Cadernos do IUM

A MODERNIZAÇÃO DAS CAPACIDADES MILITARES NO MUNDO DIGITAL

Coordenação de:
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

IUM

Outubro 2024

INSTITUTO UNIVERSITÁRIO MILITAR

A MODERNIZAÇÃO DAS CAPACIDADES MILITARES NO MUNDO DIGITAL

Coordenadora

Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

IUM – Centro de Investigação e Desenvolvimento (CIDIUM)
Outubro de 2024

Como citar esta publicação:
Esteves, A. C. C. S. M. (Coord.), (2024). *A Modernização das Capacidades Militares no Mundo Digital*. Cadernos do IUM, 63. Lisboa: Instituto Universitário Militar.

Diretor
Tenente-General Hermínio Teodoro Maio

Editora-chefe
Coronel Joana Isabel Azevedo do Carmo Canhoto Brás

Coordenadora Editorial
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

Capa – Composição Gráfica
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves
Imagem gerada por Inteligência Artificial em agosto de 2024

Secretariado
Assistente Técnica Gisela Cristina da Rocha Basílio

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

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

ISBN: 978-989-35731-1-2
ISSN: 2183-2129
Depósito Legal: 544060/25
Tiragem: 90 exemplares

Nota do Editor:

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

iii

NOTA EDITORIAL

Estimados leitores,

Esta obra reúne seis estudos sobre a modernização das capacidades militares, com foco na defesa estratégica e no desenvolvimento industrial. O primeiro estudo aborda a necessidade de revitalizar a capacidade operacional da Marinha do Brasil, enfatizando a sua importância como primeira linha de defesa. O segundo explora a transformação digital nas Forças Armadas Portuguesas, visando a interoperabilidade com a NATO. O terceiro estudo analisa a implementação do modelo *Intelligence-Led Policing* na GNR, destacando a importância da análise de dados na tomada de decisões.

O quarto estudo investiga o contributo da *Identity Intelligence* nas operações militares, demonstrando como a combinação de dados biométricos e a análise de redes pode aumentar a eficiência em cenários complexos. Os últimos dois estudos focam-se na Base Tecnológica e Industrial de Defesa, abordando a necessidade de modernização e transição para a Indústria 4.0, fundamentais para a autonomia estratégica de Portugal e da Europa.

Este compêndio oferece uma visão abrangente e atualizada dos desafios e soluções para a modernização das Forças Armadas e da indústria de defesa, sendo uma leitura essencial para decisores e especialistas na área.

Boa leitura!

Ana Esteves
Tenente-coronel
Coordenadora editorial do CIDIUM

ÍNDICE

PREFÁCIO

A presente edição dos Cadernos do IUM (edição N.º 63), sob coordenação da Tenente-Coronel Ana Carina da Costa e Silva Martins Esteves e intitulada "A modernização das capacidades militares no mundo digital", reúne um conjunto de textos, que resultam de trabalhos desenvolvidos no âmbito dos Cursos de Promoção a Oficial General 2023/2024 e de Estado-Maior Conjunto 2023/2024. O desafio lançado ao Coordenador das Área de Ensino de Operações Militares e Área de Ensino de Técnicas e Tecnologias Militares para elaborar o prefácio desta edição, permite-nos sinalizar a importância que o conteúdo destas reflexões nos presenteia.

As guerras em curso na Ucrânia e no Médio Oriente mostram-nos, diariamente, o quanto a tecnologia é importante para o sucesso das operações militares. Verificamos que as guerras são conduzidas em ambientes operacionais multidomínio, que a utilização das capacidades militares e das capacidades não militares é um facto e que cada vez mais, se verifica a utilização de todos os recursos do estado para alcançar os efeitos desejáveis no campo de batalha. Para que tal possa ocorrer, os estados e as organizações de segurança e defesa, devem dispor de capacidades militares tecnologicamente evoluídas, interoperáveis e que possam ser rapidamente integradas em forças multinacionais, prontas para operar em quaisquer tipos de ambientes operacionais e capazes de conduzir operações num conflito armado de grande intensidade.

Os textos presentes nesta edição dos Cadernos do IUM, ajudam-nos a perceber, através do olhar dos autores, como é que as Forças Armadas e a Guarda Nacional Republicana, estão a acompanhar este desiderato de exigente concretização, que consiste em garantir capacidades tecnologicamente modernas no mundo cada vez mais digital. É oportuno e justo relevar o papel da Base Tecnológica e Industrial de Defesa, que compreende o universo da oferta tecnológica e industrial nacional com competências relevantes para o domínio da defesa e a sua ligação a outros interlocutores internacionais. Podemos considerar como transversal a todos os textos, que a melhor forma de assegurar um acompanhamento mais assertivo e eficaz da evolução tecnológica em curso e potencialmente integrar processos de aquisição de equipamentos, passa por trabalhar em parcerias com outros agentes, militares e civis, ligados à inovação tecnológica, permitindo ainda um acesso mais rápido ao estado da arte da indústria de defesa.

Para a modernização das capacidades militares é absolutamente central falar dos equipamentos, das suas possibilidades, da sua interoperabilidade, da tecnologia que incorporam, do seu *hardware* e *software*, assim como das respetivas

licenças de utilização e atualização destes. Mas há outras dinâmicas associadas que não podemos descurar ou secundarizar, como são os recursos humanos que operam a tecnologia. O próprio sistema de formação e ensino militar, tem que se adaptar a esta nova realidade. Estamos assim, perante um desafio no domínio da Defesa Nacional e das Forças Armadas, em que a tecnologia assume um papel decisivo e transformador, exigindo a todos um novo olhar sobre as dinâmicas associadas ao vetor militar. Este novo olhar passa pelos processos de seleção dos militares, da sua formação e ensino, a doutrina utilizada e a forma como esta se pode tornar ultrapassada em pouco tempo.

Podemos assim concluir este prefácio dizendo que os textos que integram estes Cadernos do IUM N.º 63, ajudam-nos a melhor perceber o caminho que temos que seguir para assegurar a modernização das capacidades militares no mundo digital em que vivemos, mas também nos despertam a curiosidade para refletir sobre outras realidades que estão igualmente associadas à modernização e que, provavelmente, outros auditores irão ter o ensejo de refletir sobre as mesmas, sendo, certamente, temas a integrar futuras edições dos Cadernos do IUM.

José Carlos da Silva Mello de Almeida Loureiro
Coronel Tirocinado de Cavalaria
O Coordenador da Área de Ensino de Operações Militares
e da Área de Ensino de Técnicas e Tecnologias Militares

INTRODUÇÃO GERAL

A presente obra intitulada "A Modernização das Capacidades Militares no Mundo Digital" agrega um conjunto de seis estudos sobre temas inovadores que podem impulsionar a modernização das capacidades militares tendo em conta questões centrais relacionadas com a defesa e segurança no cenário estratégico contemporâneo. Focando-se nas especificidades das Forças Armadas de diferentes países e no desenvolvimento da indústria de defesa, esta coletânea oferece uma análise profunda e abrangente elaborada por alunos, auditores dos cursos de Promoção a Oficial General 2023/2024, e de Estado-Maior Conjunto 2023/2024, cuja investigação foi distinguida por júris especializados do Departamento de Estudos Pós-Graduados do IUM.

Como podem as nações equilibrar a modernização tecnológica e estratégica das suas Forças Armadas enquanto enfrentam desafios como restrições orçamentais, ciberameaças crescentes e a necessidade de interoperabilidade em cenários internacionais?

Estarão as Forças Armadas e as indústrias de defesa preparadas para enfrentar as complexidades de um mundo cada vez mais interconectado, onde a guerra de alta intensidade, os avanços tecnológicos disruptivos e a necessidade de autonomia estratégica desafiam o *status quo*?

São estas as principais inquietações a que os estudos procuram dar resposta. A primeira Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa (BTID) em Portugal, deu-se com a Resolução de Conselho de Ministros, n.º 35/2010, alinhada com a ambição europeia de uma base industrial de defesa mais integrada. Efetivamente, o Conceito Estratégico de Defesa Nacional de 2013, que destaca a necessidade de alinhar a BTID nacional com o Plano Nacional de Inovação para manter um elevado nível tecnológico nas Forças Armadas.

Mais recentemente, a Resolução do Conselho de Ministros a n.º 52/2023 aponta para uma nova estratégia de desenvolvimento da BTID (2023-2033), focando-se na modernização e inovação da indústria de defesa portuguesa e a Estratégia Industrial de Defesa Europeia de 2024, que estabelece uma estratégia integrada para fortalecer a indústria de defesa europeia, com medidas para aumentar os investimentos em capacidades militares e promover tecnologias de duplo uso; Bússola Estratégica de Segurança e Defesa da UE (2022), que incita os Estados-Membros a adotarem uma abordagem estratégica comum, promovendo a soberania

tecnológica europeia e a redução de dependências externas. Complementarmente, diretrizes da OTAN e da Agência Europeia de Defesa, destacam a importância de interoperabilidade, inovação tecnológica e reforço de capacidades militares para enfrentar desafios contemporâneos como ciberameaças e guerras híbridas.

