**INSTITUTO UNIVERSITÁRIO MILITAR**

**DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS**

**CURSO DE PROMOÇÃO A OFICIAL GENERAL**

**2019/2020**

**TRABALHO DE INVESTIGAÇÃO INDIVIDUAL**

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

**O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.**

**Artur José Figueiredo Mariano Alves**

**Capitão-de-mar-e-guerra**


**INSTITUTO UNIVERSITÁRIO MILITAR**

**DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS**

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

**CMG FZ Artur José Figueiredo Mariano Alves**

Trabalho de Investigação Individual do CPOG 2019/2020

Pedrouços 2020


**INSTITUTO UNIVERSITÁRIO MILITAR**
**DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS**

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

**CMG FZ Artur José Figueiredo Mariano Alves**

Trabalho de Investigação Individual do CPOG 2019/2020

Orientador: COR TIR ART António José Pardal dos Santos

Pedrouços 2020

**Declaração de compromisso Antiplágio**

Eu, **Artur José Figueiredo Mariano Alves**, declaro por minha honra que o documento intitulado "**A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas**", corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial General 2019/2020** no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, **9** de **junho** de **2020**

Assinado por : **ARTUR JOSÉ FIGUEIREDO MARIANO ALVES**
Num. de Identificação: BI074072048

Artur José Figueiredo Mariano Alves

Capitão-de-mar-e-guerra

**Agradecimentos**

Em primeiro lugar, o reconhecimento e agradecimento ao Coronel Tirocinado António José Pardal dos Santos, meu orientador, pelo avisado aconselhamento e apoio incondicional que sempre manifestou de forma amiga e profissional na orientação deste trabalho. O seu rigor académico, conhecimento sustentado e elevado espírito de compromisso, cedo me fizeram sentir que podia contar com um timoneiro exigente, mas sempre disponível para chegar a bom porto. Conhecê-lo, foi, sem dúvida, uma das experiências mais gratificantes, e profícuas deste desafio.

À minha mulher pela imprescindível compreensão e incondicional apoio e aos meus filhos, sobretudo ao mais novo, que desde cedo teve de conviver com um pai que sempre quis estar presente, com alguns hiatos, não só pela exigência do curso, mas também pelo período de confinamento a que a COVID-19 obrigou.

A todos os entrevistados, militares e civis, que, pela total disponibilidade, experiência e conhecimentos, muito contribuíram para esta investigação. Agradeço, o profissionalismo, dedicação e, acima de tudo, a amizade com que me agraciaram, o que jamais esquecerei.

Aos camaradas auditores do Curso de Promoção a Oficial General 2019/2020, pela camaradagem insigne, colaboração, partilha de experiências e perspetivas diversas, que permitiram, com tão vasto manancial, enriquecer, clarificar e unir ideias, contribuindo para uma aprendizagem, ainda mais profícua e enriquecedora, e para uma amizade, que perdurará para sempre.

À minha querida Mãe, por tudo!

# Índice

## Apêndices



## Figuras

## Tabelas



## Quadros

**Resumo**

Nos últimos anos, com a contenção das guerras interestatais convencionais, a emergência de novas ameaças transnacionais e a informatização da vida moderna têm conduzido a sociedade a um diferente paradigma civilizacional, onde as ameaças híbridas surgem como um dos principais desafios securitários e militares, que exige uma resposta cooperativa e integrada de toda a sociedade.

Neste contexto, o objetivo desta investigação consiste em propor linhas de ação para o combate às ameaças híbridas, ao nível das Forças Armadas Portuguesas e encontra-se alicerçado em três objetivos específicos, que passam por analisar: o papel do Instrumento de Poder Militar; as linhas de orientação Estratégicas da União Europeia e da Organização do Tratado do Atlântico Norte; e as capacidades das Forças Armadas para o combate às ameaças híbridas.

Adotou-se uma investigação baseada num raciocínio indutivo, apoiada numa estratégia de investigação qualitativa e num desenho de pesquisa de estudo de caso. Como técnicas de recolha de dados, recorreu-se à análise documental e a entrevistas semiestruturadas.

Como principais resultados, releva-se a proposta de doze linhas de ação que visam constituir-se como os elementos orientadores para o processo de alinhamento de uma estratégia futura, e um contributo para a clareza conceptual e compreensão das ameaças híbridas.

**Palavras-chave:**

Guerra Híbrida, Ameaça Híbrida, Combate às Ameaças Híbridas.

***Abstract***

*Over the past years, the containment of interstate conventional wars, the emergence of transnational threats, the interconnectivity and computerization of modern life have led to a civilizational paradigm shift where the hybrid threats have emerged as one of the main security and military challenges, which requires a cooperative and integrated response from the whole society.*

*In this context, the aim of this research, is to propose courses of action to counter hybrid threats, at the level of the Portuguese Armed Forces, and it is based on three specific objectives, that go through analyzing; the role of the Military Power, the European Union and the North Atlantic Treaty Organization strategic guidelines, and the capabilities of the Armed Forces to combat hybrid threats.*

*The research, based on inductive reasoning, lays on a qualitative research strategy and a case study design. Data collection techniques include extensive document analysis and semi-structured interviews.*

*The major results are the significant contributions toward the conceptual clarity and the understanding of the hybrid threats, underlining the identification of twelve Courses of Action which are intended to be perceived as guiding elements in the pursue of a future aligned strategy.*

***Keywords:***

*Hybrid War, Hybrid Threats, Counter Hybrid Threats.*

**Lista de abreviaturas, siglas e acrónimos**

| | |
|---|---|
| AH | Ameaças Híbridas |
| AD | Análise Documental |
| AED | Agência Europeia de Defesa |
| AT | Ameaças Transnacionais |
| BI | *Business Intelligence* |
| CAH | Combate às Ameaças Híbridas |
| CEDN | Conceito Estratégico de Defesa Nacional |
| CEM | Conceito Estratégico Militar |
| CDD | Cooperação no Domínio da Defesa |
| CDP | Plano de Desenvolvimento de Capacidades |
| CPDM | Ciclo de Planeamento de Defesa Militar |
| DMPDM | Diretiva Ministerial Planeamento de Defesa Militar |
| CPOG | Curso de Promoção a Oficial-General |
| C4ISR | *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance* |
| EUA | Estados Unidos da América |
| EEIN | Espaço Estratégico de Interesse Nacional |
| FED | Fundo Europeu de Defesa |
| FFAA | Forças Armadas |
| FSS | Forças e Serviço de Segurança |
| GH | Guerra Híbrida |
| Híbrid CoE | The European Centre of Excellence for Countering Hybrid Threats |
| IUM | Instituto Universitário Militar |
| I&D | Investigação e Desenvolvimento |
| LA | Linhas de Ação |
| LOE | Linhas de Orientação Estratégica |
| LPM | Lei de Programação Militar |
| MCDC | Multinational Capability Development Campaign |
| MDN | Ministério da Defesa Nacional |
| MPECI | Militar, Político, Económico Civil e Informacional |
| NATO | North Atlantic Treaty Organization |
| NEP/INV | Normas de Execução Permanente/Investigação |

| | |
|---|---|
| NRBQ | Nuclear, Radiológico, Biológico e Químico |
| OE | Objetivo Específico |
| OG | Objetivo Geral |
| OTAN | Organização do Tratado do Atlântico Norte |
| PA | Potencialidades *vs* Ameaças |
| PO | Potencialidades *vs* Oportunidades |
| PMESII | Político, Militar, Económico, Social, Infraestruturas e Informacional |
| QC | Questão Central |
| QD | Questão Derivada |
| RCM | Resolução do Conselho de Ministros |
| SWOT | *Strengths, Weaknesses, Opportunities e Threats* |
| TFUE | Tratado do Funcionamento da União Europeia |
| TII | Trabalho de Investigação Individual |
| TUE | Tratado da União Europeia |
| UE | União Europeia |
| VA | Vulnerabilidades *vs* Ameaças |
| VO | Vulnerabilidades *vs* Oportunidades |

## 1. Introdução

A globalização desregulada e o sistema internacional em transição, com novos alinhamentos geopolíticos, tende a gerar uma nova ordem mundial e a criar uma crescente instabilidade no ambiente de segurança, propiciando uma maior projeção de novas ameaças, de carácter difuso e transnacional, interdependentes, de múltiplas naturezas, dinâmicas, híbridas, assimétricas e globais, que afetam a segurança dos Estados (Garcia, 2017).

A par destas ameaças, a gama de métodos e atividades empregues por atores estatais e não-estatais, é cada vez mais ampla e de cariz combinada. A desinformação, a exploração das vulnerabilidades de carácter logístico, como a dependência energética e os transportes, a chantagem económica, a pressão diplomática, a deterioração das instituições internacionais, o terrorismo, o crime organizado, ampliadas pela nova dimensão das tecnologias disruptivas e o domínio do Ciberespaço, contribuem para o aumento de forma desmedida da insegurança. De facto, vivemos numa era de Ameaças Híbridas (AH), as quais se têm afirmado com um dos principais desafios securitários da atualidade (The European Centre of Excellence for Countering Hybrid Threats [Hybrid CoE], 2018).

Estas ameaças vivem no foro da impossibilidade de deteção imediata e usam elementos caracterizadores de "*soft"*, "*hard"* e "*smart power*"[1] atuando numa "*grey zone*"[2] com limites difusos e mal definidos, onde procuram a paridade no desenvolvimento tecnológico e na sua acessibilidade, usando as redes sociais como arma de propaganda e desinformação, manipulando e influenciando as populações de forma a corroer Governos e sociedades (Schmid, 2019).

É no contexto deste novo paradigma civilizacional que o Combate às Ameaças Híbridas (CAH) constitui um verdadeiro desafio, com reptos inigualáveis em termos de defesa e segurança, os quais têm vindo a causar apreensão e preocupação acrescidas dos Estados-Membros da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN), "[…] pelo potencial subversivo que acarretam para o Estado de direito democrático" (Pereira, 2018, p. 1).

Os conceitos de AH e Guerra Híbrida (GH), apesar de não serem novidade, ganharam definitivamente dimensão, com os acontecimentos na Ucrânia em 2014, país em que a Rússia desenvolveu ações de forma astuciosa, sincronizada e combinada, recorrendo aos

[1] Ver corpo de conceitos – Apêndice A.
[2] *Ibidem.*

instrumentos de poder, de forma a explorar as vulnerabilidades dos adversários e alcançar os seus objetivos políticos, o "[…] que levou a NATO a classificá-la como uma abordagem híbrida à guerra e a atribuir-lhe uma elevada importância na preparação do combate às futuras ameaças da Aliança" (Fernandes, 2016, p. 20).

De facto, desde 2014 até à atualidade, têm-se multiplicado as tentativas de desestabilização dos países ocidentais, através da erosão da confiança das instituições governamentais e de ataques aos valores fundamentais da sociedade (*e.g.* ciberataques, campanhas de desinformação e ações militares hostis) (Comissão Europeia [CE], 2018).

De forma a combater esta realidade, a UE e a OTAN têm vindo a desenvolver um conjunto de medidas e Linhas de Ação (LA) de forma a assegurar aos Estados-Membros e Aliados, uma base que os apoie na luta coletiva contra as AH, que evidenciam a necessidade de colaboração interinstitucional e a utilização potencial dos respetivos tratados (CE, 2016a).

As declarações no dia 29 agosto de 2019, da ex-Secretária de Estado da Defesa Nacional, Ana Santos Pinto, à agência Lusa, por ocasião da formalização da candidatura portuguesa ao Hybrid CoE, ilustram bem a prioridade e preocupação do governo no CAH e a importância atribuída a esta temática.

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

Por outro lado, o Conceito Estratégico de Defesa Nacional (CEDN) refere de forma clara, que devem ser potenciadas as capacidades civis e militares para uma abordagem integrada na resposta às ameaças transnacionais (AT) (*e.g.* crime organizado transnacional e cibercriminalidade), através de respostas estratégicas multissectoriais e integradas (Resolução do Conselho de Ministros [RCM] n.º 19/2013, de 05 de abril, pp. 1989-1990).

Ao nível das Forças Armadas (FFAA), o próprio Conceito Estratégico Militar (CEM) mostra a necessidade de edificar capacidades diversificadas, interoperáveis e integráveis, de forma a garantir a participação nacional nas Organizações Internacionais (OI), de segurança e defesa coletiva, nomeadamente na UE e OTAN (Ministério da Defesa Nacional [MDN], 2014).

Desta forma, torna-se necessária a definição de LA para o CAH ao nível das FFAA, que acomodem simultaneamente, as principais Linhas de Orientação Estratégica (LOE) da UE e da OTAN e as sinergias criadas no âmbito destas organizações, justificando-se assim o presente estudo.

O objeto de estudo centra-se nas AH e está delimitado nos domínios: (i) temporal, desde o início do século XXI até à atualidade; (ii) espacial, ao Espaço Estratégico de Interesse Nacional (EEIN); (iii) e de conteúdo, centrando-se nas AH e no seu significado para o instrumento militar, nas LOE da UE e da OTAN e nas capacidades das FFAA para o CAH.

A presente investigação encontra-se alicerçada no Objetivo Geral (OG) e nos Objetivos Específicos (OE) definidos na Figura 1.

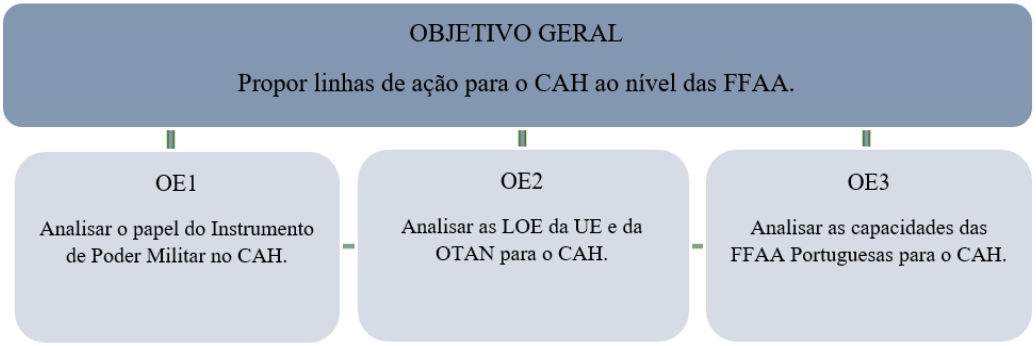


**Figura 1 - Objetivos da investigação**

Para direcionar o estudo, definiu-se uma Questão Central (QC) e três Questões Derivadas (QD), conforme exposto na Figura 2.

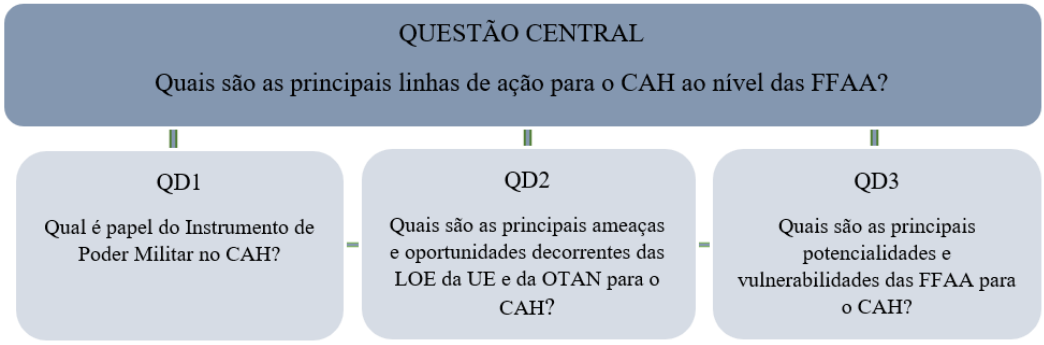


**Figura 2 - Questões da investigação**

O trabalho está organizado em sete capítulos. O primeiro capítulo corresponde à presente introdução. O segundo capítulo apresenta a revisão da literatura e aborda em detalhe a metodologia. O terceiro capítulo visa analisar o papel do Instrumento de Poder Militar (IPM) no CAH e responder à QD1. O quarto capítulo, reflete o ambiente externo, nomeadamente as principais LOE da UE e da OTAN para o CAH com implicações para as FFAA, por forma a responder à QD2. O quinto capítulo incide no ambiente interno, em particular, nas capacidades de CAH ao nível das FFAA, com a finalidade de responder à QD3. No sexto capítulo são propostas as LA para o CAH, através duma análise SWOT (*Strengths, Weaknesses, Opportunities e Threats*), respondendo-se à QC. O sétimo capítulo apresenta as conclusões do trabalho, a avaliação dos resultados obtidos em relação aos objetivos traçados e a resposta ao problema de investigação, terminando com os contributos para o conhecimento, as limitações da investigação e algumas recomendações.

## 2. Revisão da Literatura e Metodologia

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

### 2.1. Revisão da Literatura

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

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

#### 2.1.1. Evolução dos conflitos, das Velhas às Novas Guerras

Clausewitz (1987) dizia que a guerra tem duas componentes que perduram ao longo do tempo: a sua natureza que permanece constante e o seu carácter que se altera conforme o contexto. Esta alteração provoca sucessivas transformações na forma de fazer a guerra, levando a maioria dos pensadores militares a classificar a evolução dos conflitos armados em várias gerações, colocando-se, no entanto, o debate, se serão "novas" ou apenas, as guerras de sempre.

Para vários autores, conforme refere Serrano (2013, pp. 66), "[…] a adaptação da natureza da guerra mantem válida a trindade de Clausewitz – Povo, Governo e Militares" e representa a continuidade da política por outros meios, com a finalidade de forçar o adversário a submeter-se à vontade do oponente.

Outros pensadores contrapõem, dizendo que os novos conflitos já não se enquadram nesta definição clássica de Clausewitz, adicionando "novas" à classificação das guerras. Mary Kaldor, uma das principais autoras deste conceito, defende que as "velhas guerras" estão relacionadas com a versão bélica, que caracterizou a Europa entre os finais do século XVIII e meados do século XX, período em que os Estados combatiam com militares uniformizados, procurando a derrota do inimigo através da batalha decisiva, mas respeitando regras e direitos dos combatentes. Estas "velhas guerras" existiram para fazer face a conflitos interestatais com o objetivo de provocar o maior número de baixas possível, o que já não se coaduna com o carácter e a violência dos conflitos do século XXI (Kaldor, 2013, p. 1).

Kaldor (2013, p. 2) contrasta as diferenças entre "velhas guerras" e "novas" pelos atores intervenientes, objetivos, métodos e formas de financiamento como ilustra a Figura 3, realçando que a distinção entre Estados e não Estados, público ou privado e mesmo entre a guerra e a paz está cada vez mais a esbater-se.

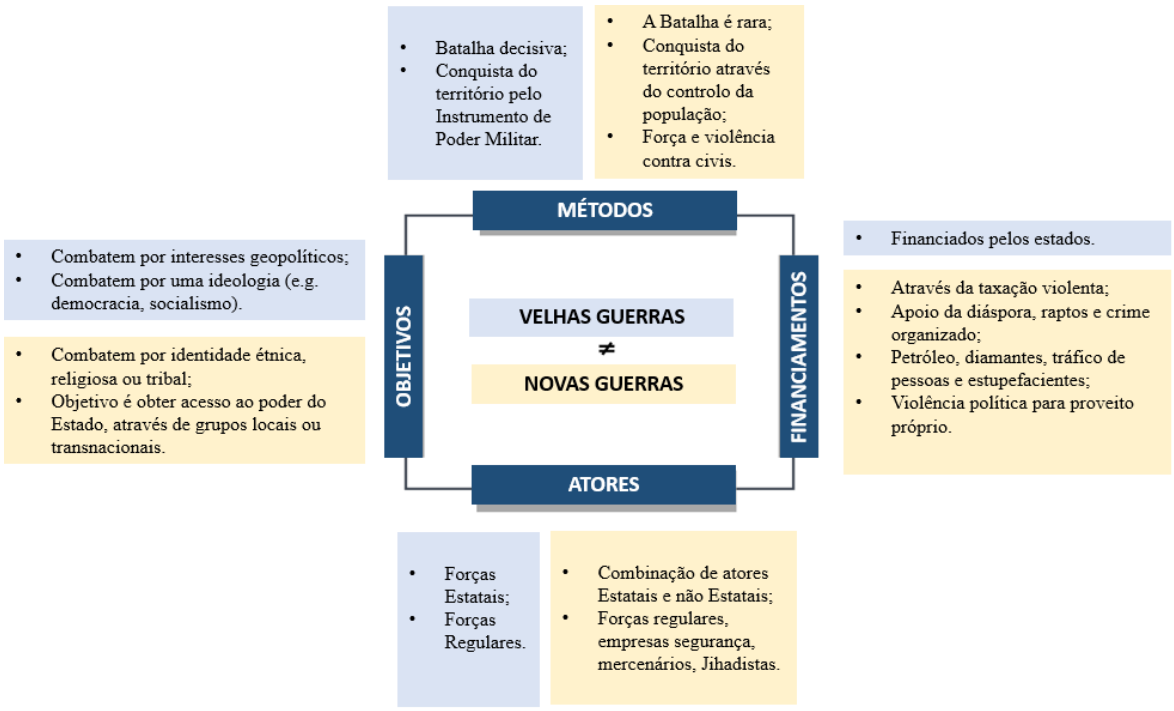


**Figura 3 - Diferença entre velhas e novas Guerras**

Fonte: Adaptado de Kaldor (2013, p. 3).

