas pode dissuadir agressões externas e contribuir para a estabilidade regional.

Em certas circunstâncias, as FFAA podem ser chamadas para apoiar as forças de segurança interna em operações de combate ao crime organizado, terrorismo ou outras ameaças à segurança interna do país.

É necessário ressaltar que as tarefas específicas das FFAA podem variar de acordo com o país, sua localização geográfica, seus compromissos internacionais e a natureza das ameaças enfrentadas.

Subsequentemente, e de forma a responder às perguntas de investigação, tem-se que na **PD1**, **quais são os conflitos em curso e ameaças à Europa?**, os conflitos em curso e ameaças à Europa rendem-se, como referido, ao conflito híbrido entre Rússia e Ucrânia. A Rússia empregou uma variedade de ações não militares, incluindo ações económicas, diplomáticas, guerra da informação e ataques cibernéticos. O seu objetivo era garantir que a Ucrânia se tornasse um estado pró-russo dentro da sua área de influência.

A Rússia utilizou várias ferramentas e modalidades no domínio cibernético, incluindo intromissões, recolha de informação sensível, negação de serviços básicos e campanhas de desinformação nas redes sociais. Além disso, empregou instrumentos de poder diplomático e informacional, como narrativas criadas e agentes enviados para criar indignação.

Depois, na **PD2**, **qual a capacidade de resposta de Portugal?** ficou claro que pode variar dependendo dos recursos disponíveis, das estratégias adotadas e das parcerias internacionais estabelecidas. É importante ressaltar que a resposta adequada a AH requer uma abordagem multidimensional e integrada, envolvendo não apenas as FFAA, mas também outras entidades governamentais e setores da sociedade.

Em termos de capacidade militar, Portugal participa ativamente na NATO e na União Europeia, o que proporciona uma maior coordenação e cooperação em matéria de segurança

e defesa. Como membro da NATO, Portugal está sujeito às obrigações de defesa coletiva e pode contar com o apoio dos seus aliados em caso de ameaças à sua segurança. Além disso, Portugal participa em exercícios internacionais e coopera na partilha de informações estratégicas com organismos internacionais, como o Sistema de Informações para a República Portuguesa (SIRP) e a SigMil.

No campo da ciberdefesa, Portugal tem trabalhado para fortalecer as suas capacidades e melhorar a resiliência cibernética. Isso inclui a participação em iniciativas da NATO e da União Europeia relacionadas à cibersegurança, bem como a colaboração com organizações internacionais no intercâmbio de informações e melhores práticas. No entanto, é fundamental destacar que a cibersegurança é um desafio em constante evolução, e Portugal continua a enfrentar ameaças nessa área.

Além disso, Portugal tem procurado fortalecer a sua capacidade de deteção e prevenção de AH por meio da cooperação com parceiros internacionais. A participação em grupos de trabalho, como os existentes na União Europeia, e a colaboração com o Centro Europeu de Excelência para CAH (Hybrid CoE) permitem o intercâmbio de informações estratégicas e a realização de exercícios conjuntos.

No entanto, é importante reconhecer que as AH são complexas e em constante evolução, e nenhum país está imune a elas. As capacidades de resposta de Portugal podem ser aprimoradas por meio do desenvolvimento de estratégias nacionais abrangentes, da melhoria da cooperação entre diferentes entidades governamentais, do fortalecimento das capacidades de ciberdefesa e do investimento em educação e conscientização da população sobre as AH (Costa, 2021).

É fundamental que Portugal continue a acompanhar de perto as mudanças no ambiente de segurança e adote medidas adaptativas para enfrentar eficazmente as AH. Isso requer uma abordagem holística que envolva não apenas as FFAA, mas também agências governamentais, setores privados e a sociedade como um todo.

Por último, na **PD3**, **que impacto tem para as FFAA Portuguesas?**, tem-se que as AH podem ter um impacto significativo nas FFAA Portuguesas, exigindo uma adaptação e resposta adequadas. Essas ameaças podem afetar diversos aspetos das operações militares e da segurança nacional.

As AH podem requerer um ajuste nas estratégias e táticas militares tradicionais. As FFAA Portuguesas precisam estar preparadas para enfrentar adversários que utilizam métodos não convencionais, como a desinformação, a sabotagem cibernética ou o uso de

grupos paramilitares. Isso pode exigir a adoção de abordagens mais flexíveis e adaptativas nas operações militares.

As AH frequentemente envolvem ataques cibernéticos, que podem comprometer a infraestrutura de comunicações, sistemas de defesa e informações sensíveis. As FFAA Portuguesas devem investir em capacidades de ciberdefesa, incluindo a deteção, prevenção e resposta a ataques cibernéticos, a fim de garantir a integridade e a segurança de suas redes e sistemas (Alves, 2020).

Depois, uma resposta eficaz às AH muitas vezes requer a cooperação e coordenação com parceiros internacionais, tanto a nível bilateral como multilateral. As FFAA Portuguesas devem estar preparadas para participar de exercícios conjuntos, partilhar informações estratégicas e colaborar em ações de defesa coletiva no âmbito de organizações como a NATO e a União Europeia.

O combate às AH exige que as FFAA Portuguesas estejam bem informadas e treinadas para identificar e enfrentar essas ameaças. Isso inclui a capacitação dos militares em áreas como a cibersegurança, a análise de informações e a compreensão dos métodos empregados pelos adversários híbridos. Além disso, é importante envolver as tropas em exercícios e simulações que reproduzam cenários realistas de AH.

Em resumo, as AH têm o potencial de impactar as FFAA Portuguesas em várias áreas, desde o planeamento e operações até a ciberdefesa e a cooperação internacional. É essencial que as FFAA estejam preparadas e capacitadas para responder a essas ameaças, adotando uma abordagem adaptativa e colaborativa, e investindo em capacidades adequadas.

CONCLUSÕES

Tendo sido realizado a parte da revisão da literatura, da investigação e previamente respondidas as PD da investigação, segue-se por consequente a resposta à PP **"Quais são as mudanças a realizar em Portugal para atingir um adequado nível de defesa contra as Ameaças Híbridas?"**. Assim sendo para atingir um nível de defesa mais eficaz contra a GH, Portugal deve considerar algumas mudanças importantes. Primeiro, é fundamental aumentar a conscientização em todos os níveis da sociedade portuguesa sobre as AH e os métodos utilizados pelos adversários. Isso envolve educar os cidadãos, os setores público e privado e os militares sobre os riscos associados à GH, promovendo uma compreensão ampla e uma postura vigilante em relação a essas ameaças.

Segundo, dada a importância crítica da segurança cibernética na GH, Portugal deve investir em capacidades de ciberdefesa robustas. Isso inclui o desenvolvimento de estratégias avançadas de proteção cibernética, a atualização constante dos sistemas de defesa, a colaboração com parceiros internacionais na troca de informações e a capacitação contínua dos profissionais de segurança cibernética.

A GH exige uma abordagem integrada e coordenada entre várias agências governamentais, forças de segurança e setores relevantes. Portugal deve procurar uma maior colaboração e coordenação entre essas entidades, partilhando informações e recursos para uma resposta mais eficaz às AH.

A recolha e análise de informações precisas desempenham um papel crucial na deteção e prevenção de AH. Deve investir em capacidades de informações e vigilância, incluindo o uso de tecnologias avançadas, para obter uma compreensão abrangente do ambiente de segurança e identificar possíveis ameaças.

A GH é um desafio global que requer uma resposta coordenada e colaborativa. Portugal deve fortalecer a sua colaboração com parceiros internacionais, como a NATO, a União Europeia e outros países, para partilhar informações, realizar exercícios conjuntos e cooperar na defesa coletiva contra AH.

As FFAA Portuguesas devem estar preparadas para enfrentar AH, adaptando as suas capacidades e estratégias em conformidade. Isso inclui investir em tecnologias avançadas, treino especializado e exercícios realistas para garantir que estejam preparadas para lidar com as táticas e métodos empregados pelos adversários híbridos.

Ao adotar essas mudanças e implementar uma abordagem abrangente, Portugal estará favoravelmente posicionado para enfrentar as AH de forma mais eficaz, protegendo

os seus interesses nacionais, garantindo a segurança dos seus cidadãos e contribuindo para a estabilidade regional e global.

Resultante da invasão russa na Ucrânia e da consequente evolução da GH, surge um novo contexto securitário mundial, na medida em que conferiu uma nova centralidade ao instrumento Militar. Nesta guerra atual, a aplicação de forças e mobilização de recursos militares tem desempenhado um papel fundamental. As ações russas demonstraram o impacto significativo que o poderio militar tem em conjunturas de conquista territorial e influência política. O uso do instrumento Militar nesta guerra, abrangeu uma série de táticas e estratégias, especificamente ocupações militares de regiões, emprego de forças especiais e ainda operações de guerra assimétrica. Mobilização de tropas, introdução de armamento de alta tecnologia e o uso de forças navais e aéreas esclareceram claramente o poder de fogo e a capacidade de projeção da Federação da Rússia.

Inclusivamente a utilização deste instrumento foi seriamente impactante na população civil e nas infraestruturas de ambos os países, escalando a significativas perdas humanas. É evidente que a capacidade do instrumento Militar tem a possibilidade de influenciar decisivamente e moldar o curso da guerra.

Todavia, é relevante salientar, que pese embora o instrumento Militar tenha ganho uma nova centralidade neste novo contexto securitário, ou outros domínios são igualmente determinantes. O domínio ciber, campanhas de desinformação, o plano diplomático, a *intelligence* assim como a proteção das infraestruturas exercem um papel destacável no desenvolver da guerra.

Portanto, sem embargo do destaque do instrumento Militar no contexto da guerra, é imprescindível ter em conta a interação e a complementaridade com os demais domínios e instrumentos numa abordagem em busca de soluções para este conflito. A coordenação entre estes elementos distintos é crucial para responder a vicissitudes e mitigar as repercussões da guerra, aspirando a promover a paz, segurança e estabilidade.

