ACADEMIA MILITAR

Contra-Ameaça Híbrida da Força Nacional Destacada de Operações Especiais Portuguesa na Roménia

Gonçalo Araújo Spínola

Trabalho de Investigação Aplicada

Mestrado Integrado em Ciências Militares na Especialidade de Infantaria

Orientador: Tenente-Coronel de Infantaria João Carlos Gonçalves dos Reis

Júri

Presidente: Professor Auxiliar Hugo Miguel Bento Rebelo

Arguente: Professor Doutor Francisco de Borja Montes Toscano

Orientador: Tenente-Coronel de Infantaria João Carlos Gonçalves dos Reis

Diretor de Curso: Tenente-Coronel de Infantaria Roberto Martins Mariano

Junho 2025

ACADEMIA MILITAR

Contra-Ameaça Híbrida da Força Nacional Destacada de Operações Especiais Portuguesa na Roménia

Gonçalo Araújo Spínola

Trabalho de Investigação Aplicada

Mestrado Integrado em Ciências Militares na Especialidade de Infantaria

Orientador: Tenente-Coronel de Infantaria João Carlos Gonçalves dos Reis

Júri

Presidente: Professor Auxiliar Hugo Miguel Bento Rebelo

Arguente: Professor Doutor Francisco de Borja Montes Toscano

Orientador: Tenente-Coronel de Infantaria João Carlos Gonçalves dos Reis

Diretor de Curso: Tenente-Coronel de Infantaria Roberto Martins Mariano

Junho 2025

EPÍGRAFE

"A guerra é a continuação da política de determinadas classes e estados, por outros meios."
Carl Von Clausewitz

DEDICATÓRIA

Á minha família,
pelo suporte psicofísico que me deram ao longo deste exigente percurso.

AGRADECIMENTOS

Durante esta jornada, contei com o apoio e a orientação de muitas pessoas, cuja contribuição foi essencial para a concretização deste trabalho. Assim, torna-se imprescindível expressar a minha gratidão a todos aqueles que, de alguma forma, me ajudaram, incentivaram e estiveram ao meu lado, proporcionando-me o encorajamento necessário para superar desafios e alcançar este objetivo.

Um agradecimento especial ao meu orientador, Tenente-Coronel de Infantaria João Carlos Gonçalves dos Reis, cujo conhecimento, paciência e orientação foram fundamentais para a realização deste trabalho. A sua disponibilidade, dedicação e conselhos valiosos foram essenciais para o desenvolvimento desta investigação.

Aos entrevistados, que gentilmente disponibilizaram o seu tempo e conhecimento para contribuir para este estudo, expresso a minha sincera gratidão. O seu testemunho e partilha de experiência foram indispensáveis para a construção deste trabalho, enriquecendo a investigação com perspetivas e informações fundamentais.

Ao Diretor de Curso, Tenente-Coronel de Infantaria Roberto Martins Mariano, pelo compromisso e empenho na formação dos alunos, garantindo sempre as condições necessárias para o nosso desenvolvimento académico e profissional.

À minha família e ao meu parelha Aspirante de Infantaria Tomás Cardoso o meu mais profundo agradecimento pelo amor, paciência e apoio incondicional. Foram o meu pilar em todos os momentos, incentivando-me a seguir em frente, mesmo nos desafios mais exigentes. Sem o vosso suporte e motivação, esta jornada teria sido muito mais difícil.

Aos meus amigos, que estiveram sempre ao meu lado, proporcionando momentos de apoio, encorajamento e descontração ao longo desta caminhada. A vossa amizade e companheirismo foram essenciais para manter a motivação e superar os desafios deste percurso.

Aos meus camaradas de curso, e em especial aos 18 duros infantes, expresso a minha mais sincera gratidão. Juntos, enfrentámos desafios exigentes, superámos dificuldades e crescemos lado a lado, sempre com espírito de sacrifício, resiliência e união. A camaradagem, a entreajuda e a determinação que partilhámos ao longo deste percurso foram fundamentais para cada conquista. Foi uma honra trilhar este caminho convosco.

A todos o meu muito obrigado.

Gonçalo Spínola

RESUMO

As ameaças híbridas representam um desafio crescente no domínio da segurança e defesa, caracterizando-se pela conjugação coordenada de estratégias convencionais e não convencionais. Estas abordagens incluem a desinformação, a guerra cibernética, a pressão económica e o emprego de forças irregulares, com o intuito de desestabilizar estruturas institucionais e comprometer a segurança nacional. Tendo em conta a complexidade desta ameaça, a eficácia de resposta à mesma, depende da preparação e precaução da força. O presente trabalho pretende investigar as táticas de contra-ameaça híbrida utilizadas pela Força Nacional Destacada de Operações Especiais Portuguesa na Roménia de forma a melhorar a resposta desta força a uma ameaça ambígua. Para tal, a investigação assenta em três eixos fundamentais: a análise do contexto e das características específicas das ameaças híbridas na atuação da FND, a investigação das táticas de contra-ameaça híbrida atualmente empregues e o estudo das dinâmicas de coordenação e cooperação com forças aliadas para fortalecer a capacidade de resposta. A metodologia adotada baseia-se numa abordagem qualitativa, recorrendo à análise documental e a entrevistas com especialistas na área, de forma a obter um quadro abrangente e fundamentado sobre o fenómeno das ameaças híbridas e as respetivas contramedidas. Conclui-se que, apesar dos avanços na preparação e atuação da FND no contexto híbrido, persistem fragilidades estruturais que limitam a sua eficácia de resposta. A ausência de doutrina, carência de treino e a necessidade de modernização tecnológica reforçam a urgência de uma abordagem integrada e multidimensional. Este trabalho propõe, assim, linhas de ação que visam colmatar essas lacunas, contribuindo para o fortalecimento da capacidade de resposta da FND face aos desafios impostos pela crescente complexidade das ameaças híbridas.

Palavras-chave: Força Nacional Destacada de Operações Especiais; Contra-Ameaça Híbrida; Ameaças Híbridas; Roménia

ABSTRACT

Hybrid threats represent a growing challenge in the field of security and defense, characterized by the coordinated combination of conventional and unconventional strategies. These approaches include disinformation, cyber warfare, economic coercion, and the use of irregular forces, with the aim of destabilizing institutional structures and compromising national security. Given the complexity of this threat, the effectiveness of the response depends on the preparedness and precautionary measures of the force. This study aimed to investigate the hybrid counter-threat tactics employed by the National Deployable Special Operations Force in Romania, with the objective of enhancing its response to such an ambiguous threat. To achieve this, the research is structured around three fundamental axes: the analysis of the context and specific characteristics of hybrid threats in the National Deployable Special Operations Force operations, the investigation of currently employed hybrid counter-threat tactics, and the study of coordination and cooperation dynamics with allied forces to strengthen response capabilities. The adopted methodology follows a qualitative approach, relying on document analysis and interviews with experts in the field to obtain a comprehensive and well-founded framework on the phenomenon of hybrid threats and their respective countermeasures. It is concluded that, despite the advances in the preparation and operational performance of the National Deployable Force in the hybrid context, structural weaknesses persist that limit its response effectiveness. The absence of doctrine, lack of specific training, and the need for technological modernization highlight the urgency of adopting an integrated and multidimensional approach. This study therefore proposes lines of action aimed at addressing these gaps, contributing to strengthening the National Deployable Force response capacity in the face of the growing complexity of hybrid threats.

Keywords: National Deployable Special Operations Force; Hybrid Counter-Threat; Hybrid Threat; Romania

ÍNDICE GERAL

ÍNDICE DE FIGURAS

ÍNDICE DE QUADROS

ÍNDICE DE TABELAS

LISTA DE APÊNDICES

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

AAR- *After Action Review*

AM- Academia Militar

AH- Ameaça Híbrida

AOp- Área de Operações

BICES- *Battlefield Information Collection and Exploitation System*

CAH- Contra-Ameaça Híbrida

COCiber- Comando de Operações de Ciberdefesa

CSMIE- Centro de Segurança Militar e Informações do Exército

CTOE- Centro de Tropas de Operações Espaciais

FIR- *First Impression Report*

FND- Força Nacional Destacada

FND OEsp/ROU- Força Nacional Destacada de Operações Especiais/Roménia

FOEsp- Força de Operações Especiais

MCDC- *Multinational Capability Development Campaign*

NAC- *North Atlantic Council*

NATO- *North Atlantic Treaty Organization*

NEP- Norma de Execução Permanente

NSWAN- *NATO Secret Wide Area Network*

OE- Objetivo Específico

OG- Objetivo Geral

OTAN- Organização do tratado Atlântico Norte

PD- Pergunta Derivada

PP- Pergunta de Partida

QBRN- Químico Biológico Radiológico Nuclear

RAP- *Readiness Action plan*

SOCC/ROU- *Special Operations Component Command Romeno*

SOLTG- *Special Operations Land Task Group*

SOLTU- *Special Operations Land Task Unit*

SOMTU- *Special Operations Maritime Task Unit*

SOTG - *Special Operations Task Group*

SOTU- *Special Operations Task Unit*

tFP- *tailored Forward Presence*

TG- *Task Group*

TO- Teatro de Operações

TTP- Táticas, Técnicas e Procedimentos

TU- *Task Unit*

UE- União Europeia

INTRODUÇÃO

O presente trabalho de investigação insere-se no plano curricular do mestrado integrado em Ciências Militares na especialidade de Infantaria da Academia Militar. Neste contexto, a investigação centra-se no tema "Contra-Ameaça Híbrida da Força Nacional Destacada de Operações Especiais portuguesa na Roménia". Este tema surge da necessidade de compreender e aperfeiçoar as táticas utilizadas pela Força Nacional Destacada (FND) de Operações Especiais no combate às ameaças híbridas no contexto específico da Roménia, face ao crescente desafio que estas representam para a segurança e defesa.

As ameaças híbridas caracterizam-se pela combinação coordenada de meios convencionais e não convencionais, incluindo desinformação, operações cibernéticas, pressão económica e o emprego de forças irregulares, com o objetivo de desestabilizar estruturas institucionais e comprometer a segurança nacional (Jacuch, 2020). Conforme argumenta Hoffman (2007), as ameaças híbridas combinam táticas de guerra tradicional com abordagens irregulares, explorando vulnerabilidades políticas, económicas e sociais para enfraquecer Estados e organizações. A European Commission (2016) destaca ainda que a crescente interligação entre o ciberespaço e o ambiente geopolítico amplia a capacidade de atores estatais e não estatais para lançar operações híbridas sofisticadas. Neste sentido, a atuação da FND assume um papel crucial na mitigação destas ameaças, exigindo uma abordagem multidimensional e altamente especializada para garantir uma resposta eficaz e adaptada ao ambiente operacional.

A crescente complexidade do ambiente de segurança internacional reforça a importância da otimização das táticas de contra-ameaça híbrida, assegurando que as unidades da FOEsp se encontram devidamente preparadas para enfrentar desafios dinâmicos e assimétricos. Assim, a presente investigação tem como Objetivo Geral (OG) melhorar e propor táticas de contra-ameaça híbrida na FND de Operações Especiais portuguesa na Roménia, de forma a maximizar a eficácia da sua atuação face a um contexto de ameaça híbrida.

Como Objetivos Específicos, pretende-se analisar o contexto e as características específicas das ameaças híbridas na atuação da FND na Roménia, investigar as táticas de contra-ameaça híbrida atualmente empregues e, por fim, estudar as dinâmicas de coordenação e cooperação entre a FND e forças aliadas, de modo a fortalecer a resiliência e a capacidade de resposta conjunta.

A presente investigação adota uma abordagem metodológica qualitativa, baseada na análise documental e na realização de entrevistas com especialistas na área. Este método permite a recolha de dados aprofundados e contextuais, proporcionando uma compreensão abrangente e sustentada do fenómeno das ameaças híbridas, bem como das estratégias de contramedida mais eficazes.

Relativamente à estrutura do presente trabalho, este encontra-se dividido em quatro capítulos, conclusões e referências bibliográficas. A introdução apresenta o tema da investigação, a sua relevância, bem como os objetivos gerais e específicos. No Capítulo 1, são explanados os principais conceitos e fundamentos teóricos necessários à compreensão da problemática em estudo. No Capítulo 2, detalha-se a metodologia utilizada, incluindo os métodos e estratégias de investigação, os procedimentos de recolha e tratamento de dados, e a abordagem qualitativa adotada. No Capítulo 3, são analisadas as táticas de contra-ameaça híbrida atualmente utilizadas pela FND na Roménia, identificando desafios e limitações. No Capítulo 4, são exploradas estratégias de coordenação e cooperação com forças aliadas, visando o reforço da capacidade de resposta. Por fim, apresentam-se as conclusões da investigação, sintetizando os principais resultados obtidos e as implicações para a melhoria das operações da FND.

CAPÍTULO 1 – REVISÃO DA LITERATURA

Este capítulo tem como objetivo explorar os conceitos principais que sustentam a compreensão da problemática abordada ao longo do estudo. Inicialmente, serão explorados vários conceitos que descrevem a ameaça que a FND enfrenta, de forma a perceber como as mesmas atuam e de que forma se deve ter cuidado e cautela em arranjar medidas de precaução. De seguida, será detalhado medidas de precaução e estratégias a utilizar para repelir os efeitos destas ameaças. Por fim, será feita uma análise à FOEsp e à FND de forma a perceber qual o papel e a missão desta força no teatro de operações em questão e de que forma tem influência no mesmo. A análise destes conceitos permitirá uma compreensão mais clara das ameaças enfrentadas pela FND, bem como a sua envolvência no cenário de guerra.

1.1. Guerra Híbrida

Ao longo do tempo, o conceito guerra híbrida passou por uma constante evolução, sendo que a sua definição nunca foi totalmente clara ou consensual. Face a esta diversidade conceptual, torna-se pertinente focar a análise nas definições mais recentes e atualizadas, que procuram refletir o panorama contemporâneo.

Neste sentido, Fernandes (2021) partilha desta visão sobre a complexidade inerente à guerra híbrida, reconhecendo a ausência de consenso em torno da sua definição. O autor destaca, no entanto, a descrição de Cullen & Reichborn-Kjennerud (2017), que caracterizam a guerra híbrida como "o uso sincronizado de múltiplos instrumentos de poder, confecionados com vista a lidar com as vulnerabilidades específicas que atravessam todo o espetro das funções sociais, de modo a obter efeitos sinergéticos".

Complementando esta perspetiva, o Parlamento Europeu propõe uma abordagem que sublinha a componente multidimensional da guerra híbrida, definindo-a como “uma situação em que um país recorre ao uso aberto de forças armadas contra outro país ou um ator não estatal, em combinação com outros meios, como instrumentos económicos, políticos e diplomáticos” (European Commission, 2017).

Apesar da proximidade entre algumas definições, subsistem diferenças significativas nas formas como o conceito é interpretado. Por exemplo, Wither (2019) define guerra híbrida como "uma combinação de métodos convencionais e não convencionais, que vão desde o uso da força militar até ciberataques, pressão económica e propaganda, com o objetivo de explorar vulnerabilidades e alcançar objetivos estratégicos, sem ultrapassar o limiar de um conflito aberto."

Numa abordagem distinta, mas complementar, a Multinational Capability Development Campaign (MCDC) apresenta uma definição com padrões distintos dos restantes autores e aborda o conceito enfatizando a assimetria e a ambiguidade: "A guerra híbrida é assimétrica e recorre a múltiplos instrumentos de poder ao longo de um eixo horizontal e vertical, partilhando, em diferentes graus, uma maior ênfase na criatividade, ambiguidade e nos elementos cognitivos da guerra." (Cullen & Wegge, 2019).

A União Europeia reforça esta visão integrada ao descrever a guerra híbrida como uma estratégia coordenada, que integra táticas encobertas e abertas, utilizando meios militares e não militares, incluindo operações de informação, ciberataques, pressão económica e forças convencionais (citado em Fernandes, 2021).

A definição da OTAN apresenta uma perspetiva ainda mais abrangente e detalhada, evidenciando a complexidade deste fenómeno, "A guerra híbrida consiste na utilização criativa do poder hard, soft e smart por atores estatais ou não estatais com intenções hostis, com o objetivo de alcançar fins bélicos e metas políticas. As ações maliciosas englobam um amplo leque de instrumentos de poder coercivo, militares e não militares, que vão além do tradicional conceito de campo de batalha multidimensional. A guerra híbrida abrange política, diplomacia, informação, economia, tecnologia, forças armadas e sociedade, bem como dimensões como a cultura, psicologia, legitimidade e moral. A realização coordenada destas ações ocorre tanto de forma explícita como encoberta, nas zonas cinzentas e ambíguas onde se esbatem as fronteiras entre guerra e paz, amigo e inimigo, relações internas e externas, civil e militar, e entre atores estatais e não estatais. Além disso, estas ações ocorrem frequentemente abaixo do limiar do conflito armado tradicional, ou como complemento a operações militares mais convencionais" (NATO, 2024).