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

### 2.1.2. Guerra Híbrida

O conceito de GH é uma noção emergente, pouco consensual nos estudos dos conflitos. Refere-se ao uso de métodos não convencionais como parte de uma abordagem de combate em múltiplos domínios, que visam interromper e anular as ações de um oponente sem haver um envolvimento em hostilidades abertas (Treverton et al., 2018).

Como se ilustra na Figura 4, o termo híbrido é uma mistura diversificada de tipos de guerras que se sobrepõem, através da combinação de capacidades convencionais e formações irregulares, terrorismo e criminalidade (Fernandes, 2016).

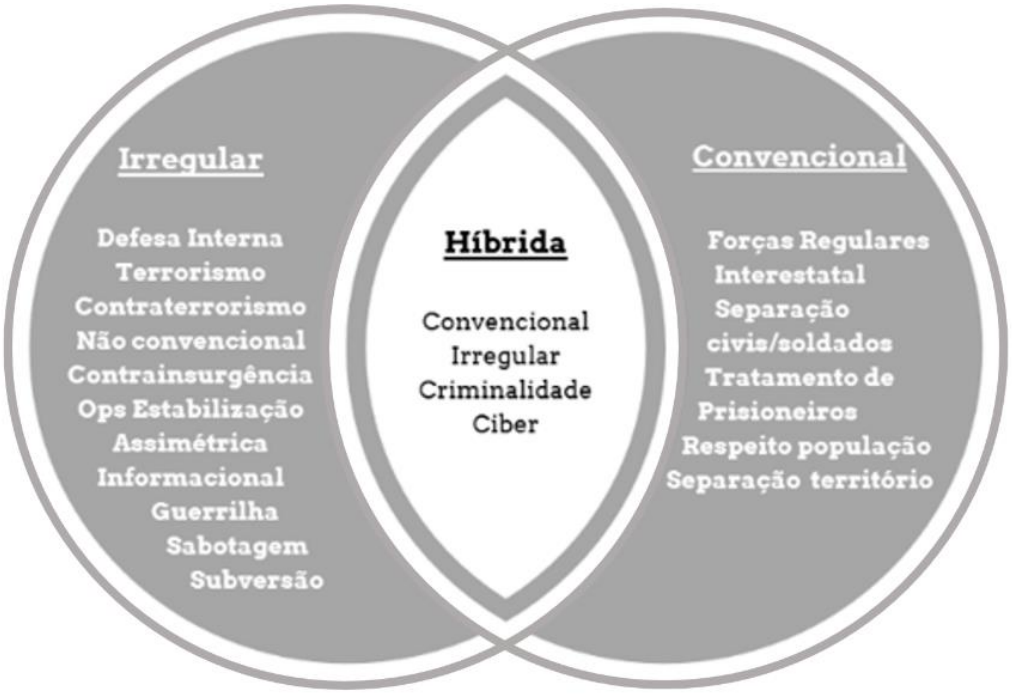


**Figura 4 - Modelo Concetual GH**

Fonte: Adaptado de *United States Government Accountability Office* (2010).

Embora o conceito não seja novo, os seus efeitos e resultados começaram a aparecer com frequência na literatura especializada, desde a abordagem híbrida da Rússia à Ucrânia, que envolveu uma combinação de atividades, incluindo desinformação, manipulação económica, uso de forças paramilitares e milícias, pressão diplomática e ações militares (Guindo, 2015).

No entanto, o conceito de GH só começou a aparecer no vocabulário militar em 2005, com o artigo de Mattis e Hoffman "*Future Warfare: The Rise of Hybrid Wars",* publicado na prestigiada revista *Proceedings*. Estes autores evidenciam que a superioridade convencional dos Estados Unidos da América (EUA) estava a criar uma lógica, que iria levar os seus oponentes a abandonarem a maneira tradicional de travar a guerra (Guindo, 2015).

O termo GH, originalmente referia-se a atores não-estatais irregulares com capacidades militares avançadas. Por exemplo, na Guerra Israel-Líbano de 2006, o *Hezbollah* empregou uma série de táticas diferentes contra Israel, que incluíram a guerrilha, o uso inovador da tecnologia e campanhas efetivas de informação, coordenadas com operações militares convencionais, guerra cibernética e atividades criminosas, procurando dessa forma anular a superioridade tecnológica de Israel (Hoffman, 2009).

Desde então, surgiram outros conflitos que se encaixavam neste novo modo de atuação, como a intervenção da Rússia na Ucrânia e as ações do Estado Islâmico do Iraque

e do Levante, por apresentarem características que a distinguiam de conflitos anteriores. (Fernandes, 2016).

Após o conflito da segunda guerra do Líbano, Frank Hoffman, volta a desempenhar um papel importante, expandindo os termos de AH e GH para descrever conflitos onde se empregam várias táticas em simultâneo. Para este investigador, "[…] h*ybrid wars incorporate a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts, including indiscriminate violence and coercion and criminal disorder*" (Hoffman, 2007, p. 14).

Desde então, têm sido propostos vários modelos para se obter um melhor entendimento da GH, muitas vezes complexos, mas que Schmid (2019) vem explicar de forma simples. Para este investigador do Hybrid CoE, ao contrário do *Military-Centric-Warfare*, a GH passa por orquestrar diversas operações nos diferentes domínios, procurando explorar Centros de Gravidade não militares que, mutáveis no tempo, criam ambiguidade e impedem a compreensão da situação por parte do oponente, conforme ilustra a Figura 5.

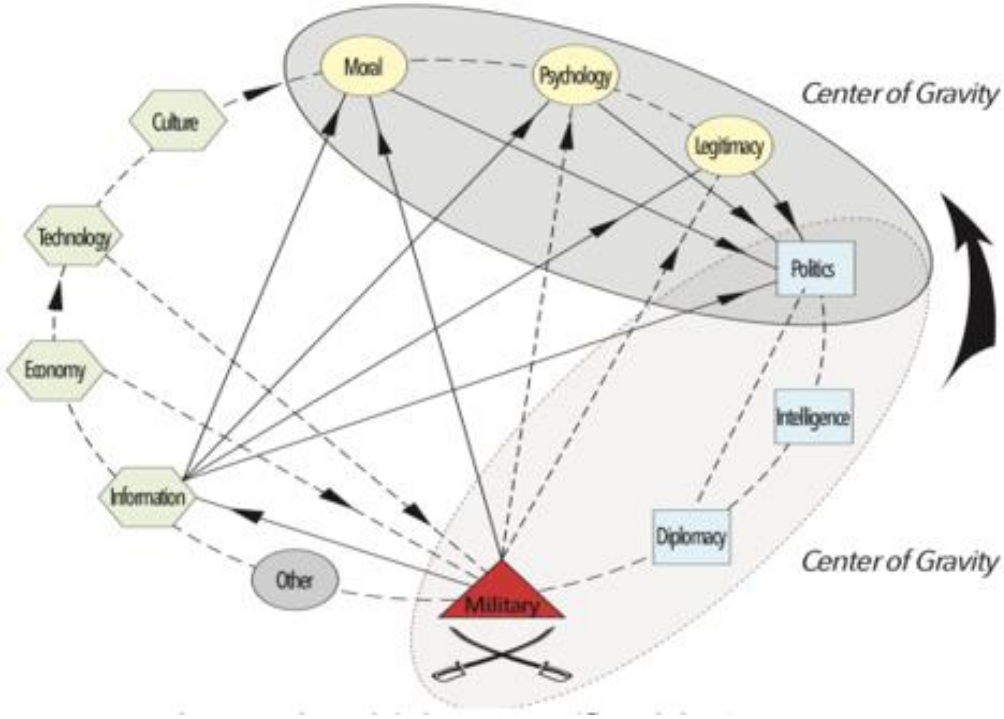


**Figura 5 - Centro de gravidade da Guerra híbrida**

Fonte: Schmid (2019, p. 3).

Essas operações são conduzidas fundamentalmente numa "*grey zone*", designação sugestiva quanto à complexidade de identificação dos seus elementos e fronteiras, que compreende múltiplas interfaces (*e.g.* paz e guerra, amigo e inimigo, militar e civil) e destinam-se a enfraquecer a segurança interna, para que a pressão nos sistemas, exponha

vulnerabilidades do país a explorar. Nesse sentido a GH não é mais do que uma mistura de *soft power* com *hard power*, catalisado com a criatividade do *smart power* (Schmid, 2019).

### 2.1.3. As ameaças híbridas

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

O conceito de AH surge pela primeira vez em 2008, ano em que o Chefe do Estado-Maior do Exército americano o definiu, como um adversário que incorpora combinações diversas e dinâmicas de capacidades convencionais irregulares, terroristas e criminosas (Fleming, 2011), aparecendo ligeiramente mais tarde em 2010 em documentos oficiais da OTAN com o seguinte significado, "[…] *hybrid threats are those posed by adversaries, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives*" (OTAN, 2010, p. 2).

Em 2016, a UE define as AH como "[…] *a mixture of coercive and subversive activity, conventional and unconventional methods, which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below […] of open organized hostilities*" (CE, 2016a, p. 4).

Desde então, têm surgido muitas definições com algumas divergências no seu conteúdo. O que todas têm em comum é menos a GH de Hoffman e mais a sabedoria antiga de Sun Tzu, quando dizia que lutar e conquistar em todas as batalhas não é uma excelência suprema, esta consiste em quebrar a resistência do inimigo sem lutar (Tzu, 2009). Na verdade, a maioria das aceções apresenta como denominador comum, o uso de múltiplos meios ambíguos para atingir vulnerabilidades em toda a sociedade, a fim de alcançar objetivos de forma gradual, sem desencadear respostas decisivas ou armadas (MCDC, 2019a).

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

que a personificação e alavancagem dessa influência através de ferramentas híbridas e dos instrumentos de poder (*e.g.* político, económico e militar).

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

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

Em súmula, a GH "[…] surge da combinação de meios convencionais, assimétricos e irregulares; de formas de coação económica e política; de guerra da informação e controlo dos meios de comunicação; de ataques cibernéticos e de grupos terrorista e criminosos." (Santos, 2017, p. 22), Por outro lado, as AH combinam uma ampla gama de meios não violentos para visar vulnerabilidades em toda a sociedade, de forma a atingir gradualmente os objetivos dos perpetradores sem desencadear respostas decisivas (MCDC, 2019a).

Para melhor entendimento desta distinção, a Figura 6 explana o posicionamento das AH durante as diferentes fases de um conflito.

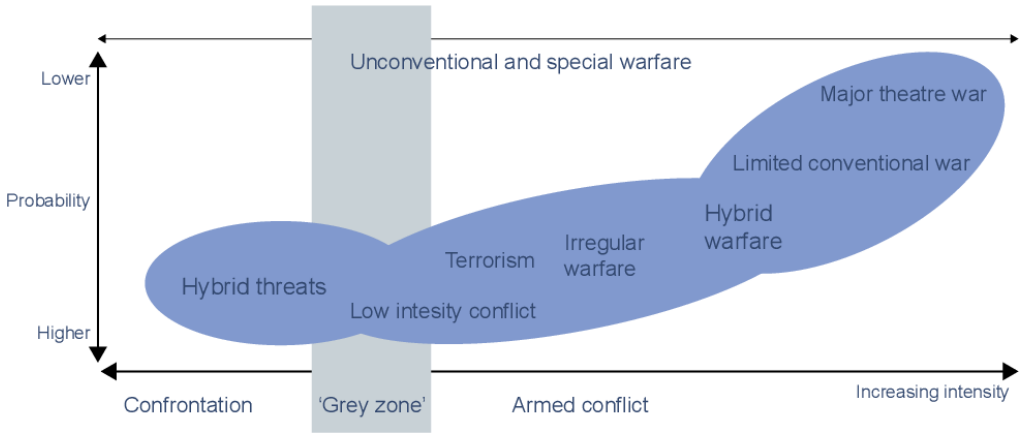


**Figura 6 - AH vs GH**

Fonte: MCDC (2019a, p. 4).

### 2.1.4. Tipologia das ameaças híbridas

Atendendo à evolução do conceito de AH já mencionada, torna-se evidente a dificuldade em identificar as ocorrências que podem ser classificadas como híbridas ou não, sobretudo pela natureza complexa e pela multiplicidade de meios que podem ser utilizados.

De facto, as AH são conduzidas através de uma ampla gama de meios e instrumentos, abrangendo, entre outros, "[…] campanhas mediáticas à utilização de armas químicas, biológicas, radiológicas e nucleares [NRBQ], passando por ciberataques contra sistemas informáticos de infraestruturas estratégicas ou pela utilização de meios de subversão da paz social ou da ordem económica" (Pereira, 2018, p. 11).

As ocorrências deste tipo de ameaças verificam-se essencialmente no âmbito do ciberespaço. Por um lado, este domínio catalisador, permite explorar a tecnologia residente para obter informação, monitorizar a situação e interferir na comunicação entre sistemas. Por outro, como vetor da comunicação, possibilita a manipulação da sociedade, fomentando a desordem, a confusão generalizada e a desconfiança da população (Hybrid CoE, 2018).

Os ataques cibernéticos podem manifestar-se, através da ciberespionagem, do cibercrime e da cibermanipulação, envolvendo ações de *malware*, negação de serviços, sabotagem dos sistemas, coleta de informações (*e.g.* "*scan", "phishing" ou "sniffing"*), entre outros (Duarte, 2020).

Neste contexto, importa ainda destacar a desinformação e a propaganda como uma das armas mais eficazes das AH, que procuram a manipulação de informações, tirando proveito do acesso generalizado à Internet e à proliferação dos media e das redes sociais (Duarte, 2020).

Para além desses domínios catalisadores, as AH podem manifestar-se através de todo o espectro das ameaças, desde que, sejam utilizadas de forma combinada para atingir um determinado objetivo. A Figura 7 representa as principais tipologias.

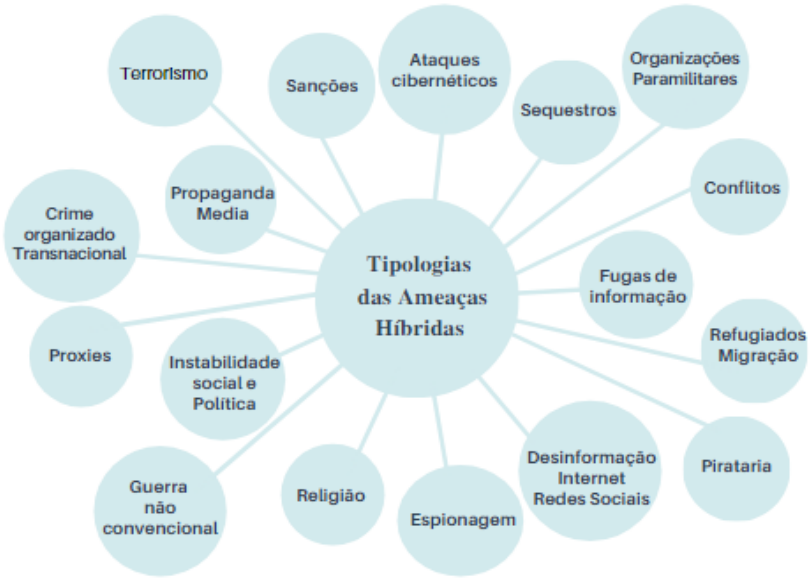


**Figura 7 - Tipologia das AH**

Fonte: Adaptado Treverton et al. (2018).

## 2.2. Metodologia

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

Na investigação seguem-se as orientações metodológicas definidas pelo Instituto Universitário Militar (IUM) (Santos & Lima, 2019), tendo como referências as Normas de Execução Permanente/Investigação (NEP/INV) aprovadas, a NEP/INV 001 (IUM, 2018) e a NEP/INV 003 (IUM, 2020). Na Figura 8 sistematiza-se a metodologia adotada.

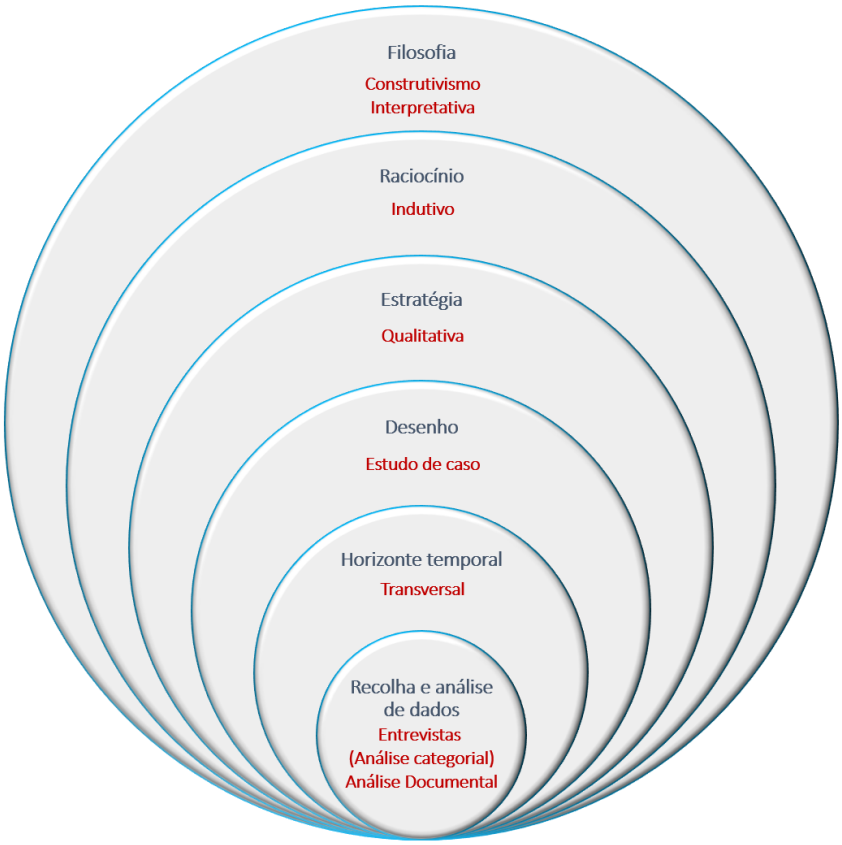


**Figura 8 - "Cebola" da investigação**

Fonte: Adaptado de Saunders, et al. (2009, p. 108).

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

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

O percurso metodológico integra as fases exploratória, analítica e conclusiva (IUM, 2018), conforme apresentado na Figura 9.