No que concerne às limitações enfrentadas nesta investigação, apresentam-se algumas que requerem uma análise cuidadosa. Em primeiro lugar, é importante reforçar que o conceito de AH é relativamente incipiente em Portugal, havendo escassez de informações e conhecimentos disponíveis sobre o tema. Como resultado, o presente estudo teve de basear-se fortemente em estudos internacionais e entrevistas realizadas para a coleta de dados relevantes. Essa dependência de fontes externas pode introduzir enviesamentos e limitações em termos de sua aplicabilidade ao contexto português.

Adicionalmente, destaca-se a ausência de uma estratégia nacional para enfrentar AH, o que representa um desafio significativo. A inexistência de um órgão centralizado de decisão e coordenação, dotado da necessária agilidade e autoridade, dificulta a formulação de diretrizes estratégicas abrangentes. Essa limitação prejudica a capacidade de enquadrar a análise e interpretar os resultados de forma mais pragmática e específica ao contexto português.

É possível elencar outra limitação, como tal a carência de diversidade de especialistas entrevistados, tendo dificultado a validação e incorporação de novos indicadores. Do número total de entrevistas previamente planeadas, apenas seis foram realizadas. É indispensável frisar que, por ser uma temática recente o conhecimento nesta área não se encontra extensamente consolidado.

Além disso, vale ressaltar a inexperiência do investigador neste campo de estudo. Embora tenha havido empenho e dedicação intensos, é necessário reconhecer que a experiência é adquirida com o tempo e o amadurecimento do investigador podem trazer melhorias consideráveis.

Diante dessas limitações, enfatiza-se a necessidade de uma investigação mais aprofundada, recolha de dados abrangente e o desenvolvimento de uma estratégia nacional robusta para enfrentar de forma eficaz as AH em Portugal. Torna-se imprescindível ampliar a base de conhecimentos no país e estabelecer uma abordagem coordenada que envolva múltiplos atores relevantes e garanta agilidade nos processos de tomada de decisão. Ao abordar essas limitações, estudos futuros poderão fornecer uma visão mais detalhada e contribuir para o desenvolvimento de estratégias eficazes no combate às AH.

REFERÊNCIAS BIBLIOGRÁFICAS

Almeida, L., & Freire, T. (2000). *Metodologia da Investigação em Psicologia e Educação.* Braga: Psiquilíbrios.

Alves, A. (2020*). A prevenção e o combate às ameaças híbridas: impacto para as forças armadas portuguesas.* Trabalho de Investigação Individual do CPOG 2019/2020. Instituto Universitário Militar: Departamento de Estudos Pós-Graduados.

Andersson, J. J. & Tardy, T. (2015). Hybrid: what's in a name? *EUISS Brief*, 32. European Union Institute for Security Studies.

Bachmann, S. (2015). Hybrid Wars: The 21st-Century's New Threats to Global Peace and Security. *Scientia Militaria: South African Journal of Military Studies*, *43*(1), 77-98. https://doi.org/10.5787/43-1-1110

Bilal, A. (2021). *Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote.* https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Blum, R.; Zouganeli, E.; Rao, S. & Elcheikh, S. (2015). *The Future of NATO in the Face of Hybrid Threats*. Belgium: NATO.

Bogdan, R. & Blinken, S. (1994). *Investigação qualitativa em educação. Uma introdução à teoria e aos métodos.* Porto: Porto Editora.

Branco, C. (2009). A participação de Portugal em operações de paz. Êxitos, problemas e desafios. E-Cadernos CES, 6 [online]. Disponível em: http://eces.revues.org/365 [acedido a 18 de março de 2021].

Branco, C. (2015). A participação portuguesa em missões de paz da ONU. Relações Internacionais, 47, pp. 101-126.

Brito, N. (2005). Política Externa Portuguesa. O futuro do passado. Relações Internacionais, 5, pp. 147-161.

Campbell, R., Goodman-Williams, R., Feeney, H. & Fehler-Cabral, G. (2018). Assessing Triangulation Across Methodologies, Methods, and Stakeholder Groups: The Joys, Woes, and Politics of Interpreting Convergent and Divergent Data. *American Journal of Evaluation, 41*(1), 125–144. https://doi.org/10.1177/1098214018804195

Carmo, H. & Ferreira, M. (1998). *Metodologia da. Investigação. Guia para Auto-aprendizagem.* Lisboa: Universidade Aberta.

Comissão Europeia (2018). *Comunicação Conjunta ao Parlamento Europeu, ao Conselho Europeu e ao Conselho – Aumentar a resiliência e reforçar a capacidade de enfrentar ameaças híbridas.* Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018JC0016&from=PT.

Comissão Europeia (2020). *Joint Communication to the European Parliament and the Council – The EU's Cybersecurity Strategy for the Digital Decade.* Disponível em https://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

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

Costa, R. (2021a). *Hybrid Threats in the Context of European Security.* https://www.idn.gov.pt/pt/publicacoes/ebriefing/Documents/E-Briefing%20Papers/E-Briefing%20Papers%203.pdf

Costa, R. (2021b). *Hybrid Threats in the Context of European Security – Report of the international conference organized at the National Defence Institute (IDN) on 18 May 2021 under the framework of the Portuguese Presidency of the Council of the European Union.* Lisboa: Instituto da Defesa Nacional.

Cravinho, J. (2010). A campanha portuguesa para o Conselho de Segurança. Relações Internacionais, 28, pp. 5-37.;

Cravinho, J. (2021). Intervenção do Ministro da Defesa Nacional, João Gomes Cravinho, por ocasião da sessão de apresentação das FND para 2021 aos Órgãos de Comunicação Social. Auditório do JALLC, Unidade de Apoio do Reduto Gomes Freire (CCOM), Oeiras, 6 de janeiro de 2021. Disponível em: https://www.defesa.gov.pt/pt/comunicacao/intervencoes/Lists/PDEFINTER_IntervencoesList/20210106_MDN_DiscursoApresentacao-FND-2021.pdf.

Cullen, P. & Reichborn-Kjennerud, E. (2017*). MCDC Countering Hybrid Warfare Project. Understanding Hybrid Warfare*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf

Davis Jr., J. R. (2013). Defeating Future Hybrid Threats: The Greatest Challenge to the Army Profession of 2020 and Beyond. *Military Review*, XCIII(5): 21-29

Davis Jr., J. R. (2014). *The Hybrid Mindset and Operationalizing Innovation: Toward a Theory of Hybrid*. Fort Leavenworth, Kansas Fort: U.S. School of Advanced Military Studies.

DeJonckheere, M. & Vaughn, L. (2019). Semistructured interviewing in primary care research: a balance of relationship and rigour. *Fam Med Community Health, 7*(2), e000057. https://doi.org/10.1136/fmch-2018-000057

Dourado, M. E.; Leite, A. C. & Nobre, F. F. (2020). Guerra Híbrida vs. Gibridnaya Voyna: os diferentes significados dos conflitos híbridos para o ocidente e para a Rússia. *Revista da Escola de Guerra Naval*, 26(1): 39-64.

Drab, L. (2018). Defence diplomacy – an important tool for the implementation of foreign policy and security of the state. *Security and Defence Quarterly, 20*(3), 57–71. https://doi.org/10.5604/01.3001.0012.5152

Duarte, A. (2013). Estratégia: Origem e Fundamento. Nação e Defesa, 136, pp. 34-65.

European External Action Service (2015). *Food-for-thought paper* "*Countering Hybrid Threats*". Brussels: European Union.

Fernandes, A. H. (2017). *Livro dos Contrastes. Guerra e Política (Homo Strategicus III)*. Porto: Fronteira do Caos.

Fernandes, H. (2016). As novas guerras: o desafio da guerra híbrida. *Revista de Ciências Militares, IV*(2), 13-40.

Fernandes, N. (2021). *A prevenção e o combate de ameaças híbridas: identificar instrumentos de medida: variáveis e indicadores de resiliência do instrumento de poder económico face às ameaças híbridas*. Trabalho Final de Curso do CEMC. Instituto Universitário Militar: Departamento de Estudos Pós-Graduados.

Fortin, M.-F. (1999). *O processo de Investigação: da Concepção à Realização*. Loures: Lusociência.

Fortin, M.-F. (2009). *Fundamentos e etapas do processo de investigação*. Loures: Lusodidacta.

Freire, M. e Brito, R. (2010). Ensaio bibliográfico: estudos sobre política externa portuguesa após 2000. Relações Internacionais, 28, pp. 157-179.

Galito, M. (2019). Ensaio sobre Política Externa Portuguesa. Working Paper CEsA CSG. 176/2019.

Garcia, F. (2008). A participação portuguesa nas missões militares: Iraque, Afeganistão e Líbano. Nação e Defesa, 121, pp. 177-209.

Gaspar, C. (2008). Portugal e as Missões Militares Internacionais. Revista Militar [online] n.º 2479/2480.

Geers, Kenneth (2015). *Cyber War in Perspective Russian Agression against Ukraine*. Tallin: NATO Cooperative Cyber Defence Centre of Excellence.

Gerrits, A. (2018). Disinformation in International Relations: How Important Is It?. *Security And Human Rights*, 29(1-4): 3-23.

Giannopoulos, G., Smith, H., & Theocharidou, M. (2020). *The Landscape of Hybrid Threats: A Conceptual Model Public Version*. Bruxelas: Comissão Europeia, Ispra, JRC123305.

Grilo, A. (2021*). A defesa nacional na prevenção e combate às ameaças híbridas*. Trabalho de Investigação Individual do CPOG 2020/2021. Instituto Universitário Militar: Departamento de Estudos Pós-Graduados.

Hoffman, F. (2009). Hybrid Warfare and Challenges. *Joint Force Quarterly*, 52, pp. 34-39.

Hoffman, Frank (2007). *Conflict in the 21st century: The Rise of Hybrid Wars*.