Após esta análise conceptual, importa relacionar estas definições com o cenário operacional atual, nomeadamente no contexto da Roménia, integrada no flanco oriental da OTAN. Conforme refere Wei (2024), esta guerra pode ser conceptualizada como composta por dois conflitos assimétricos distintos, operando em níveis diferentes. O primeiro corresponde a um conflito militar convencional, entre a Rússia e a Ucrânia, que decorre predominantemente dentro dos limites territoriais ucranianos. O segundo configura-se como uma nova forma de guerra no domínio cibernético, caracterizada por operações de guerra informática e de manipulação da opinião pública, conduzidas pelos Estados Unidos e países ocidentais contra a Rússia. No primeiro caso, trata-se de uma guerra assimétrica marcada por uma acentuada desigualdade de capacidades militares, com a Rússia a deter uma clara superioridade. No segundo, observa-se uma mobilização global do Ocidente contra a Rússia, assumindo igualmente a forma de guerra assimétrica, ainda que com uma natureza distinta, centrada no ambiente informacional e digital.

Complementando esta perspetiva, Pynnöniemi (2021) destaca que a doutrina militar russa

integra uma conceção de guerra híbrida como um mecanismo de coerção estratégica, onde a combinação de forças militares e não militares é usada tanto como uma ameaça externa quanto como uma ferramenta para moldar o ambiente de segurança de acordo com os interesses estratégicos russos.

Além disso, autores como Voyger (2021) referem-se ao modelo de Gerasimov, que combina elementos descritivos, representando a forma como a liderança russa compreende a guerra, e prescritivos orientando as forças armadas russas na aplicação destes elementos contra os seus oponentes. Este modelo reforça a centralidade da guerra política e da guerra da informação como princípios chave da estratégia russa contemporânea.

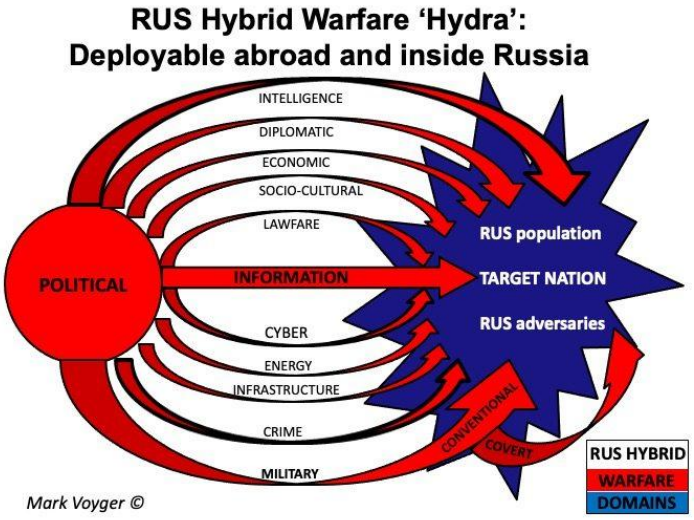

Figura 1: Gerasimov model

Fonte: Mark Voyger (2021)

Mark Voyger conclui que, ao longo da história, diversos atores utilizam estratégias não militares para enfraquecer e desestabilizar os seus adversários. Contudo, no século XXI, a guerra híbrida emergiu como um instrumento estratégico de crescente relevância, particularmente para potências revisionistas e revanchistas que, embora ambicionem expandir a sua influência no sistema internacional, evitam deliberadamente um confronto convencional de larga escala. Deste modo, estas entidades recorrem a uma combinação integrada de ferramentas militares e não militares, explorando vulnerabilidades estruturais dos seus oponentes através de operações assimétricas e subversivas, sem ultrapassar limiares que justifiquem uma resposta militar direta. Assim, a guerra híbrida constitui uma alternativa tática que permite aos seus intervenientes atingir objetivos geopolíticos sem incorrer nos custos e riscos inerentes a um conflito convencional.

1.2. Tipologia de Ameaças Híbridas

De forma a avaliar a tipologia de ameaças híbridas presentes no TO da Roménia, consequentes do cenário de guerra entre a Rússia e a Ucrânia, torna-se essencial, em primeiro lugar, proceder a uma análise breve e clara do conceito de ameaça híbrida.

A OTAN define este conceito como envolvendo, "ações militares e não militares, potencialmente abertas ou encobertas, que um ator estatal ou não estatal pode realizar com o objetivo de desestabilizar uma sociedade-alvo e alcançar os seus objetivos políticos. Estas ações ultrapassam a interação habitual entre Estados, sem que, necessariamente, tenham como finalidade iniciar um conflito armado." (NATO, 2024).

Complementando esta visão, a European Commission (2016) descreve as ameaças como um conceito abrangente que envolve diferentes formas de atividades hostis, como operações de influência, campanhas estratégicas, interferência política e guerra híbrida. Estas ações são vistas como intervenções indesejadas que procuram desestabilizar o espaço interno de um Estado.

No mesmo sentido, Monaghan (2019) aprofunda a análise ao afirmar que as ameaças híbridas consistem na utilização coordenada de múltiplos meios não violentos para explorar vulnerabilidades estruturais de uma sociedade, com o objetivo de comprometer a sua estabilidade, coerência e capacidade de resposta sem desencadear uma retaliação direta. Este tipo de estratégia é frequentemente utilizado por atores revisionistas, que procuram alterar o equilíbrio geopolítico global sem recorrer a um confronto militar convencional.

Considerando a diversidade de definições, para efeitos desta investigação, adotar-se-á a definição apresentada pela Hybrid CoE, por ser aquela que, pela sua abrangência e atualidade, melhor enquadra a realidade em análise. A Hybrid CoE define as ameaças híbridas como “atividades nocivas planeadas e executadas com intenções maliciosas, que têm como objetivo fragilizar um alvo, como um Estado ou uma instituição, recorrendo a diversos meios, frequentemente combinados entre si. Estes meios podem incluir manipulação da informação, ciberataques, influência ou coerção económica, manobras políticas encobertas, diplomacia coerciva ou ameaças de uso de força militar. As ameaças híbridas englobam uma ampla variedade de atividades hostis, com diferentes finalidades, que vão desde operações de influência e interferência até à guerra híbrida propriamente dita.” (CoE, n.d.).

Após esta análise conceptual, torna-se pertinente destacar que existem diferenças relevantes entre o conceito de ameaças híbridas e o de guerra híbrida. Estas distinções são ilustradas de forma clara no gráfico seguinte, permitindo compreender melhor a especificidade de cada conceito e orientar a sua aplicação prática no contexto da presente investigação.

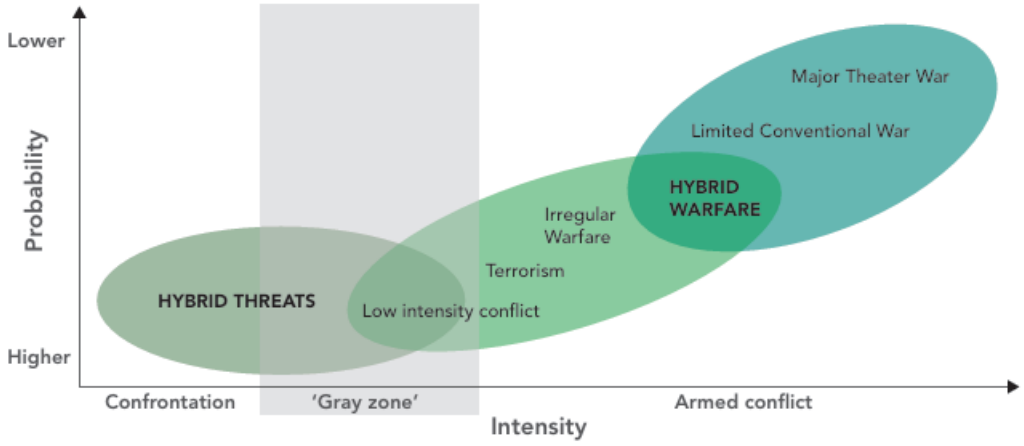

Figura 2: Hybrid Threat and Hybrid warfare shown on a continuum of conflict

Fonte: Sean Monaghan (2019)

Analisados os conceitos e percebida a diferença entre eles, observamos agora a imensa variedade de ameaças híbridas que se manifestam através de todo o espetro de ameaças, sendo que, utilizadas de forma combinada para atingir um determinado alvo (A. J. F. M. Alves, 2020).

Figura 3: Tipologia das AH

Fonte: Alves (2020)

Passamos agora a analisar a tipologia de AH que podemos encontrar no TO da Roménia. Para tal torna-se necessário compreender as dinâmicas do conflito entre a Rússia e a Ucrânia, dado o seu impacto direto na região e na atuação de atores híbridos.

De acordo com Praks (2024), a Rússia recorre a operações de influência e desinformação para fragilizar a credibilidade da Ucrânia e enfraquecer o apoio ocidental. A sua estratégia assenta

na disseminação de narrativas manipuladoras, incluindo a alegação de que o governo ucraniano é corrupto, a insinuação de que a resistência militar é inútil e a tentativa de responsabilizar a NATO pela escalada do conflito.

Complementarmente, segundo a Eu Council (2024), houve um aumento significativo no número de ciberataques dirigidos a infraestruturas e instituições europeias. Estes ataques são uma das principais ferramentas da estratégia híbrida russa, sendo utilizados para desestabilizar redes críticas e comprometer a segurança da informação.

Neste mesmo enquadramento, conforme Pillai (2023), a Rússia tem realizado atos de sabotagem direcionados a infraestruturas essenciais, incluindo ferrovias, redes de comunicação e sistemas de GPS. Estas ações visam criar instabilidade, dificultar operações logísticas e aumentar o custo da defesa europeia. Um exemplo foi a destruição de cabos de comunicação submarinos na França, que causou graves interrupções nos serviços de telecomunicações.

A dimensão económica da guerra híbrida também se manifesta, como refere Audrey (2025), a Rússia utiliza o fornecimento de energia como método de coerção económica, especialmente na Europa, onde muitos países dependem do gás natural russo. Ao manipular os preços ou interromper o fornecimento, Moscovo exerce pressão política e económica sobre os países ocidentais. Além disso, a Rússia explora redes financeiras ilícitas e corrupção para influenciar elites políticas e económicas no Ocidente.

Sob uma vertente sociopolítica, Praks (2024), a Rússia provoca crises migratórias deliberadamente, forçando migrantes a atravessar fronteiras europeias para sobrecarregar sistemas de asilo e destabilizar governos ocidentais.

No plano da segurança marítima e das infraestruturas críticas, Edwards (2024), em novembro de 2024, a Rússia foi suspeita de sabotar dois cabos submarinos no Mar Báltico, indicando um aumento nas suas operações de guerra híbrida na Europa.

Em síntese, as ações da Rússia no contexto da guerra com a Ucrânia revelam a aplicação de um leque alargado de ameaças híbridas, integrando múltiplos domínios, informacional, ciber, energético, logístico, económico e humano, com o objetivo permanente de obter vantagem estratégica sobre o adversário.

1.3. Estratégias de Combate às Ameaças Híbridas

O combate às ameaças híbridas exige uma abordagem multifacetada, devido à sua natureza complexa e imprevisível. Estas ameaças combinam frequentemente táticas convencionais, não convencionais e irregulares, afetando diferentes áreas como a política, a economia e a informação. “O prémio maior de uma vitória é triunfar por meio de estratagemas, sem usar as tropas” (Sun, n.d.). Neste contexto, torna.se essencial recorrer a estratégias adaptadas e diferenciadas, capazes

de antecipar e contrariar ações hostis em vários domínios.

Uma das estratégias fundamentais para enfrentar estas ameaças é a deteção precoce, a qual garante uma resposta eficaz e atempada. Assim, como nos diz Wijnja (2022), a consciência situacional apoia a compreensão da situação atual, permite reconhecer quaisquer mudanças subtis no panorama das ameaças, possibilita o alerta sobre as operações do adversário antes de serem executadas e ajuda a formular uma resposta adequada à situação em desenvolvimento. O autor formula uma tabela com várias fases de resposta a ameaças híbridas.

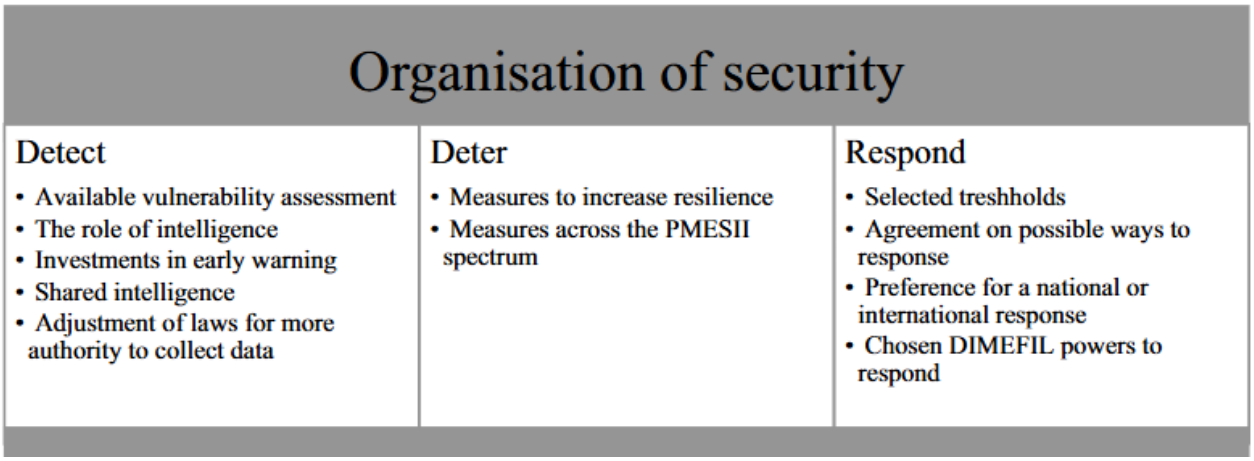

Figura 4: Framework to counter hybrid threats

Fonte: Kim Wijnja (2022)

Vários autores e instituições defendem o modelo analisado anteriormente, observamos agora outro exemplo um pouco mais aprofundado.

Figura 5: Estratégias de CAH

Fonte: Alves (2020)

Dando continuidade à análise de modelos de resposta a ameaças híbridas, destaca-se o contributo da OTAN, que apresenta uma abordagem muito semelhante à anteriormente explorada.

Como refere NATO (2024), a OTAN recolhe, partilha e avalia continuamente informações com o objetivo de detetar e atribuir responsabilidades relativamente a qualquer atividade híbrida em curso. A Divisão Conjunta de Inteligência e Segurança no Quartel-General da OTAN melhora a compreensão e análise da Aliança sobre as ameaças híbridas. Além disso, a unidade de análise de ameaças híbridas fornece aos decisores uma visão mais clara sobre possíveis ameaças híbridas. A OTAN apoia os esforços dos Aliados para identificar vulnerabilidades nacionais e reforçar a sua resiliência, caso solicitado. A Aliança também funciona como um centro de conhecimento especializado, prestando apoio aos Aliados em áreas como preparação civil, resposta a incidentes químicos, biológicos, radiológicos e nucleares (QBRN), proteção de infraestruturas críticas, comunicação estratégica, proteção de civis, ciberdefesa, segurança energética e contraterrorismo. O treino, os exercícios e a formação desempenham um papel fundamental na preparação para enfrentar ameaças híbridas. Isto inclui simulações de processos de tomada de decisão e respostas conjuntas militares e não militares em cooperação com outros atores. Para dissuadir ameaças híbridas, a OTAN está determinada a agir prontamente, sempre que e onde for necessário. Continua a aumentar o nível de prontidão das suas forças e fortaleceu o seu processo de tomada de decisão e a sua estrutura de comando, como parte da sua postura de dissuasão e defesa. Isto envia um sinal forte de que a Aliança está a melhorar a sua capacidade política e militar e a sua aptidão para desencadear respostas adequadas no local e momento certos. Além disso, a OTAN expandiu o seu conjunto de ferramentas para enfrentar ameaças híbridas. Os Aliados desenvolveram opções preventivas e de resposta abrangentes, que combinam ferramentas civis e militares, permitindo uma resposta ajustada a situações específicas. Se a dissuasão falhar, a OTAN está pronta para defender qualquer Aliado contra qualquer ameaça. Para tal, as forças da OTAN devem ser capazes de reagir de forma rápida e ágil, sempre que e onde for necessário.