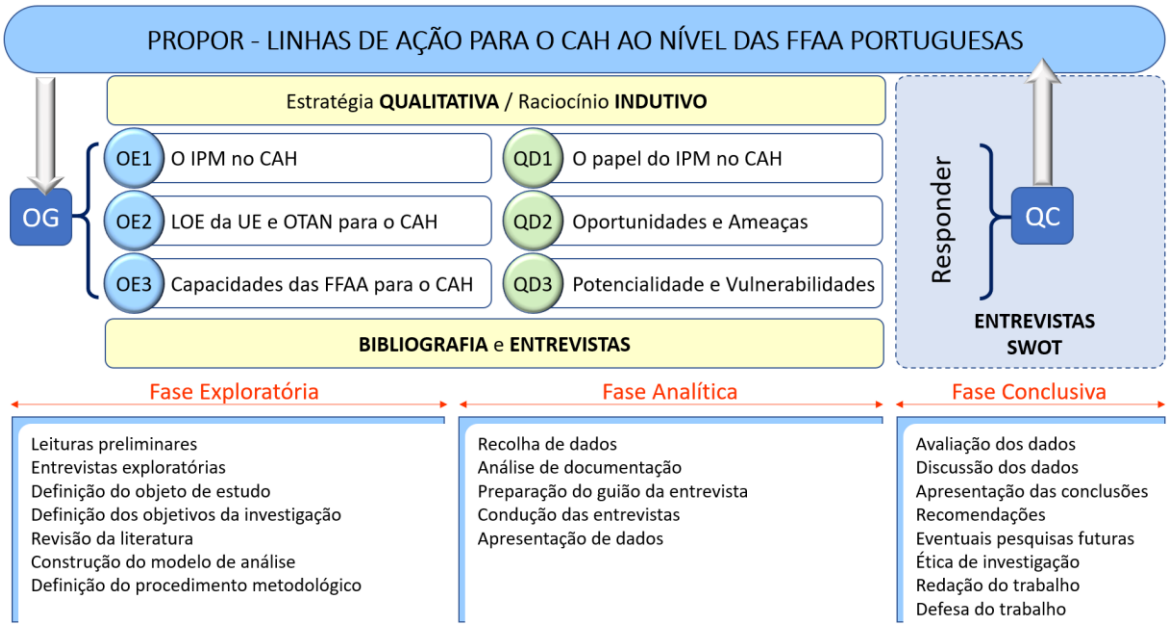


**Figura 9 - Percurso metodológico.**

O modelo de análise consta no Apêndice B e identifica as dimensões, as variáveis e os indicadores utilizados durante a investigação.

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

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

- As entrevistas são do tipo semiestruturadas (Sarmento, 2013, p. 34), com recurso a tópicos e perguntas, alinhadas com os problemas e principais eixos da pesquisa. O guião contém quatro perguntas: as duas primeiras são orientadas para responder à QD1, a terceira à QD2 e a quarta à QD3. A listagem dos entrevistados e o guião constam no Apêndice C;

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

A técnica de análise dos dados recolhidos nas entrevistas é a análise categorial. Por questão, procede-se da seguinte forma: (i) constituem-se as unidades de contexto, determinam-se as unidades de registo e elabora-se um quadro com as unidades de contexto e registo; (ii) constrói-se um quadro com a análise conteúdo, no qual as unidades de registo são quantificadas de acordo com as suas características comuns (unidades de enumeração: soma e percentagem na amostra) e reagrupadas em categorias, a que se atribui uma designação; (iii) elaboram-se as conclusões, evidenciando os resultados $\geq 50\%$ e enfatizando os $\geq 80\%$ (verificação das unidades de registo: não verificadas se $x < 50\%$; parcialmente verificadas se estiverem no intervalo $50\% \leq x < 80\%$; verificadas se $x \geq 80\%$) (Sarmento, 2013, pp. 14-15 e 48-66).

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

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

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

# 3. O papel do Instrumento do Poder Militar no CAH

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

## 3.1. Estratégia de combate às ameaças híbridas

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

A Figura 10 resume as principais ações no âmbito dessas três componentes, que podem ser consultadas mais em detalhe no Apêndice D.


**Figura 10 - Estratégia CAH**

Fonte: Adaptado da MCDC (2019a, p. 5).

## 3.2. Conceito análise das ameaças híbridas da MCDC

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

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

As funções críticas são definidas como atividades ou operações distribuídas no espectro Político, Militar, Económico, Social, Informacional e das infraestruturas (PMESII) que se forem descontinuadas, podem levar a uma interrupção ou disrupção dos serviços ou de determinadas funções de que uma sociedade ou um Estado dependem (MCDC, 2017).

A estrutura analítica que se ilustra na Figura 11 permite refletir esses vetores de poder de um ator face às vulnerabilidades do seu oponente, no espectro das funções mais críticas da sociedade, e apresenta um exemplo prático de visualização.

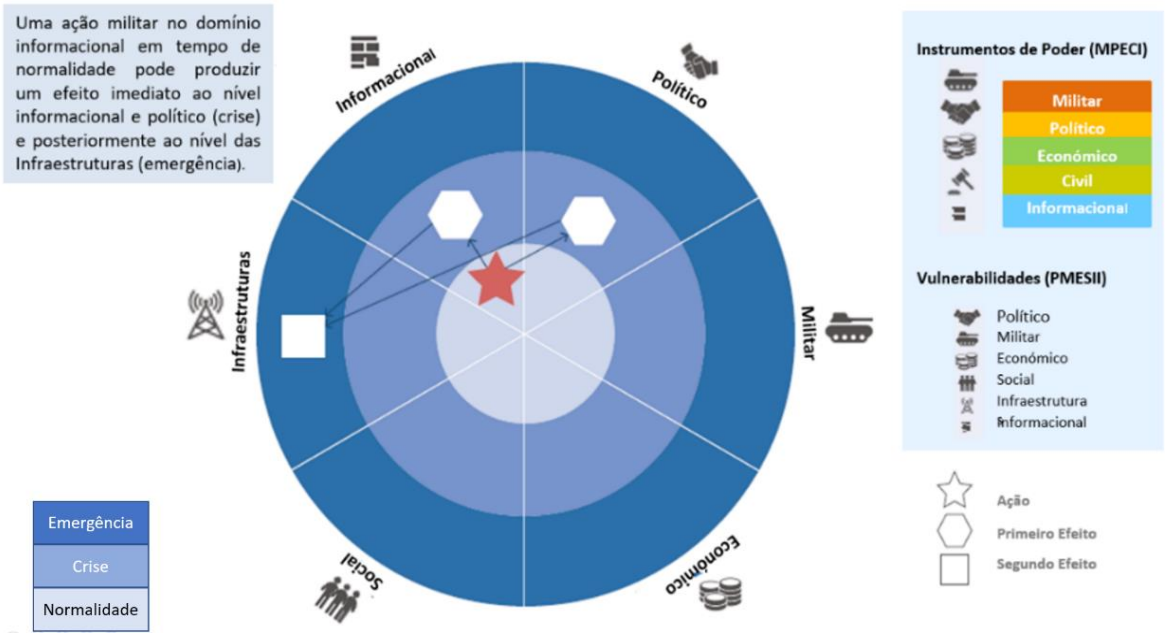


**Figura 11 - Instrumentos de poder e funções críticas**

Fonte: Adaptado MCDC (2017, p. 15).

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

### 3.3. A atividade híbrida no conflito Rússia/Ucrânia

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

região de Donetsk e Luhansk (Figura 12) (J.M.P. Teixeira entrevista presencial, 11 de março de 2020).


**Figura 12 - Agitação pró-russa**

Fonte: Adaptado de Wikimedia (s.d.).

Constatou-se que a Ucrânia teve vários desafios políticos e ao nível do seu capital social, "[…] foi fácil para a Rússia desencadear operações na Crimeia e no leste da Ucrânia, explorando as divisões regionais e as tensões nacionais polarizadas, pela diferença da língua e da cultura" (J.M.P. Teixeira, *op. cit.*).

Roberts descreve de forma resumida a gama de capacidades e meios, que foram empregues pela Rússia neste conflito, incluindo a camuflagem, deceção, negação, subversão, sabotagem, espionagem, propaganda e operações psicológicas.

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

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

operações que estavam a ocorrer em simultâneo. Desta forma, introduziu no território ucraniano armamento e forças paramilitares que alegadamente iriam prestar ajuda humanitária (Davis, 2015).

Concomitantemente, empregou militares encobertos, os *little green men*, dando início a uma campanha psicológica, informacional e subversiva junto da população local, com o propósito de desacreditar o governo ucraniano (Davis, 2015).

Em súmula, a Rússia explorou ativamente as divisões da sociedade ucraniana e o seu governo instável com FFAA mal equipadas, utilizando uma ampla gama de instrumentos, desde a alavancagem económica, forças especiais, ciberataques, a influência da diáspora e a desinformação, entre outros.

### 3.4. Apresentação e discussão dos resultados da QD1

A partir das respostas dadas à pergunta 1, elaboraram-se os quadros com a respetiva análise categorial (Apêndice E). A Figura 13 apresenta as unidades de registo verificadas (resultados ≥ 50%) e permite visualizar a correlação direta das principais ferramentas híbridas utilizadas pela Rússia (ação direta) contra as funções críticas da Ucrânia.

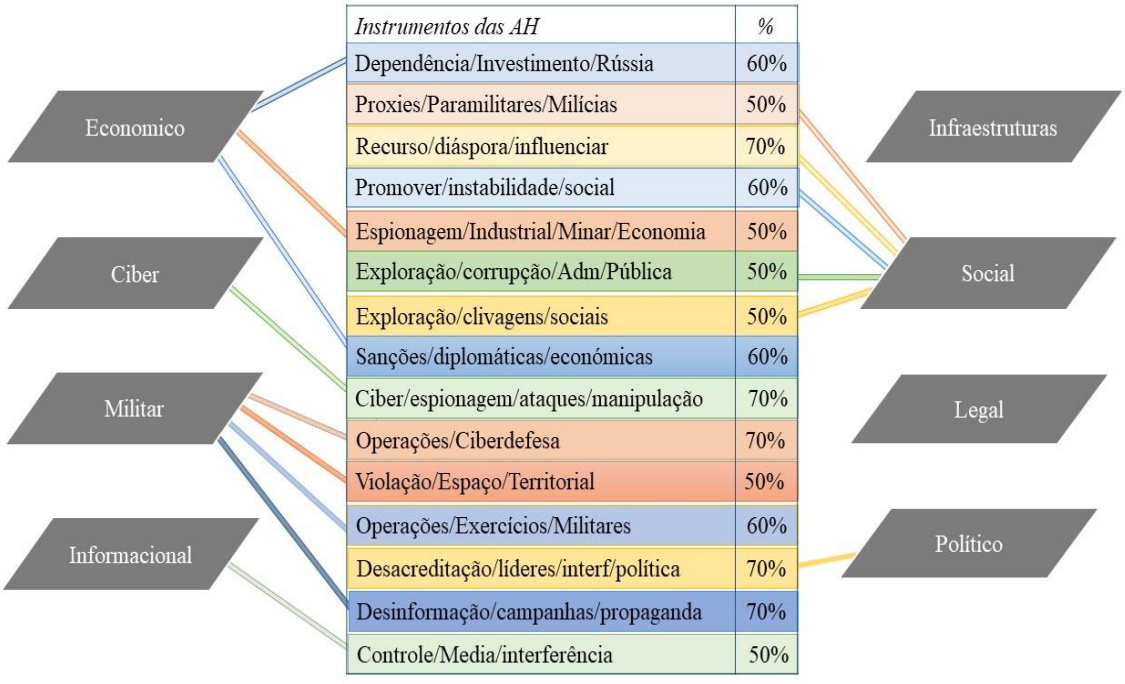


**Figura 13 - Unidades de registo verificadas da pergunta 1**

Os resultados obtidos foram também escrutinados e relacionados criticamente através da folha de cálculo *Excel* e do *software Power BI*, para se ter uma visualização mais holística que permita identificar os efeitos lineares e não lineares que ocorreram em todo o espectro da sociedade, onde se inclui o IPM. O Apêndice F permite visualizar de forma integrada a

correlação entre todas as variáveis e indicadores desta dimensão (i.e., instrumentos de poder da Rússia, meios e efeitos das AH, funções críticas da Ucrânia e componentes do CAH).

A Figura 14 ilustra um exemplo aleatório das unidades de registo ≥ 50%, em concreto a Violação do Espaço Territorial da Ucrânia, para melhor esclarecer o potencial deste tipo de visualização integrada, que permitiu complementar a análise efetuada. Este exemplo tem a seguinte explicação:

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

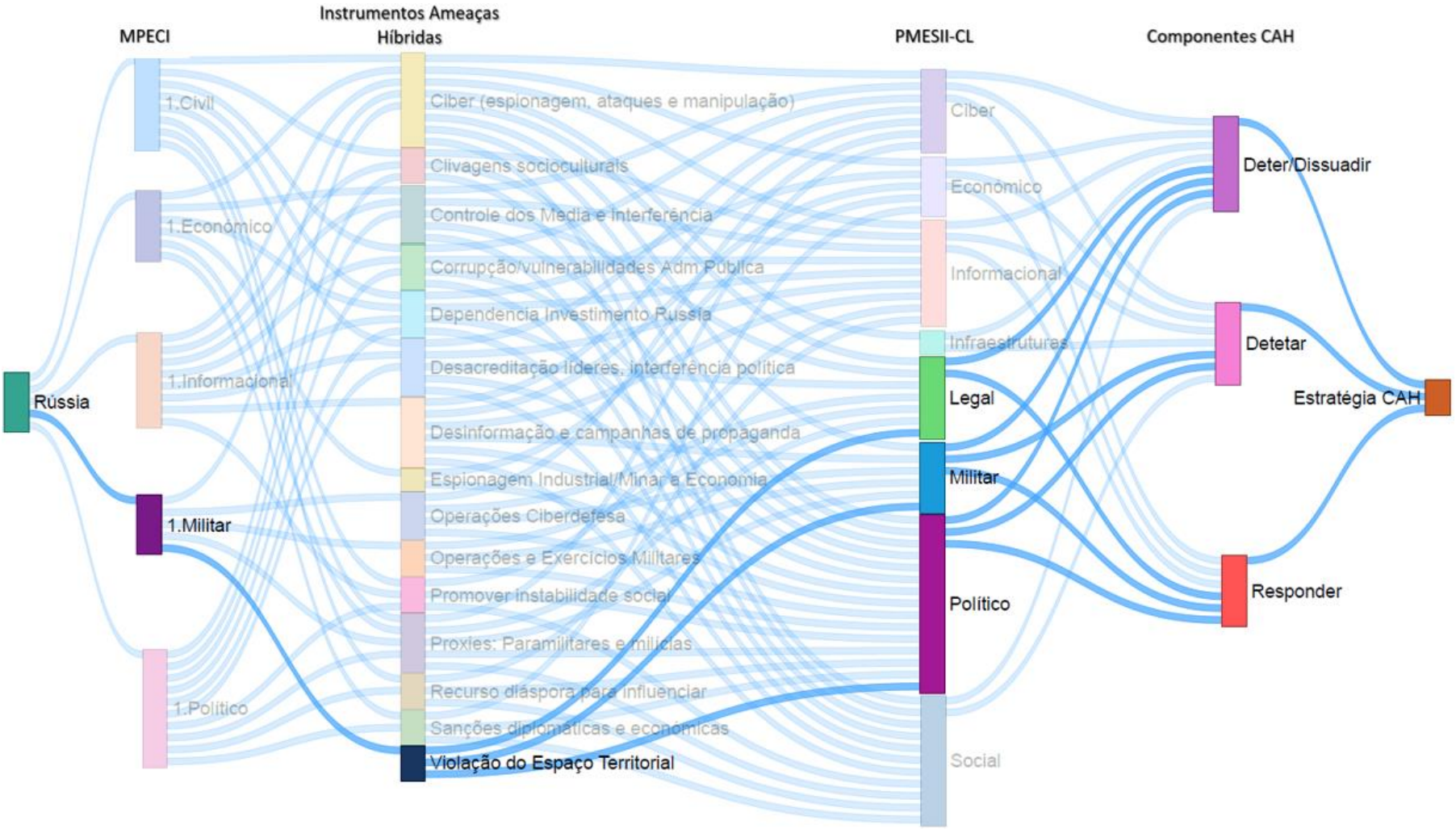


**Figura 14 - Exemplo - Violação do Espaço Territorial**

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

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

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

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

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

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

A ferramenta *Power BI* permite ainda verificar de forma individual as ações e respostas que deveriam ter sido dadas. A Figura 15 ilustra a atuação expectável da Defesa Militar, face às principais ferramentas que foram utilizadas pela Rússia contra esse domínio. Dela pode-se inferir que as principais ferramentas híbridas com ação direta e efeitos não lineares no domínio militar dizem respeito ao ciberespaço, desinformação e campanhas de propaganda, operações de ciberdefesa, operações e exercícios militares, forças paramilitares e milícias e violação do espaço territorial.

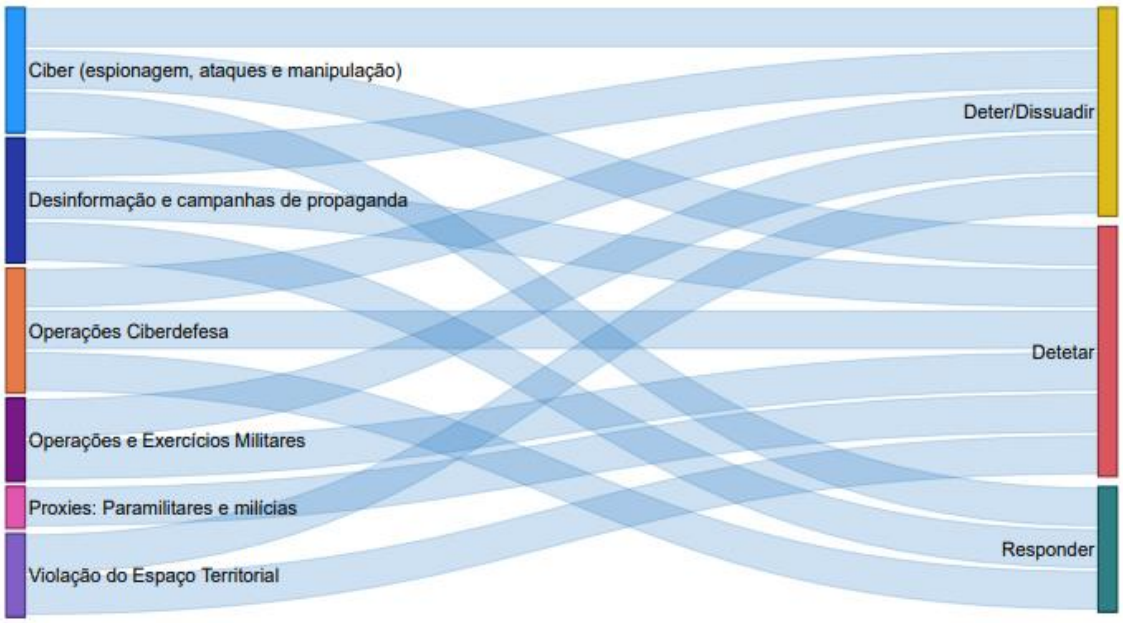


**Figura 15 - Visualização do domínio Militar**

A partir das respostas à pergunta 2, elaboraram-se os quadros com a respetiva análise categorial (Apêndice E). A Figura 16 apresenta as unidades de registo principais (resultados ≥ 50%).