Huovinen, P. (2011). *NATO Multimedia Library*. Belgium: NATO.

Hybrid CoE (2020). Hybrid threats and the law: Concepts, trends and implications. *Hybrid CoE Trend Report 3*.

Hybrid CoE (June 2022). AI-based technologies in hybrid conflict: The future of influence operations. *Hybrid CoE Paper 14*.

Jennings, G. (2005). Business, Social Science Methods Used in. *Encyclopedia of Social Measurement*, 1, 219-230. https://doi.org/10.1016/B0-12-369398-5/00270-X

Johnson, M. & McLean, E. (2020). Discourse Analysis. *International Encyclopedia of Human Geography* (Second Edition), 377-383. https://doi.org/10.1016/B978-0-08-102295-5.10814-5

Kleinheksel, A., Rockich-Winston, N., Tawfik, H. & Wyatt, T. (2020). Demystifying Content Analysis. *Am J Pharm Educ., 84*(1), 7113. https://doi.org/doi: 10.5688/ajpe7113

Kyngäs, H. (2019). Qualitative Research and Content Analysis. In: Kyngäs, H., Mikkonen, K., Kääriäinen, M. (eds) *The Application of Content Analysis in Nursing Science Research*. Springer, Cham. https://doi.org/10.1007/978-3-030-30199-6_1

Lima, W. & Newell-McLymont, E. (2021). *Qualitative Research Methods: A Critical Analysis.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3845254

Limnel, Jarno (2015). The Exploitation of Cyber Domain as Part of Warfare: Russo-krainian War. *International Journal of Cyber-Security and Digital Forensics*, 4, pp. 521- 532.

Mendes, P. (2018). Identidade, ideias e normas na construção dos interesses em política externa: o caso português. Análise Social, 53(227), pp. 458-487.

Ministério da Defesa Nacional (2018). Despacho n.º 7861/2018 – Diretiva de Orientação Política para o Planeamento das Forças Nacionais no Exterior para o Ano Civil de 2019. Diário da República, n.º 157/2018, Série II de 16 de agosto, pp. 22501-22502.

Moreira, A. (2000). Situação internacional portuguesa. Análise Social, 35(154-155), pp. 315-326.

Multinational Capability Development Campaign (MCDC) (2019). *Projeto de guerra híbrida de combate ao MCDC: Combatendo a Guerra Híbrida*.

NATO (2010). *Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. Belgium: NATO

NATO (2015). *Hybrid Warfare: NATO´s New Strategic Challenge*?, Brussels: NATO Parliamentary Assembly.

Neris, R., Papathanassoglou, E., Leite, A., Garcia-Vivar, C., DeMontigny, F. & Nascimento, L. (2023). Five tips for conducting remote qualitative data collection in COVID

times: theoretical and pragmatic considerations. *Rev Esc Enferm USP*., 57, e20220277. https://doi.org/10.1590/1980-220X-REEUSP-2022-0277en

Nunes, I. (2017). A União Europeia como Sistema de Governação Regional no Domínio da Segurança. In: V. Viana e I. Nunes, orgs., Segurança Europeia. Lisboa: Instituto da Defesa Nacional, pp. 37-74

Pereira, C. (2011). Dez Anos de Guerra no Afeganistão. Nação e Defesa, n.º 130, pp. 179-216.

Pinto, Inês de Sousa (2022). *O Impacto das Ameaças Híbridas no Contexto de Estados Frágeis em África: As Respostas da União Europeia à crise de desinformação no Mali*. Lisboa: ISEG – Lisbon School of Economics & Management.

Pinto, M. (2012). Portugal: a participação em missões de paz como factor de credibilização externa. Janus.net – e-journal of International Relations, 3(1), pp. 66-78.

Presidência do Conselho de Ministros (2013). Resolução do Conselho de Ministros n.º 19/2013 que Aprova o Conceito Estratégico de Defesa Nacional. Diário da República,n.º 67/2013, Série I de 5 de abril, pp. 1981-1995.

Prodanov, C. & Freitas, E. (2013). *Metodologia do trabalho científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico* (2.ª ed.). Brasil: Universidade Feevale.

PRONE – Centro de Excelência Jean Monnet (2021). A participação de Portugal em missões de paz: objetivos, prioridades e capacidades. Relatório 1, março 2021. Disponível em:https://coe.uc.pt/wpcontent/uploads/2021/06/MesaRedonda_PolicyBrief_PT_final_17mar2021.pdf.

Quivy, R. & Campenhoudt, L. (2008). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.

Reis, B. (2013). Ensaio em torno de uma cultura estratégica portuguesa. Nação e Defesa, n.º 136, pp. 9-33.

Reis, B. e Gaspar, C. (2013). Uma Estratégia Global para Portugal numa Europa em Crise. Cadernos IDN, 9. Lisboa: Instituto de Defesa Nacional.

Reis, J. e Menezes, S. (2020). The Portuguese Special Operations Forces as Instrument of Foreign Policy. In Á. Rocha e R. Pereira, orgs., Developments and Advances in Defense and Security. Singapore: Springer Nature Singapore Pte Ltd., pp. 245-255.;

Robinson, S. (2016). Still focused on the Atlantic: accounting for the limited Europeanization of Portuguese security policy. European Security, 25(1), pp. 134-158.

Rodrigues, D. (2011). As Forças Armadas Portuguesas no Afeganistão. Nação e Defesa, 130, pp. 131-155.

Rogers, E. L., 2012. Defense Technical Information Center

Santiáñez, N. (2018). *Wittgenstein's Ethics and Modern Warfare*. Waterloo, Ontario: Wilfrid Laurier University Press.

Selvi, A. (2019). *Qualitative content analysis*. London: Routledge.

Smith, H., & Giannopoulos, G. (2020). The Landscape of Hybrid Threats: A Conceptual Model Public Version. European Commission & Ispra.

Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research*, 104, 333-339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sousa, F. (2011). A Participação de Portugal nas Operações de Paz e a Segurança Nacional. Revista Militar, n.º 2509/2510, pp. 271-297.

Sun, Y. (2017). Coding of data. In *The SAGE Encyclopedia of Communication Research Methods*. https://doi.org/10.4135/9781483381411

Teixeira, N. (1999). Portugal e a NATO: 1949-1999. Nação e Defesa, n.º 89, pp. 15-41.

Teixeira, N. (2010). Breve Ensaio sobre a Política Externa Portuguesa. Relações Internacionais, 28, pp. 51-60.

Teixeira, N. (2015). Portugal. In: M. Freire, org., Política Externa: As Relações Internacionais em Mudança, 2.ª edição. Coimbra: Imprensa da Universidade de Coimbra, pp. 355-363.

Telo, J., Borges, J. & Pires, N. (2018). *Dar uma razão à força e uma força à razão* (1ª Edição). Alcochete: Nexo Editora.

U.S. Army (2010). *Training Circular 7-100, Hybrid Threat*. Washington: U.S. Government Printing Office (GPO).

U.S. Army (2011). *Army Doctrine Publication (ADP) 3-0, Unified Land Operations*. Washington, DC: Headquarters, Department of the Army

U.S. Government Accountability Office (2010). U*.S. Government Accountability Office*.

Vaismoradi, M., & Snelgrove, S. (2019). Theme in Qualitative Content Analysis and Thematic Analysis. *Forum: Qualitative Social Research, 20*(3), 1-14. https://doi.org/10.17169/fqs-20.3.3376

Walliman, N. (2011). Research theory, Research methods: the basics: USA and Canada (1sted.). New York: Routledge.

Wahyuni, D. (2012). The Research Design Maze: *Understanding Paradigms, Cases, Methods and Methodologies*. Journal of Applied Management Accounting Research, 10(1), 69–80.

Young, J., Rose, D., Mumby, H., Benitez-Capistros, F., Derrick, C., Finch, T., Garcia, C., Home, C., Marwaha, E., Morgans, C., Parkinson, S., Shah, J., Wilson, K. & Mukherjee, N. (2018). A methodological guide to using and reporting on interviews in conservation science research. *Methods in Ecology and Evolution, 9*(1), 10-19. https://doi.org/10.1111/2041-210X.12828

APÊNDICES

APÊNDICE A – MODELO DE ANÁLISE

TEMA	**Portugal face às Ameaças Híbridas: o imperativo de adequação a um novo desafio.**						
Objetivo Geral	Analisar a evolução teórico-prática das AH com enfoque no posicionamento de Portugal						
Objetivos Específicos	**Questão Central**	Quais são as mudanças a realizar em Portugal para atingir um adequado nível de defesa contra as Ameaças Híbridas?"					
	Questões Derivadas	**Conceito**	**Dimensões**	**Variáveis**	**Indicadores**	**Técnicas de recolha**	**Ferramentas**
OE1 Identificar e caracterizar as Ameaças Híbridas e a sua multidimensionalidade.	**QD1** Quais são os conflitos em curso e ameaças à Europa?	O CAH ao nível das FFAA	Instrumentos: Militar, Político, Económico, Civil e Informacional (MPECI)	Político, Militar, Social Economico, Infraestruturas, Informacional – Ciberespaço, Legal (PMSEII-CL)	Instrumento de Poder Militar Meios e efeitos das AH (Rússia/Ucrânia) Componentes da Estratégia CAH	• Análise documental • Entrevistas	• Conceito analítico
OE2 Analisar a inserção internacional de Portugal nos quadros de resposta às AH da UE e da NATO.	**QD2** Qual a capacidade de resposta de Portugal?		Estratégia da UE e da NATO para o CAH	Conhecimento situacional Resiliência Prevenção e resposta a crises Apoio e Cooperação Internacional	Ameaças Oportunidades Vulnerabilidades Potencialidades	• Análise documental • Entrevistas	• SWOT
OE3 Identificar os conflitos europeus e as suas repercussões. **OE4** Compreender o contributo de Portugal e das FFAA.	**QD3** Que impacto tem para as FFAA Portuguesas?		Capacidades das FFAA	Conhecimento situacional Resiliência Prevenção e resposta a crises Apoio e Cooperação Internacional	Ameaças Oportunidades Vulnerabilidades Potencialidades	• Análise documental • Entrevistas	• SWOT

Modelo de análise
Elaboração própria

APÊNDICE B – ESTRUTURA BASE DO BLOCO DE ENTREVISTAS

Guião do Bloco de entrevista

Caracterização do entrevistado Entrevista n.º _____

Nome do entrevistado: _____ Ramo:_____Posto___Classe:_

Cargo:_____ Local:_____Data: _____

Excelentíssimo Senhor Oficial,

O meu nome é Diogo Augusto Mesquita Fonte, Aspirante-Aluno de Infantaria, e de momento estou a desenvolver o meu Trabalho de Investigação Aplicado (TIA) para desta forma concluir mais uma etapa da minha formação na Academia Militar.