Na sequência da deteção precoce e da resposta operacional, é pertinente abordar a vertente da prevenção, como componente essencial do ciclo de gestão de ameaças híbridas. Alguns autores apresentam modelos concetuais de prevenção que podem ser interpretados como medidas de contra-ameaça híbrida. Como refere Filipec (2021), "As ameaças híbridas seguem, de certo modo, um ciclo de vida: desde o seu surgimento até adquirirem relevância, passando pela maturação, podendo posteriormente tornar-se obsoletas, desaparecer ou, pelo contrário, materializar-se, ser ativadas e exploradas. Com base nesta lógica funcional, é possível delinear um conjunto de processos e atividades gerais que podem contribuir para a prevenção das ameaças híbridas."

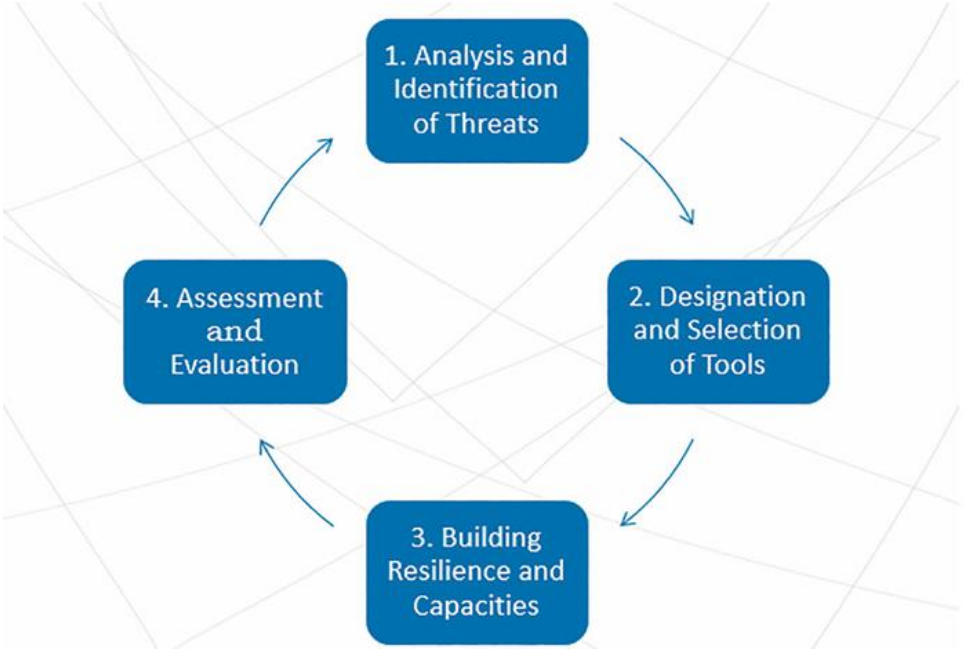

Figura 6: Set of Activities Aimed at the Prevention of Hybrid Threats

Fonte: Ondřej Filipec (2021)

Alguns autores defendem teorias para fazer frente a ameaças híbridas, como refere Sarjito (2024), que formula duas teorias diferentes. A teoria da difusão da inovação, explora como novas tecnologias e metodologias se disseminam e são adotadas dentro de organizações e sociedades. Os investigadores podem utilizar esta teoria para analisar como novas ideias na ciência da defesa se propagam e são aplicadas em áreas como a cyber segurança, a guerra de informação e a comunicação estratégica. Isso permite avaliar a eficácia dessas novas abordagens no combate às ameaças híbridas. Defende ainda, a teoria da dissuasão, analisa estratégias para desencorajar adversários de realizarem ações hostis através da ameaça credível de retaliação. Os investigadores podem avaliar como a ciência da defesa contribui para as capacidades de dissuasão contra ameaças híbridas, seja através do desenvolvimento de sistemas avançados de cyber defesa ou da utilização da comunicação estratégica para moldar as perceções e o comportamento dos adversários.

Para além das abordagens teóricas, é igualmente essencial considerar os princípios operacionais fundamentais no combate às ameaças híbridas, dos quais se destaca o princípio da segurança da informação. Referem Khriapynskyi et al. (2023) que "face aos riscos decorrentes das ameaças híbridas no domínio da informação para um Estado democrático, os países da União Europeia começaram a desenvolver as suas próprias estratégias nacionais de segurança da informação, com o objetivo de combater as ameaças híbridas." Assim, os autores criaram um modelo de princípios que devem ser respeitados pelos estados de forma a manter a segurança da informação.

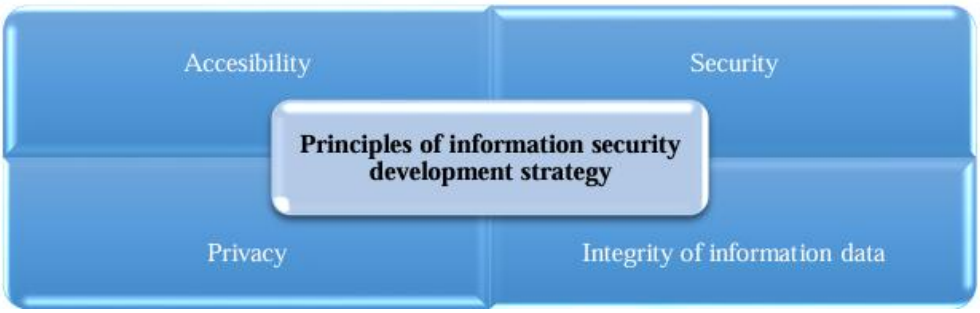

Figura 7: The principles of information security

Fonte: Khriapynskyi et al., 2023

São variadas as estratégias definidas e propostas por vários autores e instituições, cada uma apresentando abordagens específicas para a prevenção e combate a esta ameaça recente e alarmante. A European Commission (2016) procura responder a este problema baseando o combate em quatro pontos fundamentais. Aumentar a sensibilização através da criação de mecanismos dedicados à troca de informações entre os Estados-Membros e da coordenação das ações da UE para garantir uma comunicação estratégica eficaz. Reforçar a resiliência abordando setores estratégicos e críticos, como cyber segurança, infraestruturas críticas (Energia, Transportes, Espaço), proteção do sistema financeiro, proteção da saúde pública e apoio aos esforços para combater o extremismo violento e a radicalização. Prevenir, responder a crises e recuperar, definindo procedimentos eficazes a seguir, mas também analisando a aplicabilidade e as implicações práticas da Cláusula de Solidariedade e da Cláusula de Defesa Mútua, no caso de um ataque híbrido de grande escala e gravidade. Reforçar a cooperação entre a UE e a OTAN, bem como com outras organizações parceiras, num esforço conjunto para combater as ameaças híbridas, respeitando os princípios de inclusão e autonomia de cada organização no seu processo de tomada de decisão.

1.4. As Operações Especiais

No que diz respeito ao combate às Ameaças Híbridas, as Operações Especiais devem possuir um caráter flexível, capacidade de projeção, além de serem sustentáveis, interoperáveis, bem informadas e tecnologicamente avançadas. As forças convencionais, por sua vez, não dispõem dessas mesmas capacidades, uma vez que a sua atuação envolve, frequentemente, o emprego de elevados níveis de violência contra o adversário, o que se torna um desafio quando este se encontra inserido no meio da população. Assim, verifica-se que as Forças de Operações Especiais (FOEsp) são as mais adequadas para este tipo de missões, devido à sua natureza e ao seu treino específico para operar nesse contexto.

Para compreender o papel e a adequação das Operações Especiais no combate às ameaças

híbridas, importa analisar a forma como estas forças são definidas e caraterizadas pelas doutrinas nacionais e internacionais. As Operações especiais são definidas como atividades militares conduzidas por forças especialmente selecionadas, organizadas, treinadas e equipadas, que utilizam técnicas, táticas e procedimentos não padronizados para outro tipo de forças. Essas atividades são realizadas em todo o espectro das operações militares, de forma independente ou integradas com operações de outras forças ou agências para alcançar um estado final desejado. Considerações de natureza político-militar podem requerer um modo de atuação discreto, coberto ou aberto, e a aceitação de um elevado grau de risco, que normalmente não está associado a operações conduzidas por outras forças (Exército Português, 2014).

Esta perspetiva é corroborada também por organizações internacionais. No ano de 2013, a OTAN referiu que as operações especiais consistem em ações militares realizadas por forças específicas, que são organizadas, treinadas e equipadas de forma especializada e compostas por pessoal selecionado. Estas forças utilizam táticas, técnicas e métodos de atuação não convencionais. Podem ser executadas ao longo de todo o espectro das operações militares, tanto de forma autónoma como em coordenação com forças convencionais, com o propósito de atingir os objetivos estratégicos estabelecidos.

O Exército Português (2014) aprofunda esta definição, sublinhando que as operações especiais distinguem-se das operações convencionais pelo seu elevado nível de risco, pelas técnicas operacionais específicas, pela forma como são executadas, pelo grau de autonomia em relação ao apoio de forças amigas e pela utilização de forças locais. Além disso, baseiam-se, frequentemente, em informações detalhadas para o seu planeamento e execução. Estas operações priorizam a surpresa e a segurança como fatores fundamentais para o sucesso das missões, recorrendo frequentemente a estratégias de deceção para desorientar o adversário. O êxito das operações depende da competência individual e coletiva em diversas capacidades operacionais especializadas, muitas delas não convencionais, sendo aplicadas com um alto grau de adaptabilidade, improvisação, inovação e autossuficiência.

Deste modo, torna-se evidente que as operações especiais são as forças mais bem preparadas para enfrentar o caráter multidimensional das ameaças híbridas. Como refere Lambakis (2021), a utilidade estratégica das operações especiais oferece opções aos líderes políticos e militares. Isto é particularmente relevante em tempos de paz, quando a sua precisão e a sua capacidade de atuar de forma encoberta e clandestina podem ser empregues para alcançar objetivos estratégicos significativos. Estas caraterísticas diferenciadoras são ainda reforçadas por autores como Podloch (2017), que sublinha que as capacidades das Operações Especiais para enfrentar ameaças decorrem das suas habilidades únicas, que as tornam aptas a conduzir operações não convencionais e de contrainsurgência em conflitos assimétricos.

1.4.1. Força de Operações Especiais (FOEsp)

Depois de analisado o conceito de Operações Especiais, observamos que a Força de Operações Especiais é a única capaz de responder a todos os desafios e dificuldades apresentadas pelas ameaças híbridas. Neste sentido, estas forças são definidas, segundo o Exército Português (2014) como "forças especialmente selecionadas, organizadas, treinadas e equipadas, que utilizam técnicas, táticas e procedimentos não padronizados para outro tipo de forças, para o cumprimento de operações especiais."

A singularidade das FOEsp não reside apenas nos seus equipamentos ou métodos de atuação, mas também na dimensão humana e organizacional. Como nos diz a STANDARD (2013), embora as Forças de Operações Especiais (FOEsp) frequentemente utilizem métodos e equipamentos sofisticados e exclusivos, o sucesso das operações depende, essencialmente, do desempenho individual de cada operador. Por isso, é fundamental que os planos, ordens e procedimentos que orientam o seu emprego sejam claros e diretos, garantindo que a intenção do comandante seja compreendida, mesmo em operações complexas.

Em coerência com esta estrutura operacional única, as FOEsp organizam-se de forma distinta das forças convencionais. "As FOEsp organizam-se em Special Operations Task Group (SOTG) que exercem diretamente o comando e controlo das Special Operations Task Unit (SOTU), orgânicas ou colocadas sob uma relação de comando" (Exército português, 2014). Esta configuração permite uma maior agilidade, flexibilidade e capacidade de resposta autónoma no terreno.

Tendo em conta estas caraterísticas organizacionais e funcionais, esta força, dotada de capacidades únicas e distintas, torna-se um ativo estratégico essencial no combate a ameaças híbridas. Segundo Mammadov (2024) as unidades das Forças de Operações Especiais devem ser capazes de se integrar de forma fluída com forças convencionais, agências de inteligência e parceiros locais, a fim de garantir o sucesso da missão em diferentes ambientes operacionais. Para além dos domínios tradicionais da guerra, esta força tem uma elevada capacidade tecnológica que desempenha um papel crucial no ciberespaço, onde as unidades das Forças de Operações Especiais estão cada vez mais envolvidas em operações ofensivas e defensivas. Com conhecimentos avançados em guerra cibernética e análise forense digital, os operadores da FOEsp podem interromper comunicações inimigas, sabotar infraestruturas críticas e recolher informações através de meios cibernéticos. Ao integrar capacidades cibernéticas no seu arsenal tático, as unidades FOEsp obtêm uma vantagem significativa no domínio da informação, permitindo-lhes superar adversários e alcançar objetivos estratégicos com maior agilidade e precisão.

A FOEsp possui assim várias capacidades que a permitem desempenhar a sua missão da maneira mais eficaz possível, sendo elas as seguintes: Exército Português (2014)

(1) Conduzir operações especiais em todo o espectro das operações militares.

(2) Dispor de organização e aptidão para planear, executar, comandar e controlar as suas missões, e capacidade para comandar as SOTU subordinadas; podendo empregar numa mesma operação, mais do que uma SOTU no mesmo objetivo.

(3) Conduzir operações de forma aberta, coberta ou discreta.

(4) Inserir e extrair da AOp por meios navais, terrestres e aéreos.

(5) Conduzir operações e garantir a sustentação de elementos operacionais em território hostil ou negado, e garantir a sua sobrevivência, evasão e recuperação deste território, se necessário.

(6) Garantir a proteção da força.

(7) Operar como parte de uma estrutura conjunta-combinada, quando empenhada nestas circunstâncias.

Tendo em conta as suas variadas capacidades, a FOEsp pode atuar em variadas tipologias de operações (Exército Português, 2014).

<table>
<tr><td>Ação Direta
Tarefas Primárias
• Golpes de mão e emboscadas
• Sniping
• Guiamento terminal
• Recuperação
• Resgate de reféns
• Operações de destruição de precisão</td><td>Reconhecimento Especial
Tarefas Primárias
• Avaliação de objetivo
• Avaliação da ameaça
• Reconhecimento pós-ataque
• Reconhecimento ambiental</td></tr>
<tr><td>Assistência Militar
Tarefas Primárias
• Treino
• Aconselhamento
• Mentoria/Parceria</td><td>Ação Indireta
Tarefas Primárias
• Organizar, equipar, treinar, assessorar, apoiar e, se necessário, dirigir forças de resistência
• Treinar, assessorar, equipar e apoiar FIrreg
• Treinar, equipar e apoiar o estabelecimento de redes de fuga e evasão</td></tr>
<tr><td colspan="2">Outras tarefas primárias
• Proteção de Altas Entidades em zonas de conflito
• Ligação com fações</td></tr>
</table>

Figura 8: Tipologia de operações das FOEsp

Fonte: Exército português, 2014

1.4.2 Destacamento de Ações Especiais

Em paralelo com as Operações Especiais do Exército, temos o Destacamento de Ações Especiais da Marinha, pertencente ao Corpo de Fuzileiros. Esta unidade intercalou a FOE na sua presença na Roménia, participando na 3ª e 6ª FND.

O conceito desta força é muito semelhante ao das Operações Especiais e a Marinha (2025) define-a como sendo capaz de executar a totalidade das missões no âmbito das Operações Especiais, esta força tem a capacidade de operar desde elementos de pequena dimensão até ao nível de uma Special Operations Maritime Task Unit (SOMTU). A sua utilização pode ocorrer de forma independentes ou integrada numa Special Operations Task Group (SOTG), seja de constituição nacional ou em articulação com forças de Operações Especiais de países aliados. Adicionalmente, pode desempenhar funções de estado-maior em estruturas nacionais ou internacionais, bem como prestar apoio a unidades de Fuzileiros ou outras forças convencionais. Dada a diversidade de missões que lhe são atribuídas, o Destacamento de Ações Especiais realiza operações de elevado risco e sensibilidade, muitas das quais fora de conhecimento público, exigindo dos seus militares um elevado grau de preparação técnica, capacidade física, destreza operacional e conhecimento especializado. A sua inserção no teatro de operações pode ocorrer por diferentes meios e vetores – marítimo, aéreo e terrestre – utilizando plataformas como navios de superfície, submarinos ou aeronaves, e técnicas como fast rope, paraquedismo e mergulho de combate, entre outras. Esta unidade de Operações Especiais distingue-se por um elevado grau de autonomia e por uma capacidade de combate significativa, assente na aplicação de técnicas específicas de forma dissimulada e no emprego de equipamentos tecnologicamente avançado e altamente eficaz. Estas caraterísticas impõem elevados padrões de treino, aptidão e competência tanto a nível individual como coletivo.