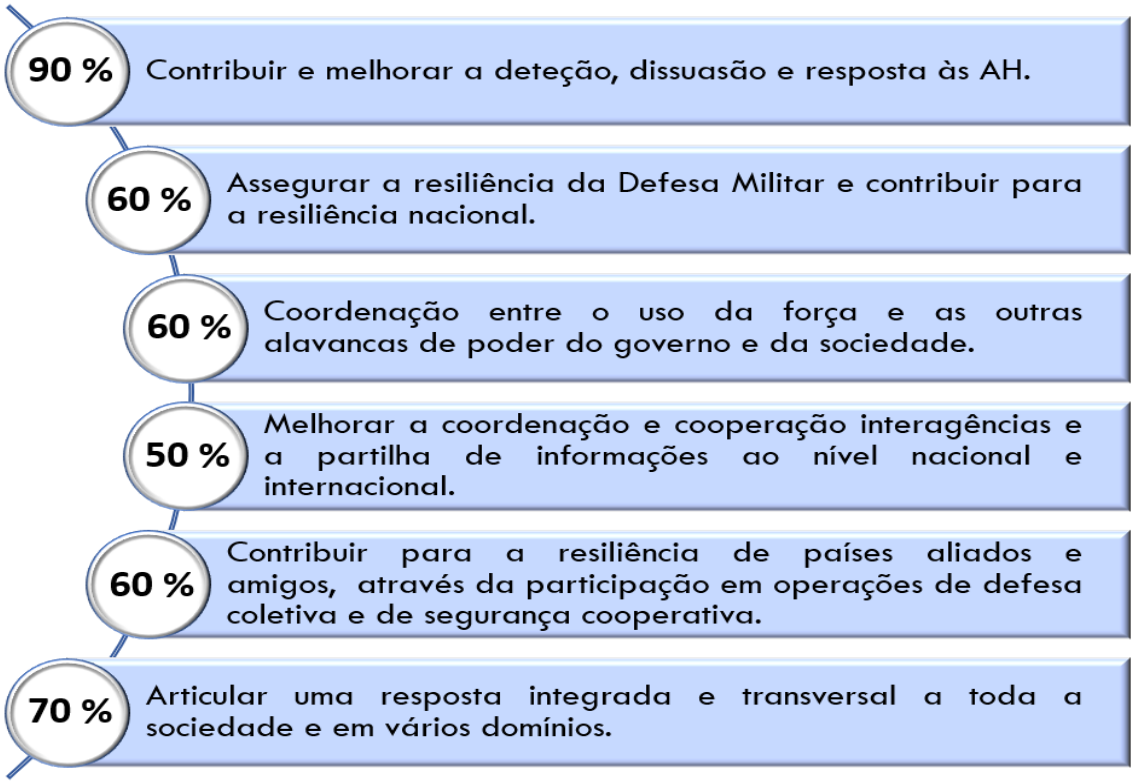


**Figura 16 - Desafios do IPM face às AH**

Esta análise permite inferir os principais desafios das FFAA no CAH, que se consubstanciam em: assegurar a resiliência da Defesa Militar e contribuir para a resiliência nacional; coordenar o uso da força com os outros instrumentos de poder do Governo numa estratégia de segurança cooperativa e integrada de toda a sociedade; melhorar a cooperação e coordenação interagências e a partilha de informações ao nível nacional e internacional; contribuir para a resiliência de países Aliados e amigos, através da cooperação e participação em operações de defesa coletiva e segurança cooperativa; e o contributo para a deteção, detenção e resposta às AH, que foi mencionado pela maioria dos entrevistados (90%).

Neste âmbito, importa enfatizar que a atuação militar ao nível da deteção não será substancialmente diferente da prática existente, embora requeira, conforme refere A.J.G. (Marques, *op. cit.*) "[…] uma cooperação mais estreita com os nossos Aliados e parceiros e deverá explorar sobretudo a partilha de informação, a inteligência estratégica e os recursos técnicos e físicos a que tem acesso no âmbito da comunidade militar internacional".

Em termos de dissuasão e resposta, os militares devem garantir a sua dissuasão convencional e eventual escalada para um conflito armado, quer em termos nacionais quer

no âmbito dos compromissos internacionais de defesa. Nesse sentido, devem "[…] continuar a assegurar capacidades para conduzir operações credíveis de negação (i.e., coagir, interromper, negar e impedir), no âmbito da defesa naval, terrestre e aérea, inclusive nos novos domínios do espaço e do ciberespaço" (J.M.S. Coelho, entrevista presencial em 3 de março de 2020).

Nesse contexto, o papel das FFAA, passa obrigatoriamente "[…] por assegurar a sua própria resiliência para continuar a cumprir as suas missões e contribuir para a resiliência nacional na prevenção e resposta a crises, através de uma abordagem coordenada, transversal, transdisciplinar e multi-institucional com toda a sociedade" (*Ibid*).

### 3.5. Síntese conclusiva e resposta à QD1

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

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

Com esta súmula, apresentou-se o papel do IPM, o que responde à QD1 e cumpre o OE1.

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

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

## 4.1. Ambiente externo e as novas ameaças híbridas

A dinâmica da revolução tecnológica transformou o mundo numa aldeia global, com um nível de progresso e integração sem precedentes, criando, ao mesmo tempo, terreno fértil para uma difusão equivalente de ameaças e riscos em todas as dimensões, que se alimentam desenfreadamente das tecnologias disruptivas e do potencial devastador do ciberespaço (*Training and Doctrine Command* [TRADOC], 2019).

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

A Leste, a ameaça de uma campanha híbrida, conjugada com operações de desinformação, ataques cibernéticos e constantes violações do espaço aéreo de diversos países, consubstanciadas pela anexação da Crimeia pela Rússia e no seu apoio aos separatistas de Donbass (Treverton et al., 2018).

No flanco Sul-Médio-Oriente, a instabilidade endémica com a implantação do *Daesh*, a guerra na Síria e no Iémen, a intensificação da crise na Líbia, a par do recrudescimento de Estados frágeis nas regiões da África subsariana e Sahel, configuram desafios securitários que podem ser instrumentalizados para fins que não a sua natureza, designadamente o terrorismo, pirataria, criminalidade organizada, tráfico humano e sobretudo o incremento exponencial de fluxos migratórios e das vagas de refugiados (Rodrigues & Borges, 2016).

Para além destes desafios, a exígua cooperação ao nível de segurança e defesa, potenciada pelos ataques cibernéticos, a guerra das perceções, o *Information gathering*, o *Big Data*, a desinformação, as assimetrias económicas e as divergências políticas no continente europeu, propiciam o desenvolvimento e a confirmação das AH, como uma das principais preocupações securitárias e militares (Treverton et al., 2018).

Estas ameaças não reconhecem fronteiras e manifestam-se em todas as funções críticas de um Estado, requerendo por isso uma resposta global e uma aproximação concertada de toda a sociedade. A maioria dos países ainda não está preparada para essa realidade. Nesse sentido, "[…] é recomendável seguir de perto o que se está a fazer neste âmbito na UE e na

OTAN, adaptando a doutrina e as boas práticas à nossa realidade e procurando total interoperabilidade e coordenação com essas organizações" (A.J.G. Marques, *op. cit.*).

#### 4.1.1. União Europeia

Em abril de 2016, a CE e a Alta Representante adotaram um quadro comum para fazer face às AH e reforçar a resiliência da UE, dos seus Estados-Membros e dos países parceiros e, simultaneamente, aumentar a cooperação com a OTAN. Esse quadro propõe vinte e duas ações operacionais destinadas a dar aos Estados-Membros uma base para a luta coletiva contra as AH e é apoiado por um vasto leque de instrumentos e iniciativas, incluído a utilização de todo potencial dos Tratados (CE, 2016b).

Mais tarde, no dia 13 de junho de 2018, a Alta Representante para a UE, em conjunto com a CE, publicou uma comunicação conjunta, na qual ficaram definidas as principais LOE para combater as AH (CE, 2018).

Esta declaração evidencia que o CAH deve basear-se fundamentalmente nas seguintes áreas: melhorar a consciência situacional; reforçar a resiliência; reforçar a prevenção e a resposta a situações de crise; e melhorar a cooperação internacional e interagências (CE, 2018).

Estes vetores prioritários constituem as variáveis do modelo de análise do presente estudo, e podem ser consultados mais em detalhe no Apêndice G.

#### 4.1.2. Organização do Tratado Atlântico Norte

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

No entanto, no que concerne às AH, a Aliança declarou um conjunto de medidas em julho de 2016 e atualizou-as em 2018. Estas propostas contemplaram também um conjunto de ações para incrementar a cooperação e delinear uma estratégia comum (OTAN, 2018a).

Apesar de ser perentória em afirmar, que a principal responsabilidade de responder a AH recai sobre o país-alvo e na sua capacidade de resiliência, a Aliança tem vindo a

disponibilizar um conjunto de mecanismos de cooperação e colaboração para aprofundar o conhecimento e contribuir para a criação de sinergias, que se estendem por várias medidas, em áreas civis e militares (OTAN, 2019).

Destas medidas destacam-se as seguintes: incrementar e incentivar a partilha de informações entre Aliados através do *Hybrid Analysis Branch*; incrementar os eventos híbridos nos exercícios (*e.g. Crisis Management Exercise*); implementar o uso das *Counter Hybrid Support Teams* (CHST); intensificar a cooperação com parceiros e organizações, nomeadamente a UE; encorajar o fortalecimento da resiliência nacional ao nível do planeamento civil de emergência; encorajar o uso das comunicações estratégicas para contrariar e denunciar campanhas híbridas; continuar a desenvolver o esforço na Ciberdefesa; considerar opções de resposta coletiva no CAH (*Ibid*).

#### 4.1.3. Cooperação OTAN-UE

O Hybrid CoE foi estabelecido em 11 de abril de 2017 com o patrocínio da UE e da OTAN. A iniciativa teve origem na CE (2016b) tendo sido aprovada no conjunto comum de propostas para a implementação da Declaração Conjunta, endossada pelo Conselho da UE e pelo Conselho do Atlântico Norte em 6 de dezembro de 2016 (OTAN 2016a).

Estas propostas contêm um conjunto de medidas para incrementar a cooperação OTAN-UE no CAH, o que permitiu que estas organizações começassem a trabalhar em estreita ligação no sentido desenvolver *playbooks*[3] e operacionalizar procedimentos conjuntos, nomeadamente nas seguintes áreas: consciência situacional; prevenção e resposta a crises; segurança cibernética; comunicação estratégica; e realização de exercícios de AH (OTAN, 2016b).

Esta declaração conjunta vem reforçar a necessidade de aumentar a cooperação entre as estruturas mais relevantes destas organizações, ao mesmo tempo, que os países avaliam as suas próprias vulnerabilidades, de forma a garantir uma resposta horizontal *"whole-of society"* apoiada por ambas instituições. A Figura 17 reflete essa abordagem abrangente, que passa por uma resposta conjunta e integrada em termos nacionais e internacionais, onde se privilegia o conhecimento situacional, a prontidão e a resiliência, numa dinâmica de segurança cooperativa (OTAN, 2018b).

[3] Protocolos operacionais para o combate às AH.

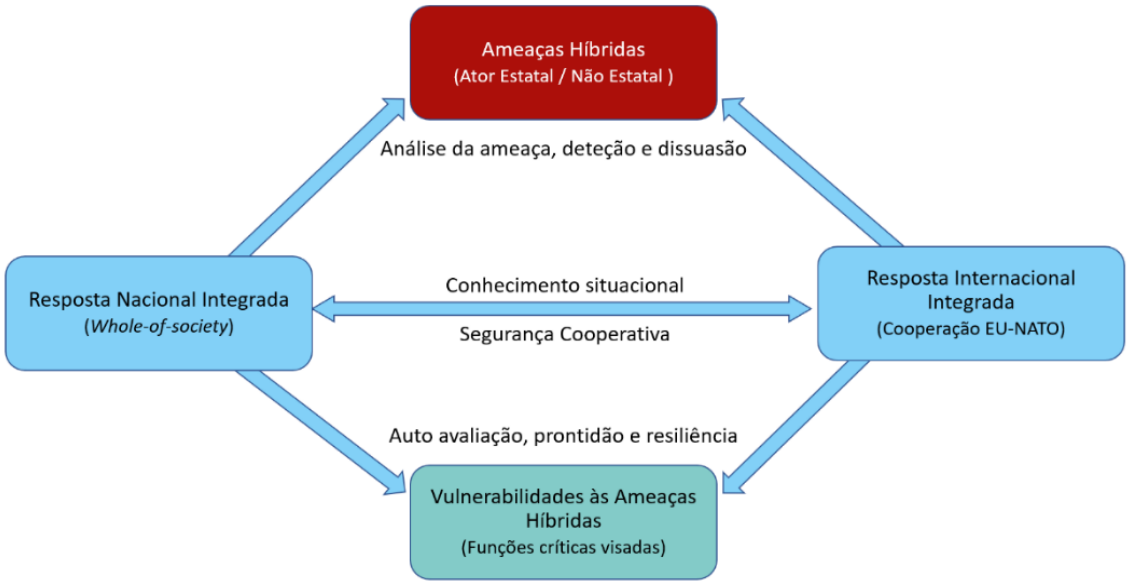


**Figura 17 - Abordagem abrangente da UE e OTAN às AH**

Fonte: Adaptado de OTAN (2018b, p. 1).

## 4.2. Apresentação e discussão dos resultados da QD2

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

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

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

- Na criação de sinergias ao nível da comunicação estratégica;

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

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

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

Relativamente à análise de conteúdo, inferiram-se 11 oportunidades e dez ameaças que podem ser consultadas no Quadro 9 do Apêndice E. A Figura 18 apresenta as seis oportunidades e as seis ameaças que foram verificadas ($x \geq 80\%$) ou parcialmente verificadas ($50\% \leq x < 80\%$).

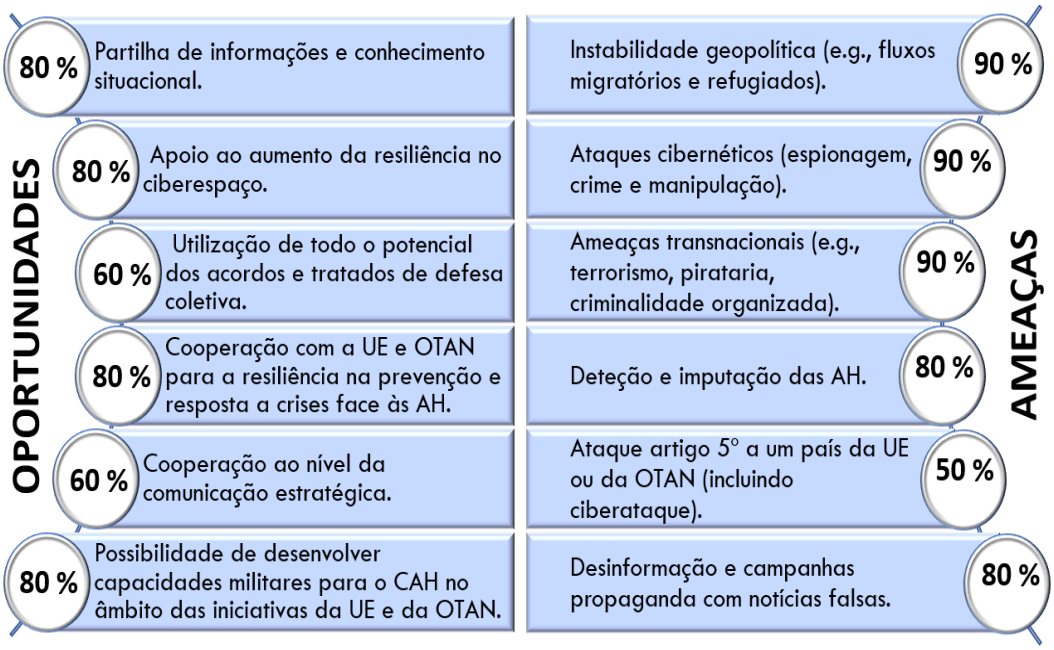


**Figura 18 - Oportunidades e ameaças**

Relativamente às oportunidades, merecem especial destaque por se terem verificado com 80 % dos entrevistados as seguintes: partilha de informações e a melhoria do conhecimento situacional, apoio ao aumento da resiliência no ciberespaço, cooperação com a UE e OTAN para a resiliência na prevenção e resposta a crises e a possibilidade de desenvolver capacidades para o CAH no âmbito das iniciativas da UE e da OTAN.

As ameaças que mais se destacaram são: (i) com 90 %, o aumento da instabilidade geopolítica, os ataques cibernéticos e as AT; (ii) com 80 %, a dificuldade de deteção e imputação das AH e a desinformação e campanhas de propaganda.

### 4.3. Síntese conclusiva e resposta à QD2

Conclui-se que existe um conjunto de ferramentas e de oportunidades no âmbito das estratégias delineadas pela UE e OTAN para apoiar os Estados-Membros, Aliados e parceiros, que podem potenciar as capacidades nacionais para o CAH.

Ainda neste âmbito, deduziu-se que a melhor forma de consolidar uma estratégia nacional, passa por acomodar as principais LOE destas organizações, que assentam nos seguintes pilares: melhorar o conhecimento situacional; reforçar a resiliência; reforçar a prevenção e resposta a crises; e melhorar a cooperação internacional e interagências.

Tendo em conta essas variáveis do ambiente externo, a análise de conteúdo realizada às respostas da pergunta 3 do guião permitiram inferir e validar, seis oportunidades (quatro verificadas e duas parcialmente verificadas) e seis ameaças (cinco verificadas e uma parcialmente verificada). Responde-se assim à QD2 e cumpre-se o OE2.

# 5. Capacidade das Forças Armadas para o combate às ameaças híbridas

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

## 5.1. Análise ambiente interno e as novas ameaças híbridas

A localização geográfica de Portugal, a extensão dos seus limites marítimos e a sua vulnerabilidade económica no âmbito da UE, constituem um terreno fértil para a influência híbrida e para o uso combinado de ameaças associadas, das quais se destacam: (i) crime organizado transnacional, branqueamento de capitais, tráfego de estupefacientes e imigração ilegal; (ii) ciberataques; (iii) terrorismo transnacional; (iv) espionagem ao nível político, militar e económico; (v) definhamento económico-financeiro; (vi) disputa de recursos; (vii) pirataria; (vii), vagas de refugiados e fluxos migratórios (RCM n.º 19/2013, de 05 de abril).

Estas ameaças podem manifestar-se de forma mais cinética, através de impactos físicos diretos, através do uso da força, e de forma menos cinética, que tem mais a ver com a perceção, influência e manipulação (Duarte, 2020).

Comparado a outros Estados europeus, Portugal não tem sido um alvo significativo de ataques híbridos cinéticos devido à sua dimensão geopolítica. No entanto, não escapa ao que está a acontecer na Europa, que cada vez mais, tem vindo a ser alvo de ataques não cinéticos, especialmente através do ciberespaço, em campanhas de desinformação e por pressões económicas e financeiras (*Ibid.*).

Neste contexto, a Tabela 1 evidencia os dados estatísticos das ocorrências das AH em Portugal durante os anos de 2017 a 2018 com realce para a debilitada situação financeira portuguesa, que tem propiciado vulnerabilidades de âmbito económico, principalmente chinesas. A Tabela 2 realça a evolução dos ataques cibernéticos no mesmo período.

**Tabela 1 - AH em Portugal - 2017/2018**

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

Fonte: Duarte (2020, p. 15).

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

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

Fonte: Duarte (2020, p. 12).

#### 5.1.1. Enquadramento legislativo da atuação das FFAA

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

Não obstante esta necessidade imperativa, a Constituição da República Portuguesa (CRP) é perentória em atribuir a defesa militar da República às FFAA, a satisfação dos compromissos internacionais e a participação em missões humanitárias e de paz, no quadro

dos compromissos internacionais assumidos (Lei Constitucional n.º 1/2005, de 12 de agosto, p. 4682).

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

Ainda de acordo com o CEDN (2013), Portugal deverá garantir em todos os momentos a funcionalidade dos sistemas vitais de segurança nacional, nomeadamente a capacidade de vigilância e controlo do território nacional e do espaço interterritorial, incluindo a fiscalização do espaço aéreo e marítimo, as redes de energia, comunicações, transportes, abastecimentos e informação assegurando a resiliência nacional (RCM n.º 19/2013, de 05 de abril, pp. 1989-1990.

Finalmente, e não menos importante, as FFAA também têm um papel fundamental na estabilização da vizinhança próxima alargada, fundamental para defender os interesses nacionais, nomeadamente através da Cooperação no Domínio da Defesa (CDD), reforçando as capacidades dos nossos parceiros para uma resposta às AH mais eficaz (MDN, 2020).

#### 5.1.2. Estratégia de desenvolvimento de capacidades

A Diretiva Ministerial Orientadora do Ciclo de Planeamento de Defesa Militar (DMPDM) "[…] estabelece o Ciclo de Planeamento de Defesa Militar (CPDM), baseado em capacidades militares, […] articulado com o ciclo de planeamento da OTAN e com o Processo de Desenvolvimento de Capacidades da UE" (MDN. 2020, p. 36).