É em função da pertinência e justificação apresentadas das capacidades de defesa que constituem desideratos principais da presente publicação, gerar contributos para: o incentivo à inovação e à colaboração entre setores civis e militares, promovendo tecnologias de duplo uso; o reforço da autonomia estratégica da Europa num contexto de crescente tensão geopolítica; o fortalecimento da colaboração internacional; a integração de avanços tecnológicos em áreas como o ciberespaço e o espaço.

The Military Balance, publicado anualmente desde 1959, fornece uma avaliação exaustiva das Forças Armadas e dos inventários de equipamento de 173 países, juntamente com dados económicos sobre a defesa (Iiss, 2023). Constitui-se é uma fonte indispensável para todos os envolvidos na definição, análise e investigação de políticas de defesa e segurança, oferecendo dados pormenorizados sobre os países e avaliações regionais de questões militares importantes.

Estudos recentes sobre a modernização e as capacidades da indústria militar centraram-se em áreas-chave, diversas refletindo a natureza evolutiva da guerra e os avanços tecnológicos.

Os avanços tecnológicos têm desempenhado um papel crucial na modernização militar. O surgimento da Indústria 5.0, que enfatiza a colaboração homem-máquina, tem implicações para a produção e para as operações militares. Esta nova mudança de paradigma centra-se na sustentabilidade, na resiliência e na integração de tecnologias avançadas como a robótica e a cobótica (Alojaiman, 2023).

A tecnologia *laser* registou progressos notáveis em aplicações militares, incluindo armas de energia dirigida, indicadores de alvos e telémetros. A divergência de feixe estreito das emissões *laser* oferece vantagens em transmissões seguras e operações críticas para a segurança. Os avanços recentes revolucionaram o campo de batalha militar em evolução, com aplicações em destacamentos aéreos, drones e operações espaciais (Ahmed et al., 2020).

De forma sumária, percebe-se que, a modernização da indústria militar e o reforço das suas capacidades nos últimos anos, têm como objetivo aumentar a eficácia do combate, melhorar a eficiência operacional e enfrentar os desafios de segurança emergentes no panorama militar moderno.

É neste cenário multifacetado que se inserem os seis estudos apresentados nesta coletânea que apontam soluções inovadoras e práticas para a modernização e o fortalecimento das capacidades militares.

O primeiro estudo, intitulado "A Capacidade Operacional da Marinha do Brasil: Perspetivas Estratégicas", examina a postura de defesa de um Brasil que, historicamente, manteve uma política pacífica, mas que, diante de novos desafios, como a ascensão da China no Pacífico e a degradação das suas próprias Forças Armadas devido a limitações orçamentais, precisa de repensar as suas estratégias de defesa. Este estudo propõe medidas para revitalizar a Marinha Brasileira, posicionando-a como um vetor essencial para a defesa do país, a primeira linha de defesa, especialmente em confrontos navais, considerando os Estados Unidos e a China como as principais potências com as quais o Brasil interage.

O segundo estudo, "Contributos para o *Digital Backbone* da Marinha Portuguesa", aborda a urgência da transformação digital da Marinha Portuguesa, com foco na necessidade de integrar novas tecnologias e práticas digitais robustas. Destaca a importância da interoperabilidade com a NATO e com outros aliados estratégicos, garantindo que as operações possam ser conduzidas de forma eficiente, segura e ágil, especialmente no contexto das operações multinacionais e dos novos desafios da cibersegurança e das operações no domínio digital.

No terceiro estudo, "*Intelligence-Led Policing*: Contributos para a sua Implementação na GNR", explora-se a implementação do modelo *Intelligence-Led Policing* na Guarda Nacional Republicana (GNR), indiciando como a integração de inteligência estratégica e a utilização de novas tecnologias podem fortalecer a segurança interna e a capacidade da GNR de antecipar e responder proativamente a ameaças, melhorando o processo de tomada de decisão e a eficiência operacional.

O quarto estudo, "A *Identity Intelligence* Enquanto Instrumento Contribuinte para as Operações Militares: Desafios Face ao Ambiente Contemporâneo", foca-se na crescente importância da *Identity Intelligence* nas operações militares. Este estudo explora como o uso de dados biométricos e informações de identidade pode otimizar as operações das Forças Armadas Portuguesas, permitindo uma resposta mais eficaz às ameaças, ao mesmo tempo que levanta questões sobre a privacidade e a ética da utilização dessas tecnologias.

O quinto e sexto estudos, "Os Contributos da Base Tecnológica e Industrial de Defesa para o Desenvolvimento das Capacidades das Forças Armadas" e "Os Contributos para a Implementação da Estratégia de Desenvolvimento da

Base Tecnológica e Industrial de Defesa 2023-2033", focam o desenvolvimento e modernização da BTID em Portugal e na União Europeia. Num cenário em que a guerra de alta intensidade se reintroduz na Europa, a importância de uma indústria de defesa robusta e autossuficiente torna-se um ponto central das estratégias de segurança. Estes estudos examinam a evolução da BTID, com ênfase na integração de tecnologias avançadas da Indústria 4.0, como a automação e a digitalização, bem como a sua aplicação para garantir a soberania e a autonomia estratégica da defesa europeia, além de destacar as questões políticas e económicas associadas à sua implementação.

Em conjunto, estudos oferecem uma análise profunda e detalhada de diversos aspetos da modernização das Forças Armadas e da indústria de defesa, abordando desde as tecnologias emergentes e a transformação digital até às questões estratégicas e geopolíticas que moldam as capacidades militares de diferentes países. Através desta compilação, espera-se fornecer uma visão holística e atualizada sobre os desafios e as oportunidades que se apresentam para os decisores e profissionais da área de defesa e segurança, destacando soluções inovadoras e práticas para enfrentar o futuro da guerra e da segurança internacional.

A Coordenadora

Ana Esteves
Tenente-coronel
Coordenadora editorial do CIDIUM

REFERÊNCIAS BIBLIOGRÁFICAS

Alojaiman, B. (2023). Technological Modernizations in the Industry 5.0 Era: A Descriptive Analysis and Future Research Directions. *Processes, 11*(5), 1318. https://doi.org/10.3390/pr11051318

Ahmed, A. S., Mohsin, M., & Ali, S. M. Z. (2020). Survey and technological analysis of laser and its defense applications. *Defence Technology, 17*(2), 583–592. https://doi.org/10.1016/j.dt.2020.02.012

The International Institute for Strategic Studies. (2023). *The Military Balance 2023* (1st ed.). Routledge. https://doi.org/10.4324/9781003400226

ESTUDO 1 – A CAPACIDADE OPERACIONAL DA MARINHA DO BRASIL: PERSPETIVAS ESTRATÉGICAS[1]

THE BRAZILIAN NAVY'S OPERATIONAL CAPABILITY: STRATEGIC PERSPECTIVES

Raphael Corrêa Silva
Capitão-de-mar-e-guerra BRA

Marcos Aurélio de Oliveira Simas
Capitão-de-mar-e-guerra BRA

RESUMO

O Brasil possui excelentes relações diplomáticas com os países vizinhos, sendo naturalmente protegido por montanhas, selvas e oceano. Isto cria na população brasileira uma perceção de pacifismo, e a defesa perde prioridade, fazendo com que os recursos financeiros destinados às Forças Armadas sejam constrangidos sistematicamente. A consequência é a degradação da capacidade operacional das Forças e o depauperamento da mentalidade estratégica de defesa, aspetos que constituem o problema/objeto estudo deste trabalho. A estratégia de investigação mista foi escolhida para aferir os indicadores com maior precisão. A recolha de dados requereu pesquisa documental, inquéritos com oficiais experientes e entrevistas com um Comandante de Esquadrão e com o Chefe de Operações da Esquadra. O estudo pautou-se na prospetiva de confrontos entre forças navais, considerando os Estados Unidos da América e a China como atores principais. A formulação de uma hipótese estratégica que considerou a Marinha como a primeira linha de defesa do Brasil, a hierarquização de ameaças, a definição dos meios operativos necessários para se contrapor às ameaças e a avaliação da capacidade operacional atual da Marinha foram a base e o caminho para a proposta de medidas que permitam à Marinha manter uma capacidade para defender o Brasil.

Palavras-chave: ameaças, ambiente operacional, capacidade operacional, estratégia, plano estratégico da Marinha, primeira linha de defesa do Brasil

[1] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Promoção a Oficial General (CPOG 2023/2024). A versão integral encontra-se disponível no Centro de Recursos do Conhecimento do Instituto Universitário Militar.