Durante todo este percurso dedicado à investigação e elaboração do TIA cujo o tema foi intencionalmente escolhido pela minha pessoa uma vez que este me despertou interesse, surge agora a necessidade de proceder a entrevistas a personalidades especialistas na área.

Neste âmbito, encontro-me a realizar uma investigação com o seguinte título: "*Portugal face às Ameaças Híbridas: o imperativo de adequação a um novo desafio."* O objetivo geral deste TIA é perceber quais as adaptações necessárias que a Defesa Nacional (DN) e as Forças Armadas (FFAA) devem aplicar de modo a acompanhar a evolução e o combate às Ameaças Híbridas (AH).

A metodologia utilizada neste TIA segue uma estratégia de investigação qualitativa através da pesquisa e análise documental e com recurso a entrevistas.

Peço a sua autorização para proceder à gravação destas entrevistas e da mesma forma fazer referência no trabalho associando à sua pessoa. Caso não esteja de acordo com estes termos, garanto uma total confidencialidade e o tratamento de dados será anonimo. Esta entrevista terá um tempo estimado de 25 minutos. Todo seu conhecimento bem como a sua experiência será fulcral no desenvolvimento deste trabalho garantido qualidade e veracidade pelas suas palavras. Mais uma vez um enorme agradecimento pela sua disponibilidade.

Nestas condições gostaria de colocar um grupo de cinco questões, em que as respostas são fundamentais na resolução da questão central desta investigação. Portugal face às Ameaças Híbridas.

Enquadramento:

O modelo conceptual, do Hybrid CoE (2020), *The Landscape of Hybrid Threats: A Conceptual Model,* foi desenvolvido pela UE em 26 de novembro de 2020, com o intuito de contribuir para definição de estratégias nacionais para a prevenção e combate das AH.

O modelo conceptual é um guia que apresenta diferentes áreas e ferramentas utilizadas no combate às AH. É importante que os decisores políticos o utilizem como referência para criar

políticas e ações mais eficientes e eficazes, especialmente quando se trata de detetar e atribuir responsabilidades.

Questões:

Intro: "Hybrid Threats is a broad overarching concept that includes many types of activity: interference, influence, operations, campaigns and warfare/war. All of these activities can be seen as unwelcome interventions of one sort or another to a country's internal space." (Smith e Giannopoulos, 2020, p.14)

1ª Questão:

Durante o conflito híbrido da Rússia/Ucrânia, quais foram as modalidades de ação, os domínios e as ferramentas usadas pela Rússia nas funções críticas da Ucrânia de forma a explorarem as respetivas vulnerabilidades e alcançarem os seus objetivos políticos?

Intro: "Uma melhor coordenação e cooperação em matéria de comunicação estratégica em todas as instituições da UE, com os Estados-Membros e com os parceiros e organizações internacionais, é essencial e exige preparação e prática antes da reação a crises em tempo real." (Comissão Europeia, 2018, p.7)

2ª Questão:

Relativamente à cooperação internacional e no âmbito da inserção de Portugal na NATO e na UE, existe uma partilha informações estratégicas com organismos internacionais relativamente às ameaças híbridas e às suas ferramentas bem como a participação em exercícios internacionais?

3ª Questão:

Tendo por base as orientações estratégicas da UE e da NATO para o CAH e os pilares em que a mesma se suporta, quais são as principais ameaças e oportunidades para o CAH ao nível das FFAA Portuguesas?

4ª Questão:

Quais as vulnerabilidades e potencialidades no ambiente interno que identifica para Portugal, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH?

5ª Questão:

De que forma pode a Defesa Nacional e as FFAA adaptar-se temporalmente às AH e combatê-las eficazmente?

APÊNDICE C – LISTA E CARATERIZAÇÃO DOS ENTREVISTADOS

Entrevista				
DATA	MODO	POSTO	NOME	FUNÇÃO
201400ABR23	Presencial	Tenente-General	Paulino Serronha	CEMCCOM/EMGFA
041130MAI23	Presencial	Major-General	Lemos Pires	DGPDN/MDN
181100ABR23	Presencial	Major-General	Vieira Borges	Presidente, Comissão Portuguesa de História Militar
191400ABR23	Telemática	Coronel	Fernandes de Oliveira	-
131730ABR23	Telemática	Coronel	Nascimento Rocha	Chefe do Gabinete da Secretária-Geral do Sistema de Segurança Interna
270900ABR23	Presencial	Tenente-Coronel	Moutinho Fernandes	2ºCmdt Regimento de Comandos

APÊNDICE D – CODIFICAÇÃO ALFANUMÉRICA DAS ENTREVISTAS

Pergunta da Entrevista	Categoria	Subcategoria	Unidade de Registo
1ª Questão: Durante o conflito híbrido da Rússia/Ucrânia, quais foram as modalidades de ação, os domínios e as ferramentas usadas pela Rússia nas funções críticas da Ucrânia de forma a explorarem as respetivas vulnerabilidades e alcançarem os seus objetivos políticos?	Político	Interferência Política	UR 1.1.1
		Operações	UR 1.1.2
		Corrupção	UR 1.1.3
	Militar	Espaço Territorial	UR 1.2.1
		Ciberdefesa	UR 1.2.2
		Exercícios Militares	UR 1.2.3
		Campanhas	UR 1.2.4
		Desinformação	UR 1.2.5
	Económico	Dependência	UR 1.3.1
		Investimento	UR 1.3.2
		Sanções	UR 1.3.3
		Espionagem	UR 1.3.4
	Social	Instabilidade	UR 1.4.1
		Paramilitares	UR 1.4.2
		Corrupção	UR 1.4.3
		Influenciar	UR 1.4.4
	Informacional	Media	UR 1.5.1
		Desinformação	UR 1.5.2
	Infraestrutura	Sabotagens	UR 1.6.1
		Infraestruturas	UR 1.6.2
	Ciber	Ciber ataques	UR 1.7.1
		Espionagem	UR 1.7.2
		Manipulação	UR 1.7.3

2ª Questão: Relativamente à cooperação internacional e no âmbito da inserção de Portugal na NATO e na UE, existe uma partilha informações estratégicas com organismos internacionais relativamente às ameaças híbridas e às suas ferramentas bem como a participação em exercícios internacionais?	Cooperação Internacional	Existe a participação em exercícios internacionais com presença da temática das AH e suas ferramentas	UR 2.1
		Existe partilha de informações com organismos internacionais relativamente às AH e às suas ferramentas	UR 2.2
3ª Questão: Tendo por base as orientações estratégicas da UE e da NATO para o CAH e os pilares em que a mesma se suporta, quais são as principais ameaças e oportunidades para o CAH ao nível das FFAA Portuguesas?	Oportunidades	Cooperação com EU e NATO	UR 3.1
		Exercícios	UR 3.2
		Partilha de conhecimento	UR 3.3
		Desenvolvimento de capacidades	UR 3.4
	Ameaças	Ataques Cibernéticos	UR 3.5
		Instabilidade Política	UR 3.6
		Propaganda	UR 3.7
		Espionagem	UR 3.8
		Ameaças Transacionais	UR 3.9
4ª Questão: Quais as vulnerabilidades e potencialidades no ambiente interno que	Potencialidades	----------	UR 4.1

identifica para Portugal, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH?	Vulnerabilidades	----------	UR 4.2
5ª Questão: De que forma pode a Defesa Nacional e as FFAA adaptar-se temporalmente às AH e combatê-las eficazmente?	Componentes a ter em consideração	Doutrina	UR 5.1
		Organização	UR 5.2
		Treino	UR 5.3
		Material	UR 5.4
		Infraestruturas	UR 5.5