1.4.3 Força Nacional Destacada de Operações Especiais na Roménia

O relacionamento entre a Organização do Tratado do Atlântico Norte (OTAN) e a Federação Russa tem sido caracterizado por dinâmicas disjuntivas, destacando-se, em particular, a questão ucraniana a partir de 2014 como um ponto de inflexão. Neste contexto, face à crise na Ucrânia, o North Atlantic Council (NAC) da OTAN aprovou a implementação de um programa coerente, sustentável e visível, composto por um conjunto de medidas de natureza defensiva, no âmbito do Readiness Action Plan (RAP) da OTAN. Posteriormente, na Cimeira de Varsóvia de 2016, a OTAN deliberou o reforço da sua presença militar na zona oriental do território da Aliança, nomeadamente na Roménia. Em conformidade com esta decisão, e tendo em consideração o enquadramento anteriormente referido, Portugal, enquanto Estado-membro da OTAN, tem participado na tailored Forward Presence (tFP) no flanco sudeste da Aliança, com presença destacada em território romeno (Miranda, 2024).

Na sequência da invasão da Ucrânia pela Rússia e da ativação dos Planos de Resposta Gradual da OTAN, foi desenvolvido um conceito de dissuasão e defesa da área euro-atlântica, no âmbito do qual foram projetadas Forças de Operações Especiais para a Roménia, entre 2022 e

2024, numa lógica de cooperação bilateral entre Portugal e Roménia (Roxo, 2024).

Esta Força Nacional Destacada de Operações Especiais na Roménia (FND OEsp/ROU) foi integrada no SOTG 51, ficando na dependência do Comando da Componente de Operações Especiais romena, sediado em Târgu Mures (Roménia), tendo iniciado a sua missão em 17 de maio de 2022 (Matias, 2024).

Desde os primeiros momentos, a cooperação entre as Forças de Operações Especiais (FOEsp) portuguesas e romenas tem-se revelado altamente proveitosa, alicerçada numa relação de confiança mútua e respeito institucional, destacando-se as capacidades técnicas e a experiência profissional de ambas as forças. Esta parceria bilateral assume particular relevância não apenas pelo seu valioso contributo para a presença da NATO na região Leste da Europa, mas sobretudo pelo desenvolvimento conjunto de técnicas, táticas e procedimentos. Estes, em articulação com a inovação tecnológica que acompanha a evolução das Forças Armadas contemporâneas, contribuem de forma significativa para potenciar as capacidades operacionais das FOEsp nacionais (Fonseca, 2024).

A FND OEsp/ROU, situada na cidade de Târgu Mures, encontra-se articulada e integrada no Special Operations Component Command Romeno (SOCC/ROU) com a Special Operations Land Task Unit (SOLTU) a colaborar em exercícios combinados com o Special Operations Land Task Group 51 (SOLTG 51), pertencente ao SOCC/ROU (Miranda, 2024).

Assim sendo, a 15 de abril de 2022 Portugal enviou para a Roménia a 1ª Força Nacional Destacada (FND), constituída pelo Comando e Estado-maior; uma companhia de atiradores mecanizada de rodas; um módulo conjunto de Informações; um módulo de defesa-anti-aérea; um módulo geográfico e meteorológico; um módulo de apoio e uma SOTU de Operações Especiais constituída por 20 militares (Exército Português, 2022).

Figura 9: Flanco oriental da OTAN

Fonte: NATO, 2022

Tabela 1: Cronologia da Cooperação bilateral com a Roménia

Fonte: Elaboração própria

	PROJEÇÃO	RETRAÇÃO
1ª FND	Abril de 2022	Setembro de 2022
2ª FND	Setembro de 2022	Janeiro de 2023
3ª FND	Janeiro de 2023	Maio de 2023
4ª FND	Maio de 2023	Outubro de 2023
5ª FND	Outubro de 2023	Fevereiro de 2024
6ª FND	Fevereiro de 2024	Junho de 2024
7ª FND	Junho de 2024	Outubro de 2024

A FND na Roménia tem mantido o efetivo de SOTU ao longo dos anos, até que, a 7 de novembro de 2024, o CTOE enviou para a Roménia a 1ª Força Nacional Destaca Special Operations Land Task Group (SOLTG), duplicando assim o seu efetivo no teatro de operações. "Transitando de uma Task Unit (TU) para um Task Group (TG), finalizando assim esta fase de empenhamento e preparando-se para uma nova fase mais robusta e com enquadramento NATO, cuja projeção para o TO está prevista para o último trimestre de 2024, com a designação 1FND/SOLTG/ROU" (Matias, 2024). Esta força tem como missão reforçar as capacidades de resposta dos Aliados, no âmbito das atividades de Vigilância do Flanco Leste da NATO, contribuindo para os planos de defesa coletiva e de dissuasão da Aliança Atlântica (Exército Português, 2024).

CAPÍTULO 2 – METODOLOGIA

Este capítulo apresenta o percurso metodológico adotado nesta investigação científica, detalhando a formulação dos objetivos e questões de investigação, o delineamento do estudo, a metodologia e estratégia investigativa, a natureza da abordagem escolhida, os procedimentos de recolha de dados, os critérios de amostragem e as técnicas utilizadas para o tratamento e análise dos dados.

2.1. Desenho da investigação

A presente investigação encontra-se delimitada temporalmente, do ano 2022 até 2024, ano em que foi enviada a última FND (SOTU/ROU) para a Roménia.

O OG do presente trabalho foca-se em "Melhorar e propor táticas de contra-ameaça híbrida na Força Nacional Destacada de Operações Especiais Portuguesa na Roménia.".

Na sequência da identificação do OG e consequentes OE da investigação, foi formulada a PP, que pretende responder à essência da investigação, e respetivas Perguntas Derivadas (PD), de forma a responder aos objetivos resultantes da temática da investigação.

− PP: Como podem ser melhoradas e propostas táticas de contra-ameaça híbrida na FND na Roménia?

− PD1: Quais são as características específicas das ameaças híbridas enfrentadas pela FND na Roménia?

− PD2: Que táticas de contra-ameaça híbrida estão a ser usadas pela FND na Roménia?

− PD3: Que táticas de coordenação e cooperação existem entre a FND e outros países para fortalecer a resiliência e a capacidade de resposta a ameaças híbridas?

Como linha orientadora desta investigação, foi adotado o desenho de investigação apresentado no Quadro n.º 1, que incorpora um modelo de análise misto, assim como os indicadores pretendidos, com o objetivo de facilitar a recolha e organização dos dados necessários.

Quadro 1: Desenho da investigação

OG	Melhorar e propor táticas de contra-ameaça híbrida na Força Nacional Destacada de Operações Especiais Portuguesa na Roménia				
PP	Como podem ser aprimoradas e propostas táticas de contra-ameaça híbrida na FND na Roménia?				
OE	**PD**	**Conceitos**	**Dimensões**	**Indicadores**	**Técnicas de recolha de dados**
OE1: Analisar o contexto e as caraterísticas específicas das ameaças híbridas na atuação da FND na Roménia	**PD1**	Ameaças híbridas	Realidade Conflitual	-Foco das Ameaças Híbridas -Tipologia de AH	Análise documental Entrevista exploratória
OE2: Investigar táticas de contra-ameaça híbrida que estão a ser usadas pela FND na Roménia	**PD2**	Contra-ameaça híbrida	Realidade Conflitual	-Estratégias de contra-ameaça híbrida	Análise documental Entrevista exploratória
OE3: Investigar táticas de coordenação e cooperação eficientes entre a FND e outros países com o objetivo de fortalecer a resiliência e a capacidade de resposta a ameaças híbridas	**PD3**	Contra-ameaça híbrida	Realidade Conflitual	-Exercícios conjuntos -Interoperabilidade	Análise documental Entrevista exploratória

De forma a responder às PD foram realizadas entrevistas a militares de operações especiais com um cargo direto ou indireto na FND na Roménia, como também, foi feita uma pesquisa baseada na análise documental de documentos oficiais.

2.2. Método e Estratégia de Investigação

Foi seguida uma abordagem qualitativa que reconhece a interação entre o sujeito e o mundo, bem como as suas relações, sem desconsiderar a subjetividade tanto dos participantes do estudo quanto do investigador (Mineiro et al., 2022).

O método que a presente investigação seguiu foi o método descritivo, tem como objetivo representar com precisão os factos e os fenômenos de uma determinada realidade. Esta abordagem é utilizada quando o investigador pretende compreender uma comunidade específica, analisar as suas características, valores e questões culturais associadas (Oliveira, 2011). O tipo de investigação que iremos seguir é um estudo de caso não experimental, num estudo de caso, as análises e reflexões ocorrem ao longo de todas as etapas da investigação, especialmente durante a recolha de informações, dados e evidências. Nessas circunstâncias, resultados parciais podem indicar a necessidade de ajustes ou redireccionamentos no percurso da pesquisa (Martins, 2008).

2.3. Técnica de recolha de dados

Para a recolha de dados deste estudo, destacam-se dois momentos distintos: o enquadramento teórico e a fase empírica.

Inicialmente, durante a elaboração do enquadramento teórico, a recolha de dados centrou-se na análise documental de fontes primárias e secundárias. As fontes primárias consistiram em documentos institucionais disponibilizados pela estrutura interna do Exército português. Já as fontes secundárias foram obtidas por meio da consulta a livros, e-books, artigos científicos, revistas académicas e dissertações de mestrado.

A pesquisa em fontes secundárias foi realizada em plataformas online, recorrendo a um motor de busca, Google Académico, bases de dados como a EBSCO e repositório científico como o RCAAP. Para delimitar a área de investigação, foram utilizadas palavras-chave como "Ameaças híbridas", "Contra-ameaça híbrida" e "Força de Operações Especiais".

Na fase seguinte, correspondente à parte empírica, foi adotada a técnica de inquérito por entrevista. Esta assumiu um caráter exploratório, sendo conduzida numa fase inicial da investigação com o objetivo de aprofundar o conhecimento sobre o tema em estudo.

Esta teve como principal função "a obtenção de informação mais detalhada e profunda - dificilmente conseguida por meio de um questionário, devido ao caráter flexível e reversível dos processos de condução e formulação de questões" (A. T. A. da R. B. A. Alves et al., 2021) e adotou-

se o formato de entrevista semiestruturada, uma vez que se procura observar aspetos mais relacionados com o contexto situacional da entrevista enquanto género discursivo e o seu componente interativo na relação entre entrevistador e entrevistado (Castro & Oliveira, 2023).

2.4. Amostragem

Relativamente aos inquéritos por entrevista, estes foram direcionados aos comandantes das FND OE destacados para a Roménia e ainda a um militar pertencente à célula de informações do Estado Maior General das Forças Armadas (EMGFA), conforme o Apêndice B.

2.5. Tratamento dos dados

Após a recolha de dados, foi essencial proceder à sua análise e tratamento. No caso das informações obtidas através das entrevistas exploratórias, foram elaboradas sínteses, apresentadas no Apêndice C, com o objetivo de reunir as principais ideias e identificar pontos comuns entre os entrevistados, facilitando assim a sua comparação futura. Dessa forma, a sistematização e tratamento dos dados permitiram a formulação das conclusões desta investigação.

CAPÍTULO 3 – DESAFIOS E LIMITAÇÕES DA REAÇÃO A AMEAÇAS HÍBRIDAS PELA FND NA ROMÉNIA

Com o intuito de complementar a investigação desenvolvida com recurso às ferramentas metodológicas anteriormente expostas, este capítulo dedica-se à apresentação e descrição dos dados obtidos por via da realização das entrevistas.

Foi realizada uma análise direta das entrevistas conduzidas, estruturada com base nas questões definidas no guião, tendo sido delimitados os fatores e critérios relevantes, em conformidade com os objetivos específicos associados ao corpo das questões. Os dados recolhidos foram, assim, analisados de forma objetiva, assegurando a coerência entre os resultados obtidos e os propósitos da investigação. A análise procurou ainda, identificar padrões recorrentes, divergências significativas e implicações operacionais das respostas obtidas, permitindo uma análise mais precisa da realidade da FND no contexto das ameaças híbridas.

Neste capítulo, serão identificados principais desafios e limitações da reação a ameaças híbridas por parte da FND na Roménia, tendo como finalidade responder à PD1: "Quais são as características específicas das ameaças híbridas enfrentadas pela FND na Roménia?" e à PD2: "Que táticas de contra-ameaça híbrida estão a ser usadas pela FND na Roménia?".

Dentro das variadas questões apresentadas aos entrevistados, neste capítulo, e para obtermos uma análise objetiva e concreta, vamos focar a atenção nas respostas às questões 1-9 e 12. Estas questões abordam dimensões essenciais da atuação da FND, desde a perceção das ameaças até à resposta tática e organizacional, incluindo aspetos como formação, interação local e modernização tecnológica.

Quando questionados sobre quais as ameaças híbridas predominantes enfrentadas pela FND na Roménia, as entrevistas, apesar das diferentes ênfases de cada depoimento, emergem cinco eixos comuns de interpretação.

Ameaças híbridas de baixa intensidade, mas presentes. Todos os entrevistados reconheceram a existência de ameaças híbridas no TO da Roménia, ainda que por vezes sem contacto direto com incidentes. As ameaças foram descritas como discretas, indiretas e adaptativas, atuando em domínios variados e com diferentes intensidades. Esta perceção converge para a caraterização das ameaças como atuando abaixo do limiar do conflito aberto. Estas ameaças não são visíveis, mas manifestam-se por via de pequenas alterações no ambiente operacional ou em padrões de comportamento, exigindo atenção redobrada por parte da força.

Guerra de informação e desinformação como vetores centrais. A guerra informacional é

amplamente referida pelos entrevistados. Dois deles apontam especificamente para a existência de campanhas de desinformação dirigidas à opinião pública romena, com o objetivo de descredibilizar as forças da OTAN. Outro militar referiu a influência sobre a população nativa como um dos objetivos centrais dos serviços russos, procurando deslegitimar a presença da OTAN na região.

Centralidade do ciberespaço como domínio de ameaça. Foi salientado o uso de atividades maliciosas, APTs, sabotagem digital, bots e desinformação. Esta visão é complementada com referência à ameaça a infraestruturas críticas, nomeadamente, fontes de energia e sistemas de informação próximos de bases da OTAN.

Ameaças aos serviços de apoio e infraestruturas. É feita menção à tentativa de prejudicar serviços de saúde, segurança e energia próximos de campos militares, como parte do esforço subversivo russo. Esta observação liga-se diretamente às preocupações com a resiliência do ambiente envolvente, um aspeto crítico em ambiente híbrido.

Atividades de espionagem e recolha de informação. É relatado restrições a determinados locais por indícios de espionagem. Em paralelo, é mencionado expressamente os objetivos dos serviços de informações russos em recolher dados sobre as forças da OTAN e o seu grau de prontidão. A espionagem e recolha de informação sensível é vista como uma ameaça presente, operando de forma camuflada e integrada em ações híbridas.

Quando inquiridos sobre a existência de um padrão específico na forma como as ameaças híbridas são desencadeadas contra forças da NATO na região, as entrevistas, relatam que existem várias ideias convergentes que sugerem padrões operacionais consistentes por parte de agentes hostis, apesar de algumas limitações ao nível da perceção direta dos entrevistados.

Utilização de meios sociais e humanos para recolha de informação. É referido formas de interação humana e social como mecanismo de recolha de informação ou comprometimento da força. São exemplos, a aproximação de mulheres em contextos noturnos com possível objetivo de extorsão; utilização de locais de lazer e estabelecimentos comerciais para observação e contacto com militares; emprego de ativos pró-Rússia como elementos facilitadores.

Coordenação entre diferentes vetores de ataque (ciber, desinformação, criminalidade organizada). É mencionado a combinação entre campanhas de desinformação e ataques cibernéticos (associados a momentos de tensão ou operações da OTAN) e ainda, é feita ligação entre o crime organizado, serviços secretos russos e o uso de estabelecimentos civis para infiltração e monitorização.

Ciberespaço como ferramenta de atuação regular e estratégica. É destacado ciberataques a redes sociais, plataformas digitais e infraestruturas. Padrões de intensidade de ataques correlacionados com eventos políticos, como por exemplo, visitas diplomáticas. Uso do ciberespaço como meio de pressão diplomática ou influência.

Repetição e temporalidade dos ataques. É notado a existência de padrões temporais, nomeadamente, ataques informacionais/cibernéticos e grandes eventos (exercícios miliares, crises políticas), e também, regularidade nas abordagens sociais e comportamentos suspeitos.

Quando sondados sobre a forma como a desinformação e a manipulação da opinião pública afeta a perceção e a eficácia da FND na Roménia, as entrevistas revelam que existem várias ideias em comum, que se convergem numa perceção crítica e informada da relevância do ambiente informacional para a missão.

Risco direto para a credibilidade e imagem da FND. É reconhecido que a desinformação pode afetar negativamente a perceção externa da FND, com impactos diretos na sua credibilidade junto da opinião pública local, das autoridades nacionais e das entidades da OTAN. A desinformação compromete a imagem institucional e pode afetar o apoio popular à presença da FND. Pode ser explorada por atores hostis para fragilizar a cooperação com autoridades locais e forças aliadas. Pequenas falhas comportamentais dos militares podem ser amplificadas e manipuladas, contribuindo para cenários de rejeição.