ABSTRACT

Brazil has excellent diplomatic relations with neighboring countries, being naturally protected by mountains, jungles and the ocean. This creates a perception of pacifism among the Brazilian population, and defense loses priority, causing financial resources allocated to the Armed Forces to be systematically constrained. The consequence is the degradation of the operational capacity of the Forces and the depletion of the strategic defense mentality, aspects that constitute the problem/object of study of this work. The mixed research strategy was chosen to measure the indicators with greater precision. Data collection required documentary research, surveys with experienced officers and interviews with a Squadron Commander and the Squadron Chief of Operations. This study was based on the prospect of clashes between naval forces, considering the United States of America and China as the main actors. The formulation of a strategic hypothesis that considered the Navy as Brazil's first line of defense, the hierarchization of threats, the definition of the operational means necessary to counter threats and the assessment of the Navy's current operational capability were the basis and the path to propose measures that keep Brazilian Navy able to defend Brazil.

***Keywords**: threats, operational environment, operational capacity, strategy, Navy strategic plan, Brazil's first line of defense*

1. INTRODUÇÃO

Na década de 1960, Raymond Aron (1962, p. 318) apresentou uma análise, afirmando que entre os Estados da época, apenas a República Popular da China (RPC), a Índia e o Brasil estariam na escala dos dois gigantes que eram os Estados Unidos e a União das Repúblicas Socialistas Soviéticas (URSS).

Impulsionados por orçamentos de defesa com taxas de crescimento anuais superiores a 10% desde 2000, alguns países aumentaram significativamente os seus gastos com equipamentos de defesa, e.g.: + 197% na RPC, + 134% na Índia, + 92% na Coreia do Sul e + 61% em Taiwan, enquanto os gastos globais cresceram cerca de 43%. O Brasil, por sua vez, aumentou os seus gastos em 30%, i.e., muito abaixo da média mundial (Belais, 2014, pp. 8-9).

A economia brasileira tem por base a exportação de matérias-primas. Dados do Ministério do Desenvolvimento, Indústria, Comércio e Serviços (Brasil, 2023) comprovam que as matérias-primas foram os principais produtos exportados em 2022. Essa situação indica que o Brasil não possui um desenvolvimento industrial consolidado, o que torna difícil a criação e a manutenção de alta tecnologia no país.

A literatura de economia política identifica uma relação positiva entre despesas militares e crescimento económico. Argumenta-se que a estabilidade geopolítica assegurada pela defesa é um pré-requisito para a criação de riqueza nacional (Louis, 2014, p. 145). Precursor destes pensamentos, Adam Smith explicou na sua obra literária "A riqueza das Nações", que o primeiro dos deveres do Soberano é a proteção da sociedade contra a violência e a invasão (Smith, 1776, livro 5, p. 10).

Observa-se que a abordagem feita por Smith está vinculada à perceção de ameaças. Ainda que a identificação de ameaças não engendre reações urgentes, revela-se necessário ter forças militares capazes de ampliar o poder de combate estatal num curto lapso temporal. O poder de combate só pode ser potenciado rapidamente se o conhecimento tático for pleno entre os militares em tempo de paz. Segundo Clausewitz, "uma boa estratégia pode ser criada por um principiante inspirado, mas uma tática eficaz é o trabalho de uma vida." (Clausewitz, s.d., cit. por Hughes Jr., 1999, p. 27)

Para manter e transmitir os conhecimentos táticos é preciso conhecer as armas. Tipificando o que seriam as armas dos marinheiros, muito pertinente é a frase do Marechal Foch publicada por Marion Soller (2022, p. 3): "Nós soldados, temos os nossos homens para armar, vocês marinheiros, têm os vossos homens para armar vossos Navios"[2]. As armas dos marinheiros são os navios, sem navios, os marinheiros não existem.

Inspirados em Adam Smith, os soberanos brasileiros deveriam, acima de tudo, proteger o país. Mas as dúvidas giram sempre em torno das ameaças. Valladão (2014, p. 2) afirmou que distante dos grandes teatros de confronto estratégico do planeta, o Brasil nunca foi confrontado com um desafio concreto em termos de segurança. A interpretação desse aspeto é crucial para o desenvolvimento da estratégia de defesa no Brasil. A população brasileira não possui perceções de ameaças externas. Como consequência, quem está no poder não atribui valor às Forças Armadas (FFAA) ou à base industrial de defesa.

O General Beaufre (2012, p. 34) conceptualiza que a estratégia é "a dialética das vontades com o uso da força", sendo o objetivo: atingir as metas políticas com os meios disponíveis. Para Bellais (2014, p. 21), a existência da indústria de defesa para sustentar as FFAA é o reflexo de uma vontade política antes de ser uma

[2] Tradução do autor de "*Nous terriens, nous avons des armes pour équiper nos hommes: vous marins, vous avez des hommes pour armer vos bateux*".

atividade económica. Este ponto de vista permite-nos compreender plenamente a situação descrita por De Melo (2015, p. 25), quando afirmou que as FFAA brasileiras estavam depauperadas e que a base industrial de defesa fora desmantelada durante a década de 1990. Constata-se, portanto, que os governantes a partir da década de 1990 demonstraram pouco interesse em desenvolver estratégias de defesa.

O Comandante da Marinha (CM), Almirante Marcos Sampaio Olsen, alertou os senadores da Comissão de Relações Exteriores e Defesa Nacional quanto à capacidade operacional deficiente da Marinha na defesa do Brasil. A causa primordial está vinculada às sistemáticas restrições orçamentais, cuja consequência será a desativação de 40% dos meios operativos até 2028, decorrente da obsolescência dos meios e das dificuldades de manutenção (Olsen, 2023, cit. por Caiafa, 2023, 1º parágrafo). Mencionou, ainda, que:

> Uma *percepção* menos acurada dessas ameaças influencia a alocação de recursos em defesa, reduzindo essa prioridade. Essa realidade é perigosa e traz consequências graves. A presença de potências extrarregionais no entorno estratégico brasileiro deve ser motivo de preocupação para o Estado. (Olsen, 2023, cit. por Caiafa, 2023)

Assim, a problemática do decréscimo da capacidade operacional da Marinha do Brasil (MB) na defesa do país apresenta-se concreta e ameaçadora para o Estado nos últimos anos. O Ministério da Defesa (MD) (2015, p. 55) do Brasil define capacidade operacional como "a condição efetiva de cumprir uma tarefa tática, assegurada pela integração de recursos humanos capacitados e adestrados, meios adequados e a correspondente fundamentação doutrinária".

O objetivo geral (OG) desta investigação é propor uma forma da MB defender o Brasil, por meio do PBC. Para o alcançar foi necessário definir os seguintes objetivos específicos (OE): OE1 - identificar as possibilidades de emprego das Forças Navais em cenários de crises ou conflitos até 2040; OE2 - identificar as linhas de defesa do Brasil; OE3 - estimar os meios operativos para combater as ameaças vislumbradas no Plano Estratégico da Marinha 2040; e OE4 - avaliar a capacidade operacional da MB em defender o Brasil até 2040. Definiu-se como objeto de estudo desta investigação: a capacidade operacional da MB (CapOpeMB) e como questão central (QC): De que forma a MB, por meio do PBC, pode manter uma capacidade operacional para defender o Brasil?

O estudo encontra-se estruturado da seguinte forma: a presente introdução, seguida de três capítulos e de uma conclusão. No capítulo dois, abordam-se a revisão da literatura, as teorias e os conceitos estruturantes. A metodologia e o

método utilizados serão apresentados no capítulo 3, descrevendo-se a estratégia de investigação e o desenho de pesquisa. Os participantes das entrevistas serão identificados, bem como a técnica de recolha e tratamento de dados. O quarto capítulo apresentará a compilação e a análise do material pesquisado, procurando-se responder às QD e QC. No capítulo cinco, concluindo a investigação, o enquadramento do tema, o sumário da metodologia adotada, a avaliação dos resultados obtidos em relação ao problema investigado e a proposta de como a MB pode manter uma capacidade operacional para defender o Brasil. Ademais, incluir-se-ão as limitações do estudo e as sugestões para estudos futuros.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Este capítulo apresenta os conceitos que resultam do processo de revisão da literatura, identificando o contexto e a base conceptual em que a investigação está inserida.

Num primeiro momento, sob a ótica geopolítica, são apresentadas as análises do ambiente operacional de potências como os Estados Unidos da América (EUA), Reino Unido (RU) e Espanha. Abordar-se-á, igualmente, a análise da NATO. Sob a ótica estratégica, propor-se-á uma perspetiva de linhas de defesa do Brasil, algo que pode ser percebido como defesa em camadas, em que a atuação da Marinha do Brasil é apresentada, ineditamente, como a primeira linha de defesa.