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

Por outro lado e tendo em conta os cenários de atuação perspetivados e as ameaças à segurança nacional, foi definido como prioridade, o desenvolvimento de capacidades que

possam contribuir para: (i) a manutenção da capacidade de dissuasão; (ii) a vigilância e defesa das áreas sob jurisdição nacional; (iii) a participação em teatros internacionais; (iv) a participação em missões humanitárias e de apoio ao desenvolvimento e bem-estar das populações; (v) e o aumento da capacidade de atuar no ciberespaço e no espaço (MDN, 2020).

Neste contexto, deve ser considerado "[…] o desenvolvimento da economia nacional, promovendo a indústria nacional, em parceria com os centros de investigação e as universidades nacionais" (MDN, 2020, p. 37).

No entanto, para o CAH importa desenvolver e consolidar outras capacidades fundamentais, bem como, adaptar de forma conjunta, o conceito de "Batalha Multi-Domínio" através de "[…] estruturas e organizações mais flexíveis, modelares, com menor sustentação logística […] tirando o máximo partido de programas de I&D [Investigação e Desenvolvimento] e de edificação de capacidades […], em desenvolvimento na NATO e na UE" (Pires, 2018, p. 44).

#### 5.1.3. Lei de Programação Militar

Um dos principais objetivos do Plano de Desenvolvimento de Capacidades (CDP/2018), aprovado pela Agência Europeia de Defesa, consiste na identificação das capacidades prioritárias de defesa, no curto, médio e longo prazos, assim como, na identificação das áreas tecnológicas críticas até 2040 (AED, s.d.).

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

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

A Figura 19 ilustra os principais programas da LPM.


**Figura 19 - Principais programas da LPM**

Fonte: Correia (2019).

A Figura 20 mostra, a inter-relação dos programas da LPM, por áreas de capacidades, com o CDP/2018, o que permite inferir a existência de uma percentagem bastante significativa de prevalência entre projetos, propiciando condições favoráveis para aceder a fundos do Fundo Europeu de Defesa (FED) (Correia, 2019).

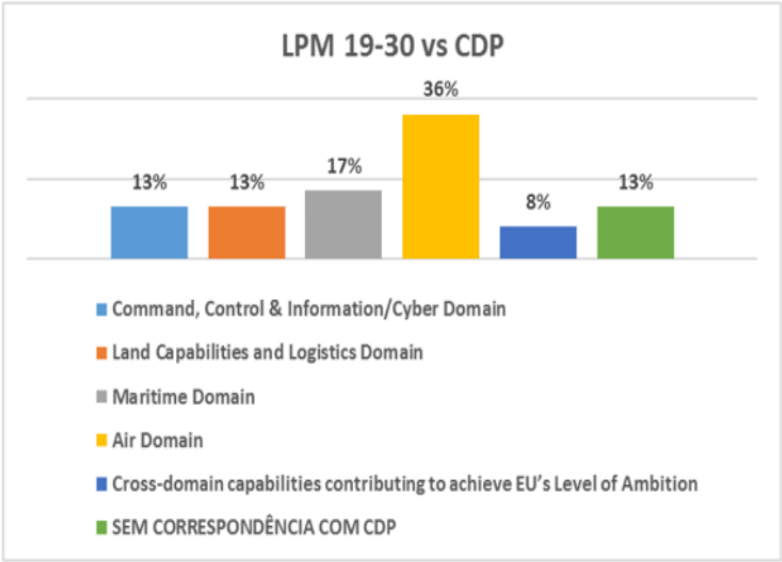


**Figura 20 - Programas da LPM *vs* CDP/2018**

Fonte: Correia (2019).

### 5.2. Apresentação e discussão dos resultados da Q3

A atuação das FFAA no CAH encontra-se vertida de forma implícita no normativo legislativo vigente, essencialmente pela natureza transnacional, transversal e multidisciplinar deste tipo de ameaças e a sua similitude com as existentes.

Neste âmbito, a resposta às AH deve incluir as FFAA, as Forças e Serviços de Segurança (FSS) e o Sistema de Proteção Civil, assumindo uma responsabilidade primária do Estado, a que se devem associar os cidadãos, numa estratégia de segurança cooperativa.

A LPM contempla programas e, nesses, a possibilidades de ajustar projetos para fazer face às AH, que se enquadram nas iniciativas da OTAN e da UE, nomeadamente: a ciberdefesa; os serviços de informações e comunicações baseados no espaço; as capacidades de apoio logístico e médico; a superioridade de informação; a projeção de força; e as tecnologias disruptivas.

Ao comparar as capacidades indicadas na LPM com o CDP/2018, verifica-se que existe uma significativa sintonia entre os diferentes programas e projetos, que podem contribuir para a edificação e consolidação de capacidades essenciais para o CAH.

Tendo em conta o enquadramento do ambiente interno e a análise de conteúdo às respostas da pergunta 4 do guião, inferiram-se 12 potencialidades e 11 vulnerabilidades, conforme constam no Quadro 10 do Apêndice E.

Desse resultado selecionaram-se seis potencialidades e sete vulnerabilidades que se apresentam na Figura 21, por terem sido verificadas ou parcialmente verificadas, todas com uma frequência de registos ≥ 50%.

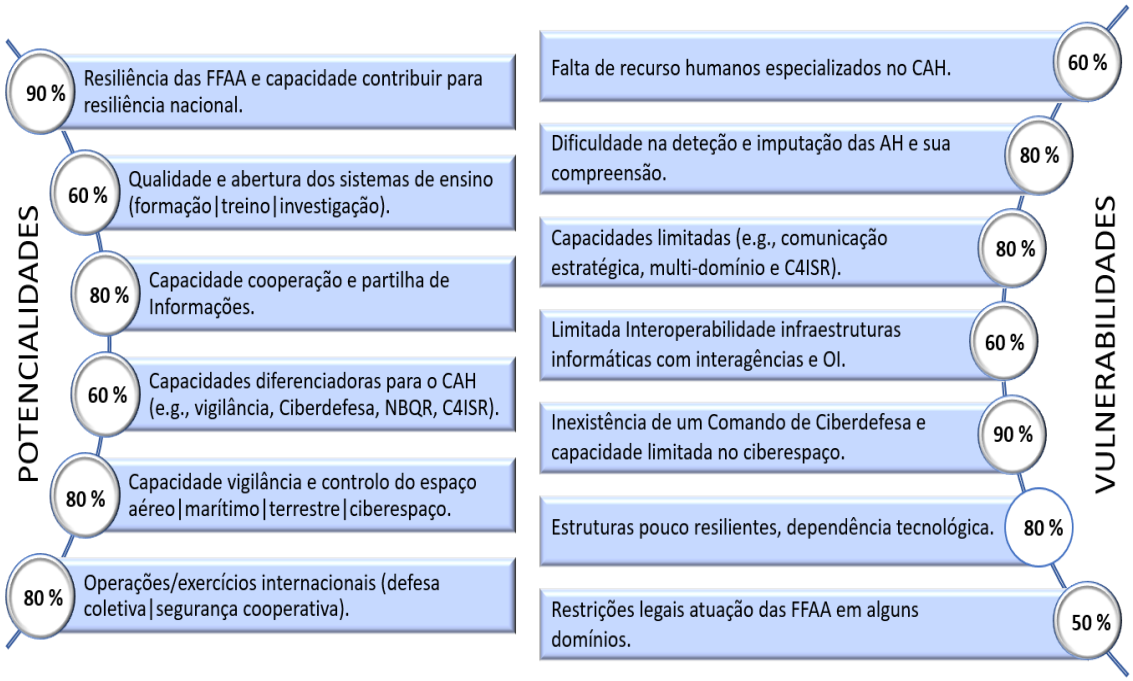


**Figura 21 - Potencialidades e Vulnerabilidades**

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

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

### 5.3. Síntese conclusiva e reposta à QD3

A atuação das FFAA está enquadrada de forma implícita no normativo legislativo vigente. Nesse sentido, a resposta às AH deve incluir a cooperação civil-militar e a articulação interagências nomeadamente com o Sistema de Proteção Civil, numa estratégia de segurança cooperativa de toda a sociedade. Neste contexto, as FFAA desempenham uma função única, pelos seus recursos materiais, humanos, capacidades diferenciadoras, infraestruturas e treino, que permitem assegurar a sua própria resiliência e contribuir para a resiliência nacional.

Tanto a LPM, como os projetos, de I&D e de edificação de capacidades, na UE e na OTAN, refletem presentemente, a maioria das necessidades para o CAH, pelo que, bastará adaptar os projetos que estão em curso às lacunas mais prementes nas FFAA.

Este capítulo permitiu analisar o ambiente interno face às AH e examinar a estratégia de desenvolvimento de capacidades de forma a enquadrar a análise de conteúdo da pergunta 4, permitindo inferir e validar seis potencialidades (quatro verificadas e duas parcialmente verificadas) e sete vulnerabilidades (quatro verificadas e três parcialmente verificadas). Responde-se assim à QD3 e cumpre-se o OE3.

# 6. Análise SWOT e resposta à QC

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

## 6.1. Desafios estratégicos

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

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

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

DE3 - Reforçar capacidade para prevenir e responder a situações de crise, de forma a dar uma resposta rápida aos acontecimentos desencadeados pelas AH. O objetivo é que as FFAA participem no planeamento e desenvolvimento das atividades que concorrem para a resiliência nacional de modo a prevenir, responder e recuperar de crises, de forma rápida e coordenada;

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

## 6.2. Análise SWOT

A análise SWOT, tem por objetivo estabelecer prioridades de atuação e respetivas LA e baseia-se em quatro ideias chave: usar as potencialidades para obter vantagens sobre as oportunidades (PO); as oportunidades para superar as vulnerabilidades (VO); as potencialidades para evitar ameaças (PA); e em minimizar as vulnerabilidades para evitar ameaças (VA). A Figura 22 sintetiza a matriz SWOT efetuada.


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

**Figura 22 - Análise SWOT**

### 6.3. Linhas de Ação

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

**Quadro 1 - Linhas de Ação**

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

### 6.4. Síntese conclusiva e resposta à QC

A dimensão multidimensional e transnacional das AH, vem reforçar a necessidade de existir uma visão alargada, com uma abordagem multi-instituicional, transversal e integrada de toda a sociedade para se enfrentar este novo espectro de ameaças, aumentando a necessidade de reforçar a cooperação civil-militar (com entidades públicas e privadas) nos diferentes patamares de decisão, exigindo, na máxima extensão possível, sinergias nacionais e internacionais, de acordo com o quadro de alianças e acordos existentes.

As FFAA devem por isso estar preparadas para antecipar, prevenir e defenderem-se contra as AH, dissuadindo potenciais atores hostis, tornando ineficientes os seus ataques e limitando o seu impacto. Para esse efeito, devem procurar um alinhamento institucional, nos domínios genético, estrutural e operacional (*e.g.* edificação de novas capacidades multi-domínio, estruturas mais flexíveis e fomentando a necessária resiliência através do treino e formação) para apropriar as suas capacidades de forma mais efetiva para o CAH.

De forma a acomodar as principais LOE da UE e da OTAN neste âmbito, as FFAA deverão procurar superar, no âmbito da sua estratégia para o CAH, os seguintes desafios: aumentar o conhecimento situacional; aumentar a resiliência nomeadamente no domínio do ciberespaço, da comunicação estratégica e na segurança das suas infraestruturas críticas; potenciar as suas capacidades para prevenir e responder a situações de crise e recuperar de forma rápida; e fomentar a cooperação civil-militar nacional e internacional.

A resposta a estes desafios, culmina neste capítulo com uma avaliação SWOT e a dedução das correspondentes LA para o CAH ao nível das FFAA, tendo por base o papel do IPM e as análises efetuadas ao ambiente interno (ameaças e oportunidades) e externo (potencialidades e vulnerabilidades). Assim, considera-se respondida a QC e cumprido o OG.

## 7. Conclusões

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

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

O assunto passou a ser prioridade nas agendas da UE e da OTAN. Em 2016 a CE e o Serviço Europeu para Ação Externa desenvolveram 22 medidas para aumentar a resiliência dos seus Estados-Membros. A OTAN declarou um conjunto de ações em 2016 e atualizou-as em 2018. Estas propostas contemplaram também um conjunto de medidas para incrementar a cooperação e delinear uma estratégia comum.

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

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

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

No que respeita à estrutura, após a introdução no primeiro capítulo, apresentou-se no segundo a metodologia preconizada para a consecução da investigação, verificou-se o estado da arte para obter a necessária clareza conceptual dos principais termos e conceitos,

utilizados ao longo da investigação. Este capítulo revelou-se fundamental para o estudo, já que um dos maiores desafios consiste no uso de terminologia imprecisa, generalizações abrangentes e muitas das vezes, ocorrência de misturas de conceitos, o que dificulta o debate racional e, por conseguinte, justifica uma investigação neste âmbito. Nesse contexto, efetuou-se uma revisão da literatura, onde sobressaíram os seguintes aspetos:

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

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

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

No terceiro capítulo, foi analisado o papel do Instrumento de Poder Militar no CAH, tendo como referência o conflito da Rússia na Ucrânia. Para tal, foi efetuada uma análise de conteúdo das respostas às perguntas 1 e 2, permitindo inferir as principais ferramentas híbridas que foram utilizadas pelos instrumentos de poder da Rússia nas funções críticas da Ucrânia, em termos de ações e efeitos. Posteriormente, realizou-se uma análise integrada com todas as variáveis e indicadores desta dimensão, representadas graficamente pelo software *Power Business Intelligence*, o que permitiu responder à QD1 e alcançar o OE1. Dos resultados obtidos, concluiu-se que:

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

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

Para que esse papel seja determinante, torna-se necessário: (i) garantir uma melhor coordenação entre o uso da força e as outras alavancas de poder do Governo e dos países

Aliados e parceiros; (ii) garantir capacidades para conduzir operações credíveis no âmbito da defesa naval, terrestre e aérea, incluindo nos domínios do espaço e do ciberespaço, mantendo a necessária dissuasão convencional; (iii) e contribuir para a resiliência nacional.

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

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

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

Analogamente, as respostas à pergunta 4 foram reforçadas com o estudo do ambiente interno, inferindo-se como principais:

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

- Vulnerabilidades: inexistência de um Comando de Ciberdefesa e capacidade limitada no ciberespaço; dificuldade na deteção e imputação das AH e sua compreensão; capacidades limitadas; estruturas pouco resilientes, com forte dependência tecnológica; restrições legais para a atuação das FFAA em alguns domínios; e limitada interoperabilidade das infraestruturas informáticas que assegure as ligações interagência, com as organizações nacionais e internacionais.

No sexto capítulo, respondeu-se à QC, através duma matriz SWOT, que foi realizada com base nas respostas às QD, permitindo propor 12 Linhas de Ação listadas no Quadro 2, para integrar uma estratégia de CAH ao nível das FFAA, que acomodam as principais linhas

de orientação da UE e da OTAN e permitem superar os desafios estratégicos a elas associados, cumprindo-se o OG.

**Quadro 2 – Proposta de Linhas de Ação**

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

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

Não obstante, o domínio militar é uma ferramenta do Estado e ao mesmo tempo, uma função crítica da sociedade, sujeito a ser visado nas suas vulnerabilidades, pelo que se revela importante assegurar a sua própria resiliência e o seu contributo para a resiliência nacional.

Neste contexto, e como corolário desta investigação e principal contributo para o conhecimento, relevam-se a proposta de 12 LA para o CAH ao nível das FFAA, que visam constituir-se como elementos orientadores para o processo de alinhamento de uma estratégia

futura, e um contributo para a clareza conceptual e compreensão das AH do papel das FFAA no seu combate.

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

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

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

Este trabalho regeu-se pelos princípios éticos fundamentais e valores em vigor no IUM, designadamente a qualidade e originalidade da pesquisa, verdade científica e liberdade de investigação, bem como o respeito pela propriedade intelectual, o rigor metodológico e experimental. Assim, considera-se que a investigação tem validade interna, ou seja, cumpriu os objetivos definidos, e é credível.

**Referências bibliográficas**

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

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

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

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

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

Comissão Europeia. (2016a, 06 de abril). Joint Communication to the European Parliament and The Council Joint Framework on countering hybrid threats a European Union response [Página *online*]. Retirado de https://eur-lex.europa.eu/legal-content/EN/TXT /HTML/?uri=CELEX:52016JC0018&from =EN

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

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

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

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

Davis Jr., J. R. (2015). *Continued Evolution of Hybrid Threats. The Russian Hybrid Threat Construct and the Need for Innovation.* The Three Swords Magazine. Retirado

de https://pdfs.semanticscholar.org/08c6/b9e234cd5c918f36dfd91b88967725a2be97.pdf?_ga =2.253064073.1650783760.1591290871-352523493.1591290871

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

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

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

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

Fernandes, H. (2016). *As Novas Guerras: O Desafio da Guerra Híbrida.* Revista de Ciências Militares, novembro de 2016 IV (2), pp. 13-40. Retirado de http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes

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

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

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

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

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

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

Instituto Universitário Militar. (2018). NEP/INV-001(O), *Trabalhos de investigação.* Pedrouços.

Instituto Universitário Militar. (2020). NEP/INV-003 (Al), *Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no Instituto Universitário Militar*. Pedrouços.

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

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

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

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

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

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

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

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

Multinational Capability Development Campaign. (2019a, s.d.). *Countering Hybrid Warfare* [Versão PDF]. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf

Multinational Capability Development Campaign. (2019b, s.d.). *Conceptual Foundations and Implications for Defence Forces* [Versão PDF]. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf

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

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

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

Organização do Tratado do Atlântico Norte. (2016a, 08 de julho). Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_133163.htm?selectedLocale=en

Organização do Tratado do Atlântico Norte. (2016b, 06 de dezembro). Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the NATO [Página online]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_138829.htm

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

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

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

Organização do Tratado do Atlântico Norte. (2019, 08 de agosto). NATO's response to hybrid threats [Página online]. Retirado de https://www.nato.int/cps/en/natohq/topics_156338.htm

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

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

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

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

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

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

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

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

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

Santos, L.A.B., & Lima, J.M.M. (Coord.), (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2ª ed, revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

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

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

Schmid, J. (2019). *The Hybrid face of warfare.* Hybrid Center of Excellence Serrano, M.O.L. (2013). *A Guerra é Filha Única.* Coleção Meira Mattos - Revista das Ciências Militares. 7(28), pp.65–78.

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

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

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

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

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

Tzu. S. (2009). *The Art of War*. Edição em Português. Betrand Editora.

United States Government Accountability Office (2010). U.S. GAO [Versão PDF]. Retirado de: http://www.gao.gov/assets/100/97053.pdf

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

## Apêndice A - Corpo de Conceitos

**Ameaça** - Qualquer acontecimento ou ação, em curso ou previsível, de variada natureza, militar, económica, ambiental, que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais ou morais, sendo que no âmbito da estratégia consideram-se principalmente as ameaças provenientes de uma vontade consciente (Couto, 1988).

**Ameaça Híbrida** (Hybrid CoE) – São ações coordenadas e sincronizadas que visam deliberadamente afetar as vulnerabilidades dos Estados democráticos e das suas instituições, empregando um leque particularmente amplo de meios políticos, económicos, militares, civis e de informação (Hybrid CoE, s.d.).

**Ameaça Híbrida** (OTAN) – Consistem numa combinação ampla, complexa e adaptável, de meios convencionais e não-convencionais e de medidas militares, paramilitares e civis, encobertas e abertas, utilizadas de forma integrada por atores estatais e não estatais para alcançar os respetivos objetivos (OTAN, 2016c).

**Análise externa** ‑ Estudo da envolvente externa de uma organização para escolher os fatores que têm maior potencial para a influenciar, tendo em consideração a probabilidade de ocorrência e o grau de impacto positivo ou negativo (Cadle et al., 2010).

**Análise interna** ‑ Estudo da situação de uma organização em termos das suas potencialidades e vulnerabilidades (*Ibid.*).

**Análise SWOT** ‑ É uma técnica usada para fazer um diagnóstico estratégico de uma organização. A nível interno são diagnosticados os pontos fortes (*Strenghts*) e os pontos fracos (*Weakness*) e a nível externo são diagnosticadas as oportunidades (*Opportunities*) e as ameaças (*Threats*). Os fatores essenciais constituem a base para a definição da estratégia da organização (*Ibid.*).

**Ator não-estatal –** São todas as unidades coletivas de dimensão variável, internas e externas, que se constituem como entidades políticas, asseverando a sua identidade e os seus interesses no seio da comunidade internacional. (Treverton et al., 2018).