1

APÊNDICE E – ANÁLISE DE CONTEÚDO DAS ENTREVISTAS

1ª Questão: **Durante o conflito híbrido da Rússia/Ucrânia, quais foram as modalidades de ação, os domínios e as ferramentas usadas pela Rússia nas funções críticas da Ucrânia de forma a explorarem as respetivas vulnerabilidades e alcançarem os seus objetivos políticos?**		
Entrevistado	**Unidade de contexto**	**Unidade de Registo**
#1	«A estratégia Híbrida da Rússia foi fazer um ensaio da Crimeia em 2014 e a partir de 2014 foi empregado um conjunto de ações não militares que estão perfeitamente estruturadas naquilo que é um modelo da Guerra não linear de Asimov. A ação de 24 de fevereiro de 2022 foi o culminar da Operação Decisiva Militar, isto porque foi utilizado um conjunto de ações económicas, ações diplomáticas, ações da guerra da informação, ações do domínio militar fez ataques cyber. 22 de fevereiro concentrou forças, fez exercícios, pressão militar, infiltrou forças de Operações Especiais. O Sistema de Informações Ucraniano estava ciente do que a Rússia ia fazer e impediu a tomada do aeroporto que dias mais tarde após ter sido tomado pelo russo, este já se encontrava inoperacional. O grande objetivo da Rússia na Ucrânia na minha interpretação não é conquistar a Ucrânia, é garantir politicamente que a Ucrânia é um estado na área de influência da Rússia "Um estado pró-russo"»	1.1.1; 1.1.2; 1.2.3; 1.3; 1.4.2; 1.7.1; 1.7.2;
#2	«Pese embora não haja um conhecimento extenso e profundo das modalidades, domínios e ferramentas, utilizadas pela Rússia, em sede de ameaças híbridas, contra a Ucrânia, podemos, pelo menos, identificar duas ações concretas: No domínio do ciberespaço, e através de diversas ferramentas e modalidades, verificaram-se diversos incidentes de intromissão, recolha de informação sensível e denegação de serviços básicos e essenciais da Ucrânia, como por exemplo a interrupção do funcionamento da rede elétrica nacional, a recolha de informação sensível de organismo do Estado, dentre outras. Ainda neste domínio, verificou-se uma extensa campanha de desinformação ocorrida nas redes sociais e em alguns órgãos de comunicação social, contra o Governo da Ucrânia e seus dirigentes, assim como de influência da população em prol da causa russa. No domínio da informação, verificou-se uma extensa campanha de desinformação da população russa, tendente a associar a Ucrânia, e os seus dirigentes políticos, à nazificação do país, à perseguição das minorias russófonas presentes em algumas províncias e à perigosidade que a mesma vinha crescentemente a apresentar para a própria segurança da Rússia. Neste mesmo domínio, é ainda de salientar a campanha de desinformação ocorrida em território ucraniano, aumentando a contestação interna das minorias russófonas contra o Governo ucraniano, apelando à sua sublevação, assim como a desacreditação do próprio Governo da Ucrânia e seus dirigentes, dentre outros.»	1.5: 1.5.1; 1.5.2; 1.7; 1.7.1; 1.7.2; 1.7.3;
#3	«As modalidades de ação utilizadas pela Rússia, foram o conjunto de instrumentos de poder que tinha, numa primeira fase instrumento de poder diplomático e informacional, criar uma narrativa que de facto havia um problema na Ucrânia. Atuação abaixo daquilo que é a zona cinzenta, criando essas narrativas, enviando os GreenMans criando indignação nas pessoas. Utilização dos instrumentos de poder Militar, Político e Diplomático, com algumas forças paramilitares também para criar alguma destabilização e aproveitando para ocupar parte do terreno, para tornar ineficazes sistemas de apoios ucranianos acabando por invadir a Ucrânia Os domínios foram praticamente todos, domínio militar com a destruição da capacidade de reação ucraniana, domínio informacional no que diz respeito a narrativas criadas, narrativa das operações psicológicas. Utilização de todos os instrumentos. As ferramentas utilizadas foram das forças militares, forças paramilitares, espionagem, violação de águas territoriais. A questão da Rússia aproveitar a região da grey zone e atuar no limite da legalidade. Operações clandestinas, utilizar das redes das embaixadas espalhadas pelo mundo. Exercícios Militares. Financiamento a grupos militares. Todos os domínios.	1.1.1; 1.2.1; 1.2.3; 1.2.5; 1.4.2; 1.7.1; 1.7.2;

	Objetivos políticos, a Rússia garantir internamente a esfera de influência na própria Federação Russa, aumentar a coesão, ganhar influência no mar Negro»	
#4	«É um tema que ainda está bem compreendido pelas elites dos países ocidentais. O conceito de GH não está ainda definido a nível NATO, nem todos os países concordam e daí a não existir um conceito NATO. O caso da Ucrânia é um caso interessante, pois embora houvesse conflito militar entre forças armadas Ucranianas e milícias do próprio Donbass, não havia uma guerra convencional entre a Ucrânia e a Rússia, no entanto era aceite que havia uma guerra híbrida por parte da Rússia contra a Ucrânia. Se a GH não levar ao emprego ao emprego da componente militar não pode haver uma resposta militar do adversário. A falta de definição de conceito leva a que juridicamente não possa ser possível acusar um país de GH mesmo que esta exista. A Rússia inseriu a sua estratégia baseada em vários fatores, com principal destaque nas Operações de Informação. Que tem como objetivo contruir desinformação utilizando os sistemas que tem à disposição como os media, redes sociais, internet, etc. Explorou e continua a explorar as vertentes da informação, Information Warfare. Criando a Political Warfare, isto é, a utilização dos sistemas de informação com o objetivo de "mexer" politicamente em outros países, de maneira ter influência e causar determinadas decisões. A componente Cyber potenciou a componente comunicacional. Ainda a Rússia utiliza os ciberataques em prol dos seus objetivos políticos. A Ucrânia é o expoente máximo de GH porque aqui estão a ser usados todos os tipos de instrumentos. Vive-se na Ucrânia aquilo que é o conceito de GH total, completo com todos os vetores e mecanismo, influenciadores de população, mudanças de poder, divisões de território. Modalidades de ação, todos os possíveis com principal destaque na Information Warfare e Political Warfare. Os meios convencionais não chegam para atingir os objetivos políticos.»	1.5; 1.5.1; 1.5.2; 1.7; 1.7.1; 1.7.2; 1.7.3;
#5	«Utilização de vários instrumentos de coação, que não só exclusivamente o militar para atingir os objetivos políticos. Em 2014 começou-se a perceber que entraram várias componentes, a componente Ciber, a componente Política, a componente de desinformação. De tal maneira que parece que convenceu o mundo de que a Crimeia era mesmo russa. Este conflito tem uma dimensão Híbrida numa fase inicial e depois transforma-se numa guerra convencional. Mais do que um conflito híbrido, a Rússia acusa o próprio ocidente de GH Há duas dimensões desta guerra, a dimensão no teatro de Operações inicialmente com um conjunto de ações para atingir aqueles 3 grandes objetivos, Desnazificar, desmilitarizar e libertar do Donbass. Usaram a desinformação, sanções económicas, ações psicológicas, ataques ciber As ferramentas usadas foram a política, económica, ciber, desinformação, não temos a noção de todas Guerra Multi-dominio, todos os domínios foram utilizados nesta guerra, Ar terra, ciber, espaço Ambos os lados da guerra usaram estes domínios Não atingiram os objetivos políticos, na prática tem o Dondass conquistado a Crimeia e 4 repúblicas, este poderão servir na liberdade de ação para negociar A Rússia, tem objetivos políticos muito genéricos pode dizer sempre que conseguiu os objetivos políticos, Desmilitarizar – com a destruição do Batalhão AZOV»	1.3.3; 1.4.2; 1.5.2; 1.7; 1.7.1; 1.7.2; 1.7.3;
#6	«Relativamente à guerra entre a Rússia e a Ucrânia, as coisas não ficam apenas entre estes dois países, ficam numa campanha de Desinformação e Informação que afetam a nível mundial. Aquilo que a Rússia consegue fazer através da GH está a fazê-lo exatamente em todo o mundo e ao fazer em todo o mundo ganha vantagens para o seu esforço de guerra direto na Ucrânia e mas não só. Muita da ação militar que está a ser feita na Ucrânia tem muito a ver com aquilo que está a ser feito em África. E é a partir daí que através do que a Rússia faz em África consegue ir buscar meios, complementos e estratégias que permitem alimentar o esforço de guerra contra a Ucrânia. E, portanto, não há dúvida que relativamente ao uso da guerra híbrida, que neste momento tem sido feita pelo estado e pelas empresas militares privadas e por várias atividades, nomeadamente ciber mas não só tem um objetivo que é muito para além das fronteiras da Ucrânia.»	1.4.2; 1.5.2; 1.7; 1.7.1; 1.7.2; 1.7.3;

2ª Questão: **Relativamente à cooperação internacional e no âmbito da inserção de Portugal na NATO e na UE, existe uma partilha de informações estratégicas com organismos internacionais relativamente às ameaças híbridas e às suas ferramentas bem como a participação em exercícios internacionais?**		
Entrevistado	**Unidade de contexto**	**Unidade de Registo**
#1	«Portugal participa num conjunto de organizações e tem partilha do sistema de informações quer no SIRP quer na área das informações militares na SigMil, no entanto é uma partilha de informações genérica. Não destaca se a ameaça é de natureza híbrida ou não. Esta partilha existe, bem como um conjunto de exercícios para testar, desenvolver e certificar forças, no entanto não são especificamente face a AH. Pois a AH não tem um conceito oficializado pela NATO. A essência da conflitualidade Híbrida é que tudo pode ser utilizado, desde a compra de empresas, criação de intercomplexidade e dependência energética, tudo pode ser incluído dentro da complexidade híbrida. Porque o grande objetivo da GH é um objetivo político, do controlo de um determinado estado.»	2.1; 2.2;
#2	«Em sede da NATO Portugal coopera com a própria organização e com os Estados Membros em sede do estudo, preparação, prevenção, sinalização, mitigação, combate e recuperação, no que concerne às ameaças híbridas, designadamente à adoção de metodologias e ferramentas, à partilha de informação estratégica e na participação em exercícios internacionais. Em sede da União Europeia, Portugal integra o Grupo de Trabalho Horizontal sobre o Reforço da Resiliência e o Combate às Ameaças Híbridas (HWP ERCHT), participa na Célula de Fusão Híbrida do Centro de Inteligência e de Situação da União Europeia (EU INTCEN), assim como nos Grupos de Trabalho onde são desenvolvidas as temáticas da Resiliência de Entidades Críticas, da Cibersegurança e da Informação, instância onde se procede ao intercâmbio de informação estratégica, onde se definem abordagens comuns e harmonizadas e em sede das quais se realizam exercícios. Paralelamente, e ainda a nível europeu, Portugal tem uma participação efetiva e ativa no Centro Europeu de Excelência para Combate às Ameaças Híbridas (Hybrid CoE), onde se estudam as tendências e inovações, assim como análises e estudos, a par de formação, com relevância para o combate às ameaças híbridas.»	2.1; 2.2;
#3	«Existe uma cooperação, nomeadamente entre EU e NATO. A criação nível NATO das *"Readiness Action Plan, Assurance Measures e Adaptation Measures"*. Foi criado uma serie de NATO Response Forces para responder a este tipo de ameaças e contrabalançar esta influência russa. Criaram células de estudo da GH, para perceber como funcionam e como se combatem. Rede de segurança para incrementar a capacidade, oportunidades e influencias através do aumento das parcerias e interação entre parceiros, alertaram da necessidade da criação de resiliência, que deve ser criada primeiro em cada país e depois uma resiliência partilhada.	2.1; 2.2;