Em seguida, abordar-se-ão as perceções do Brasil na Política Nacional de Defesa (PND) e na END, sendo estes dois documentos, as bases da formulação do PEM2040. Analiticamente, a partir da combinação lógica da proposição estratégica de PLDB e do PEM, pretende-se definir o tipo de meios operativos para se obter uma capacidade de dissuasão. Esta definição será balizada pelo PBC e pelo contexto do entorno operacional das grandes potências.

Encerrando o capítulo, serão apresentadas as potenciais ameaças, segundo o PEM2040, e a capacidade da MB em defender o Brasil até 2040.

2.1. A Geopolítica contemporânea do Sistema Internacional

A competição entre as grandes potências indica que a geopolítica mundial está novamente em voga. Os analistas das grandes potências assumem que será necessário concentrar imensos recursos para moldar a futura ordem internacional.

Empregando o seu poder financeiro e militar, as grandes potências permanecem intensamente focadas umas nas outras (Kimmage & Notte, 2023).

Kimmage e Notte (2023) consideram que as grandes potências são os EUA, a Rússia, a RPC e Europa. Apresentam como *hot-spots*: a Guerra da Ucrânia, o conflito Nagorno-Karabakh e Azerbaijão, o Mar do Sul da China (MSC), incluindo Taiwan e o conflito Israel-Hamas.

Neste prisma, segundo a avaliação da geopolítica contemporânea do Sistema Internacional (SI), os documentos estratégicos dos EUA, RU e Espanha, que analisam os *hot-spots* para a respetiva preparação político-militar, serviram de base para este estudo.

O Departamento de Defesa (DoD) dos EUA apresentou, por meio do DoD *Strategic Managment Plan Fiscal Years* 2022-2026 a *National Defense Strategy* (NDS), as seguintes prioridades de defesa nacional: dissuadir ataques estratégicos contra os Estados Unidos, Aliados e parceiros; dissuadir agressões, estando preparado para prevalecer em conflito quando necessário, priorizando o desafio da RPC no Indo-Pacífico, depois o desafio da Rússia na Europa; e construir uma Força Conjunta resiliente (DoD, 2021, p. 6).

O *Centro Conjunto de Desarrollo de Conceptos* (CCDC), órgão do MD espanhol, elaborou um documento chamado Entorno operativo 2035 com base no panorama de tendências geopolíticas. Este documento possui o propósito de avaliar a necessidade de evolução das FFAA espanholas para enfrentar as ameaças das próximas décadas (CCDC, 2022, p. 7). Destarte, há o apontamento que a segurança e o funcionamento normal das sociedades avançadas dependem de um amplo conjunto de infraestruturas críticas e de serviços essenciais. Consequentemente, estes apresentam-se como objetivos prioritários de possíveis adversários, estatais ou não estatais (CCDC, 2022, p. 47).

Além disso, o CCDC (2022, p. 45) define que o espaço marítimo é de grande importância para Espanha. A sua configuração geográfica, em razão da dependência de recursos energéticos e comerciais, faz do controlo do mar um objetivo prioritário, enfatizando que os conflitos armados constituem a ameaça mais significativa à segurança nacional (2022, p. 62).

Na visão do CCDC, o mundo possui características multipolares com tendência a formar dois blocos concorrentes, liderados em graus variados pelos EUA, pela RPC, pela União Europeia e pela Rússia. Há a expectativa que estes blocos se aliem a outros *polus* como a Índia ou o Brasil (2022, p. 21).

Coadunando com a NDS, o CCDC afirma que a diferença de interesses económicos e geopolíticos entre os EUA e a RPC aumenta significativamente, sendo secundária a rivalidade com a Rússia, apesar da guerra na Ucrânia (2022, p. 20).

O MD britânico, por meio do *Development, Concepts and Doctrine Centre* (DCDC), apresenta como tendência a mudança no equilíbrio de poder mundial. O DCDC avalia que o *centro da gravidade* do poder económico global está a deslocar-se dos EUA e Europa, em direção à Ásia, tornando o mundo multipolar. Entretanto, considera que os EUA continuarão sendo o principal poder militar até 2035, mas tendo a sua vantagem militar em relação à RPC. Adicionalmente, categoriza o Brasil e a Índia como potências emergentes que terão interesse estratégico além de suas fronteiras em procura de recursos (2015, p. 2).

O DCDC (2015, p. 12) reitera que a NATO continuará a ser a principal aliança de defesa e que em 2035, o mais importante desafio da segurança marítima concentrar-se-á em torno de Zonas Económicas Exclusivas (ZEE). Estima-se que a produção de petróleo *offshore* seja de 48% da produção mundial. As plataformas *offshore* crescerão de 270 para mais de 600 nos próximos 20 anos. Menciona ainda que o volume de mercadorias transportadas pelas Linhas de Comunicação Marítima (LCM) aumentará dramaticamente (DCDC, 2015, p. 23).

Os conceitos dos Estados acima mencionados abrangem pontos comuns e relevantes. Dentre os quais se destacam: a participação na NATO e que o maior desafio militar será contrapor-se à estratégia *Anti-access and Area Denial* (A2AD) da RPC.

A NATO, por meio do seu Conceito Estratégico 2022, apresenta a Rússia e a RPC como potenciais adversários (2022, pp. 4-5), afirma que defenderá a liberdade de navegação, protegendo as suas principais LCM (2022, p. 7) e enfatiza a importância da região do Indo-Pacífico (2022, p. 11). Destarte, sintetiza a visão dos Estados supracitados sobre a geopolítica contemporânea do SI.

2.2. A Estratégia e as Linhas de Defesa do Brasil

Os fatores que condicionam a evolução das nações são de natureza geográfica e económica. Nos planeamentos de alto nível, estes fatores balizam a seleção de objetivos e o emprego do poder na conceção de estratégias que podem ser predominantemente: marítimas ou continentais. A seleção das estratégias pelos Estados depende da natureza das suas comunicações com outras regiões do

mundo, de inimigos tradicionais ou presumíveis e da sua localização geográfica (Caminha, 1983, pp. 26-27).

Quando se estudam os aspetos geopolíticos, percebe-se que o Brasil tem todas as possibilidades de se tornar uma grande potência. Tem todas as potencialidades ligadas a um território: o clima, a geografia e a geologia. É possível transpor o Brasil ao conceito proposto pelo geopolítico Olivier Zajec (2016, p. 119), quando tipifica os EUA de Ilha-Mundo (IM). Ele argumenta que os EUA são naturalmente protegidos por dois oceanos.

Ainda sob o argumento de que os EUA são uma IM, um estudo mostrou que entre 1946 e 1975, de 215 incidentes em que os EUA empregaram suas FFAA com propósitos políticos, as unidades navais participaram de 177 (Caminha, 1983, p. 36).

O Brasil, ainda que possua dimensões continentais, pode ser visualizado por meio de uma figura geométrica, conforme ilustrado na Figura 1, imaginando-o como um triângulo com um dos vértices voltado para o sul. O lado Norte, paralelo à Linha do Equador, seria a selva amazónica, o lado oeste seria a Cordilheira dos Andes e o lado leste seria o Oceano Atlântico. Estas características tornariam o Brasil, tal como os EUA, segundo Zajec, uma IM, i.e. naturalmente protegido.

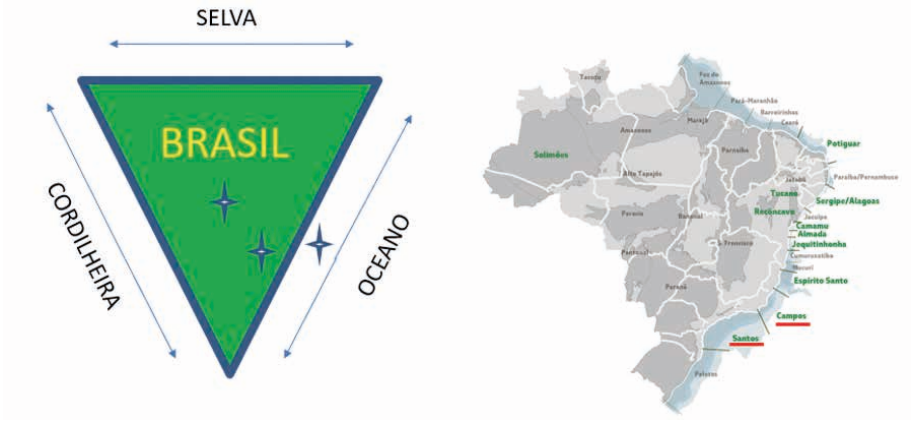

Figura 1 – O Brasil e a sua forma geométrica

A probabilidade de invasão transpondo uma selva densa ou uma cordilheira é mínima, pois a logística é difícil e com custos altíssimos.