Necessidade de controlo e comunicação estratégica. É sublinhado a importância de gerir proactivamente a comunicação da FND para evitar a propagação de informação falsa ou prejudicial. A implementação de uma estratégia de comunicação bilateral com forças romenas e com a OTAN, revelou-se uma ferramenta essencial. Esta estratégia, além de blindar a força contra potenciais riscos informacionais, contribuiu para reforçar a imagem positiva dos militares portugueses, potenciando a continuidade da presença nacional, desta vez como Special Operations Land Task Group (SOLTG). O controlo rigoroso das mensagens veiculadas à comunicação social contribui para reforçar a imagem positiva da FND.

Desinformação como instrumento de guerra híbrida. Exploração de falhas sistémicas (serviços públicos, segurança, saúde) para atribuir responsabilidade à OTAN e alimentar narrativas hostis. Utilização de meios encobertos (bots, redes sociais) para disseminar desinformação e moldar opiniões.

Consequências para a moral e cooperação local. O efeito da desinformação na qualidade da interação com a população e autoridades locais. A perceção negativa da força pode reduzir a capacidade de atuação e colaboração. A oposição pública à presença da OTAN pode comprometer a estabilidade social no TO.

Quando indagados sobre a forma como a FND avalia a presença e a influência de agentes estatais e não estatais nas dinâmicas de ameaça híbrida na região, os entrevistados revelam níveis distintos de perceção e envolvimento na avaliação da presença e influência de agentes estatais e não estatais na região da Roménia. Ainda assim, é possível identificar três eixos comuns.

Limitações de avaliação direta. Dois dos entrevistados reconhecem não ter meios próprios

ou autonomia para uma avaliação fundamentada da presença destes agentes. A ausência de ativos de recolha de informação no terreno ou a falta de contacto direto com elementos hostis limita a perceção sobre a ameaça. Esta realidade traduz-se numa dependência de estruturas externas para recolha e análise de informação. Esta limitação evidencia uma vulnerabilidade estrutural, particularmente relevante em ambientes híbridos, onde a deteção precoce e o mapeamento de atores hostis são determinantes para a resposta eficaz.

Avaliação por intermédio de cooperação com entidades aliadas. Outros dois entrevistados indicam que a FND procede à avaliação dessas ameaças por via de cooperação institucional, nomeadamente com autoridades locais romenas, serviços de informações nacionais e aliados, elementos de forças especiais OTAN e estruturas de contraespionagem digital (monitorização de redes sociais dos militares). É assim realçado que, mesmo na ausência de meios próprios, a partilha de inteligência e a coordenação multinacional são essenciais para manter o conhecimento situacional e prevenir ações hostis.

Quando abordados sobre que medidas proativas a FND tem implementado para detetar e neutralizar ações híbridas antes da sua materialização, os entrevistados confirmaram que a eficácia no combate às ameaças híbridas depende em larga medida da capacidade de antecipação e resposta precoce das forças no terreno. A análise das entrevistas revela que a FND tem adotado medidas proativas, com enfoque na formação, monitorização informacional e sensibilização situacional, ainda que com limitações reconhecidas ao nível estrutural e doutrinário.

Formação e sensibilização como base preventiva. Todos os entrevistados referem, de forma direta ou indireta, que a preparação dos militares para lidar com ameaças híbridas começa na fase de aprontamento, através de palestras e ações de formação. São mencionadas sessões promovidas pelo Centro de Segurança Militar e de Informações do Exército (CSMIE) e pelo Comando de Operações e Ciberdefesa (COCiber), que abordam temas como ciberdefesa, segurança da informação e riscos de espionagem. Estas ações foram percecionadas como medidas fundamentais de prevenção, contribuindo para elevar a consciência dos militares sobre os riscos presentes no TO.

Monitorização e análise contínua da informação. Três dos quatro entrevistados indicam que existem mecanismos internos de observação e análise regular, com destaque para a produção de relatórios (como o "Situational Awareness Report") e o acompanhamento diário de fontes selecionadas. Esta prática permite manter a força informada sobre os desenvolvimentos regionais e internacionais, criando um quadro de vigilância contínua.

Colaboração com entidades externas. É referido a cooperação com entidades de segurança locais, como os serviços de Contra Informação (CI) romenos e outras forças da OTAN, que ajudam na troca de informação e no apoio à identificação de ameaças. A partilha de inteligência é apontada como essencial para a antecipação de riscos.

Aplicação de TTP's existentes de forma adaptativa. Apesar de não existir uma doutrina formalizada de contra-ameaça híbrida, é mencionado que existem TTP's que são aplicadas conforme a situação identificada, revelando uma capacidade adaptativa por parte da força.

Quando interpelados sobre a existência de doutrina ou TTP's (Táticas, Técnicas e procedimentos) desenvolvido pela FND para lidar com ameaças híbridas, os entrevistados enunciaram que a doutrina e a aplicação de TTP's (Táticas, Técnicas e Procedimentos) assumem um papel central na padronização da atuação das forças em contextos operacionais complexos. No entanto, a análise das entrevistas revela um cenário de transição e construção doutrinária no seio da FND no que se refere à resposta às ameaças híbridas. Embora os militares entrevistados reconheçam a existência de alguns procedimentos e comportamentos adotados no terreno, não há ainda uma doutrina formalizada, nem um conjunto de TTP's especificamente estruturados e disseminados para este tipo de ameaça.

As respostas indicam que a atuação das FND, é na maioria dos casos, orientada por práticas empíricas e adaptativas, baseadas na experiência, no bom senso operacional e em formações anteriores. É descrito comportamentos padronizados de vigilância, gestão de incidentes e reporte como medidas de autoproteção, o reporte formal para o escalão superior de qualquer suspeita de ocorrência é de grande importância, pois permite despistar eventuais processos de investigação de segurança nacional. É salientado que estas ações não decorrem de uma orientação doutrinária específica, sendo, antes, respostas táticas e conscientes do contexto.

Importa destacar que a missão permitiu recolher lições identificas e aprendidas (LI/LA), as quais estão em fase de conversão para TTP's futuras. Esta afirmação evidencia a existência de um processo de amadurecimento doutrinário ainda que em curso, mas que carece de sistematização e implementação prática.

De forma geral, a resposta a ameaças híbridas por parte da FND continua a assentar numa lógica reativa, com forte dependência da iniciativa individual e de canais informais de comunicação e proteção. A inexistência de TTP's formais representa uma fragilidade, sobretudo perante a crescente sofisticação e imprevisibilidade das ameaças híbridas.

Quando consultados sobre o treino específico que os militares da FND recebem para lidar com ameaças híbridas no contexto da Roménia, os entrevistados apontam para uma realidade formativa pouco estruturada e assimétrica no que diz respeito ao treino específico para lidar com ameaças híbridas. Há um consenso generalizado de que a formação recebida é pontual, fragmentada e, em muitos casos, centrada apenas na sensibilização teórica.

Em primeiro lugar, destaca-se que as ações de formação identificadas são maioritariamente ministradas por entidades como o Centro de Segurança e de Informações do Exército (CSMIE) e o Comando de Operações de Ciberdefesa (COCiber), centrando-se em ciberdefesa, combate à

desinformação, medidas preventivas e orientação para o manuseamento de redes sociais. Estas formações são descritas como de partilha de informação, ou seja, sem a componente prática ou sistematizada, o que revela uma abordagem informativa mais do que operacional.

Em segundo lugar, verifica-se a existência de diferenças entre militares com diferentes responsabilidades dentro da força, que recebem formação especializada oriunda de serviços dedicados ao combate a ameaças híbridas, e o restante efetivo, apenas recebe briefings genéricos sobre o estado da ameaça no TO. Esta distinção contribui para uma disparidade na preparação dentro da força, criando potenciais vulnerabilidades na uniformidade da resposta.

Em terceiro lugar, é evidenciado que parte significativa da preparação dos militares baseia-se em apoio informal, como contactos pessoais ou reuniões reservadas com partilha seletiva de informação. Este fator aponta para uma ausência de doutrina e treino estruturado e transversal, substituído por práticas informais e não institucionalizadas.

Além disso, não foi referida a realização de exercícios práticos ou simulações, o que compromete a capacidade dos militares em aplicar, de forma eficaz, o conhecimento teórico adquirido. Em contexto híbrido, onde a ambiguidade e a imprevisibilidade são predominantes, a ausência de treino adaptado pode representar um risco significativo para a força.

Quando inquiridos sobre a existência de um modelo de alerta precoce que permita antecipar ataques híbridos e mobilizar a FND de forma eficiente, as respostas recolhidas demonstram uma ausência generalizada de um modelo formal, estruturado e institucionalizado de alerta precoce no contexto da atuação da FND na Roménia. Em vez disso, a resposta às ameaças híbridas depende sobretudo de experiência individual, perceções subjetivas e sinais contextuais informais.

Dois dos entrevistados reconhecem abertamente a inexistência de mecanismos de alerta precoce, seja por desconhecimento direto, seja pela ausência de meios próprios de recolha de informação no terreno, o que limita drasticamente a capacidade da FND em antecipar e reagir proactivamente a ameaças emergentes.

Um dos entrevistados admite que não existe fisicamente um modelo, mas que o conhecimento e a experiência operacional permitem, em certa medida, detetar indícios de ameaças híbridas. Esta afirmação sugere a presença de competência técnica e sensibilidade operacional, mas não substitui a eficácia de um sistema de alerta estruturado, sistematizado e institucionalmente validado.

Por último, é referido que alguns sinais de alerta informal podem derivar de comportamentos específicos de nativos, como interações insistentes com militares, em especial através de canais digitais ou físicos. Esta observação, embora relevante, não configura um modelo de alerta, mas sim uma perceção individual baseada na observação e intuição.

Quando questionados sobre a forma como a interação com as comunidades locais contribui

para a eficácia das operações da FND, tendo em conta as ameaças híbridas, os entrevistados argumentaram que, apesar da missão ter decorrido num ambiente de cooperação bilateral e não operacional, a relação com as autoridades locais foi positiva e estratégica. É sublinhado que o bom relacionamento institucional contribuiu para a construção de uma imagem sólida e respeitada da FND, o que reforça o seu capital de legitimidade e confiança junto da população e das estruturas locais. Embora não se refira diretamente a ameaças híbridas, é evidente que essa aceitação local constitui uma barreira indireta à ação de agentes hostis, nomeadamente em tentativas de desinformação.

A interação local como elemento facilitador da missão. Todos os entrevistados apontam que, mesmo não sendo uma missão operacional, o bom relacionamento com as autoridades e comunidades locais favorece o ambiente operacional da FND. Este fator contribui não apenas para uma imagem positiva da força, mas também para a aceitação social da sua presença, minimizando tensões e prevenindo interpretações hostis da sua atuação.

Utilidade estratégica da ligação com atores locais. As respostas indicam que a colaboração com autoridades locais é valorizada como uma ferramenta estratégica, potenciando a partilha de informações relevantes e a consciencialização situacional. Esta ligação pode funcionar como uma forma indireta de alerta precoce para ameaças não convencionais, aumentado a capacidade de prevenção da força.

Papel da interação na luta contra a desinformação. Foi destacado que o contacto com as comunidades pode ajudar a contrariar falsos testemunhos, especialmente aqueles disseminados por campanhas de influência hostil. O envolvimento com a população local serve, assim, como barreira à descredibilização da presença da OTAN.

Ausência de doutrina formal, mas prática operacional existente. Apesar de não existir uma diretiva formalizada sobre este tipo de interação, os entrevistados reconhecem a lógica e relevância operacional da prática. A relação com o meio local, depende do bom senso, da experiência e da sensibilidade dos comandantes em contexto.

Quando interpelados sobre como a FND avalia a necessidade de modernização das suas capacidades em reposta ao caráter dinâmico das ameaças híbridas, as entrevistas revelam que existe uma consciência transversal, entre os militares entrevistados, da necessidade urgente de modernização da FND para responder eficazmente às ameaças híbridas.

Todos os entrevistados concordam que as ameaças híbridas exigem uma adaptação constante das capacidades da FND. Essa modernização deve abranger áreas como ciberdefesa, guerra eletrónica, inteligência e novos equipamentos, especialmente face ao surgimento de novas tecnologias e formas de ataque (ex.: uso de drones).

Lacunas atuais na resposta às ameaças híbridas. As respostas identificam vulnerabilidades

persistentes, como a ausência de sistemas de inibição ou neutralização de drones, onde a resposta disponível ainda depende de medidas convencionais de destruição física, em detrimento de soluções tecnológicas como a inibição de sinal ou sistemas anti-drone de nova geração, a falta de integração entre domínios operacionais e a inexistência de padrões uniformes de sensibilização. Estes fatores limitam a capacidade da FND em responder de forma eficaz e coordenada.

Resistência à mudança e lentidão nos processos institucionais. Foi apontado que, apesar de existirem esforços e consciência da necessidade de mudança, a implementação prática enfrenta barreiras culturais e burocráticas. A tendência para manter práticas tradicionais e a morosidade nos processos de inovação dentro das Forças Armadas portuguesas são vistas como obstáculos à modernização urgente.

Avaliação baseada em feedback operacional. É referido que a FND procura ajustar capacidades com base em exercícios internacionais e relatórios AAR (After Action Review) e FIR (First Impression Report), evidenciando uma prática de aprendizagem contínua baseada na experiência no terreno. No entanto, essa prática não é suficiente se não for acompanhada por mudanças estruturais e investimento estratégico.

Importância da integração multidomínio. Existe uma convergência sobre a necessidade de integrar a FND nos conceitos multidomínio da OTAN, especialmente no que diz respeito à coordenação entre domínios físico, informacional e cibernético. Esta integração é vista como um passo essencial para aumentar a eficácia operacional no combate a ameaças híbridas.

CAPÍTULO 4 – COORDENAÇÃO E COPERAÇÃO ENTRE A FND E OUTRAS FORÇAS ALIADAS

No presente capítulo será analisado a forma como é feita a cooperação entre a FND e as forças aliadas presentes no TO da Roménia, quais as implicações, benefícios e vantagens desta cooperação, tendo como finalidade responder à PD3: "Que táticas de coordenação e cooperação existem entre a FND e outros países para fortalecer a resiliência e a capacidade de resposta a ameaças híbridas?". Igualando o capítulo anterior, será feita uma análise objetiva da resposta dos entrevistados ao guião de entrevista. Para isto, iremos considerar as restantes questões que não foram previamente analisadas, ou seja, questões 10,11 e 13.

Quando abordados sobre a forma como é feita a partilha de informações de inteligência entre a FND e as restantes forças da NATO presentes na Roménia, os entrevistados declararam que existem mecanismos estabelecidos e funcionais para a partilha de informações de inteligência entre a FND e os restantes elementos da OTAN, tanto a nível nacional como internacional.

Existência de canais formais e seguros de partilha de informação. As repostas sugerem a utilização de sistemas próprios e seguros para a partilha de inteligência, como os canais NSWAN (NATO Secret Wide Area Network) e BICES (Battlefield Information Collection and Exploitation System). Esta referência indica uma prática padronizada dentro da OTAN que também é seguida pela FND. A nível nacional, a partilha de informação é feita entre a FND e o módulo de informações e comunicações do Exército.

Realização de briefings regulares como mecanismo de intercâmbio de informação. É destacada a realização de briefings semanais ou reuniões regulares entre elementos da FND e forças aliadas, como forma de partilhar dados relevantes sobre o teatro de operações. Este método complementa os sistemas digitais com uma componente presencial e colaborativa. Além disso, os briefings constituem um espaço privilegiado para alinhar perceções, identificar vulnerabilidades comuns e promover a confiança mútua entre contingentes multinacionais, fatores decisivos para o sucesso da ação coordenada.

Estando a FND inserida numa força romena, a partilha de informação é mediada através do Comando das Operações Especiais da Roménia, havendo assim uma elevada fluidez no intercâmbio de dados.

Quando sondados sobre de que forma a interoperabilidade entre a FND e forças especiais de outros países influência a eficácia no combate a ameaças híbridas, os entrevistados confirmaram que a interoperabilidade é considerada um pilar essencial para o sucesso em ambientes

operacionais complexos, como os associados às ameaças híbridas. Esta permite que as forças atuem com maior eficácia, fluidez e sincronização, garantindo uma resposta conjunta mais robusta.

As respostas apontam diretamente para a importância crítica da interoperabilidade como fator do sucesso na atuação conjunta contra ameaças híbridas. Os entrevistados destacam que a interoperabilidade não se limita à partilha de equipamentos ou doutrina, mas estende-se a elementos como mentalidade comum (mindset), compreensão situacional e comunicação entre forças. É evidenciado que, no contexto da missão da FND, a procura por uma maior interoperabilidade com as forças especiais romenas, permitiu o treino conjunto e o contacto direto com os equipamentos dos aliados, contribuindo para a adaptabilidade e preparação da força nacional. Esta prática contribui não só para o desenvolvimento técnico-tático da força, mas também para a harmonização cultural e procedimental, fatores que reduzem a margem de erro em operações conjuntas e aumentam a eficiência global.