	Criação de uma consciência de que os países tinham que desenvolver os seus instrumentos de poder, criar condições para fazer face a este tipo de ameaça, consciência institucional em termos da população, organizações e instituições para que pudessem estar alertadas para isto e para que dessem uma resposta comum e partilhada. Criação da narrativa da aliança, a comunicação estratégia. Existe a partilha de informação, mas depois não existe uma compreensão e atuação imediata. A partilha ocorre, mas depende da vontade dos países, ou seja, um país pode ter informações estratégicas e só o partilha se assim o entender. Participação em exercícios Internacionais existem, mas essa participação acaba por ser diminuta, CSMIE e SIG Mil fazem o acompanhamento destas informações bem como a sua partilha. O que se verifica é o atraso da partilha de informação. *"EU INTCEN Hybrid Fusion Cell"* referente as AH»	
#4	«Tanto a NATO como a UE têm feito algum caminho nesta área, há doutrina há artigos escritos. Mas há sempre uma postura reativa. Está tipificado o problema e sabem quais são os vetores e instrumentos que as AH usam, está identificado um conceito de modo as lhes fazer face, mas depois na prática surge o problema. As organizações ocidentais têm mostrado muitas vulnerabilidades às AH. Nesta luta global o que está aqui são ideologia e modelos de organizações políticas diferenciados em jogo. A questão aqui é a possibilidade de alterar um sistema político que seja autoritário que ponha no poder pessoal de natureza autoritária que estará mais recetivo a países como a Rússia. Há de facto um desenvolvimento no ponto de vista do estudo, mas este estudo e estas conclusões tomadas pelas organizações responsáveis não estão a dotar suficientemente os países para o efeito. Ações na prática não estão suficientemente capazes para fazer face a AH»	2.1; 2.2;
#5	«Há uns anos atras foi criado na Finlândia um centro de comando para fazer face às AH A entrada da Finlândia na NATO, promoveu este combate Hybrid CoE Houve trabalho em diplomas para orientações Gerais para GH, a nível da NATO não houve so orientações houve também ações concretas relativamente ao aproximar de forças para junto de países fronteiriços com a Rússia A doutrina mais operacional multi-dominio foi trabalhada.»	2.1; 2.2;
#6	«Portugal como outros países fazem parte de várias organizações, não so da NATO e da EU mas mesmo com outras multilaterais em que os princípios de transferência de informação estão consignados. Existe o centro de excelência de Ameaças Híbridas que esta em Helsínquia, onde Portugal participa. Temos obviamente várias plataformas multinacionais onde nós participamos e há transferência de informação. A resposta à Ameaça Híbrida é o princípio consignado na defesa de todos os estados da UE de todos os estados da NATO que neste momento tem múltiplas plataformas e formas de combinar estratégias e de fazerem doutrina comum. Para se fazer face a estas ameaças existe o próprio conceito do multi-domínio, que já é doutrina da NATO, que permite responder a isso. Portanto a partilha de saberes e a presença de observadores portugueses em Helsínquia, verifica-se e é feita.»	2.1; 2.2;

3ª Questão: **Tendo por base as orientações estratégicas da UE e da NATO para o CAH e os pilares em que a mesma se suporta, quais são as principais ameaças e oportunidades para o CAH ao nível das FFAA Portuguesas?**		
Entrevistado	**Unidade de contexto**	**Unidade de Registo**
#1	«A NATO e a UE não tem uma estratégia de CAH, o que há é uma chamada de atenção para que há uma conflitualidade híbrida para o que é necessário criar a Resiliência Nacional face às AH. Um conjunto de países estão a construir um conceito, que é um conceito da Resiliência Nacional que envolve a defesa em todos os setores do estado, As oportunidades e as ameaças quando olhamos para FFAA, o que teríamos de fazer era um exercício comparativo entre aquilo que são as ameaças e como funcionam os vetores das AH face aquilo que são as capacidades das FFAA, especialmente quando falamos na parte do vetor militar. Em termos genéricos onde é necessário ter forças armadas para fazer face as AH têm a ver com domínios novos, ou seja, a ameaça Cyber. Esta é critica, as FFAA têm que continuar a desenvolver o domínio cyber na perspetiva da defesa contra Ataques Cyber, temos que desenvolver a capacidade de resiliência face a ameaças Cyber e como é que nós recuperamos face a esta ameaça. Naquilo que são os domínios da capacidade terrestre e da capacidade naval, temos que ter capacidade dissuasão para impedir que haja um determinado tipo de operações no domínio militar que nos provoquem uma ameaças definitiva. Isto significa haver uma ação cinética sobre a nossa soberania. O que é necessário termos é o domínio cyber e nos outros domínios é a capacidade de defesa mínima, capacidade de dissuasão e capacidade de resistir o tempo necessário para que possamos inovar o artº5 e as potencias aliados nos poderem ajudar.»	3.1; 3.2; 3.4; 3.9;
#2	«As principais ameaças decorrem da nossa participação em ambas as organizações, não sendo de descurar a relevância que a posição geoestratégica de Portugal possa ter algum interesse em particular para qualquer outro Estado. Assim, as grandes fontes de ameaça provêm dos Estados que, de alguma forma, se opõem à NATO e à União Europeia, e que, através do nosso País, possam aceder a informação sensível e relevante, colocar em causa a coesão e funcionamento de ambas as instituições ou ter um acesso privilegiado a estas organizações através de Portugal. As principais ameaças prendem-se com as vulnerabilidades de cibersegurança sentidas pelas Forças Armadas – designadamente a segurança da informação e a inutilização de capacidades de comando, coordenação, controlo e informação -, assim como da deficiente resiliência de algumas empresas relevantes para as indústrias de defesa, assim como da permeabilidade a campanhas de desinformação. Já no que tange a oportunidades, a participação das Forças Armadas em sede da NATO, da União Europeia, e até do Hybrid CoE, permitem a adoção de uma doutrina comum e harmonizada, da adoção de mecanismos e ferramentas de deteção, prevenção , combate e resiliência, uniformes e mais avançados, de uma atuação em rede e reforçada por uma ação comum, de formação e treino num cenário	3.1; 3.3; 3.4; 3.5; 3.8; 3.9;

	internacional e europeu, e de fundos financeiros para a implementação, manutenção e desenvolvimento de ferramentas específicas de combate às ameaças híbridas.»	
#3	«As principais ameaças que consideraria, em termos das FFAA, as operações físicas contra infraestruturas militares, exploram dependências, espionagem, espionagem industrial Ciber espionagem. Violação do espaço a aéreo e de águas territoriais. Elementos desestabilizadores dentro das organizações. Aliciamento de militares para fazer espionagem. Atuação de organizações paramilitares. Criação de narrativas contraditórias nos media e nas redes sociais, que mesmo não sendo diretamente contra as FFAA acabam por ter uma ele influencia. Em termos de oportunidades, não sendo em concreto das FFAA, seria a criação de estratégias nacionais daquilo que que é o contributo de cada um dos organismos dos instrumentos de poder para o combate a estas ameaças. Criar aquilo que é o entendimento destas ameaças e aquilo que é no fundo conceito para combater estas ameaças com uma estratégia não só instrumento militar, mas também das redes de instrumentos poder. Outra oportunidade será também esta questão da Cyber espionagem da parte da ciberdefesa penso que aqui também temos a oportunidade de desenvolver esta área, já demos um salto grande mas penso que nos falta ainda muito mais, também considero que seja uma oportunidade para nos desenvolvermos também aquilo que é a nossa capacidade para o combate a estas ameaças cibernéticas.»	3.3; 3.4; 3.5; 3.6; 3.8; 3.9;
#4	«Fruto da nossa geografia estamos pouco habituados a este tipo de guerras, o que dá a entender que não nos acontece nada. No entanto nós já estamos a ser afetados por instrumentos da GH fruto da nossa inserção no espaço político. Falta doutrina portuguesa, mesmo no que diz respeito à Cyber Segurança ainda estamos frágeis até pela capacidade que não está instalada. Temos ameaças que resultam da falta de organização contra instrumento não cinéticos. Os instrumentos das FFAA não passam das operações de informação e Cyber e mesmo este não estão desenvolvidos o suficiente.»	3.8; 3.9;
#5	«As FFAA fazendo parte da NATO, tendo de momento forças na Roménia Ameaças no âmbito da Organização Internacional, neste âmbito nós temos feito face no território nacional em termos de vigilância, como no recente caso de navios russos em águas nacionais, podendo detetar comunicações bem como no espaço aéreo nacional, em termos de operações estamos a fazer esse trabalho na Roménia e no Báltico As Oportunidades tem sido feita ações em termos de formação, mas sobretudo de preparação de exercícios. Dentro das academias militares numa perspetiva doutrinaria a pouco e pouco desde 2014. Bem como no IUM, tem sido feito eventos, congressos seminários neste âmbito da GH e do multi-domínio. Temos visto as dificuldades da Rússia em Donbass, em que numa primeira fase, falhou completamente a operação Multi-domonio, falta de coordenação. Numa perspetiva de haver forças armadas do país que combatem no multi-dominio, no sentido em que há vários instrumentos e por outro lado forças regulares.»	3.1; 3.3; 3.6; 3,9;