O Manual de *Jungle Operations* ATP 3-90.98 do Exército dos EUA (2020, p. 1-1) define que selvas são massas de vegetação tropical, normalmente, impenetráveis.

Indica que existem em áreas tropicais do mundo, e.g.: o sudeste da Ásia, a África e a América latina, apresentados na Figura 2.

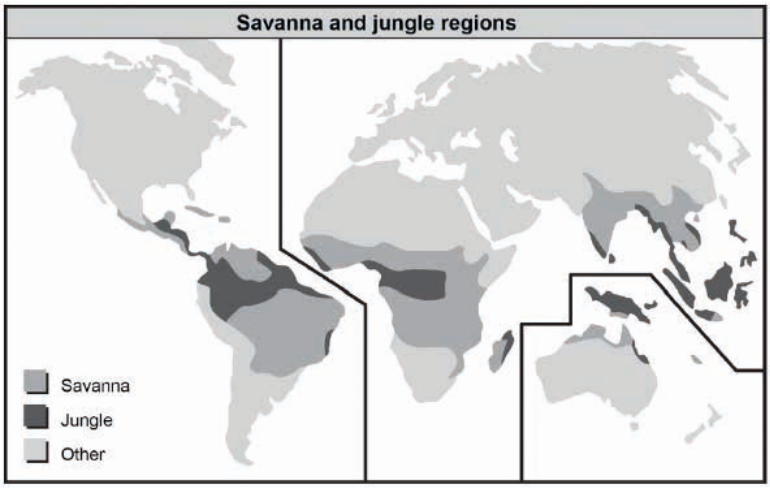

Figura 2 – As regiões de selva e savana no mundo
Fonte: Disponível em US Army (2020).

Sob a ótica logística, o Manual reitera estas dificuldades, afirmando ser inerente ao sucesso de qualquer operação tática o planeamento de uma logística contínua. A ausência de portos, aeródromos, ferrovias e rodovias limita o abastecimento das tropas. A inexistência de água potável, item básico da sobrevivência, aumenta a procura de purificadores de água, transporte e locais para armazenamento. Outrossim, o ambiente pode afetar, severamente, os equipamentos de combate, requerendo um alto nível de manutenção. (US Army, 2020, p. 3-28).

Outro aspeto vinculado à dificuldade das comunicações é a velocidade de avanço das tropas no terreno. O Manual apresenta na tabela 1 as velocidades de avanço para efeito de planeamento. Constata-se que a velocidade de avanço das tropas é baixíssima, sendo qualquer progressão lenta, penosa e custosa.

Tabela 1 – Velocidade de avanço das tropas na selva durante o dia

Type Terrain	*Maximum Distance (in meters per hour)*
Tropical Rainforest	up to 1,000
Deciduous Forest, Secondary Jungle, Tall Grass	500
Swamps	100 to 500
Rice Paddies (Wet)	800
Rice Paddies (Dry)	2,000
Plantations	2,000
Trails	up to 3,000

Fonte: Disponível em US Army (2020).

Quanto à cordilheira, o Manual de *Mountains Operations* FM 3-97.6 (90-6) (2000, p. vi) do Exército dos EUA enfatiza duas características do terreno montanhoso: o impacto severo das condições ambientais nas tropas e a extrema dificuldade de mobilidade.

As principais cadeias de montanhas do mundo situam-se ao longo de cinturões mostrados na Figura 3 (US Army, 2000, p. 1-2).

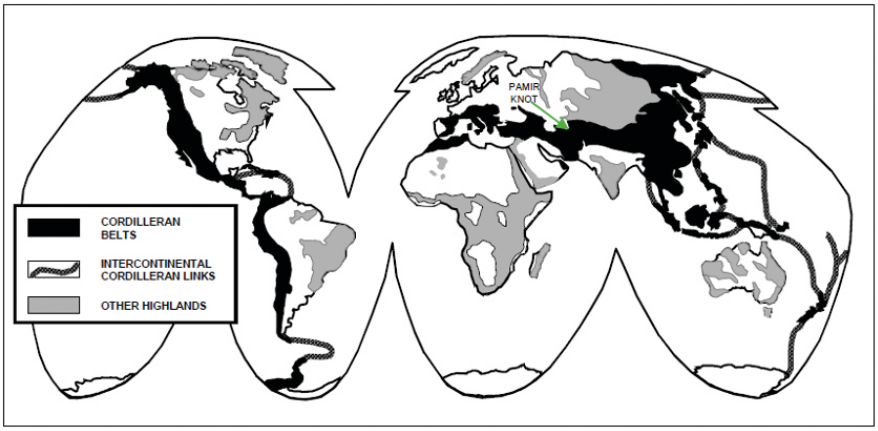

Figura 3 – As regiões montanhosas do mundo
Fonte: Disponível em *US Army* (2000).

O Manual (2000, 1-3) menciona que a Cordilheira dos Andes possui uma altitude superior a 3.000 metros por uma distância de 3.200 quilómetros, sendo as principais dificuldades de operar neste tipo de terreno: as linhas de comunicação e a logística (US Army, 2000, 2-3).

Quanto às linhas de comunicação terrestres, as rotas de abastecimento são limitadas aos caminhos estreitos. O número limitado de rotas aumenta o volume de tráfego e impõe grandes desafios às unidades de engenharia. Devido à má qualidade dos caminhos com inclinações acentuadas, a velocidade dos deslocamentos é baixa (US Army, 2000, p. 5-6).

As especificidades supracitadas indicam que uma agressão de outro Estado contra o Brasil, provavelmente, seria conduzida pelo mar. Isto torna a MB, por intermédio da sua Esquadra, a PLDB. Neste prisma, a Força Aérea Brasileira (FAB) seria a segunda linha e teria de operar de forma conjunta com a MB. O Exército Brasileiro (EB), indubitavelmente e não menos importante, seria o último bastião, i.e. a terceira linha.

Caminha (1983, p. 29) corrobora a lógica de defesa acima, afirmando que militarmente, as experiências das duas Guerras mundiais e a subsequente evolução de acontecimentos na Europa não foram suficientes para tornar evidente para os dirigentes brasileiros que prováveis agressões contra o Brasil **não mais seriam exercidas através das suas fronteiras terrestres, mas sim no Atlântico.**

2.3. Plano Estratégico da Marinha 2040

No seguimento desta investigação, torna-se importante analisar o PEM2040 sob duas vertentes: a primeira estará focada na base legal e a segunda nas ameaças.

A base legal constitui a materialização da legitimidade das ações e reações propostas para a defesa do Brasil a serem executadas pela MB. As ameaças apresentadas no PEM2040 servirão de base para a elaboração de cenários que comporão o item seguinte do enquadramento teórico e conceptual.

2.3.1. Base Legal

O Planeamento de Alto Nível da Marinha consolida-se no PEM para a gestão de ameaças. Este Plano é condicionado, conforme mostrado na Figura 4, pelos documentos de alto nível da Defesa, tais como a PND e a END (MB, 2020, p. 7).

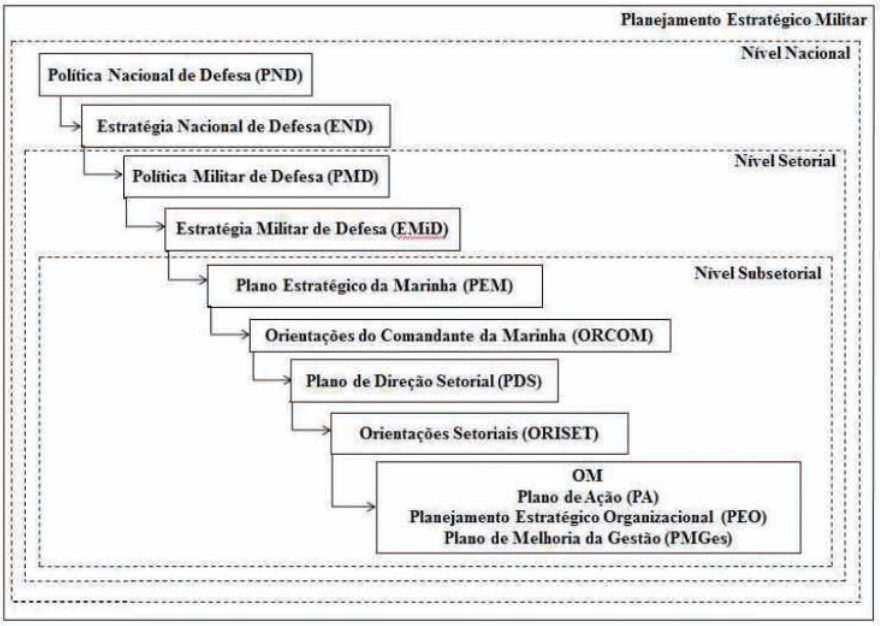

Figura 4 – Subordinação do PEM
Fonte: (Marinha do Brasil, 2011, pp. 3-1).