A cooperação reforça a capacidade de resposta e adaptabilidade. É consensual entre os entrevistados que a interoperabilidade promove melhor adaptabilidade, resposta rápida e compreensão alargada do ambiente operacional, aspetos fundamentais no combate a ameaças de natureza híbrida.

Partilha de experiências, meios e doutrinas. É referido que a troca de experiências, táticas e recursos é uma vantagem prática da interoperabilidade. O treino conjunto com forças romenas reforça a ideia de que a cooperação multinacional permite a evolução técnica e tática contínua da FND. A adoção de boas práticas oriundas de outras forças, bem como a capacidade de executá-las em ambiente multinacional, favorece a melhoria contínua da FND e contribui para a sua evolução.

Quando indagados sobre a existência de exercícios conjuntos ou mecanismos de treino específicos para fortalecer a cooperação entre a FND e as restantes forças da NATO, os entrevistados afirmam que a cooperação operacional entre forças multinacionais, em especial no contexto da OTAN, exige mais do que integração formal, requer interoperabilidade, construída através de exercícios conjuntos, treino cruzado e desenvolvimento de procedimentos comuns. As entrevistas revelam que existe um consenso quanto à existência e relevância de exercícios conjuntos e mecanismos de treino específicos para fortalecer a cooperação entre a FND e as restantes forças da OTAN. Estes treinos são percebidos como essenciais para garantir a prontidão operacional, a interoperabilidade e a resposta coordenada a ameaças híbridas.

As respostas reconhecem, de forme direta, que existem exercícios conjuntos entre a FND e outras forças da OTAN. São mencionados exercícios bilaterais e multinacionais. Esta prática é vista como uma mais-valia tanto a nível técnico como institucional, contribuindo para o reforço da imagem de Portugal como aliado comprometido e proativo no seio da Aliança Atlântica.

Importância dos exercícios para o fortalecimento da interoperabilidade e prontidão. É

destacado que estes exercícios são essenciais para desenvolver sinergia operacional, validar procedimentos e aumentar a interoperabilidade, considerado fundamental para a eficácia em ambientes híbridos.

Participação da FND em grandes exercícios da OTAN. Exercícios com o TROJAN FOOTPRINT e o Defender Europe, são identificados como plataformas de cooperação, treino multinacional e reforço da capacidade de resposta conjunta.

Lacunas na dimensão cibernética e necessidade de aprofundamento técnico-estratégico. É salientado que o domínio do ciberespaço, embora abordado nos treinos, continua demasiado centrado na técnica, com escassa integração da perspetiva estratégica e das implicações operacionais reais, apontando para uma lacuna a colmatar.

CONCLUSÕES

A presente investigação teve como objetivo central, melhorar e propor táticas de contra-ameaça híbrida na Força Nacional Destacada (FND) de Operações Especiais Portuguesa na Roménia, tendo como base uma abordagem metodológica qualitativa e descritiva, sustentada na análise de entrevistas semiestruturadas a militares com experiência no teatro de operações. A investigação procurou não só compreender o estado atual da resposta nacional face às ameaças híbrida, mas também identificar áreas críticas de vulnerabilidade e oportunidade para a evolução doutrinária e operacional da FND. Através da sistematização dos dados empíricos obtidos e da sua articulação com os quadros teóricos e estratégicos contemporâneos, foi possível construir uma visão integrada sobre o contexto atual das ameaças híbridas, as respostas em curso e as lacunas existentes na atuação da FND neste domínio.

No que respeita às características específicas das ameaças híbridas enfrentadas pela FND, verificou-se que estas se materializam de forma assimétrica, indireta e multivetorial, atuando de forma combinada nos domínios físico, informacional e cibernético. Destacam-se, entre os principais vetores, a desinformação, a sabotagem cibernética, a espionagem, a exploração de vulnerabilidades cognitivas e a tentativa de subversão do apoio popular à presença da OTAN. A sua natureza difusa, persistente e adaptativa obriga à implementação de mecanismos de vigilância estratégica e a uma preparação contínua e multidimensional por parte da FND. Estas ameaças exigem da força destacada uma capacidade de perceção contextual e de antecipação particularmente apurada.

Quanto às táticas de contra-ameaça híbrida atualmente empregues pela FND, a análise empírica evidenciou a existência de práticas dispersas de sensibilização, monitorização e comunicação estratégica. Destacam-se iniciativas como os relatórios de situational awareness, os briefings de segurança e a cooperação com forças aliadas. Contudo, a inexistência de uma doutrina formal e de Táticas, Técnicas e Procedimentos específicos para ameaças híbridas, aliada à ausência de um modelo de alerta precoce e à escassa formação prática, configura não apenas uma limitação técnica, mas também uma fragilidade estrutural que pode comprometer a eficácia e a padronização da resposta em contextos de elevada complexidade operacional.

Relativamente às táticas de coordenação e cooperação entre a FND e forças aliadas, constata-se que a interoperabilidade constitui um dos pilares da eficácia operacional, sendo potenciada por mecanismos de partilha de inteligência e por exercícios conjuntos com parceiros da OTAN. Ainda assim, o domínio cibernético e informacional permanece, muitos casos, sob valorizado nas dimensões estratégicas e operacionais da cooperação multinacional, o que requer

um reforço conceptual e técnico no futuro imediato.

Importa ainda, sublinhar que, os resultados obtidos evidenciam uma necessidade inequívoca de modernização da FND, a nível de equipamento tecnológico, como sistemas anti-drone e capacidades de cyber intelligence, mas também a nível doutrinário e organizacional. A resistência à mudança, a lentidão nos processos de adaptação e a dependência de iniciativas individuais constituem barreiras significativas à transformação exigida por um ambiente operacional em constante mudança. A modernização da FND deve ser compreendida como uma prioridade estratégica, indispensável para garantir a sua eficácia, agilidade e capacidade de dissuasão no contexto contemporâneo de segurança.

Com base nos dados empíricos recolhidos e na análise crítica efetuada, propõem-se as seguintes recomendações, estruturadas de forma a orientar a evolução operacional da FND.

- Desenvolvimento de doutrina para ameaças híbridas. Elaboração de uma doutrina nacional orientada para o combate a ameaças híbridas, alinhada com os conceitos da OTAN sobre operações multidomínio (MDO), que inclua os domínios informacional, cibernético e cognitivo como áreas críticas.
- Formalização de TTP's. Criação de TTP's específicas, que orientem as ações da FND perante ameaças híbridas, assegurando a coerência, uniformidade e eficácia da atuação no terreno.
- Implementação de programas de formação multidisciplinar e prático. Instituir programas de treino que integrem cenários práticos, incluindo módulos sobre ciberdefesa, combate à desinformação, análise OSINT e gestão de perceção pública.
- Criação de um sistema de alerta precoce. A implementação de um modelo estruturado de alerta precoce, baseado na análise de tendências, monitorização informacional e deteção de sinais anómalos, é essencial para garantir a prontidão necessária da FND.
- Modernização tecnológica. Deve ser feito um investimento em tecnologias emergentes, como sistemas anti-drone, inteligência artificial aplicada à análise de ameaças híbridas, e plataformas de ciberinteligência.

A concretização destes vetores visa contribuir para a transformação operacional da FND, tornando-a mais resiliente, eficiente e adaptada aos desafios impostos pelo ambiente híbrido.

No desenvolvimento da investigação foram sentidas muitas limitações relativamente à obtenção de contactos e sucessivas respostas por parte de alguns militares das FND, que restringiu a recolha de dados e, por consequência, afetou a amostra e as respostas obtidas, condicionando a abrangência da investigação.

Para trabalhos futuros, foi feita uma proposta por um dos entrevistados, estudar a

inteligência emocional nos militares de Operações Especiais. Outra sugestão para futuras investigações é executar o mesmo estudo, mas desta vez a um cenário operacional e não de cooperação bilateral, percebendo que outro tipo de ameaças a força está sujeito e que formas existem para combater a ameaça. Por fim, e indo de acordo com as conclusões tiradas na investigação relacionadas com a necessidade de modernização de equipamento, nomeadamente, com as capacidades anti-drone, fazer um estudo comparativo entre as várias capacidades anti-drone disponíveis e perceber quais as que melhor se adequam às capacidades operacionais das Operações Especiais.

REFERÊNCIAS BIBLIOGRÁFICAS

Alves, A. J. F. M. (2020). *A prevenção e o combate às ameaças híbridas: impacto para as Forças Armadas Portuguesas* [Instituto Universitário Militar]. http://hdl.handle.net/10400.26/33605

Alves, A. T. A. da R. B. A., Nascimento, A., Ulhôa, A., Batista, B., Capela, C., Venturine, C., Rodrigues, D., Moreira, E., Silva, F., Ribeiro, E., Demba, J., Lapa, L. D. P., Mota, M., & Silva, P. C. B. da. (2021). *Reflexões em torno de Metodologias de Investigação: técnicas de recolha de dados (Vol. 2)* (Issue March). https://doi.org/10.34624/ka02-fq42

Audrey, M. (2025). *Russia's Hybrid Warfare: Five tatics that shape the threat*. United24. Russian Hybrid Warfare: Disinformation, Cyber Attacks, and Pressures | UNITED24 Media

Castro, E. de, & Oliveira, U. T. V. de. (2023). A entrevista semiestruturada na pesquisa qualitativa-interpretativa: um guia de análise processual. *Entretextos*, *22*(3), 25–45. https://doi.org/10.5433/1519-5392.2022v22n3p25-45

CoE, H. (n.d.). *Hybrid threats as a concept*. https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

Cullen, P., & Reichborn-Kjennerud. (2017). *Understanding hybrid warfare*. https://doi.org/10.1080/09557571.2020.1837737

Cullen, P., & Wegge, N. (2019). *Countering Hybrid Warfare Project: Countering Hybrid Warfare*. *March*, 1–90. https://wss.apan.org/public/MCDCpub/default.aspx

Edwards, C. (2024). *Russia's hybrid war in Europe enters a dangerous new phase*. IISS. Russia's hybrid war in Europe enters a dangerous new phase

Eu Council. (2024). *Hybrid threats / Russia: Statement by the High Representative on behalf of the EU on Russia' s continued hybrid activity against the EU and its member state*. *32*(0), 6319. Hybrid threats/Russia: Statement by the High Representative on behalf of the EU on Russia's continued hybrid activity against the EU and its Member States - Consilium

European Commission. (2016). *Security: EU strengthens response to hybrid threats* (Issue April). https://ec.europa.eu/commission/presscorner/detail/en/IP_16_1227

European Commission. (2017). *Relatório conjunto ao parlamento europeu e ao conselho relativo à aplicação do quadro comum em matéria de luta contra as ameaças híbridas - uma resposta da União Europeia*. eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52017JC0030

Exército Português. (2014). *PDE 03-67-00 Operações Especiais*.

Exército Português. (2022). *Cerimónia de Despedida da 1.ª Força Nacional Destacada conjunta*

para a Roménia. https://c8oujqcdfcvk9i8uz915r4kie8psa7nc.rd.exercito.pt/Paginas/Noticias-Detalhe.aspx?urlNoticia=https://c8oujqcdfcvk9i8uz915r4kie8psa7nc.rd.exercito.pt/Exercito/CEME/GabCEME/Paginas/Noticias/Cerimónia-de-Despedida-da-1-ª-Força-Nacional-Destacada-conjunta

Exército Português. (2024). *Rangers renovam equipa e reforçam missão*. https://c8oujqcdfcvk9i8uz915r4kie8psa7nc.rd.exercito.pt/Paginas/Noticias-Detalhe.aspx?urlNoticia=https://c8oujqcdfcvk9i8uz915r4kie8psa7nc.rd.exercito.pt/Exercito/CEME/GabCEME/Paginas/Noticias/Rangers-renovam-equipa-e-reforçam-missão.aspx

Fernandes, A. H. (2021). O que É a Guerra. A Falácia do Conceito de Guerra Híbrida-Breve Excurso. *Nação e Defesa*, *160*, 99–117. https://doi.org/10.47906/ND2021.160.06

Filipec, O. (2021). Preventing hybrid threats: From identification to an effective response. *European Studies: The Review of European Law, Economics and Politics*, *8*(1), 17–38. https://doi.org/10.2478/eustu-2022-0063

Fonseca, P. (2024). Ponto de Reunião. *Revista Das Operações Especiais Do Exército*.

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

Jacuch, A. (2020). Countering Hybrid Threats: Resilience in the EU and Nato'S Strategies. *The Copernicus Journal of Political Studies*. https://doi.org/10.12775/cjps.2020.001

Khriapynskyi, A., Khmyrov, I., Svoboda, I., Shevchuk, M., & Iastrebova, V. (2023). *Стратегії інформаційної безпеки держави в умовах гібридних загроз*. *12*(69), 84–93. 10.34069/AI/2023.69.09.7

Lambakis, S. (2021). Colin Gray on the strategic utility of special operations. *Comparative Strategy*, *40*(2), 205–208. https://doi.org/10.1080/01495933.2021.1880841

Mammadov, R. (2024). The application of special operations forces combat tactics. *Boletim Da Academia Nacional de Administração Pública*, *2*(58), 92–99. https://doi.org/10.56132/2791-3368.2024.2-49-08

Marinha. (2025). *Ações Especiais*. https://fuzileiros.marinha.pt/pt/como_fazemos/fuzileiros/Paginas/acoesespeciais.aspx

Martins, G. A. (2008). Estudo de caso: uma reflexão sobre a aplicabilidade em pesquisa no Brasil. *Revista de Contabilidade e Organizações*, *2*(2), 8–18. https://doi.org/10.11606/rco.v2i2.34702

Matias, R. (2024). Ponto de Reunião. *Revista Das Operações Especiais Do Exército*.

Mineiro, M., A. Alves da Silva, M., & Gracia Ferreira, L. (2022). Pesquisa Qualitativa E

Quantitativa: imbricação de múltiplos e complexos fatores das abordagens investigativas. *Momento - Diálogos Em Educação*, *31*(03), 201–218. https://doi.org/10.14295/momento.v31i03.14538

Miranda, P. (2024). Ponto de Reunião. *Revista Das Operações Especiais Do Exército*.

Monaghan, S. (2019). Countering Hybrid Warfare. *PRISM*, *8*(2), 82–99. https://www.jstor.org/stable/26803232

NATO. (2024). *Countering Hybrid Threats*. https://www.nato.int/cps/en/natohq/topics_156338.htm?selectedLocale=en

Oliveira, M. F. de. (2011). Metodologia científica: um manual para a realização de pesquisas em Administração. In *Universidade Federal de Goiás*. http://medcontent.metapress.com/index/A65RM03P4874243N.pdf%5Cnhttps://books.google.com/books?id=zUDsAQAAQBAJ&pgis=1%5Cnhttp://materiaprima.pro.br/extensao/pesquisa/metodologia_pesquisa_cientifica.pdf

Pillai, H. (2023). Protecting Europe's critical infrastructure from Russian hybrid threats. *Centre for European Reform*, *April*. Protecting Europe's critical infrastructure from Russian hybrid threats | Centre for European Reform

PODLOCH, M. (2017). The Special Forces in the Age of Hybrid Warfare. *Journal of Science of the Military Academy of Land Forces*, *49*(2), 48–58. https://doi.org/10.5604/01.3001.0010.4897

Praks, H. (2024). *Russia's hybrid threat tactics against the Baltic Sea region: From disinformation to sabotage*. www.hybridcoe.fi

Pynnöniemi, K. (2021). *The concept of hybrid war in Russia: A national security threat and means of strategic coercion*. www.hybridcoe.fi

Roxo, P. (2024). Ponto de Reunião. *Revista Das Operações Especiais Do Exército*.

Sarjito, A. (2024). Countering Hybrid Threats: Challenges and the Role of Defense Science. *PUBLICNESS: Journal of Public Administration Studies*, *3*(1), 101–111. https://doi.org/10.24036/publicness.v3i1.188

STANDARD, N. (2013). *AJP-3.5 ALLIED JOINT DOCTRINE FOR SPECIAL OPERATIONS: Vol. I* (A).

Sun, T. (n.d.). *A Arte Da Guerra*.