#6	As FFAA portuguesas são apenas um pilar da ação do Estado e as Ameaças Híbridas combatem-se numa base de *"whole of government approach"*. Portanto para combater eficazmente estas ameaças tem que haver uma ação consertada dos envolventes do estado e as FFAA participam nesse esforço. Vai muito para alem do que são as ações das FFAA. Porque para combater as ameaças é preciso de ter noção da *"multi-domain operations"* , tens terra, mar, ar, espaço e ciberespaço existe também dois domínios complementares que é o espaço eletromagnético e o domínio cognitivo. Neste momento nós já temos uma arquitetura multi-dominio e estamos a trabalhar no CEDN.	3.3; 3.4;

4ª Questão: **Quais as vulnerabilidades e potencialidades no ambiente interno que identifica para Portugal, suscetíveis de integrar uma abordagem estratégica nacional de combate à AH?**		
Entrevistado	**Unidade de contexto**	**Unidade de Registo**
#1	«As democracias por natureza são mais suscetíveis de serem ameaçadas de forma híbrida pois são mais abertas às ações não militares, no nosso caso vivemos numa sociedade e numa economia muito aberta, somos mais suscetíveis a manipulações ações por via económica, ações por via de manobras informacionais utilizando os meios de comunicação social, vias diplomáticas, etc. Em termo genérico esta é a grande ameaça que não tem a haver só com Portugal, mas sim com as democracias em geral. Em termos militares a vulnerabilidades tem a ver com o facto de sermos um estado muito suscetível a uma ação decisiva por parte de uma potência muito maior e nós não temos capacidade de defesa autónoma. Por isso a nossa grande potência nesta área é estramos dentro de uma aliança. Temos que ter alguma capacidade autónoma, mas depois temos que nos fazer valer de estarmos na UE e NATO e podermos invocar as clausulas da defesa coletiva e de apoio mútuo»	4.1; 4.2;
#2	«Atenta a fragilidade de alguns sectores nacionais e as imensas vulnerabilidades que o País apresenta, nas mais diversas áreas e sectores, os vetores de ameaça tradicionais das ameaças híbridas colocam Portugal numa situação bastante crítica, porquanto, somos um País muito permeável ao investimento estrangeiro de origem desconhecida – veja-se a política de vistos "*gold"* e a tomada de participação estrangeira em empresas críticas -, os nossos níveis de cibersegurança são reduzidos, quer ao nível da Administração do Estado, quer ao nível das empresas – veja-se a quantidade e consequências dos mais recentes ataques informáticos -, a resiliência das nossas entidades críticas é relativamente baixa – conforme se verificou com os recentes ataques informáticos à empresa Vodafone, Continente, Germano de Sousa, etc. -, e a literacia informacional da população portuguesa é baixa, o que permite a sua manipulação através de ações de desinformação cometidas através de redes sociais ou de meios de comunicação social específicos – na realidade não temos por hábito verificar a autenticidade das fontes e a veracidade das notícias -.	4.1; 4.2;

	No entanto, a nossa boa capacidade de adaptação a novas realidades e a nossa participação ativa em diferentes organizações, instituições e organismos, internacionais e europeus, podem ser oportunidades e vantagens a considerar numa abordagem estratégica nacional de combate às ameaças híbridas.»	
#3	«As vulnerabilidades são entendidas como os pontos negativos, as desvantagens nacionais relativamente a outros países, os principais erros já cometidos e o que foi reconhecido como erro. No domínio político, ausência pela política, falta de uma cultura política. A corrupção da esfera política. Ausência de estratégia dissuasora. E a localização periférica em relação à europa. Instrumento económico a dependência de cadeias de abastecimento exterior, a pouca diversidade cadeias de abastecimento de bens de serviços essenciais, a dependência de capital direto estrangeiro, fraco tecido empresarial, a dificuldade em impor instrumentos de política económica, a resiliência da economia a corrupção económica a dependência tecnológica, etc. Triagem de investimento estrangeiro direto Em termos militares e defesa, são recursos limitados de resposta a emergências ou gestão de crises. A coordenação efetiva entre as autoridades militares e civis, a questão das capacidades militares e defesa que são limitadas, as nossas capacidades militares. A questão da integração efetiva nos mecanismos de resposta às crises da União Europeia e da NATO, a participação no quadro das iniciativas, a questão de desenvolver a sua capacidade de comando e controlo C4ISR, capacidade de comando e controlo terrestre, capacidade de estar associado a logística da força no ramos, a proteção e sobrevivência, engenharia de combate, capacidade cibernético. A União Europeia desenvolveu uma série de respostas, de células de resposta na NATO, na União Europeia criou uma série de mecanismos, criou a questão dos centros de defesa cibernética, criou um centro de combate às AH, criou uma série de outras agências e células para tentar combater isto e desenvolver doutrina e criar mecanismos e resiliência tudo isso a nossa participação nessas células a nossa colocação lado pessoal a participação exercício estudo acaba por ser muito diminuta e muito limitada Depois do fraco desenvolvimento dos projetos onde Portugal participa relacionados com as prioridades de desenvolvimento de capacidades hoje é "*opinion capability development"*. Papel das forças especiais eu penso que continuamos em Portugal a ter um papel reduzido em termos daquilo que é as forças especiais com meios limitados com papel desvalorizado forças especiais»	4.1; 4.2;
#4	«A AH é aquela que explora melhor os países onde há uma separação entre a segurança interna e a segurança externa. Países que tenham um conceito de segurança integral alargado existe maior disponibilidade de coordenar esforços. Existe uma separação em que as ameaças internas são apenas da responsabilidade das forças de segurança e as ameaças externas das FFAA ao contrário do que seria ideal como uma cooperação em ambos os lados. Tem que haver sinergia e atuação conjunta. A pouca compreensão do problema ao nível político e militar. Não existe um foco por parte do estado relativamente a GH, não há exercícios militares neste âmbito. Falta de capacidade para a guerra de informação. Potencialidades, a capacidade do "desenrascar" como atitude, o que não é de facto o ideal.	4.1; 4.2;

	Justifica-se haver uma estratégia nacional contra as AH, como prevenção.»	
#5	«Há vulnerabilidades decorrentes deste tipo de ameaças, dado que elas implicam atuam integrada de todas as potencialidades do Estado. E isto nem sempre acontece, porque em tempo de paz precisamos de trabalhar um conselho de segurança nacional em vez de trabalhar a segurança Interna a nível do 1ºMinistro. Já foi apresentada uma proposta. Sentimos essa necessidade com as AH de trabalharmos em conjunto uma serie de atores das áreas económicas, política externa, áreas da Administração Interna, área da defesa, todos a trabalhar em conjunto para fazer face a essas ameaças. Aquilo que é a legislação portuguesa muito circunscrita à separação entre "Defesa" e "Segurança" não esta adaptada a este tipo de Ameaças, quer em termos de identificação quer em termos de combate. As Potencialidades é que os nichos de operação estão a ser trabalhados, a parte da ciberdefesa, a parte da defesa em exercícios. Constitui Potencialidade no sentido em que se criou a lei de Segurança Interna Portuguesa para efeitos de Ameaças Transnacionais que no fundo cruza a segurança com a defesa. Preparou-nos para esta situação Ou seja, haver um secretariado que trabalhe em coordenação com o Chefe de Estado-Maior General. A abordagem estratégica vem em termos conceptuais nos conceitos estratégicos, não para criar uma estratégia nacional de GH. Deviam ser criados estruturalmente órgãos como um Conselho de Segurança Nacional. Com a participação de todos os atores nacionais. Numa ação integrada. Segunda ação era a criação de um Centro de Gestão de Crises. Dois órgãos que resolveriam esta situação, haver uma estratégia especifica.»	4.1; 4.2;
#6	«Portugal não está diferente dos restantes estados europeus nessa àrea. Nós ainda não temos uma arquitetura de desenho de sistema de crise de resiliência nacional que nos permita responder a uma só voz sobre todas as ameaças. O facto de sermos uma democracia resiliente é uma vantagem, mas é também uma vulnerabilidade na medida em que mós não temos um "big brother" para olhar por todos nós para garantir que não há interferências, ingerência, liberdade de pensamento, liberdade de expressão, etc. Coloca obviamente riscos a que isto seja utilizado por atores maliciosos, nomeadamente na manipulação de informação consegue atingir certos objetivos. Do estado português como qualquer democracia ocidental são estados que são mais vulneráveis à agência externa. Mas por outro lado o estado português tem a sua educação, o seu sistema político sustenta-se em valores e princípios fortes permitindo à população como um todo ser mais resiliente. Os nossos sistemas são facilmente atacáveis porque se baseiam em sistemas abertos, mas a resiliência do nosso sistema educativo e a forma da nossa democracia madura em termos de princípios e valores permite-nos defender melhor.»	4.1; 4.2;