**Batalha Multi-Domínio** – É um conceito desenvolvido pelas Forças Armadas dos EUA para responder, essencialmente, ao desafio colocado por adversários sofisticados num ambiente em que todos os domínios serão contestados - terra, ar, mar, espaço, ciberespaço e espectro eletromagnético. (TRADOC, 2017)

**Capacidade Militar** - O conjunto de elementos que se articulam, de forma harmoniosa e complementar, e que contribuem para a realização de um conjunto de tarefas operacionais,

ou efeitos que são necessários atingir, englobando componentes da doutrina, da organização, do treino, da logística, da liderança, do pessoal, das infraestruturas e da interoperabilidade, entre outras (MDN, 2014).

**Centro de Gravidade** - É a fonte de poder que fornece força moral ou física, liberdade de ação, ou vontade de agir, a um sistema, ator estatal ou não-estatal (Couto, 1998).

**Conflito híbrido** é uma situação em que as partes se abstêm do uso manifesto das Forças Armadas, contando com uma combinação de intimidação militar, com a exploração de vulnerabilidades económicas e políticas, e por meios diplomáticos ou tecnológicos para perseguir seus objetivos (Hybrid CoE, s.d.).

**Desafios estratégicos** - São os objetivos da estratégia para combater as ameaças híbridas. (MCDC, 2019a).

**Efeitos não lineares** - Refere-se a efeitos imprevistos de ataques híbridos que não resultam de uma ação direta. São o resultado de interações sinérgicas nos quais o todo é maior que a soma das partes. Os efeitos não lineares nem sempre podem ser previstos (MCDC, 2019a).

**Estratégia combate às ameaças híbridas (CAH) -** Consiste num conjunto articulado de ações transversais a toda a sociedade, que visam prevenir, deter ou dissuadir e responder às ameaças híbridas. A estratégia CAH, assenta numa resposta conjunta e integrada em termos nacionais (civil-militar) e internacionais, onde se privilegia o conhecimento situacional, a prontidão e a resiliência, numa dinâmica de segurança cooperativa (MCDC 2019a).

**Estratégia Estrutural** - Tem por objetivo a deteção e análise das vulnerabilidades (ou pontos fracos) e das potencialidades das estruturas existentes, com vista à definição das medidas mais adequadas, incluindo a criação de novas estruturas, que conduzam à eliminação ou atenuação das vulnerabilidades, a um reforço de potencialidades e, em última análise, a um melhor rendimento dos meios e recursos (Couto, 1988).

**Estratégia Genética -** Tem por objetivo a invenção, construção ou obtenção de novos meios, a colocar à disposição da estratégia operacional, no momento adequado, e que sirvam o conceito estratégico adotado (Couto, 1988).

**Estratégia Operacional** - Trata da conceção e execução da manobra estratégica com as possibilidades proporcionadas pelas táticas e técnicas do domínio considerado, mas também orientar a evolução daquelas de forma a adaptá-las às necessidades da estratégia (Couto, 1988).

**Funções críticas** - São funções ou sistemas distribuídos no espectro político, militar, económico, social, informacional e infraestruturas (PMESII); cuja descontinuação pode levar à interrupção dos serviços dos quais um sistema operacional depende. As funções críticas podem ser divididas em indivíduos ou organizações, infraestruturas (*e.g.* redes de energia nacionais críticas) e processos (*e.g.* legais, jurisdicionais, técnicos, políticos) (MCDC, 2019a).

**Guerra Híbrida -** Consiste no desafio apresentado pela crescente complexidade do conflito armado, em que os adversários podem combinar diferentes tipos de guerra com meios não militares para neutralizar o poder militar convencional (MCDC, 2019).

**Grey Zone** – refere-se às interações competitivas entre atores estatais e não estatais conduzidas na "zona cinzenta" do conflito, em que as operações podem não atravessar claramente o limiar da guerra. Isso pode ser devido à ambiguidade do direito internacional, ambiguidade de ações e imputação, ou porque o impacto das atividades não justifica uma resposta (Kapusta, 2015).

***Hard Power*** **-** É quando se emprega a coação, seja através do emprego da força militar ou económica (Nye Jr, 2008).

**Interagências** – São ações efetuadas por elementos de várias organizações governamentais, desde o nível nacional ao local, podendo alargar-se a outras agências internacionais, intergovernamentais, não-governamentais e de âmbito privado (TRADOC, 2017).

**Instrumento de Poder Militar –** É a expressão do poder nacional constituída de meios predominantemente militares de que dispõe a nação para, sob a direção do Estado, promover, pela dissuasão ou pelo uso da força militar, a conquista ou manutenção dos objetivos nacionais (Ministério da Defesa, s.d.).

***Opportunities*** (Oportunidades) - São os caminhos ou espaço para crescimento, que podem ser desenvolvidos para suprir necessidades. Em outras palavras, são aspetos externos positivos, que quando utilizado em conjunto com o que a organização tem de positivo internamente, podem ser transformados em oportunidades de melhoria (Dias, Varela, & Costa).

**Planeamento de Defesa Militar** – Processo sistémico de planeamento, integrado num esforço agregado, que incorpora as alterações do enquadramento legislativo, e da metodologia do ciclo de planeamento da OTAN, em articulação com o processo de

desenvolvimento de capacidades da UE, designadamente, baseado em capacidades militares (MDN, 2014).

***Pooling & Sharing*** **-** É um conceito da UE que diz respeito a projetos e iniciativas colaborativas, lideradas por países membros da UE, tendo em vista o incremento da colaboração e partilha de meios e capacidades militares (Comissão Europeia, 2016).

**Resiliência** - É a capacidade que a sociedade tem para resistir e recuperar com facilidade de choques que causem grande impacto, como é o caso de calamidades, falhas de infraestruturas críticas ou um ataque armado, utilizando os meios da Proteção civil e a Capacidade Militar (OTAN, 2020). A resiliência deve ser vista como a capacidade de recuperar da adversidade, implicando um processo de crescimento e em enfrentar as situações adversas. Neste sentido, resiliência significa mais do que sobreviver ou resolver situações problemáticas, implicando a capacidade de resolver, recuperar e prosseguir perante as adversidades (Luthar et al., 2000).

***Smart power*** **-** É a combinação de *hard power* com o *soft power*, onde não se descarta o uso da força militar quando necessário para que os objetivos sejam alcançados (Nye Jr, 2008).

***Soft Power*** **-** É a capacidade de um ator das relações internacionais obter o que deseja através do poder da atração e não da coação (Nye Jr, 2008).

***Strengths*** (Potencialidades) - São os pontos positivos, aspetos em que a organização se destaca internamente e que constituem uma vantagem face a outras organizações, (Dias et al., 2013).

***Threats*** (Ameaças) - São os imprevistos ou potenciais problemas que podem ser considerados como fatores de risco, desafios que já são reconhecidos ou que surgem como obstáculos novos. Em outras palavras, aspetos externos que representam riscos para a organização (*Ibid*).

***Weaknesses*** (Vulnerabilidades) - São os pontos negativos, desvantagens da organização em relação a concorrentes, principais erros já cometidos, o que já foi reconhecido com um problema ou erro. (*Ibid*).

## Apêndice B - Modelo de análise

**Quadro 3 - Modelo de análise**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **TEMA** | **A PREVENÇÃO E O COMBATE ÀS AMEAÇAS HÍBRIDAS. IMPACTO PARA AS FORÇAS ARMADAS PORTUGUESAS** | | | | | | |
| **Objetivo Geral** | Propor linhas de ação para o Combate às Ameaças Híbridas ao nível das FFAA. | | | | | | |
| **Objetivos Específicos** | **Questão Central** | Quais são as principais linhas de ação para o Combate às Ameaças Híbridas ao nível das FFAA? | | | | | |
| | **Questões Derivadas** | **Conceito** | **Dimensões** | **Variáveis** | **Indicadores** | **Técnicas de recolha** | **Ferramentas** |
| **OE1** Analisar o papel do Instrumento Militar no Combate às Ameaças Híbridas. | **QD1** Qual é papel do Instrumento de Poder Militar no CAH? | O CAH ao nível das FFAA | Instrumentos de poder Rússia: Militar, Político, Económico, Civil e Informacional (MPECI) | Funções críticas Ucrânia: Político, Militar, Social Economico, Infraestruturas, Informacional – Ciberespaço, Legal (PMSEII-CL) | Instrumento de Poder Militar<br>Meios e efeitos das AH (Rússia/Ucrânia)<br>Componentes da Estratégia CAH | • Análise documental<br>• Entrevistas semiestruturadas (pergunta 1 e 2) | • Excel<br>• *Power Business Intelligence*<br>• Conceito analítico MCDC |
| **OE2** Analisar as linhas de orientação Estratégica da UE e da OTAN para o CAH. | **QD2** Quais são as principais ameaças e oportunidades decorrentes das LOE da UE e da OTAN para o CAH? | | Linhas de orientação Estratégia da UE e da OTAN para o CAH | Conhecimento situacional<br>Resiliência<br>Prevenção e resposta a crises<br>Apoio e Cooperação Internacional | Ameaças Oportunidades | • Análise documental<br>• Entrevistas semiestruturadas (pergunta 3) | • SWOT |
| **OE3** Analisar as capacidades das Forças Armadas Portuguesas para o CAH | **QD3** Quais são as principais potencialidades e vulnerabilidades das FFAA para o CAH? | | Capacidades das FFAA para o CAH | Conhecimento situacional<br>Resiliência<br>Prevenção e resposta a crises<br>Apoio e Cooperação Internacional | Vulnerabilidades Potencialidades | • Análise documental<br>• Entrevistas semiestruturadas (pergunta 4) | • SWOT |

## Apêndice C - Guião das entrevistas e lista de entrevistados

### Entrevista em Guião

### Cabeçalho do guião

Excelentíssimo Senhor,

Chamo-me Artur José Figueiredo Mariano Alves, Capitão-de-mar-e-guerra Fuzileiro, e sou Auditor do Curso de Promoção a Oficial-General (CPOG) 2019/2020, que decorre no Instituto Universitário Militar (IUM). Durante este curso, os auditores elaboram Trabalhos de Investigação Individual (TII), em que se abordam questões relevantes e importantes para o futuro das Forças Armadas (FFAA) Portuguesas. Neste âmbito, encontro-me a realizar uma investigação com o seguinte enunciado: "**A prevenção e o Combate às Ameaças Híbridas: Impacto para as Forças Armadas Portuguesas**".

O objetivo geral deste TII consiste em propor as principais linhas de ação para o Combate às Ameaças Híbridas (CAH) ao nível das FFAA. O projeto de investigação está assente em três áreas principais: (i) analisar o papel do Instrumento de Poder Militar; (ii) analisar as principais ameaças e oportunidades decorrentes das linhas de orientação Estratégica da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN) para o Combate às Ameaças Híbridas; (iii) e analisar as principais potencialidades e vulnerabilidades das FFAA para o CAH.

A resposta a esta necessidade passa pela metodologia identificada que segue uma estratégia de investigação qualitativa através da pesquisa e análise documental de referência e com recurso a entrevistas semiestruturadas, que são efetuadas a especialistas conhecedores do tema ou que tenham responsabilidades na área do planeamento militar. Os entrevistados são de áreas diversificadas e transversais (MDN, EMGFA, IUM, diplomatas, militares estrangeiros e militares dos três Ramos das FFAA).

Solicito a sua autorização para gravar a presente entrevista e para referir no trabalho o conteúdo da mesma associado ao seu nome. Caso não seja essa a sua vontade, garanto a confidencialidade do entrevistado e tratarei a informação recolhida de forma anónima. Estimo que a entrevista dure um máximo de 40 minutos.

O seu conhecimento e experiência são essenciais para a qualidade e relevância deste trabalho, pelo que, agradeço mais uma vez a sua disponibilidade para a prossecução da presente investigação.

## Caracterização do entrevistado

Entrevista n.º _____
Nome do entrevistado: _____
Ramo: _____Posto_____Classe:_____
Cargo: _____
Local: _____Data: _____

## Guião da entrevista

| ID. | DIMENSÃO | TEMPORAL |
|---|---|---|
| A | O papel do Instrumento Militar no CAH | 2012 a 2019 |

Síntese introdutória pergunta1.
As Ameaças Híbridas consistem no uso sincronizado de múltiplos instrumentos de poder, aplicados de forma a explorar vulnerabilidades específicas em todo o espectro das funções críticas da sociedade, para obter efeitos sinérgicos que permitam alcançar objetivos políticos.
O modelo que se apresenta na Figura 1, permite visualizar como um ator estatal ou não estatal pode usar uma ampla gama de instrumentos de poder, seja Militar, Político, Económico, Civil e/ou Informacional (MPECI), de forma a explorar vulnerabilidades (funções críticas) de um Estado ao nível Político, Militar, Económico, Social, Informacional e Infraestruturas (PMESII).

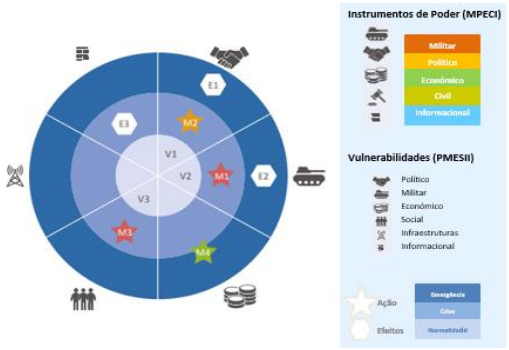


Figura 1- Estrutura analítica AH
Fonte: Adaptado MCDC (2019)

**Pergunta 1. Durante o conflito híbrido da Rússia/Ucrânia, quais foram os meios, ações e efeitos usados pela Rússia nas funções críticas da Ucrânia de forma a explorarem as respetivas vulnerabilidades e alcançarem os seus objetivos políticos?**

Síntese introdutória pergunta 2.
No que diz respeito à estratégia para CAH, há instituições que estudam este fenómeno e defendem que a mesma deverá ser projetada e implementada com base nas seguintes componentes: Detetar; deter ou dissuadir e responder (Fig. 2).

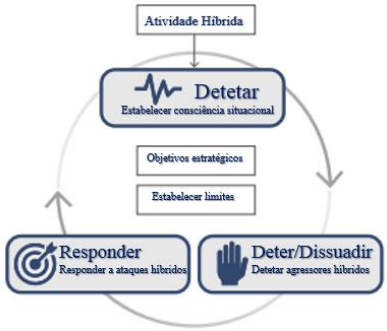


Figura 2- Estratégia CAH
Fonte: Adaptado MCDC (2019).

**Pergunta 2. Tendo em conta que a base de uma estratégia de CAH deve ser suportada nestas três componentes (Detetar, Deter/Dissuadir e Responder), na sua opinião, quais são os principais desafios que se colocam à Defesa neste contexto?**

| ID. | DIMENSÃO | TEMPORAL |
|---|---|---|
| B | Linhas de orientação Estratégica da UE e da OTAN PARA O CAH | Atualidade |

**Pergunta 3. Tendo por base as orientações estratégicas da UE e da OTAN 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?**

| ID. | DIMENSÃO | TEMPORAL |
|---|---|---|
| C | Capacidades da FFAA para o CAH | Atualidade até 2035 |

**Pergunta4. Tendo por base as orientações preconizadas no CEDN e no CEM e da realidade operacional atual, quais são as principais vulnerabilidades e potencialidades das FFAA para o CAH?**

## Entrevistados

| Cargo | Posto e Nome |
|---|---|
| Diretor Geral do Gabinete Nacional de Segurança | Contra-almirante António Gameiro Marques |
| Diretor-Coordenador do Estado-Maior do Exército | Major-general Paulo E. Maia Pereira |
| Subdiretor Geral de Política de Defesa Nacional no MDN | Brigadeiro-general Nuno Lemos Pires |
| Ex-Embaixador da UE na Ucrânia, Bielorrússia e Cabo Verde, Moçambique e na Macedónia | Embaixador José Manuel Pinto Teixeira |
| Auditor do CPOG, Ex-Diretor da Escola Comunicações e Sistemas de Informação da OTAN | Coronel Paulo Viegas Nunes |
| Ex-Diretor de Serviços do Centro de Dados da Defesa do MDN | Capitão-de-mar-e-guerra José Manuel Santos Coelho |
| Assessor de planeamento Estratégico de Defesa da DGPDN | Capitão-fragata Diogo Inácio da Rocha Guerreiro de Oliveira |
| *Military Representative Staff Officer* no Comité Militar da OTAN e UE | Tenente-coronel José Carlos Vicente Pereira |
| Assessor Técnico Coordenador do Projeto 1 em Angola- Divisão de Operações Especiais | Tenente-coronel Hugo Miguel Martinho Fernandes |
| Adjunto para área de Ensino do Exército e representante IUM para as ameaças híbridas | Major Lourenço Serrão |

# Apêndice D - Componentes da estratégia de CAH

**Quadro 4 - Medidas do PMSII para o CAH**

| | Político | Militar | Económico | Social | Infraestruturas | Informacional |
|---|---|---|---|---|---|---|
| Detetar | A exploração e o uso criativo de ferramentas não militares para atingir todas as áreas da sociedade, exige a criação de processos e métodos de inteligência de alerta visando proteger as vulnerabilidades críticas em toda a sociedade contra-ataques híbridos sincronizados provenientes de vários vetores, projetados intencionalmente para ficar abaixo dos limiares da deteção tradicional. Para o sucesso na sua deteção, é fulcral a necessária coordenação e partilha de informações a todos os níveis, em termos nacionais e internacionais. Como as formas e os meios potenciais utilizados nos ataques híbridos são difíceis (ou impossíveis) de prever, torna-se necessário abordagens totalmente novas para alertar contra as AH , baseados em indicadores e em métodos de monitorização utilizando as novas tecnologias. | | | | | |
| Deter | • Em termos preventivos, restringir ou proibir o financiamento estrangeiro de partidos políticos, organizações ou afiliados.<br>• Promover a confiança da sociedade nas Instituições.<br>• Os processos eleitorais devem ser protegidos.<br>• Todos os esforços devem ser amplamente sincronizados ao nível político e diplomático. | • As capacidades militares e a cooperação internacional no âmbito da defesa são vitais para a dissuasão tradicional (por negação e punição).<br>• A contribuição militar para a resiliência nacional é fundamental e deve ser considerado à luz das novas tecnologias híbridas, nomeadamente no ciberespaço.<br>• A resiliência da própria defesa contra as AH também é importante. | • Medidas económica preventivas credíveis contra as AH passam pela segurança e diversidade de recursos estratégicos.<br>• A consciência situacional sobre as AH e a anticorrupção é vital.<br>• Sistemas corruptos são amplamente explorados por atores híbridos. | • A exploração da divisão social e grupos de interesses especiais através do apoio e financiamento estrangeiros devem ser acautelados.<br>• A educação e formação pode melhorar a consciência situacional sobre as AH.<br>• Para maximizar a resiliência, a população deve estar ciente e envolvida. | • A resiliência exige medidas de proteção física, garantindo a segurança física, organizacional e das infraestruturas críticas e informacionais.<br>• Medidas não-físicas, incluem legislação, transparência financeira e regulamentação comercial. | • Um dos elementos centrais para combater as AH é comunicação estratégica, direcionada internamente, em relação à sociedade e externamente em relação aos agressores, e à comunidade internacional.<br>• Nesse contexto, de forma pró-ativa e transparente, a cooperação com os media (digital e tradicional) é crucial. |
| Responder | • Restrições para funcionários políticos ou titulares.<br>• Expulsão de diplomatas.<br>• Suspensão de participações ou retirada dos direitos de voto de em organizações internacionais. | • A ação militar deve ser calibrada para garantir proporcionalidade,<br>• Maximizar o potencial coercivo do instrumento militar.<br>• Contribuir para a resiliência, medidas dissuasão e prevenção. | • A eficácia das sanções económicas.<br>• Influência financeira.<br>• Congelamento de ativos. | • O estado de direito é uma das pedras angulares.<br>• Transparência e confiança da sociedade em instituições públicas | | • Apoiar a abertura e transparência aos Media com regras de confiança e acesso à informação.<br>• A Desinformação e as "*fake news*" podem ser combatidas por toda a sociedade. |