Voyger, M. (2021). *What is "Hybrid Warfare," Really?* CEPA. What is "Hybrid Warfare," Really? - CEPA

Wei, W. (2024). Analysis of the Characteristics of the "Hybrid War" between Russia and Ukraine and Its Enlightenment to China. *Journal of Economics and Law*, *1*(2), 93–102. https://doi.org/10.62517/jel.202414213

Wijnja, K. (2022). Countering hybrid threats: does strategic culture matter? Defence Studies. *Defence Studies*, *22*(1), 16–34. https://doi.org/10.1080/14702436.2021.1945452

Wither, J. (2019). Defining Hybrid Warfare. *Concordiam*, 7–9. Defining Hybrid Warfare - per Concordiam

APÊNDICES

APÊNDICE A – GUIÃO DO INQUÉRITO POR ENTREVISTA

ACADEMIA MILITAR
MESTRADO INTEGRADO EM CIÊNCIAS MILITARES
NA ESPECIALIDADE DE INFANTARIA
TRABALHO DE INVESTIGAÇÃO APLICADA

GUIÃO DE ENTREVISTA

Contra-Ameaça híbrida da Força Nacional Destacada de Operações Especiais Portuguesa na Roménia

Autor: Aspirante a Oficial de Infantaria Gonçalo Spínola

Orientador: Tenente-Coronel de Infantaria João Carlos Gonçalves dos Reis

Entrevista Semiestruturada

O presente documento integra o quadro de referência de uma Investigação Académica realizada no âmbito do Trabalho de Investigação Aplicada, ministrado na Academia Militar.
O objetivo da pesquisa realizada através deste documento visa exclusivamente servir a intenção do investigador, no sentido de concluir com aproveitamento o ciclo de estudos a que se encontra vinculado. Assim, os dados obtidos através da presente entrevista serão utilizados apenas para verificar a confirmação total ou parcial, ou ainda a informação complementar das hipóteses empíricas formuladas, em consonância com a proposta teórica defendida pelo autor deste trabalho de investigação científica.

Dados Biográficos:
Nome:
Dados Profissionais:
Posto:
Função:
Duração na Função:

Q1 – Quais as ameaças híbridas predominantes enfrentadas pela FND na Roménia (ex.: guerra de informação, subversão, forças irregulares)?
Q2 – Existe um padrão específico na forma como estas ameaças híbridas são desencadeadas contra forças da NATO na região?
Q3 – De que forma a desinformação e a manipulação da opinião pública afetam a perceção e a eficácia da FND na Roménia?
Q4 – Como a FND avalia a presença e influência de agentes estatais e não estatais nas dinâmicas de ameaça híbrida na região?
Q5 – Que medidas proativas a FND tem implementado para detetar e neutralizar ações híbridas antes da sua materialização?
Q6 – Existe alguma doutrina específica ou TTPs (Técnicas, táticas e procedimentos) desenvolvido pela FND para lidar com ameaças híbridas?
Q7 – Que tipo de treino específico os militares da FND recebem para lidar com ameaças híbridas no contexto da Roménia?
Q8 – Existe um modelo de alerta precoce que permite antecipar ataques híbridos e mobilizar a FND de forma eficiente?
Q9 – De que forma a interação com as comunidades locais contribui para a eficácia das operações da FND, tendo em conta as ameaças híbridas?
Q10 – Como é feita a partilha de informações de inteligência entre a FND e as restantes forças da NATO presentes na Roménia?
Q11 – De que forma a interoperabilidade entre a FND e forças especiais de outros países influencia a eficácia no combate a ameaças híbridas?
Q12 – Como a FND avalia a necessidade de modernização das suas capacidades em resposta ao caráter dinâmico das ameaças híbridas?
Q13 – Existem exercícios conjuntos ou mecanismos de treino específicos para fortalecer a cooperação entre a FND e as restantes forças da NATO?

APÊNDICE B – AMOSTRA DE ENTREVISTADOS

Quadro 2: Amostra de entrevistados

Entrevistado	Função	Unidade	Data
E1	Comandante da 4ª FND OE	CTOE/BrigRR	15/04/2025
E2	Chefe da Célula de Informações	EMGFA	22/04/2025
E3	Comandante da 3ª FND AE Comandante da 6ª FND AE	Base de Fuzileiros	24/04/2025
E4	Comandante da 5ª FND OE	CTOE/BrigRR	27/04/2025

APÊNDICE C – SINOPSE DAS ENTREVISTAS

Quadro 3: Sinopse das entrevistas

Questão n.º 1: Quais as ameaças híbridas predominantes enfrentadas pela FND na Roménia (ex.: guerra de informação, subversão, forças irregulares)?	
Entrevistado	**Resposta**
E1	"A 4ª FND, relativamente ao espaço, encontrávamo-nos na cidade de Târgu Mures, cidade tranquila, onde se localizam 3 Unidade militares, comando de Operações Especiais, um batalhão OE e um batalhão de apoio. A presença militar era notória e a cidade estava habituada e era acolhedora, houve uma boa aceitação dos militares portugueses. A nossa missão era de cooperação bilateral com forças romenas, com o objetivo de desenvolver capacidades militares, treino e a componente de desenvolvimento operacional. Contudo, no teatro de operações foi me dado um briefing de segurança pelas forças locais, onde foram identificados pontos geográficos (bares, discotecas, restaurantes…) que eram proibidos de serem frequentados e alguns pontos geográficos onde era preciso bastante cautela para os frequentar, isto pelo facto de haver **indícios de espionagem nesses locais**. Por parte da população, a minha **força nunca foi abordada com o intuito de retirar informação** dos militares. Para além disso, nunca nenhum militar me informou de qualquer perturbação a nível de comunicações via telemóvel pessoal."
E2	"O **Ciberespaço** é um domínio de operações que quando comparado com o domínio marítimo, terrestre, aéreo e espacial, abriga um espectro de pesquisa muito abrangente (através da Cyber Intelligence). Caracteriza-se por um ambiente complexo, de valores e interesses, materializado numa área de responsabilidade coletiva, que resulta da interação entre pessoas, redes e sistemas de informação. Este domínio tem visto mudanças significativas nos últimos anos, e houve um **aumento exponencial de ameaças reais e potenciais**. Uma ameaça no ciberespaço é descrita como uma atividade maliciosa que procura prejudicar uma entidade, e que pode influenciar eventos e decisões no cenário global. O plano de atuação dos atores "através do ciberespaço" poderá criar efeitos que se traduzem no meio militar ao nível estratégico-militar, operacional e tático, que se podem repercutir no domínio marítimo, terrestre, aéreo e espaço. A pesquisa poderá ser apoiada nas disciplinas de informações usadas na Cyber Intelligence e podendo ser complementadas com informações provenientes das disciplinas de informações tradicionais, pois todos os domínios estão dependentes de equipamentos, que estão interligados através de IoT. As ameaças vêm nas novas tecnologias uma oportunidade de baixo custo, para afetar a segurança das organizações. Os Cibercriminosos, aproveitam o anonimato e a sua atividade maliciosa para impactar as operações militares**. Podem atuar como um APT ou entidades de crime organizado ou terroristas**. A complexidade da informação e as possíveis implicações práticas das ações táticas intensificam os desafios enfrentados pelos decisores, pois as consequências das decisões poderão ser percetíveis de forma prática e mensurável no mundo físico. Nesse novo contexto informacional, onde as distinções entre os níveis estratégico, operacional e tático são menos nítidas, torna-se fundamental coordenar, sincronizar e executar atividades de informações que visem, de forma planeada, gerar impactos no muindo físico. As FFAA, necessitam de ser capazes de identificar os diferentes atores no ciberespaço e que atuam através do ciberespaço, e dar suporte às operações militares à medida que as capacidades destes atores evoluem. Atualmente as operações militares, estão dependentes do uso do ciberespaço e da informação nele presente, e as comunicações que nele ocorrem. Se por um lado é essencial, a proteção da informação crítica e sensível, reforçando as nossas defesas ao nível tático, por outro, é importante obter mais conhecimento através das subdisciplinas de CTI e constituir a base para análises adicionais de informações, que poderão ser essenciais para o apoio à decisão em momentos críticos."

E3	"As ameaças híbridas predominantes que foram detetadas durante a Força Nacional Destacada de Marinha foram essencialmente **campanhas de desinformação**. Estas ações visaram essencialmente uma tentativa de descredibilizar as Forças NATO que se encontram na Roménia. Estes tipos de ações também visaram explorar vulnerabilidades na opinião civil quanto à aceitação destas forças no TO."
E4	"Devemos ter em linha de conta que as FFAA RUS, têm como principal objetivo obter informações privilegiadas sobre as forças militares da NATO estacionadas junto à fronteira da EUROPA com a RUS, e uma contante monotorização do estado de prontidão da NATO, para tal socorre-se dos Serviços de Informações RUS (e.g. militares e civis). Em segundo, existe a preocupação do KREMLIN, em efetuar toda influência na população nativa do país (e.g. ROMÉNIA, BULGARIA, HUNGRIA e MOLDOVA), de forma que as mesmas considerem como hostil a presença da NATO nos seus países. Dedicando esforços para prejudicar os serviços de saúde e de segurança como inclusive as fontes de energia, existentes junto às Base/Campos militares da NATO no país (e.g. ROU). Para conseguir ter êxito, tem de aplicar todas as formas de Guerra Híbrida - guerra de informação, guerra cibernética, subversão, forças irregulares – para ter acesso aos militares que compõem as FND's ROU."
Ideias chave	Indícios de espionagem na região; campanhas de desinformação, cibercrime.
Questão n.º 2: Existe um padrão específico na forma como estas ameaças híbridas são desencadeadas contra forças da NATO na região?	
E1	"Não consigo dar uma resposta em primeira mão por falta de experiência. Mas verificamos que **a aproximação de mulheres no período noturno** era muito frequente, podendo levar ao comprometimento da força e, inclusive, ao roubo de dinheiro e extorsão."
E2	"Analisando os eventos recentes, padrões emergiram, notavelmente a combinação e coordenação de ações cinéticas e ciberataques, conforme observado no início do conflito Ucrânia-Rússia (relatório da Microsoft) e na invasão do Hamas a Israel, acompanhada de ciberataques ao setor energético. No âmbito do COCiber, identificámos uma correlação significativa entre as viagens de presidentes de países à Rússia e uma subsequente diminuição nos ciberataques, sugerindo a utilização do ciberespaço como ferramenta estratégica para obtenção de vantagens negociais. Especificamente no que concerne à Roménia, considero que, dada a nossa ausência de ativos de recolha de informação no terreno, carecemos da capacidade para emitir um parecer factual fundamentado sobre a situação."
E3	"Sim, durante o comando da 3FND SOMTU e 6FND SOMTU verifiquei um certo padrão observável: **ataques cibernéticos contra plataformas de redes sociais** (Facebook, WhatsApp) e que geralmente eram precedidos por campanhas de desinformação. Estes movimentos coincidiram com períodos de tensão política ou mesmo durante exercícios militares da NATO."
E4	"Existe padrão em algumas ações, nomeadamente através das ligações entre a Máfia RUS (a mando dos Serviços RUS) e os diversos Grupos de Crime Organizado (algum de origem RUS), onde se obtém acesso aos Clubes de Diversão Noturna, Clubes de Apostas de jogo, Bares e Restaurantes mais frequentados, Ginásios, Lojas de Telecomunicações (vital para o acesso ao militar), e ao tráfico de estupefacientes. Também é frequente a RUS, ter acesso ao panorama das FND's da NATO, através de nativos que são pró-Rússia."
Ideias chave	Aproximação de mulheres no período noturno; ataques cibernéticos contra plataformas de redes sociais.

Questão n.º 3: De que forma a desinformação e a manipulação da opinião pública afetam a perceção e a eficácia da FND na Roménia?	
E1	"Qualquer notícia que seja passada para membros da OTAN **que não seja verídica e sendo negativa, vai comprometer a credibilidade da força**. Sabendo eu que estava numa situação de cooperação bilateral, sempre quis mostrar o que estávamos a fazer e criar uma comunicação estratégica bilateral. Sendo a missão de carater discreto vi que esta comunicação ia ganhar credibilidade ao abrigo da OTAN. Este plano da comunicação estratégica bilateral foi muito bem recebido e foi um ótimo contributo para hoje termos uma Special Operations Land Task Group (SOLTG) a operar na Roménia. Blindei ao máximo todas as notícias que eram enviadas, garantindo sempre a proteção da força, nomeadamente na mensagem a passar, na proteção dos militares, inclusive, nas infraestruturas ao redor dos militares, tendo sempre cuidado com a proteção. Senti que esta comunicação estratégica serviu para que fosse vista a boa imagem dos militares portugueses. Tive oportunidade de falar com o Tenente-General António Flecha (Cmdt do Quartel-General de OE da OTAN), na área da comunicação sobre o que estávamos lá a fazer, e ficou bastante agradado com aquilo que viu e ouviu por parte dos romenos. Isto ajudou imenso no desenvolvimento da força. Resumidamente, **uma notícia pode influenciar a imagem da força quer a nível positivo, quer a nível negativo**. Durante toda a missão, sempre soube que uma pequena falta de atenção da minha parte poderia comprometer a credibilidade da minha força."
E2	"O ciberespaço está a ser usado também na guerra da informação e o disseminar de narrativas falsas em processos políticos tem sido verificado em todo o mundo e isso, demonstra a utilização deste novo domínio da informação como fonte de poder. O impacto existente nas forças militares no terreno, nos povos e na vida do dia a dia é por vezes não medido, e é uma ameaça à segurança e estabilidade mundial que não deverá ser desconsiderada. A principal forma utilizada é através de um novo conceito: FIMI (Foreign information manipulation and interference) descreve um padrão parcialmente legal de comportamento, que ameaça e tem o poder de impactar negativamente em valores, procedimentos e processos políticos. É de caracter manipulativo, e é conduzido de forma intencional e de forma coordenada, por intervenientes estatais ou não estatais, incluindo representantes dos países dentro e fora do seu território. O FIMI pode ser considerado uma forma de influência como diplomacia pública, assistência externa, difusão de cultura, mas conduzido sempre de forma encoberta. Exemplos de FIMI são: • Financiamento secreto ou coação de intervenientes políticos, funcionários governamentais, influenciadores, media, ONGs, através de transferências ilícitas. • Espalhar desinformação (propagação de informações comprovadamente falsas ou enganosas) Usar comportamentos pouco adequados coordenados nas redes sociais, manipulando debates para atingir objetivos estratégicos onde as contas falsas e Bots desempenham um papel importante. Conduzir ciberataques como negação de serviços, forçando líderes a tomar posições favoráveis. Ou Ex filtração de Informação."
E3	"A **desinformação acaba por influenciar a confiança pública na presença da Força Nacional Destacada na Roménia**. Isso reduz o apoio popular e pode comprometer a moral das Forças NATO. Além disso, **influencia negativamente a cooperação com autoridades locais ou outras Forças internacionais**."

E4	"É o desafio que as FND's ROU, enfrentam, todos os dias, conseguir demonstrar à opinião pública local, que as falhas (e.g. na saúde e segurança como nos serviços públicos) que porventura possam vir acontecer não são da responsabilidade da NATO. Para tal seja possível, o desempenho (nas folgas e atividades privadas à civil) de todos os militares das FND's ROU, tem impacto na retórica (híbrida) RUS junto dos nativos."
Ideias chave	Uma notícia pode comprometer a imagem e a credibilidade da força; pode influenciar negativamente a cooperação com autoridades locais ou outras forças.
Questão n.º 4: Como a FND avalia a presença e influência de agentes estatais e não estatais nas dinâmicas de ameaça híbrida na região?	
E1	"Não avaliamos, não senti influência."
E2	"Especificamente no que concerne à Roménia, considero que, dada a nossa ausência de ativos de recolha de informação no terreno, carecemos da capacidade para emitir um parecer factual fundamentado sobre a situação."
E3	"A Força tinha uma célula intel que se dedicava ativamente no acompanhamento das redes sociais dos militares, assim como verificar possíveis alterações nos comentários políticos e militares que poderiam ser sujeitos a qualquer tipo de ação cyber ataque. A FND avaliava a presença de agentes estatais e não estatais **com base na partilha de informações por parte do CI Romeno e através da cooperação com aliados da NATO** como os Navy Seal que se encontravam junto da 6FND SOMTU."
E4	"Esse dado é de cariz MUITO RESERVADO, existe militares das FND's ROU, que têm a responsabilidade de atuar em coordenação com agentes de autoridade local em defesa das FND's ROU."
Ideias chave	Com base na partilha de informações por parte do CI Romeno e através da cooperação com aliados da NATO.