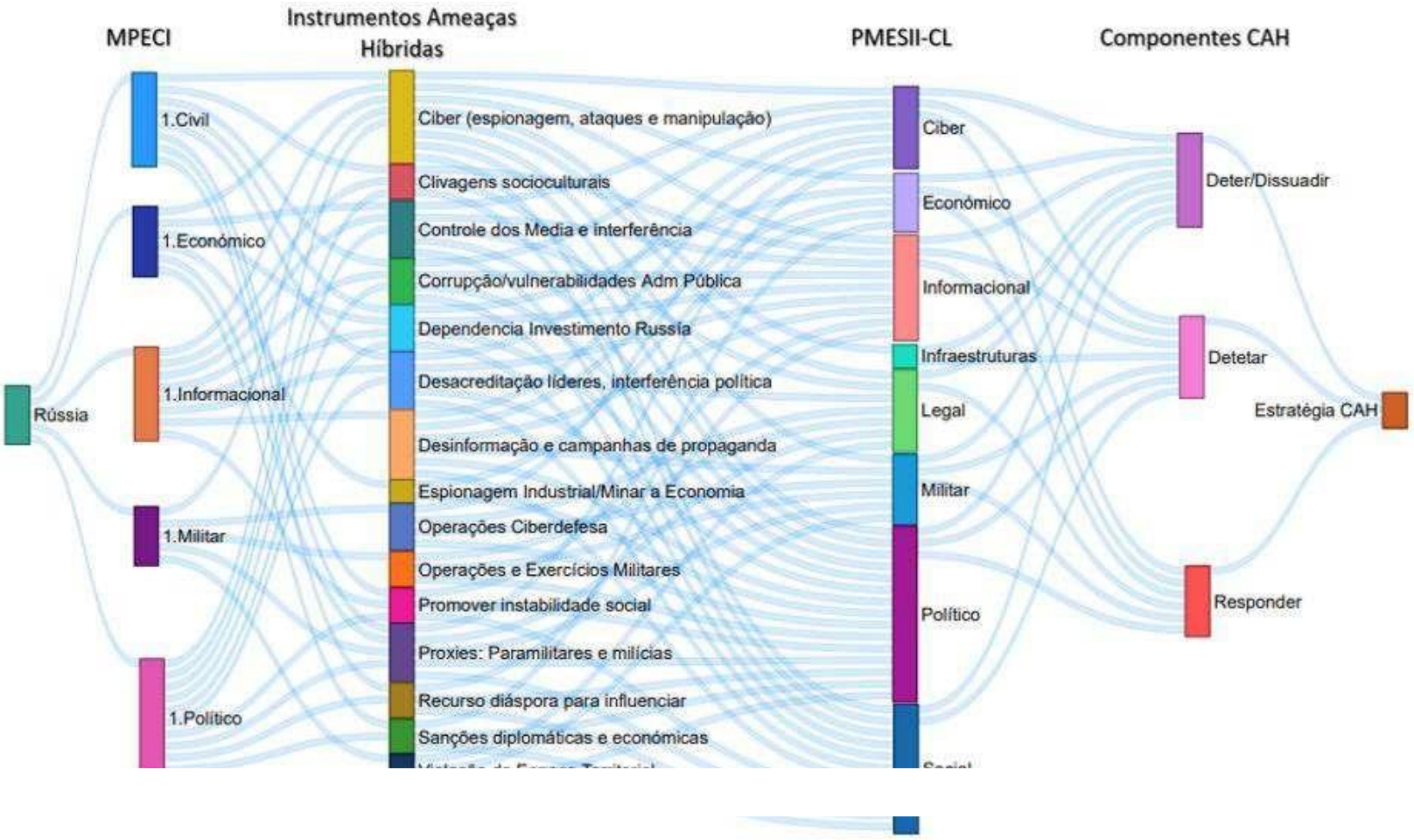
5ª Questão: **De que forma pode a Defesa Nacional e as FFAA adaptar-se temporalmente às AH e combatê-las eficazmente?**		
Entrevistado	**Unidade de contexto**	**Unidade de Registo**
#1	«A melhor forma de um estado como Portugal se adaptar e se defender contra AH é criar um sistema integrado, olhar para a Defesa Nacional como um todo e portanto criar mecanismos de proteção e resiliência em áreas não militares, desenvolver sistemas de informações que nos permitam detetar um conjunto de ameaças e depois em termos militares termos capacidade autónoma ate um determinado nível que nos permita aguentar as primeiras ações cinéticas até ser invocado o artº5 e depois termos o apoio dos nossos estados aliados. No Conceito Estratégico de Defesa Nacional está a ser equacionado a educação em termos da cidadania para os riscos do novo conjunto de ameaças, isto é, as ameaças híbridas por definição podem atacar em todos os setores do estado, não podemos olhar para isto exclusivamente como um problema militar. E termos militares temos que ter uma capacidade cyber com alguma robustez e em termos de Ciber Segurança, não tendo esta a haver com a parte militar, temos que ter uma componente muito forte. Isto porque em termos de ciber Segurança, aquilo que é atacado são as empresas de energia as empresas de transporte, as barragens, os sistemas de controle das autoestradas, os bancos, etc. Em termos militares podemos incrementar medidas tais como o conhecimento, recolha de informações, etc. Desde o início de qualquer formação, no decorrer da carreira é sempre importante aplicar este conhecimento. O problema da GH vai muito além da componente militar. A componente militar na GH só se materializa quando estão criadas as condições para que o instrumento militar tenha o efeito decisivo.»	5.1; 5.2; 5.3; 5.4; 5.5;
#2	«As ameaças híbridas, como o próprio nome indica, situam-se abaixo do limiar do conflito militar, mas dentro da área da segurança dos Estados, sendo, por isso, de grande dificuldade determinar os seus agentes, os meios e ferramentas empregues, assim como a finalidade dos seus objetivos. Daqui resulta a enorme dificuldade de situar algumas destas ameaças no campo da defesa nacional ou no campo da segurança interna, patamares que a nossa carta constitucional coloca em patamares diferenciados. De certa forma, e de acordo com a Lei da Defesa Nacional, caberão na área da defesa nacional qualquer agressão ou ameaça externa que se dirija contra a soberania do Estado, a independência nacional e a integridade territorial de Portugal, bem como contra a liberdade e a segurança das populações ou a proteção dos valores fundamentais da ordem constitucional. Por outro lado, verifica-se uma grande diversidade de vetores de ameaça que podem ser entendidos como ameaças híbridas, assim como uma evolução constante e profunda desses mesmo vetores, o que dificulta a sua deteção e consequente resposta.	5.1; 5.2; 5.3; 5.4; 5.5;

	Assim, a adaptação legislativa, sempre mais lenta e desfasada no tempo, e a adaptação da prevenção, deteção, contenção, resposta e recuperação, por parte das Forças Armadas, não se afiguram como tarefas fáceis de realizar. Especialmente no que concerne às Forças Armadas, a sua permeabilidade a ciberataques e a dificuldade no levantamento e sustentação de capacidades de ciberdefesa, assim como de ciberataque, são por demais evidentes. No combate às ameaças híbridas dirigidas à defesa nacional, a intervenção eficaz das Forças Armadas passará por um forte investimento de recursos materiais, financeiros, tecnológicos e humanos, no levantamento e sustentação de capacidades efetivas de ciberdefesa e de ciberataque, na cooperação e colaboração com entidades públicas e privadas, nacionais e estrangeiras, como sejam o Centro Nacional de Cibersegurança, o *Hybrid CoE* e as grandes empresas tecnológicas, a par de organizações internacionais, como seja a NATO.»	
#3	«Penso que a principal coisa a fazer seria no fundo aquilo que eu disse que era o desenvolvimento de uma estratégia nacional de combate às AH e que pudesse ser traduzida das organizações da NATO e da União Europeia e depois pudesse através de nossos instrumentos de poder consolidada. Em termos daquilo que é a defesa nacional mais especificamente das FFAA, dessa origem também uma estratégia do conceito estratégico militar das FFAA que pudesse dar resposta, ir de encontro à estratégia nacional de combate a estas AH e o que é que cada um dos instrumentos de poder tinha que fazer propriamente A maneira seria essa, em primeiro de facto "nós arrumarmos a casa" em termos autoritários daquilo que é a estratégia nacional para combate a estas ameaças e depois começar por pequenas coisas, seria por exemplo criar já ao nível do MDN ou do EMGFA também uma célula de resposta que pudesse ir de encontro aquilo que a NATO e a União Europeia fizeram. Estes criaram uma sala resposta específica que se pudesse estar orientada mais para esta questão do combate às AH e que funcionasse obviamente em paralelo Portugal teria mesmo a própria defesa nacional, teria de criar esta consciência situacional, esta consciência de combate às ameaças híbridas e no fundo também ter uma estratégia em termos das FFAA para de facto intensificar esta cooperação Internacional Tomada de medidas a todos os níveis hierárquicos, em todos os ramos de modo que estes estejam sensibilizados Ao nível por exemplo mesmo da cooperação civil e militar nacional ainda há muita coisa a fazer a questão dos programas de treino exercícios militares, a questão da informação partilhada no âmbito do combate às AH também uma parte podemos desenvolver a estratégia de combate à informação, os tais meios de resposta a situações de catástrofe ou crise.»	5.1; 5.2; 5.3; 5.4; 5.5;
#4	«A estratégia por si só não chega. Tem que se estruturar a resposta. Só nos apercebemos de conflitos híbridos como efetivamente somos atacados. Era ideal ter um mecanismo Intel para as AH. Se queremos defender os nossos interesses temos que rapidamente. Criação de um conceito nacional de gestão de crises. Criação de um centro nacional de gestão de crises.	5.1; 5.2; 5.3; 5.4; 5.5;

	Estratégia estrutural, que cria a organização da resposta Estratégia genética que é a forma de criar essas capacidades Estratégica operacional que é conceber ao nível estratégico o emprego dos meios. A disseminação de uma cultura base do que são AH, e, todos os escalões, em todas as categorias. *Situation Awareness»*	
#5	«A maneira de o fazer a nível das FFAA, educação e formação e treino. Serem incluídos temas de maneira que os militares tenham a noção de que a guerra não se faz só no Teatro de Operações. A guerra é muito mais do que aquilo que é o combate na guerra convencional. A melhor maneira de as combater é educação. Formação e treino. Implica exercícios a vários níveis. Adaptar a mentalidade dos militares. Do mesmo modo que foi trabalhada Guerra contra o Terrorismo, a guerra subversiva em África. Criação de um manual, Doutrina, de CAH. Retificar documentos NATO Na perspetiva conceptual, Dr. António Horta Fernandes na revista Nação e Defesa, há gente clausewitziana que recusa a aceitar que a GH é algo novo. Olhamos para a história e encontramos GH em conflitos passados, como na guerra subversiva. Os conceitos aparecem consoante em função do aparecimento, de novas realidades, equipamentos, capacidades. Temos o exemplo da Finlândia que já possuem doutrina e dão formação aos seus militares neste contexto»	5.1; 5.2; 5.3; 5.4; 5.5;

ANEXOS

ANEXO A – ATIVIDADE HÍBRIDA DA RÚSSIA NA UCRÂNIA



Atividade Híbrida da Rússia na Ucrânia