# Apêndice E - Análise de conteúdo das respostas

**Quadro 5 - Unidades de contexto e de registo da Pergunta 1**

| **Pergunta 1. Durante o conflito híbrido da Rússia/Ucrânia quais foram os meios (M) e os efeitos (E) usados pelos diferentes instrumentos de poder da Rússia, de forma a atingir as vulnerabilidades (V) nas funções críticas (PMESII) da Ucrânia?** | | |
|---|---|---|
| N.º | Unidade de Contexto | Unidade Registo |
| #1 | **"**Dependência ucraniana de gás russo (…) dívida ucraniana à Rússia (…) pressão diplomática (…) interferência política (…) espionagem (…) controle dos media (…) violação do espaço aéreo e mar territorial" | 1.3,1,6,1.8 1.9,1.10 1.18 |
| #2 | "Jogar no domínio cognitivo dependências do tempo da União Soviética (…) uso da identidade cultural (…) utilização das minorias russas na Ucrânia (…) campanhas de desinformação (…) exploração de vulnerabilidades sociais e políticas (…) exploração media (…) adesão às causas russas com criação de um clima de inevitabilidade (…) ataques cibernéticos (…) exercícios e coerção militar". | 1.3,1.4,1.7 1.12,1.13 1.14,1.5 1.18,1.19 1.20,1.17 |
| #3 | "Falta de resiliência das Instituições (…) sistema político (governo) frágil/ineficaz (…) dependência energética (…) meios e canais e informação e propaganda russos na Ucrânia (…) inexistência de um sistema/mecanismo de defesa territorial funcional e eficaz (…) cibersegurança das redes de comunicações fraca (…) Sistema de C2 das FFAA (…) herança cultural (grande percentagem de russos a viver no território) (…) criação e apoio de grupos paramilitares (…) paralisação das negociações em novembro/dezembro/2014 (…) paralisia institucional (…) isolamento do Governo, sem capacidade para comunicar e articular um plano de gestão da crise (…) anexação territorial da Crimeia – incluindo Base Naval e frota (…) desacreditação dos líderes políticos (…) Forças Armadas mal preparadas (…) comunidade internacional alheia, explorando a zona cinzenta (…) ambiguidades do Direito internacional" | 1.3,1.4 1.5,1.6 1.7,1.8 1.10,1.11 1.12,1.15 1.19,1.20 |
| #4 | "FFAA mal preparadas para enfrentar ataques não cinéticos (…) dependência económica e financeira (…) ataques cibernéticos às redes do governo e aos Sistemas C4ISR (…) operações de Informação (…) acordo UE-Ucrânia -pressão diplomática (…) obtenção de superioridade de informação russa (…) criação dos caos e perceção de ineficácia governativa (…) operações de Inteligência, espionagem e clandestinas (…) exercícios e coerção militar" | 1.1, 1.2 1.4, 1.5 1.8,1.9 1.10,1.15 1.19,1.7 |
| #5 | "Resiliência das Instituições (…) sistema político/governo frágil/ineficaz (…) exploração dos meios informacionais russos (…) propaganda e desinformação (…) ciberataque, cibermanipulação e cibercrime (…) inexistência de um sistema/mecanismo de defesa territorial funcional e eficaz (…) população de etnia Russa (…) controle do gás (…) criação e apoio de grupos paramilitares (…) influencia perceção da população local (…) criação dos caos e perceção de ineficácia governativa (…) sabotagem e controlo de infraestruturas críticas". | 1.3,1.4 1.8 1.10,1.11 1.12,1.13 1.14,1.15 1.17 |
| #6 | "Milícias treinadas (…) contrainformação (…) interrupção do abastecimento de Energia Elétrica e Gás (…) Informacional -(permeabilidade dos media à influência russa (…) capital Social, impregnação da cultura russa na sociedade ucraniana (…) Influência nas empresas (…) divergências na opinião pública (…) influência nas eleições (…) ataques cibernéticos às Infraestruturas Críticas, (…)espionagem industrial e política (…) ciberataques " | 1.3,1.5 1.8,1.9 1.11,1.12 1.14,1.18 1.19,1.20 |
| #7 | "Formação de milícias, *cossacks*, voluntários, formação com meios militares (…) população maioria de etnia russa (…) proliferação de meios de comunicação e propaganda russos no leste da Causar (…) legitimar e apoiar os separatistas (…) encorajamento das tensões interétnicas (polacos, judeus, húngaros, russos) (…) provocar deserções no exército ucraniano (…) denegrir a imagem das autoridades ucranianas demonstrando a sua incapacidade, enquanto afetava a moral nacional (…) agitação social (…) violação do espaço aéreo (…) recurso diáspora influenciar". | 1.3,1.4 1.6 1.11,1.12 1.13,1.14 1.15 |
| #8 | "Serviços de informação ucranianos infiltrados por agentes russos (…) frágil situação em que se encontravam os militares da Ucrânia (…) controle dos media pelos grupos oligárquicos, com fortes ligações à Rússia, que permitiu o lançamento da campanha de propaganda (…) fraca/inexistente proteção dos sistemas SCADA (*Supervisory* | 1.1,1.2 1.4,1.5 1.7,1.9 1.13,1.14 |

| | | |
|---|---|---|
| | *Control and Data Acquisition*) que permitiu o ataque em 23 de dezembro de 2015, à companhia de distribuição elétrica Kyivoblenergo (…) exemplos de media ucranianos controlados por Moscovo e que ainda hoje persistem (…) utilização da língua russa em larga escala por parte dos media (…) ataque a infraestrutura criticas (…) grande agitação social, terreno fértil para a campanha de propaganda de desinformação nas redes sociais e nos media (…) ataques contra infraestruturas telefónicas, bloqueando os telefones do parlamento". | 1.17,1.18 1.19 |
| #9 | "Controle do suprimento de gás ucraniano (…) pressão associada à dívida da Ucrânia à Rússia (…) Ciber (espionagem, ataques e manipulação) (…) *proxies*: Paramilitares e milícias (…) operações e exercícios militares junto à fronteira, coerção militar (…) diáspora de ascendência russa na Ucrânia (…) exploração corrupção (…) promover instabilidade social (…) operações clandestinas e de inteligência (…) sanções diplomáticas e económicas (…) desacreditação líderes, interferência política (…) guerra eletrónica (…) exploração de imigração propositada (…) controle dos Media e interferência (…) desinformação e campanhas de propaganda". | 1.1,1.2 1.3,1.4,1.6 1.5,1.7 1.8,1.9 1.10,1.11 1.12,1.14 1.15,1.16 1.18, 1.19 |
| #10 | "controlo Infraestruturas críticas (…) pressão diplomática (…) violação do espaço territorial (…) operações Ciberdefesa (…) exploração Clivagens sociais e língua e forte cultura russa (…) instabilidade social (…) controle dos Media e interferência (…) exploração limites legais (…) Desinformação (…) treino de Milícias (…) Interrupção do abastecimento da energia elétrica e do gás (…) exploração da imigração". | 1.4,1.5 1.6,1.9 1.10 1.13,1.16 1.17,1,18 1.19,1.20 |

**Quadro 6 - Análise de conteúdo das respostas à Pergunta 1**

**Pergunta 1. Durante o conflito híbrido da Rússia/Ucrânia quais foram os meios (M) usados pelos diferentes instrumentos de poder da Rússia, de forma a atingir as vulnerabilidades (V) nas funções críticas (PMESII) da Ucrânia e alcançarem os seus objetivos políticos?**

| Categoria | Unidade de Registo | Entrevistados | | | | | | | | | | Unidades Enumeração | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | | % |
| Político | 1.1 Operações/Informações | | | | x | | | | x | x | | 3 | 30% |
| | 1.2 Operações/clandestinas | | | | x | | | | x | x | | 3 | 30% |
| | 1.3 Desacreditação/líderes/interf./política | x | x | x | | x | x | x | | x | | 7 | 70% |
| Militar | 1.4 Desinformação/campanhas/propaganda | | x | x | x | x | | x | x | | x | 7 | 70% |
| | 1.5 Operações/Ciberdefesa | | x | x | x | | x | | x | x | x | 7 | 70% |
| | 1.6 Violação/Espaço/Territorial | x | | x | | | | x | | x | x | 5 | 50% |
| | 1.7 Operações/Exercícios e coerção Militar | | x | x | x | x | | | x | x | | 6 | 60% |
| Económico | 1.8 Dependência/Investimento/Rússia | x | | x | x | x | x | | | x | | 6 | 60% |
| | 1.9 Espionagem/Industrial/Minar/Economia | x | | | x | | x | | x | | x | 5 | 50% |
| | 1.10 Sanções/diplomáticas/económicas | x | | x | x | x | | | | x | x | 6 | 60% |
| Social | 1.11 Proxies/Paramilitares/Milícias | | | x | | x | x | x | | x | | 5 | 50% |
| | 1.12 Recurso/diáspora/influenciar | | x | x | | x | x | x | | x | x | 7 | 70% |
| | 1.13 Exploração/clivagens/sociais | | x | | | x | | x | x | | x | 5 | 50% |
| | 1.14 Promover/instabilidade/social | | x | | | x | x | x | x | x | | 6 | 60% |
| | 1.15 Exploração/corrupção/Adm/Pública | | | x | x | x | | x | | x | | 5 | 50% |
| | 1.16 Exploração/imigração | | | | | | | | | x | x | 2 | 20% |
| Infraest. | 1.17 Sabotagens/controlo/Infraest/críticas | | x | | | x | | | x | | x | 4 | 40% |
| Inform. | 1.18 Controle/Media/interferência | x | x | | | | x | | x | x | x | 6 | 50% |
| Ciber | 1.19 Ciber ataques/espionagem/manipulação | | x | x | x | | x | | x | x | x | 7 | 70% |
| Legal | 1.20 Exploração/ambiguidades/limites/ legais | | x | x | | | x | | | | x | 4 | 40% |

**Quadro 7 - Unidades de contexto e de registo da Pergunta 2**

**Pergunta 2. Tendo em conta que a base de uma estratégia de CAH deve ser suportada nestas três componentes (Detetar, Deter/Dissuadir e Responder), na sua opinião, quais são os principais desafios que se colocam ao Instrumento de Poder Militar neste contexto?**

| N.º | Unidade de Contexto | Unidade de Registo |
|---|---|---|
| #1 | "O incremento na complexidade e no alcance, nomeadamente através dos ataques cibernéticos, que visam não só os clássicos problemas da cibersegurança, mas têm cada vez mais propósitos políticos e com alvos bem definidos e fazem-no através da manipulação do social media mais precisamente através do ciberespaço (…) os países mais vulneráveis são os que vivem em estado democrático porque vivem em sociedades abertas em que o consumo generalizado leva à sua permeabilidade (…).ao chamado "*information gathering*" em que se permite que entidades controlem de forma ativa a vida dos seus cidadãos (…) por outro lado, a massificação digital e interconectividade é terreno fértil para as guerras das perceções e para que se crie uma "bolha da verdade" aproveitada por interesses ocultos (…) Esta atuação em zona cinzenta dificulta a sua deteção e atribuição, o que lhes permite uma atuação continua sem a devida responsabilização e punição (…) para se entender o "Híbrido" tem de se entender o conceito de influência Híbrida, que é uma influência premeditada consciente exercida por um ou mais atores utilizando métodos diversos para alcançar um determinado objetivo. As AH não é mais do que a personificação dessa influência (…) as AH surgem nas diferentes funções críticas de uma sociedade que requerem uma resposta e aproximação concertada "*Whole of Society*" (…) Portugal não está preparado par isso porque não temos uma estrutura mandatada para ter esta perspetiva transversal à sociedade. Por isso é recomendável um a estratégia de seguir o que se está a fazer neste âmbito na UE e na OTAN, adaptando a doutrina e as boas práticas à nossa realidade e procurando total interoperabilidade e coordenação com essas organizações (…) Identificar entidades no Estado que podem assumir esta responsabilidade, identificando-se desde logo de início o que existe nas diferentes áreas governativas e o que está a ser feito em termos de coordenação e ligação com a UE *Híbrid Fusion Cell*, com O Hybrid CoE e com o "*Rapid Alert System Sharing and desinformation campaign*". Finalmente, esta entidade deve gerir e coordenar a resposta nacional às AH sempre em articulação com a UE e a NATO (…) As AH para serem tratadas com eficácia, não deve ser tratado de forma vertical, ou seja nenhuma área governativa deve chamar a si a responsabilidade nem apodera-se desta responsabilidade, já que é um assunto transversal em que todas as áreas ou vetores do Estado devem analisar o que podem fazer para contribuir para o CAH e estarem prontos e resilientes para esse efeito (…) Relativamente ao papel do instrumento Militar, neste âmbito é apenas mais um dos Instrumentos de poder do Estado, conforme consta nas 22 medidas da UE é apenas um participante ativo, mas que só deve ser utilizado adequadamente, proporcionalmente e quando for necessário. e para que prepara as respostas, saber que tem essa possibilidade". | 2.1,2.2<br>2.8<br><br><br><br><br><br>2.8<br><br><br><br><br><br>2.1<br><br><br><br><br>2.1<br><br><br><br><br><br>2.1,<br>2.3,2.4,<br>2.7,2.8<br><br><br><br>2.2,2.3<br><br><br><br><br><br>2.6, 2.7 |
| #2 | "O primeiro passo para responder AH é compreender, identificar modus operandi da sua essência (…) Mudar a postura da defesa e edificar capacidades para atuar contra estas ameaças (…) Planeamento integrado. Conjunto e combinado e articulação interagências (…) O desafio principal é mais uma questão de resiliência de toda a sociedade do que do governo ou do poder militar, requerem uma visão holística para a governação da resposta a estas ameaças e que envolvem as estruturas do Estado, mas também a sociedade no seu todo. O CAH deve ser feito em estreita coordenação e cooperação com os nossos Aliados, deve ter uma resposta transnacional". | 2.3<br><br>2.5<br>2.4,2.5<br>2.2,2.6<br>2.7,2.8 |
| #3 | "Estratégia de CAH deve basear-se em três componentes, detetar, dissuadir e responder (…) O CAH requer também um planeamento orientado para a dinâmica transversal dos conflitos modernos (natureza híbrida) (…) Só quem dispõe de doutrina interagência e de um processo de planeamento conjunto e combinado, ajustado a este tipo de conflitos, poderá desenvolver um CONOPS e atuar de forma eficiente e eficaz". | 2.1<br><br>2.3,2.4<br><br>2.5 |
| #4 | "CAH deve-se basear em três funções fundamentais – deteção, dissuasão e defesa (…) A cooperação com os outros elementos de poder do Estado e a cooperação internacional com a UE e a OTAN é fundamental (…) As AH para serem tratadas com eficácia, não deve ser tratado de forma vertical". | 2.1, 2.<br>2.3,2.6,<br>2.7<br>2,8 |
| #5 | "A legislação e a partilha de informações são fundamentais para a implementação de uma estratégia nacional" (…) a capacidade de deteção é fundamental e devem ser | 2.1,2.2<br>2.3,2.6 |

| | | |
|---|---|---|
| | responsabilidade de toda a Sociedade (…) É fundamental a criação de uma efetiva capacidade de Operações de Informação e Comunicação Estratégica efetiva". | 2.8<br>2.5 |
| #6 | "O CAH deve basear-se na deteção, dissuasão e resposta efetiva se necessário (…) Deve existir uma entidade supranacional para coordenar o CAH (…) A edução, o treino, a legislação e a partilha de informações são condições essenciais para que um Estado possa assegurar as restantes componentes (…) Assegurar a resiliência militar e do Estado, garantindo os serviços críticos do governo, a necessária resiliência, o fornecimento de energia, o apoio às Forças de Segurança face à instabilidade social exagerada, a capacidade de lidar com movimentos descontrolados de pessoas, a capacidade de lidar com baixas em massa, e garantir também sistemas de comunicação e de transporte resilientes". | 2.1<br>2.8<br><br><br><br><br><br><br>2.5 |
| #7 | "Detetar, dissuadir, Responder (no quadro de identificação e respostas, há uma notável diferença entre as respostas adequadas consoante a fase de atuação / maturação das ameaças híbridas) (…) Aumentar a resiliência da Instituição e contribuir para a resiliência da sociedade (…) O CAH deve ser feito em estreita coordenação e cooperação com os nossos Aliados, deve ter uma resposta transnacional". | 2.1<br><br><br><br>2.2,2.3<br>2.4,2.7 |
| #8 | "Penso que o maior desafio que se coloca, é desde logo, a identificação da ameaça (…) A Ameaça Híbrida, desafia os métodos tradicionais baseados em indicadores, para desencadear alertas precoces nos casos das ameaças convencionais, intenção hostil ou ações que levam a hostilidade (…) Assim uma vez que os modos e os meios usados na Guerra Híbrida são dificílimos de prever, é importantíssimo desenvolver novos métodos de informação preditiva (…) Outro grande desafio é a aplicação da capacidade de dissuasão convencional que terá de ser implementada negando o acesso aos domínios críticos do Estado e contribuir para a sua resiliência". | 2.1<br><br><br><br><br>2.2<br><br>2.6 |
| #9 | "Estas Ameaças devem ter uma aproximação e holística para a governação da resposta a estas ameaças e que envolvem as estruturas do Estado, mas também a sociedade no seu todo (…) Resiliência é a palavra chave para o CAH (…) A estratégia de CAH ao nível militar deve passar pelo seu contributo para a deteção, dissuasão e eventualmente estarem preparados para responder de forma mais cinética". | 2.2, 2,8<br><br>2.2<br><br>2.1 |
| #10 | "Conduzir operações credíveis de negação, no âmbito da defesa aérea, naval e terrestre, inclusive nos novos domínios do espaço e do ciberespaço (…) Incrementar a resiliência da componente militar da defesa nacional, mantendo a capacidade de deteção e dissuasão convencional (…) Contribuir para a resiliência nacional, nomeadamente através da deteção antecipada de ameaças híbridas, da dissuasão contra agressores híbridos e da resposta a ataques mais cinéticos, edificando e consolidando capacidade neste âmbito (…) Coordenação entre as FFAA e os outros atores (públicos e privados) que contribuem para a resposta nacional a ameaças híbridas, desde Sistema de Informações da República Portuguesa, Forças e Serviços de Segurança, Autoridade Nacional de Emergência e Proteção Civil, Sistema Nacional de Saúde e Centro Nacional de Cibersegurança, até ao setor privado e às universidades (…) Articular estratégias e modelos de atuação com as organizações internacionais, nomeadamente com a OTAN e com a UE (…) Adaptar, edificar e consolidar capacidades, nos domínios genético, estrutural e operacional (…) Apoiar países africanos da CPLP a melhorar a sua resiliência face às AhH, sobretudo na sua componente de segurança e defesa, que é fundamental para enfrentar ameaças híbridas, nomeadamente onde existem interesses fundamentais para a resiliência nacional. | 2.1<br><br>2.1, 2.2<br><br>2.2<br><br>2.5<br><br>2.2,2.3<br>2.4,2.8<br><br>2.6,2.7<br><br>2.5<br><br>2.6 |

**Quadro 8 - Análise de conteúdo das respostas à Pergunta 2**

| **Pergunta 2. Tendo em conta que a base de uma estratégia de CAH deve ser suportada nestas três componentes (Detetar, Deter/Dissuadir e Responder), na sua opinião, quais são os principais desafios que se colocam ao Instrumento de Poder Militar neste contexto?** | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Categoria | Unidade de Registo | Entrevistados | | | | | | | | | | Unidades Enumeração | % | |
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | | |
| Desafios do Poder Militar face às Ameaças Híbridas | 2.1 Contribuir e melhorar a deteção, detenção/dissuasão e resposta às AH. | x | | x | x | x | x | x | x | x | x | 9 | 90% | |
| | 2.2 Assegurar a resiliência da Defesa Militar e contribuir para a resiliência nacional. | x | | | | x | | x | x | x | x | 6 | 60% | |
| | 2.3 Coordenação entre o uso da força e as outras alavancas de poder do governo e da sociedade. | x | x | x | x | x | | | | | x | 6 | 60% | |
| | 2.4 Melhorar a coordenação e cooperação interagências e a partilha de informações ao nível nacional e internacional. | x | x | x | | | | x | | | x | 5 | 50% | |
| | 2.5 Edificar/consolidar capacidades (DOMTLPII) ao nível estrutural, genético e operacional para o CAH. | | x | x | | | x | | | | x | 4 | 40% | |
| | 2.6 Contribuir para a resiliência de países Aliados e amigos, através da participação em operações de defesa coletiva e de segurança cooperativa. | x | x | | x | x | | | x | | x | 6 | 60% | |
| | 2.7 Alinhar a atuação militar com as estratégias das OI no CAH (OTAN, UE). | | x | | x | | | x | | | x | 4 | 40% | |
| | 2.8 Articular uma resposta integrada e transversal a toda a sociedade e em vários domínios. | x | x | | x | x | x | | | x | x | 7 | 70% | |