Questão n.º 5: Que medidas proativas a FND tem implementado para detetar e neutralizar ações híbridas antes da sua materialização?	
E1	"Durante o aprontamento, tivemos várias **ações de formação e palestras por parte do Centro de Segurança Militar e de Informações do Exército (CSMIE)**, que ajudaram na sensibilização para o TO. Tivemos o **pessoal do S2, no âmbito da OSINT, a sensibilizar-nos para os perigos que podem acontecer no TO**, maioritariamente acautelar a espionagem. Na Roménia, recebi um **briefing sobre os perigos no TO** e estava em **constante comunicação com o módulo de informações do exército** caso houvesse movimentos que influenciassem a minha força. Como medida interna da força, todas as sextas-feiras, juntava todos os módulos de operações e falávamos sobre o que se tinha passado nessa semana e o que se ia passar na semana seguinte. Terminava a reunião com **Situational Awareness Report (SA report)**, onde abordava três tópicos. Situação atual no mundo, onde falava de tudo o que se passava no mundo que tivesse implicações no confronto da Ucrânia. Situação atual no Leste, onde falava de tudo o que acontecia nos 5 países em redor da Ucrânia. E por fim, situação na região, onde falava de tudo o que acontecia dentro da Roménia. Para conseguir ter sempre esta informação atualizada, tinha um militar em constante observação de fontes cuidadosamente selecionadas e a fazer relatórios diariamente. O SA report fazia com que todos os militares estivessem conscientes de tudo o que se passava no conflito, garantindo sempre o alerta sobre o perigo da guerra. Foi uma política que implementei no TO e que veio a mostrar ser bastante positiva."
E2	"As medidas implementadas têm tido um carácter essencialmente preventivo, nomeadamente através de **palestras sobre Ciberdefesa e Cyber Defense Threat Assessment (CDTA) (briefing classificado) ministradas pelo COCiber** aos elementos das FND. Contudo, reconhece-se que há ainda muito por fazer. Numa fase de projeção: Seria fundamental investigar todo o ecossistema em torno das FND, desde as cadeias de abastecimento às empresas fornecedoras de serviços, de modo a garantir um apoio informado à decisão. Numa fase de execução: Apoiar a força no terreno com informações operacionais recolhidas através do ciberespaço representaria uma evolução significativa na nossa forma de atuação. Isto elevaria a análise de um âmbito meramente técnico/tático (como a imersão nas redes) para um nível operacional ou estratégico, fornecendo informações pertinentes que suportem a tomada de decisões informadas, particularmente em momentos críticos. Tal incluiria a neutralização de bots de desinformação nas plataformas digitais (recorrendo a técnicas de cyber intelligence). Numa fase de retração: Dever-se-ia proceder ao estudo e à análise dos dados recolhidos, com vista à sua incorporação na doutrina e na definição de novos procedimentos a adotar. Mas a resistência a mudança e a magnitude da transição de paradigma e a necessária alteração cultural no seio da hierarquia militar para a sua efetivação, afiguram-se como fenômenos cuja plena operacionalização desta intenção estaria, lamentavelmente, condicionada à eclosão de um conflito bélico real."
E3	"Foram adotadas **medidas de monitoramento contínuo das redes sociais, análise de ameaças cibernéticas e campanhas de desinformação**. Também existiu uma **colaboração próxima com a unidade de Contra Informação** Romeno que apoiou a FND."

E4	"Através de **briefings à força sobre os procedimentos a ter e há uma subunidade que tem ligação aos serviços de informações e de segurança locais**. Aplicando as TTP's existentes para lidar com a ameaça identificada ou detetada."
Ideias chave	Ações de formação e palestras por parte do Centro de Segurança Militar e de Informações do Exército (CSMIE); briefing sobre os perigos no TO; Situational Awareness Report (SA report); medidas de monitoramento contínuo das redes sociais, análise de ameaças cibernéticas e campanhas de desinformação; colaboração próxima com a unidade de Contra Informação.
Questão n.º 6: Existe alguma doutrina específica ou TTPs (Táticas, técnicas e procedimentos) desenvolvido pela FND para lidar com ameaças híbridas?	
E1	"Em termos de TTP's o que existe definido foi o que referi anteriormente. Depois de sensibilizado sobre estas temáticas, **nunca desvalorizar nada, estar sempre desconfiado de tudo**. De forma descontraída, perceber a envolvência no local onde estamos, perceber se existem mais pessoas envolvidas, perceber se estamos numa situação segura. Não quebrar a ligação de uma forma brusca para não levantar suspeitas e nos colocarmos numa situação onde não queremos estar, alimentar o cenário até surgir uma oportunidade segura de evasão. Assim que chegarmos ao quartel **informar o comandante e efetuar o respetivo relatório que é enviado para Portugal**, para que seja analisado. Podemos não ter noção da perigosidade do acontecimento e pode ter valor para alguma investigação em curso do ponto de vista da segurança nacional."
E2	"Existem formas de resposta a ciberincidentes, mas desconheço se estão a ser usadas nas FNDs."
E3	"A **doutrina é continuamente atualizada**. Esta missão permitiu obter LI\LA que serão convertidas para **TTP´s que estão ainda a ser desenvolvidas."**
E4	"Existe doutrina proveniente dos Serviços PRT, que são empregues pelos militares (com essa missão) em apoio aos comandos da FND's ROU."
Ideias chave	TTP's a ser desenvolvida; doutrina em constante atualização.

Questão n.º 7: Que tipo de treino específico os militares da FND recebem para lidar com ameaças híbridas no contexto da Roménia?	
E1	"**Formações do CSMIE. Formações do Comando de Operações de Ciberdefesa (COCiber)**, formações meramente de partilha de informação sobre aquilo que pode ser facultado sobre o TO e medidas preventivas sobre o TO."
E2	"A única indicação dada neste âmbito, é escreverem um report de acontecimentos, mas o que se tem passado na prática é apoio não formal através de contactos pessoais."
E3	"Os militares receberam palestras nas temáticas de cibersegurança e ciberdefesa, combate à desinformação e manuseamento das redes sociais."
E4	"Aos militares responsáveis pela defesa de ações Híbridas às FND's ROU, possuem formação diferenciada e provem de serviços específicos dedicados ao tópico de ameaça. Em relação aos militares das FND's ROU, é através de briefings sobre as ameaças existentes e o seu estado de aplicação na área/local/país, e eventuais reuniões (com militares selecionados) reservadas, onde é debatido a ameaça particular tema de reunião."
Ideias chave	Formações do CSMIE. Formações do Comando de Operações de Ciberdefesa (COCiber); palestras nas temáticas de cibersegurança e ciberdefesa, combate à desinformação e manuseamento das redes sociais.
Questão n.º 8: Existe um modelo de alerta precoce que permite antecipar ataques híbridos e mobilizar a FND de forma eficiente?	
E1	"Desconheço"
E2	"Especificamente no que concerne à Roménia, considero que, dada a nossa ausência de ativos de recolha de informação no terreno, carecemos da capacidade para emitir um parecer factual fundamentado sobre a situação."
E3	"Fisicamente **não existe nenhum modelo**, no entanto existe o conhecimento e experiência para detetar os ataques híbridos."
E4	"De forma simplista, deve-se ter em atenção à dedicação/empenho de um/uma nativo/a sobre determinado militar (e.g. fisicamente ou telemóvel, redes sociais)."
Ideias Chave	Não existe nenhum modelo.
Questão n.º 9: De que forma a interação com as comunidades locais contribui para a eficácia das operações da FND, tendo em conta as ameaças híbridas?	
E1	"Como a nossa missão era de cooperação bilateral, não tínhamos operações. Contudo, **o bom relacionamento com as autoridades locais contribuiu para a boa imagem da força e o devido respeito**."

E2	"Em qualquer teatro de operações e em muitos eventos militares, a presença de um elemento de Intel é fundamental para estabelecer, de forma estratégica, ligação com as autoridades locais, visando a partilha e a troca oportuna de informações relevantes. No âmbito das Forças Armadas, desconheço a existência de uma diretiva estratégica formalizada para este efeito, contudo, afigura-se-me uma abordagem intrinsecamente lógica e alinhada com os princípios doutrinários."
E3	"O contato com as comunidades locais é **essencial para obter informações sobre atividades incomuns e contribuir para o combate de narrativas falsas ou desinformação**. A confiança mútua fortalece a resiliência contra tentativas de subversão. Eventualmente as operações levadas a cabo pelo CIMIC poderiam também ajudar a prevenir ou mesmo neutralizar campanhas de desinformação."
E4	"É muito importante manter uma interação positiva com os diversos escalões da sociedade local, para minimizar a influência RUS sobre a mesma."
Ideias Chave	O bom relacionamento com as autoridades locais contribuiu para a boa imagem da força e o devido respeito; essencial para obter informações sobre atividades incomuns e contribuir para o combate de narrativas falsas ou desinformação.
Questão n.º 10: Como é feita a partilha de informações de inteligência entre a FND e as restantes forças da NATO presentes na Roménia?	
E1	"A **nível nacional, era feito através de relatórios entre as Operações Especiais e o módulo de informações e comunicação do exército**. A **nível internacional e por estarmos inseridos numa força romena, era feito através do Comando das OE, semanalmente através de briefings."**
E2	"Desconheço."
E3	"**A partilha de INTEL ocorre por vias de canais seguros da NATO (BICES e NSWAN) ou através de reuniões regulares em que o acesso à informação e sua análise é partilhada**."
E4	"As FND têm **sistemas de informação e comunicação que permitem a troca de informação de modo seguro (Ex. NSWAN, BICES, OPNET).** Por outro lado, nos briefings e conversas com as nossas contrapartes também é partilhado alguma informação."
Ideias chave	A nível nacional, era feito através de relatórios entre as Operações Especiais e o módulo de informações e comunicação do exército. A nível internacional e por estarmos inseridos numa força romena, era feito através do Comando das OE, semanalmente através de briefings; A partilha de INTEL ocorre por vias de canais seguros da NATO (BICES, NSWAN e OPNET) ou através de reuniões regulares em que o acesso à informação e sua análise é partilhada

Questão n.º 11: De que forma a interoperabilidade entre a FND e forças especiais de outros países influencia a eficácia no combate a ameaças híbridas?	
E1	"Se não houver **interoperabilidade (palavra-chave para o sucesso**) em tudo, mindset, meios de combate, meios de defesa, meios de comunicação, não estamos a garantir a chamada bolha geral. A **interoperabilidade é demasiado importante para estarmos todos a trabalhar da mesma forma, com os mesmos meios e objetivos.** Devido ao facto de queremos sempre aumentar cada vez mais a interoperabilidade com os romenos, permitiu-nos treinar com os equipamentos deles."
E2	"Desconheço."
E3	"A interoperabilidade entre Forças e Países Aliados garante operações mais eficazes e coordenadas, sobretudo em contextos complexos como as ameaças híbridas. **Troca de experiências, táticas e recursos modernos permite maior adaptabilidade e uma resposta mais rápida contra ameaças híbridas fortalecendo assim a presença da NATO na Roménia**."
E4	"Essencialmente ter uma boa compreensão situacional do ambiente que nos rodeia. Isto só é conseguido se houver cooperação entre as diferentes forças. Convém ter em linha de avaliação que as SOF NATO, são um dos meios (accet's), que são frequentemente utilizados para combater/defender a NATO contra ações Híbridas da RUS."
Ideias chave	Interoperabilidade é demasiado importante para estarmos todos a trabalhar da mesma forma, com os mesmos meios e objetivos; Troca de experiências, táticas e recursos modernos permite maior adaptabilidade e uma resposta mais rápida contra ameaças híbridas fortalecendo assim a presença da NATO na Roménia.
Questão n.º 12: Como a FND avalia a necessidade de modernização das suas capacidades em resposta ao caráter dinâmico das ameaças híbridas?	
E1	"Como está montado na Roménia**, está aprovado, é útil e funcional**. Em termos de proteção da força, a formação que temos em Portugal também ajuda. Tendo em conta que o comportamento dos militares no TO é que realmente determina a sua eficácia. **Devia haver um padrão de sensibilização, mas infelizmente, depende de cada comandante. Lacunas, apenas a destacar os drones. Não possuímos medidas de combate a não ser as mediadas ortodoxas que é a sua destruição**. Em termos de inibição, barreira, que façam com que o drone perca capacidade, não existe. Sabemos que há empresas a desenvolver nesta matéria, já foram feitas propostas, mas, no entanto, ainda não foram adquiridos."
E2	"Existe **maior necessidade de desenvolvimento na integração dos elementos de poder nos critérios MDO** (operações Multidominio) NATO, e estão a ser criados esforços dentro da aliança pois é um objetivo prioritário. O ciberespaço é um domínio fundamental nas operações MDO e existe a necessidade urgente a completa integração destes domínios com os outros domínios. A verdade é que a nível nacional existe uma resistência à mudança, e os processos nas FFAA são lentos e carecem de tempo para serem implementados. A importância da orquestração e sincronização entre os domínios militares e civis, bem como os desafios associados ao comando e controlo. A necessidade de utilização de tecnologias avançadas, como a inteligência artificial (IA), para otimizar a tomada de decisões. Mas no meio militar português, existe bastante a tendência de se fazer as coisas como sempre foram feitas, as novas disciplinas de informações estão em evolução assim como as ameaças que atuam de forma criativa e evolutiva. Teremos de evoluir e dar o salto porque a ameaça não espera."
E3	"A necessidade de modernização é constante, com **ênfase nas tecnologias de informação, guerra eletrónica e ciberdefesa.** A Força avalia constantemente as capacidades através de exercícios internacionais de multidominios e com os AAR (After Action Review) ou FIR (First Impression Report) produzidos no final de cada exercício, ajustando desta forma as suas necessidades de material e formação para fazer face às ameaças híbridas."

E4	"Após estudos efetuados (e.g. relatórios das ações identificadas) ao mais alto nível pelas entidades nacionais responsáveis pelo tópico - ações Híbridas RUS - contra alvos FND's ROU, o volume e resultados que as mesmas atingiram/atingem, faz com que seja eventualmente necessário alterar as TTP's em uso."
Ideias chave	Modernizar a capacidade anti-drone; maior necessidade de desenvolvimento na integração dos elementos de poder nos critérios MDO; ênfase nas tecnologias de informação, guerra eletrónica e ciberdefesa.
Questão n.º 13: Existem exercícios conjuntos ou mecanismos de treino específicos para fortalecer a cooperação entre a FND e as restantes forças da NATO?	
E1	"No âmbito da cooperação bilateral, é definido o nosso **plano de missão (plano treino) e definimos os exercícios a desenvolver**. No âmbito operacional, quando existem **exercícios a acontecer no TO, somos convidados a participar**. **TROJAN FOOTPRINT, exercício anual**. Tudo o que for **exercícios para o desenvolvimento de capacidades dos militares, a FND participa**. Sempre que há oportunidade de **exercícios de Operações Especiais a nível OTAN, Portugal participa**. É nestes exercícios que é criada a sinergia entre forças e onde é criado a interoperabilidade tão importante para o sucesso. É nestes exercícios que percebemos se estamos a ir no bom caminho ou não."
E2	"Neste momento o domínio do ciberespaço está a evoluir, e considero que esta muito voltado para o domínio técnico/tático. É bastante importante efetuar esta distinção porque considero que os aspetos técnicos têm sido muito destacados, mas o panorama geral é por vezes negligenciado. O domínio do ciberespaço está, de certa forma, "dominado" pela perspetiva técnica, resultando numa desvalorização dos efeitos e danos causados por ações maliciosas cujos efeitos são sentidos para além do ambiente ou fora do domínio estritamente digital. Embora exista um esforço crescente para desenvolver medidas de defesa ativas e passivas, a falta de consulta a especialistas que possuem a sua própria perícia nas suas áreas leva a uma falta de conhecimento sobre as consequências reais dos impactos causados pela ameaça. A complexidade do ciberespaço, com a sua dimensão geográfica inexistente e alcance abrangente, leva os profissionais de cibersegurança a estarem prontos para mitigar tecnicamente/taticamente os efeitos dos ciberataques, mas é crucial e necessário desenvolver uma dimensão de conhecimento mais aprofundada, focada na operação de todo o equipamento e sistemas dentro de cada especialidade. A ausência deste conhecimento especializado impede uma compreensão completa do âmbito dos danos e dificulta a implementação de estratégias de defesa redundantes e verdadeiramente eficazes e abrangentes. Estas estratégias devem considerar não apenas os aspetos técnicos, mas também as implicações práticas do mundo real, e a abrangência das questões operacionais e estratégicas terá de ser mais profundada."
E3	"Sim, há **exercícios conjuntos frequentes com foco em cenários híbridos**, como o "Defender Europe". É um exercício militar anual de grande escala liderado pelo Exército dos EUA, projetado para aumentar a prontidão e a interoperabilidade entre as forças militares dos EUA, da NATO e de outros países parceiros na Europa. O objetivo é fortalecer a capacidade de resposta conjunta a crises, demonstrar o compromisso dos EUA com a NATO e promover a segurança estratégica na região."
E4	"As comunidades NATO responsáveis por dar resposta (e.g. Serviços de Informações, Segurança e SOF da NATO), têm anualmente diversos exercícios NATO (multinacionais ou bilaterais) táticos de certificação sobre este tipo de ameaça (Híbrida)."
Ideias Chave	Exercícios definidos no plano de missão; exercícios a acontecer no TO.