Este estudo está assente na PND, documento orientador do planeamento de ações de contraposição às ameaças externas, que define os objetivos para o preparo e o emprego de todas as expressões do Poder Nacional, em prol da Defesa Nacional (MD, 2020b, p. 7). Derivada da PND, surge a END, cujo propósito é orientar o Estado brasileiro quanto às medidas a serem implementadas para atingir os Objetivos Nacionais de Defesa (MD, 2020b, p. 31).

A END (2020, pp. 33-34) define que a conceção estratégica de defesa do País, em tempo de paz ou de crise, está pautada pela capacidade de dissuadir ameaças, observando o estabelecido na Constituição Federal (CF), i.e, a defesa da Pátria. O Atlântico Sul é uma área de interesse geoestratégico para o Brasil. A proteção dos recursos naturais existentes nas águas, no leito e no subsolo marinho sob jurisdição brasileira é uma prioridade do País.

A dissuasão é a primeira postura estratégica a ser considerada na defesa dos interesses nacionais. A exploração da AA e a utilização das LCM do Atlântico Sul são vitais para o desenvolvimento do Brasil. Em caso de agressão externa, o País empregará o Poder Nacional, com ênfase na sua expressão militar, na defesa dos

seus interesses. "A Capacidade de Proteção do território e da população brasileira exprime o mais relevante objetivo nacional, o de garantir a soberania, o património nacional e a integridade territorial". (MD, 2020b, p. 36)

Entretanto, nem sempre é possível à direção do Estado determinar com precisão as hipóteses de guerra. Sem hipóteses consistentes não há objetivos de guerra que orientem o preparo e emprego do Poder Militar, mais especificamente, no escopo deste trabalho, o Poder Naval. Inevitavelmente, sem um inimigo real, i.e. sem um objeto de análise e conclusões, a formulação estratégica torna-se difusa. O emprego do Poder Naval é avaliado em perspetivas amplas. Procura-se antepor a uma grande gama de ameaças. Neste caso, a salvaguarda de Objetivos Estratégicos (OBEST) passa a ser a referência (Caminha, 1983, p. 164). O comprometimento de OBEST, por estarem ligados à soberania, causa ao Estado consequências catastróficas e de longo prazo.

Sob esta lógica, o CM apresentou na Câmara dos Deputados que a sociedade brasileira possui a perceção de que o Brasil é um país livre de ameaças externas, i.e., um pacifismo utópico. Acrescentou que podem ser considerados OBEST: 17 dos 27 Estados da Federação que são banhados pelo Atlântico, onde 70% da população reside a menos de 200 quilómetros do litoral, as LCM, cuja densificação até o ano de 2030 pode ser superior a 300% e os cabos submarinos, responsáveis por 99% das transmissões de dados (Olsen, 2023).

Neste sentido, o PEM2040 (2020, p. 13) procura orientar o planeamento de médio e longo prazos. Coadunando com a END, torna claro que o País necessita de exportar e importar bens, sendo que cerca de 90% do volume do comércio é feito por via marítima.

2.3.2. As potenciais ameaças

A conexão entre os oceanos faz com que os grandes atores internacionais tenham facilidade em exercer significativa influência no Entorno Estratégico brasileiro (Figura 5).

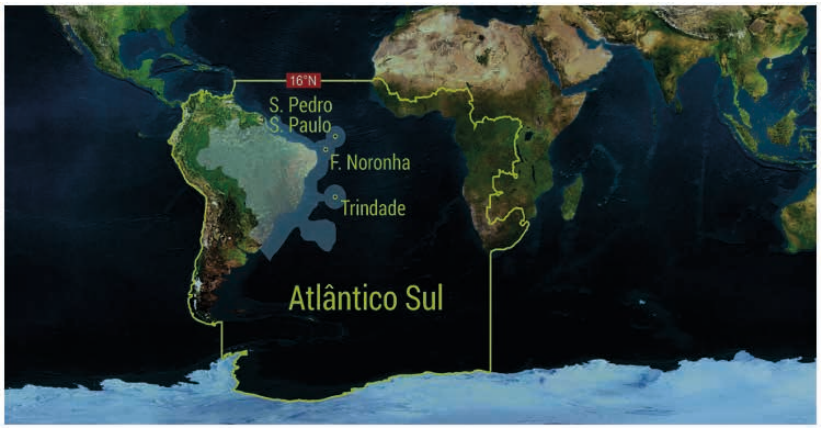

Figura 5 – Entorno Estratégico brasileiro
Fonte: Disponível em MB (2020).

No lado ocidental do Entorno Estratégico brasileiro, sobressai a AA, Figura 6, cujas dimensões são comparáveis à Amazónia. Nesta área, o Brasil detém direitos de soberania para aproveitamento económico dos recursos naturais, quer existentes na massa líquida ou no subsolo marinho.

Figura 6 – Amazónia Azul
Fonte: Disponível em MB (2020).

O SI, caracterizado por tensões e instabilidades, faz com que o Brasil possa ser envolvido em tais interações. Desta forma, foram percecionadas como principais ameaças aos interesses nacionais brasileiros na AA: a Defesa da soberania, a Pirataria, a Pesca ilegal, acessos ilegais a conhecimentos, crime organizado e conflitos urbanos, terrorismo, ameaças cibernéticas, questões ambientais e desastres naturais, e disputa por recursos naturais (MB, 2020, pp. 24-28).

Souza Jr. (2022, p. 7) afirma que há uma hierarquia entre as ameaças vislumbradas pelo PEM. Nesta mesma lógica e sob a égide dos seguintes critérios: consequências caso a ameaça se concretize, probabilidade de ocorrência, tempo de preparação intelectual dos militares para combater ameaças, complexidade das operações no combate, e meios a serem empregues, avaliar-se-á se a defesa da soberania está no topo da hierarquia, sendo esta, a referência principal para analisar a forma como a MB pode defender o Brasil. O PEM (2020, p. 35) descreve que o paradigma clássico do combate no mar mantém-se representado pelas operações e ações de Guerra Naval ligadas à Defesa da Soberania.

Vista como uma arte que emprega operativamente um poder especializado, a Estratégia Naval consiste na exploração dos atributos inerentes aos meios flutuantes. Tais atributos são a capacidade de atuação em longas extensões geográficas e a flexibilidade de emprego tático (Caminha, 1983, p. 35). Depreende-se, portanto, que os meios operativos mais apropriados para a Defesa da Soberania devem possuir um alto grau de flexibilidade.

Nas duas Grandes Guerras, os navios escoltas, representados pelos contratorpedeiros (CT), assumiram importância ímpar, tornando-se o tipo de navio com a maior participação nas operações navais planeadas (Caminha, 1983, p. 50).

2.4. A capacidade da MB em defender o Brasil até 2040

Doravante, a partir dos conceitos supracitados, será considerado um cenário que representa o comprometimento da soberania do Brasil.

Quanto ao emprego de Forças Navais em cenários de crises ou conflitos, considerando os atores geopolíticos indicados, ficou evidente que o principal efeito é a manutenção da liberdade de navegação, cuja maior ameaça é constituída pela estratégia A2AD imputada à RPC. Isto indica que os atores estão a preparar as suas Forças Navais para se contraporem à estratégia A2AD, sendo o Teatro de Operações o MSC, Figura 7. Esta região foi palco de diversas Operações Navais e Conjuntas durante a Segunda Guerra Mundial (SGM), com o emprego massivo de Forças Navais nucleadas em Navios Aeródromos (NAe).

Figura 7 – Mar do Sul da China
Fonte: Disponível em CAAML (2022).

Quanto às linhas de defesa do Brasil, a partir da ideia de que o Brasil é uma IM, a PLDB seria a Marinha. Referente ao PEM, considera-se que os navios escoltas seriam, taticamente, os mais *flexíveis* para a contraposição das ameaças identificadas.

Destarte, com o foco na garantia da soberania do Brasil, elabora-se o seguinte cenário: a título, meramente ilustrativo, suponha-se haver um país vizinho do Brasil, possuidor de NAe, com influência suficiente para formar uma aliança que decidisse ampliar a sua extensão, sob os argumentos de preservar a floresta amazónica devido às alterações climáticas. Quais seriam as suas Linhas de Ação? Invadir por terra e deparar-se com uma penosa progressão terrestre, conforme anteriormente exposto? Conduzir um assalto anfíbio e também se deparar com uma penosa progressão terrestre? Atacar alvos que comprometam a soberania do País, causando impacto direto na vida dos cidadãos, forçando uma negociação, i.e. a consolidação do conceito de estratégia mencionado por Beaufre na introdução?