**Quadro 9 - Análise de conteúdo das respostas à Pergunta 3**

| **Pergunta 3. Tendo por base as orientações estratégicas da UE e da OTAN 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?** | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cat. | Unidade de Registo | Entrevistados | | | | | | | | | | Unidades Enumeração | % |
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | |
| AMEAÇAS (A) | 3.1 Aumento da instabilidade geopolítica, que potencia vagas de refugiados e fluxos migratórios ilegais. | x | | x | x | x | x | x | x | x | x | 9 | 90% |
| | 3.2 Ataques cibernéticos (espionagem, crime e a manipulação). | x | x | x | | x | x | x | x | x | x | 9 | 90% |
| | 3.3 Desinformação/campanhas de propaganda através de meios noticiosos, redes sociais, disseminando notícias falsas. | x | x | x | x | x | | x | | x | x | 8 | 80% |
| | 3.4 Violação do Espaço Territorial e da área de jurisdição nacional. | x | | x | | | | x | | | x | 4 | 40% |
| | 3.5 Deteção e imputação das AH. | x | x | x | | x | x | | x | x | x | 8 | 80% |
| | 3.6 Espionagem e fugas de informação estratégicas. | x | | | x | x | | | x | | | 4 | 40% |
| | 3.7 Ataque artigo 5º a um país da UE ou da OTAN (incluindo ciberataque). | x | x | | x | | | x | | | x | 5 | 50% |
| | 3.8 Exploração de limites legais, ambiguidades e lacunas do Direito Internacional. | | x | | x | | x | x | | | | 4 | 40% |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 3.9 A dimensão das tecnologias disruptivas emergentes, como o 5G e a Inteligência Artificial. | | x | | x | | | x | | x | | 4 | 40% |
| | 3.10 Disputas pelas fronteiras marítimas, nomeadamente no quadro da extensão das plataformas continentais. | x | | | | x | x | | | | | 3 | 30% |
| | 3.11 Ameaças transnacionais (terrorismo, pirataria, criminalidade organizada, proliferação de armamento, exploração ilegal de recursos), catástrofes naturais, e ambientais, pandemias e outros riscos sanitários. | x | x | | x | x | x | x | x | x | x | 9 | 90% |
| OPORTUNIDADES (O) | 3.1 Cooperação e partilha conhecimento situacional e saber sobre as AH. | x | | x | x | x | | x | x | x | x | 9 | 80% |
| | 3.2 Apoio aumento da resiliência no ciberespaço. | x | | x | | x | x | x | x | x | x | 8 | 80% |
| | 3.3 Utilização de todo o potencial dos tratados de defesa coletiva da OTAN e UE. | x | x | x | x | x | | | | | x | 6 | 60% |
| | 3.4 Novas tecnologias emergentes como o 5G e a Inteligência Artificial e aproveitar a revolução digital. | x | x | x | | | | x | | | | 4 | 40% |
| | 3.5 Possibilidade de desenvolver capacidades da Defesa Militar para o CAH no âmbito das iniciativas da UE e OTAN. | | x | x | | x | x | x | x | x | x | 8 | 80% |
| | 3.6 Articulação com UE e OTAN no setor da saúde, energia e transportes. | | x | | | x | | | x | | | 3 | 30% |
| | 3.7 Exercícios da baseados em cenários de AH. | | x | | | | | x | | | x | 3 | 30% |
| | 3.8 *Security Networking*: cooperação, oportunidades e influência através do aumento das parcerias cooperação e interação entre países amigos aumentando a resiliência. | | | | x | | x | | | x | | 3 | 30% |
| | 3.9 Comunicação estratégica em cooperação e articulação com a UE e a OTAN e os Estados-Membros para AH. | x | | x | x | x | | | | x | x | 6 | 60% |
| | 3.10 Cooperação com a UE e OTAN para a resiliência na prevenção e resposta a crises face às AH | x | x | x | | x | x | | x | x | x | 8 | 80% |

**Quadro 10 - Análise de conteúdo das respostas à Pergunta 4**

| **Pergunta 4. Tendo por base as orientações preconizadas no CEDN e no CEM e da realidade operacional atual, quais são as principais vulnerabilidades e potencialidades das FFAA para o CAH?** | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Cat. | Unidade de Registo | Entrevistados | | | | | | | | | | Unidades Enumeração % | |
| | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | | |
| POTENCIALIDADES (P) | 4.1 Resiliência das FFAA e capacidade contribuir para resiliência nacional na resposta a crises (AH). | x | x | x | x | x | x | | x | x | x | 9 | 90% |
| | 4.2 Sólido quadro de valores e forte identidade institucional, associados à flexibilidade e adaptabilidade a mudanças da conjuntura externa. | | x | | x | | | x | | x | | 4 | 40% |
| | 4.3 Capacidade Proteção de força. | x | | x | | x | | | | | x | 4 | 40% |
| | 4.4 Qualidade dos sistemas de ensino, formação e treino e na área da investigação. | x | x | x | | | | x | | x | x | 6 | 60% |
| | 4.5 Capacidade de capacitação e treino, incluindo via da Cooperação no Domínio da Defesa (CDD) | x | | x | | | x | | | x | | 4 | 40% |
| | 4.6 Capacidade de relacionamento com atores institucionais em diversos níveis. | | x | | | x | | | x | | x | 4 | 40% |
| | 4.7. Capacidade de vigilância e controlo do espaço aéreo e marítimo, terrestre e do ciberespaço. | x | x | | x | | x | x | x | x | x | 8 | 80% |

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 4.8 Prontidão e capacidade de planeamento de operações com elevado grau de complexidade em resposta a crises. | x | | | x | | x | | | x | | 4 | 40% |
| | 4.9 Capacidade cooperação/ coordenação no campo da partilha de Informações Militares (OTAN e UE). | x | | x | x | x | | x | x | x | x | 8 | 80% |
| | 4.10 Experiência participação operações/exercícios internacionais, na defesa coletiva, segurança cooperativa e na CDD. | x | | x | | x | x | | | x | x | 6 | 60% |
| | 4.11 Potencialidades ao nível genético para o CAH, de acordo com as prioridades da LPM | | | | x | | x | | | x | | 3 | 30% |
| | 4.13 Capacidades diferenciadoras das FFAA para o CAH (*e.g.* Ciberdefesa, NRBQ, C4ISR). | x | x | x | | x | x | x | | x | x | 8 | 80% |
| VULNERABILIDADES (V) | 4.1 Falta de recurso humanos especializados com formação, treino e capacitação expertise no CAH. | x | | x | | x | x | | x | | x | 6 | 60% |
| | 4.2 Dificuldade na deteção e imputação das AH e sua compreensão. | x | | x | x | x | | x | x | x | x | 8 | 80% |
| | 4.3 Serviço de Informações Militares com limitações | x | | x | | x | | | | | x | 4 | 40% |
| | 4.4 Capacidades limitadas (*e.g.* comunicação estratégica, multi-domínio e C4ISR) e falta entidade coordenadora ao nível operacional - CAH. | | x | x | | x | | x | | x | x | 8 | 80% |
| | 4.5 Limitada interoperabilidade infraestruturas informáticas com interagências e OI. | | x | x | | | x | | x | | x | 5 | 50% |
| | 4.6 Inexistência de planeamento de operações multi-domínio e planeamento em conflitos híbridos. | x | | | x | | | | x | | | 3 | 30% |
| | 4.7 Redução do efetivo das FFAA | | x | | x | | | x | | | x | 4 | 40% |
| | 4.8 Mentalidade conservadora face às AH, que requer liderança ágeis e treinadas para cenários de complexidade/ ambiguidade, com "*mindset*" híbrido. | | x | | x | | x | | | | | 3 | 30% |
| | 4.9 Inexistência de um Comando de Ciberdefesa e capacidade limitada no ciberespaço e no espaço; | x | | x | x | x | | x | x | x | x | 8 | 80% |
| | 4.10 Restrições legais atuação das FFAA em alguns domínios para o CAH. | | x | | x | | x | | x | x | | 5 | 50% |
| | 4.11 Infraestruturas/estruturas pouco resilientes, dependência tecnológica. | x | | x | x | | x | x | x | x | x | 8 | 80% |

**Apêndice F - Visualização da Atividade Híbrida da Rússia na Ucrânia**

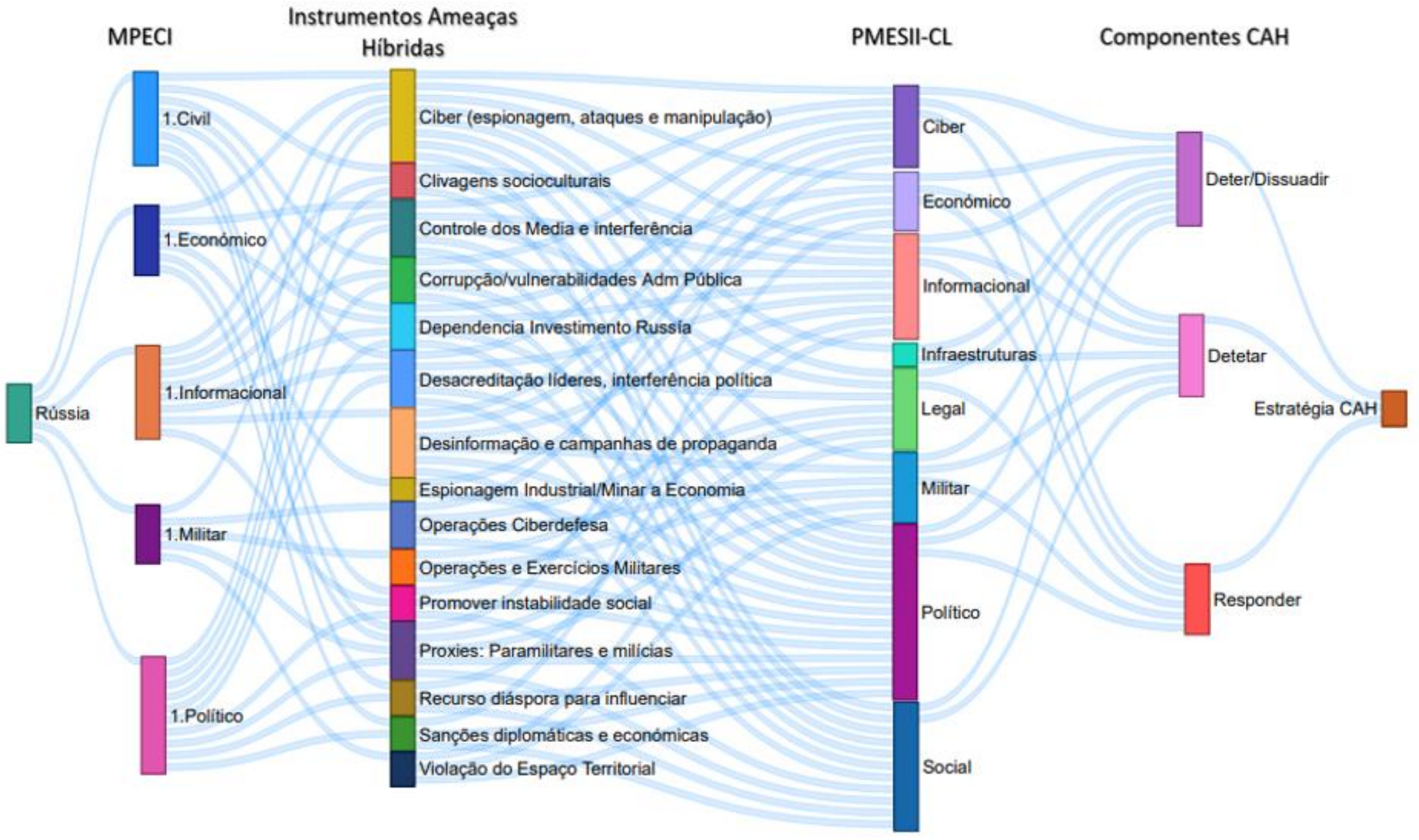


**Figura 23 - Visualização da atividade híbrida da Rússia na Ucrânia**

# Apêndice G - Linhas de Orientação Estratégica da UE e da OTAN

**Quadro 11 - Linhas de Orientação Estratégica da UE e da OTAN**

| Domínios prioritários | Medidas | Observações |
|---|---|---|
| Melhorar Consciência situacional | Estabelecimento do *Hybrid Fusion Cell* em 2017. | Localizado no *Intelligence and Situation Centre structure (INTCEN)* com a missão de processar e analisar as informações sobre AH, contra-espionagem e as ciberameaças; |
| | Reforço comunicação estratégica com os EM e Aliados. | Reconhecer que a desinformação constitui uma AH e definir uma série de ações (*e.g.* uma rede reforçada entre a Comissão, o Serviço Europeu para a Ação Externa e os Estados-Membros). |
| | Hybrid CoE. | Instituído em 2017, funciona como polo de competências e contribui para os esforços individuais e coletivos na luta contra AH, apoiado pelos países participantes por meio da investigação, formação, educação, exercícios e partilha de informação. |
| Reforçar a resiliência | Proteção e resiliência das infraestruturas críticas. | A Comissão elaborou um projeto de manual sobre os indicadores de vulnerabilidade e a resiliência das infraestruturas críticas da UE às AH, cujo objetivo será facilitar o alerta rápido logo no início dos ataques híbridos a infraestruturas críticas (*e.g.* energia, transportes, comunicações, armazenamento de dados, infraestruturas sensíveis, tecnologias de importância crítica, incluindo a inteligência artificial, a cibersegurança e as tecnologias com potenciais aplicações de dupla utilização. Segurança dos investimentos que facultem acesso a informações sensíveis ou a capacidade de controlar essas informações. |
| | Transportes e segurança da cadeia de abastecimento. | A fim de eliminar os obstáculos à mobilidade militar na UE, estudar as possibilidades de utilização civil e militar da rede transeuropeia, simplificando as formalidades aduaneiras para o transporte militar e resolver os problemas de ordem regulamentar e processual relacionados com o transporte de mercadorias. |
| | Adaptação capacidades defesa e desenvolvimento. | O Fundo Europeu de Defesa incentiva os esforços dos Estados-Membros para intensificar e manter a colaboração no domínio da defesa na Europa, a fim de responder com eficácia às AH. |
| | Mecanismos de coordenação e de preparação no domínio da saúde. | A preparação no domínio da saúde é uma componente importantíssima da preparação geral contra os riscos QBRN. A Comissão adotou medidas e incentivou, em especial, as iniciativas de partilha eficaz de conhecimentos e da realização de exercícios neste âmbito, a fim de testar a capacidade de resposta a uma AH por parte dos atuais mecanismos, sistemas e instrumentos de comunicação a nível nacional e da UE. |
| | Equipas de resposta a incidentes de cibersegurança (CERT-UE) e diretiva sobre a Cibersegurança. | As CERT-UE publicam documentos de avaliação das ciberameaças referentes a setores críticos. No que respeita aos modos de transporte (aéreos, marítimos e rodoviários), a Comissão efetua uma monitorização regular e assegura a coerência das iniciativas setoriais sobre ciberameaças com as capacidades intersectoriais cobertas pela Diretiva sobre a Cibersegurança. Contribui para os trabalhos da Célula de Fusão da UE contra as AH partilhando informações. |
| | Parceria público-privada contratual para a cibersegurança. | A Comissão assinou uma parceria público-privada em matéria de cibersegurança com a organização europeia de cibersegurança, a fim de incentivar a competitividade e as capacidades de inovação da indústria da segurança digital. |
| | Resiliência do setor da energia. | A Comissão está a trabalhar na elaboração de orientações específicas em matéria de cibersegurança que vão além da Diretiva sobre a Cibersegurança, a fim de identificar boas práticas em matéria de cibersegurança e no âmbito do setor da energia. |

| Domínios prioritários | Medidas | Observações |
|---|---|---|
| | Resiliência do setor financeiro: plataformas e redes de partilha de informação. | O plano de ação da Comissão para as tecnologias financeiras (visa combater os obstáculos que limitam a partilha de informação sobre ciberameaças entre os intervenientes dos mercados financeiros e identificar as possíveis soluções para superar estes obstáculos. A CERT-UE também desempenha um papel ativo na partilha de informação sobre incidentes. |
| | Resiliência contra ciberataques no setor dos transportes. | Proteger os modos de transporte de ataques à cibersegurança é uma das grandes prioridades da Comissão. Na aviação civil, já se registaram grandes progressos em termos de cibersegurança. |
| | Ações contra a radicalização e eliminação de conteúdos ilegais. | A Comissão criou um grupo de peritos de alto nível sobre a radicalização, com a responsabilidade de formular recomendações sobre a coordenação, o alcance e o impacto das políticas de prevenção da UE (*e.g.* o código de conduta para combater a incitação ilegal ao ódio em linha, assinado pelo Facebook, Twitter, Google YouTube e Microsoft). |
| Prevenção e resposta a situações de crise e recuperação | Protocolo/operacional comum e exercícios regulares para melhorar a resposta AH complexas. | Este documento contém os princípios fundamentais da resposta multi-institucional a situações de crise. O protocolo foi testado no contexto de um cenário híbrido e revelou-se um instrumento precioso para facilitar a interconexão entre serviços, estabelecendo pontos de contacto para a interação entre os diferentes níveis de intervenção: políticos, estratégicos, operacionais e técnicos. |
| | Analisar/aplicabilidade do artigo 222.º do TFUE e artigo 42.º, n.º 7, do TUE, em caso AH graves. | A aplicabilidade da cláusula de solidariedade da UE e do respetivo mecanismo de assistência mútua, bem como a interação entre ambos. Os mecanismos de resposta da NATO, incluindo a defesa coletiva ao abrigo do artigo 5.º, estão a ser debatidos e testadas em cenários de exercício híbridos. |
| | Integrar, explorar e coordenar as capacidades de ação militar na luta contra as AH no âmbito da política comum de segurança e defesa | Em consulta com o Hybrid CoE, o Estado-Maior da UE procura atualmente conceber de que forma as forças militares podem contribuir para a luta contra as ameaças híbridas, através das missões e operações da política comum de segurança e defesa. A contribuição militar da UE para a luta contra as AH no âmbito da CEP, concluído em julho de 2017. |
| Apoio e cooperação internacional | Cooperação mais estreita com as regiões vizinhas e os países terceiros. | No setor da segurança, a UE reforçou a tónica na consolidação das capacidades e da resiliência nos países parceiros, nomeadamente reforçando a dimensão de segurança da política europeia de vizinhança revista. Com o objetivo de reforçar as capacidades dos seus parceiros na luta contra as ameaças híbridas. |
| | Interação entre a UE e a NATO | Assenta na constatação de que, na eventualidade de uma ameaça híbrida, os recursos e as capacidades que as duas organizações conseguem mobilizar são complementares e reforçam a capacidade dos Estados-Membros e dos Aliados de prevenir, impedir e dar resposta. Exercícios da série PACE têm servido para testar os protocolos das duas organizações. |
| | Coordenação atividades de formação no domínio da cibersegurança. | Constitui um importante domínio de ação que poderá beneficiar de uma colaboração mais estreita entre a OTAN a UE e os Estados-Membros. |
| | Cooperação no Domínio da Defesa. | A Defesa tem um papel fundamental na estabilização da vizinhança próxima alargada, que passa pela CDD por forma a reforçar as capacidades dos nossos parceiros e assim reforças a resiliência internacional no CAH. |

Fonte: Adaptado Comissão Europeia (2018).