A Doutrina de Operações Conjuntas (MD, 2020a) no Brasil contempla, na análise do centro de gravidade (CG), o conceito de Vulnerabilidade Crítica (VC) (MD, 2020a, p. 219). Segundo o conceito de VC, pode-se afirmar que as LCM citadas pelo CM, as plataformas de petróleo citadas no PEM, as indústrias do sul e sudeste do Brasil que impulsionam a economia brasileira e as hidroelétricas comporiam as VC, sendo os primeiros alvos de uma crise ou conflito. A destruição ou neutralização de quaisquer destes alvos causaria enorme impacto na vida do cidadão brasileiro. Isto implicaria facilmente em uma negociação, ainda que o objeto de disputa estivesse a milhares de quilómetros destas VC.

Estas VC possuem em comum o facto de estarem localizadas na AA ou no litoral, i.e. são alvos evidentes de uma Força Naval. O corolário disto é que a Marinha, forçosamente, tem de manter a capacidade operacional para defender o Brasil.

A PND (2020, p. 35) define as Capacidades Nacionais de Defesa (CND) como aquelas compostas por diferentes parcelas das expressões do Poder Nacional. Nesta composição destaca-se a capacidade de dissuasão que se configura como fator essencial para a Segurança Nacional, cujo propósito é desincentivar possíveis agressões, consistindo na disponibilidade e prontidão de meios militares e da capacitação do seu pessoal (MD, 2020b, p. 37).

Neste contexto, o MD (2015, p. 55) conceptualiza que capacidade militar está aplicada ao nível estratégico, representando a aptidão de uma Força Armada em executar as operações como instrumento da expressão militar do Poder Nacional. A sua consecução é fruto da combinação de elementos das áreas de doutrina, organização, pessoal, educação, material, *adestramento* e infraestruturas (DOPEMAI). Fiuza (2018), num seminário na Escola Superior de Guerra, apresentou que o DOPEMAI é uma etapa da metodologia do PBC, conceptualizando o PBC como um "conjunto de procedimentos voltados ao preparo das FFAA, mediante a aquisição de capacidades adequadas ao atendimento dos interesses e necessidades militares de defesa do Estado, num horizonte temporal definido, observados cenários prospetivos e limites orçamentais e tecnológicos".

Ancorado no PBC, mais especificamente nas variáveis material e infraestrutura do DOPEMAI, avaliar-se-á o nível de CapOpeMB até 2040. Os indicadores vinculados a estas variáveis são, respetivamente, meios operativos e bases navais existentes em pontos de importância operacional (PIO). Considera-se que estes elementos são os básicos para compor a CapOpeMB, sendo, portanto,

conceptualizados pelo MD (2015, p. 55) como uma condição efetiva para cumprir tarefas táticas, assegurada pela integração de recursos humanos e meios operativos.

2.5. Modelo de análise

Quadro 2 – Modelo de Análise

Objetivo Geral	Propor uma forma como a MB, por meio do PBC, pode defender o Brasil				
Objetivos Específicos	**Questão Central**	De que forma a MB, por meio do PBC, pode manter uma capacidade operacional para defender o Brasil?			
	Questões Derivadas	**Conceitos**	**Dimensões**	**Indicadores**	**Técnica de recolha de dados**
OE1 Identificar as possibilidades de emprego de Forças Navais em cenários de crises ou conflitos até 2040	**QD1** Quais são os cenários de crise ou conflitos até 2040 com o emprego de Forças Navais?	Geopolítica Estratégia	Global	*Hot-spots* com possibilidade de confrontos entre Forças Navais	Análise documental, inquéritos e entrevista
OE2 Identificar as linhas de defesa do Brasil	**QD2** Quais são as linhas de defesa do Brasil?	Estratégia Operacional	Entorno estratégico brasileiro	Região/ fronteira mais suscetível a agressões Estatais; Linhas de defesa do Brasil	Inquéritos e entrevistas
OE3 Estimar os meios operativos para combater as ameaças vislumbradas no Plano Estratégico da Marinha 2040	**QD3** Quais são os meios operativos para serem empregues no combate às ameaças, segundo o PEM2040?	Tática	Amazônia Azul	Ameaças; Alvos a serem defendidos; Tipo de meios operativos	Análise documental, inquéritos e entrevistas

3. METODOLOGIA E MÉTODO

O desenho de pesquisa escolhido foi o estudo de caso, assumindo um caráter analítico, questionando uma situação específica e confrontando-a com teorias existentes (Freixo, 2011, cit. por Santos, & Lima, 2019, p. 37). A estratégia de investigação adotada foi a mista (qualitativa-quantitativa) (Santos & Lima, 2019, p. 29). A combinação dos métodos permitiu ter acesso a um conhecimento mais amplo e aprofundado sobre um assunto essencialmente complexo (Santos & Lima, 2019, p. 128) e desenvolver a componente do estudo referente às linhas de defesa do Brasil (Greene, et al., 1989, cit. por Santos & Lima, 2019, p. 128).

O presente estudo contou com a participação de instrutores da Escola de Guerra Naval (EGN) e de CMG com mais de 30 anos de serviço para responder a um inquérito. Para ambos os públicos-alvo (PA), foram feitas as mesmas perguntas. A separação dos grupos deveu-se ao facto de os instrutores da EGN possuírem uma base teórica mais consolidada, enquanto os CMG possuem um contacto mais próximo com a prática e as dificuldades das atividades operativas e administrativas.

A seleção da amostra foi não-probabilística por se tratar de um PA altamente especializado, com larga experiência prática e teórica nos assuntos tratados neste estudo. O Comandante do Segundo Esquadrão de Escolta (ComEsqdE-2) no período de 2021 a 2023 e o atual Chefe de Operações da Esquadra (CheOpE) foram escolhidos para responderem a entrevistas semiestruturadas, por exercerem funções diretamente relacionadas à manutenção da capacidade operacional dos meios operativos da Esquadra.

A técnica de recolha de dados materializou-se através de: análise documental, inquéritos de perguntas abertas e fechadas, questões de escolhas múltiplas em leque fechado e de avaliação, cujo tipo variou entre: facto, ação, intenção e opinião e entrevistas semiestruturadas. As fontes foram primárias, secundárias e terciárias. A amostragem foi enquadrada como não-probabilística.

Os dados obtidos por meio de inquéritos e análise documental foram enquadrados como quantitativos, havendo preponderância nos inquéritos. Quanto ao enquadramento qualitativo, a recolha dos dados ocorreu por meio de entrevistas semiestruturadas e análise documental ao ComEsqdE-2 e ao CheOpE.

A elaboração dos inquéritos considerou os seguintes indicadores: *hot-spots* no mundo com possibilidade de confrontos entre Forças Navais; região do Brasil mais suscetível a agressões por atores Estatais; primeira linha de defesa do Brasil; ameaças; alvos a serem defendidos pela MB; tipos de meios para defender o Brasil; e nível da CapOpeMB com relação ao material e infraestrutura.

Considerando os PA, foi elaborado um questionário, e divulgado por *Google Forms*[3], composto por 20 perguntas nas modalidades de perguntas abertas e fechadas, tendo as submodalidades de escolha múltipla em leque fechado e de avaliação.

[3] Os questionários podem ser consultados nos seguintes *links*: https://docs.google.com/forms/d/1Yg41mCPmidoDWVZC07pD5FqNcgmXa24HVOwuwpSB4QQ/edit#responses e https://docs.google.com/forms/d/1FUXL60ePSbLSHuK5za850Jyi1TU6TfhlyG6tIcTx__g/edit#responses

A diversidade de combinações das abordagens qualitativa e quantitativa permitiu triangular e integrar os dados, procurando convergi-los (Santos & Lima, 2019, p. 31). Entretanto, conforme definido por Greene, et al., (1989, cit. por Santos & Lima, 2019, p. 128) foi possível descobrir áreas de não-convergência, havendo a possibilidade de perceber novas perspetivas.

Os dados recolhidos dos inquéritos e uma análise prévia foram apresentados ao CheOpE que transmitiu os seus contributos para este trabalho através de uma entrevista.

4. APRESENTAÇÃO DOS DADOS E ANÁLISE DOS RESULTADOS

Neste capítulo procede-se à apresentação e análise dos resultados dos inquéritos, das entrevistas semiestruturadas com amostra não probabilística e da análise documental.

4.1. As possibilidades de emprego de Forças Navais em cenários de crises ou conflitos até 2040

Para responder à QD1 – *Quais são os cenários de crise ou conflitos até 2040 com o emprego de Forças Navais?*, foram investigados os documentos dos EUA, RU, Espanha e NATO quanto ao ambiente operacional até 2035. A perceção de oficiais da MB com mais de 30 anos de serviço foi avaliada quantitativamente por meio de inquéritos e o CheOpE apresentou o seu posicionamento, representando uma análise qualitativa.

Os conceitos estratégicos dos Estados investigados abrangem pontos comuns, sendo o mais relevante: o desafio militar de contrapor-se à estratégia A2AD desenvolvida no MSC pela RPC.

A NATO, no contexto das LCM, ainda que fora do Atlântico Norte, torna claro que a região do Indo-Pacífico é relevante e que alterações de influência nesta área podem afetar a segurança Euro-atlântica. Destarte, evidencia que para os atores acima mencionados o cenário com grande possibilidade de crise ou conflito é o MSC. Outrossim, pelas características da área, pela forma como a RPC está a desenvolver a sua estratégia militar e pela contrapartida dos atores ocidentais, deduz-se que o emprego militar desenvolver-se-á com o emprego de Forças Navais.

Quanto aos oficiais da MB, cuja perceção foi medida em dois grupos distintos, ambos os grupos, cerca de 87%, concordaram que o MSC representa

o cenário de crise ou conflito com a maior probabilidade de ocorrência com o emprego de Forças Navais.

Enfatiza-se que dentre os instrutores da EGN, 87% consideram que a estratégia A2AD possui caráter de proteção e defesa. Entre os CMG, cerca de 70% possuem a mesma perceção.

A. R. S. Selles (entrevista por *email*, 30 de novembro de 2023), CheOpE, mencionou que devido ao crescimento do poderio bélico da RPC, não se pode descartar a possibilidade de um enfrentamento entre as Forças Navais dos EUA e da RPC. Contudo, acredita que há maior probabilidade de enfrentamento entre Forças Navais no Mar Negro, no Báltico ou no Mediterrâneo, devido à postura belicosa da Rússia nas relações interestatais.

Apontou ainda que a estratégia chinesa possui características de "negação do uso do mar" com um caráter de "defesa" contra ações de potências extrarregionais, apresentando similitudes com a proposta desenvolvida pela MB. Destarte, conclui-se que o MSC representa o cenário de crise ou conflito com a maior probabilidade de ocorrência com o emprego de Forças Navais.

4.2. As linhas de defesa do Brasil

Em resposta à QD2 – *Quais são as linhas de defesa do Brasil?*, foi apresentada a hipótese de que a MB poderia ser considerada a PLDB. Esta hipótese baliza a análise deste estudo, sendo uma proposta de defesa que possui o potencial de moldar a estratégia de defesa do Brasil. Para formulação desta ideia, consideraram-se aspetos geográficos e as fronteiras brasileiras. Tal como a França, que segundo Robic (1989, p. 18), adotou a metonímia de hexágono durante o governo de De Gaulle, propõe-se que o Brasil seja comparado a um triângulo.

Robic (1989, pp. 21-22) afirma que as seis facetas francesas, bordas de uma malha de soberania nacional, seriam representações esquemáticas de um espaço que interage fisicamente com o exterior. Por analogia, as facetas deste triângulo brasileiro são confrontadas com a geografia reinante. Ao norte, a selva amazónica, a oeste, a cordilheira dos Andes e a Leste, o oceano Atlântico. Esta geografia torna o Brasil naturalmente protegido, tal como uma ilha. Novamente, por analogia, a partir do conceito de Zajec, que atribui aos EUA o título de IM, propõe-se que o Brasil assim o seja considerado.

Entretanto, o PEM2040 (2020, p. 24) é taxativo em afirmar que os oceanos estão interligados, permitindo que atores internacionais tenham facilidade em

exercer influência no entorno estratégico brasileiro. Destarte, deduz-se que o lado leste do triângulo é o mais suscetível a agressões por atores Estatais.

A pesquisa documental mostrou estatisticamente que depois da SGM, nas oportunidades em que o Brasil fez demonstração relevante de força, o fez na AA com o emprego de Forças Navais, e.g.: Guerra da Lagosta e incidentes de pesca na ZEE (Caminha, 1983, p. 37).

Alinhando-se com a estatística, Da Silva (2013, p. 25) assevera que o Brasil possui fronteiras com dez países, sem quaisquer divergências de interesses quanto aos limites territoriais vigentes. Sendo este um processo centenário de consolidação da paz com os Estados vizinhos.

Quanto à proposição de que a MB é a PLDB, os inquéritos revelaram que entre os instrutores da EGN, 93% aceitam a ideia, enquanto entre os CMG, a percentagem alcança 81%.

A. R. S. Selles (op. cit.) enfatizou que para preservar soberania brasileira é essencial que a MB seja vista como a PLDB, ampliando a capacidade de proteção e afastando eventuais ameaças do litoral brasileiro. A perceção de que as principais ameaças à soberania brasileira provenham do mar não é estranha ao MD e às demais FFAA.

Em face do exposto, considerando a dificuldade de ações militares contra o Brasil nos lados norte e oeste, decorrente da geografia, a resposta desta QD é que as linhas de Defesa seriam: a primeira-MB, segunda-FAB e a terceira-EB. O imperativo desiderato desta proposta é que a prioridade estratégica seja a defesa do Brasil no mar, i.e., distante da população brasileira.

4.3. Os meios operativos para combater as ameaças vislumbradas no PEM2040

Por forma a responder a QD3 – *Quais são os meios operativos para serem empregues no combate às ameaças, segundo o PEM2040?* foi proposta uma hierarquização das ameaças vislumbradas no PEM2040. Os seguintes critérios foram obedecidos: consequências caso a ameaça se concretize, probabilidade de ocorrência, tempo de preparação intelectual dos militares para combater a ameaça, complexidade das ações e operações no combate, e meios a serem empregues no combate. Nos inquéritos aplicados aos oficiais da MB, entre os instrutores, a maioria, perfazendo 47%, considerou que a defesa da soberania é a ameaça mais relevante. Entre os CMG, 50% percebem que a disputa por recursos naturais é

a maior ameaça, entretanto 48% possui o mesmo ponto de vista dos instrutores, considerando que a defesa da soberania é a grande ameaça.

Com os dados apresentados, é possível aceitar que a defesa da soberania está no topo da hierarquia, sendo a referência principal para analisar como a MB pode defender o Brasil contra ameaças de atores Estatais.

Segundo Da Silva (2013, p. 25), o Brasil possui como linha-mestra de política externa a solução pacífica das controvérsias. Este comportamento cria a perceção de que as ameaças Estatais são inexistentes. Neste sentido, torna-se difícil caracterizar as hipóteses de guerra. A ausência destas hipóteses inibe a materialização dos objetivos de guerra que orientam o preparo e emprego do Poder Naval. Na situação em análise, conforme dito por Caminha (1983, p. 164), a salvaguarda de OBEST essenciais passa a ser a referência.

O CM (Olsen, 2023) definiu como OBEST: 17 Estados da Federação banhados pelo mar, 70% da nossa população residindo a menos de 200 quilómetros do litoral, as LCM, e as plataformas de petróleo.

A definição destes OBEST permite visualizar as ações e operações de Guerra Naval necessárias para protegê-los, caracterizando a Defesa da Soberania. A definição das supracitadas ações e operações de Guerra Naval indica os tipos de meios operativos necessários, bem como os PIO a serem explorados.

A pesquisa documental descortinou que, nas duas Grandes Guerras, os navios escoltas foram o tipo de navio com a maior participação nas operações navais planeadas. Compunham os grupamentos operativos, constituindo o seu invólucro protetor, atuavam na proteção de comboios contra a ameaça submarina, no apoio de fogo naval nas projeções sobre terra e ainda executaram improvisadas operações de apoio logístico, evacuação de tropas cercadas em terra, desembarque de pequenos contingentes e apoio de fogo cerrado. Isto ocorreu em ambos os beligerantes da SGM (Caminha, 1983, p. 50).

Ainda na pesquisa documental, a comandante Mary Katey Hays da *US Navy* considera os CT, i.e., navios escoltas, da classe Arleigh Burke como a espinha dorsal da Marinha estadunidense, sendo o navio mais poderoso do mundo (Hays, s.d., cit. por Cadotte, 2023).

Referente aos inquéritos aplicados, há uma significativa divergência entre os grupos quanto aos meios operativos que se contraponham às ameaças estatais. Dentre os instrutores, a maioria aponta que o ideal é a combinação de NAe e Escoltas, cerca de 54%. Entre os CMG, os submarinos são apontados como os meios mais apropriados, perfazendo 63%.

A. R. S. Selles (op. cit.) pontuou que há alguns anos a MB tem propagado a ideia de que uma robusta força de submarinos seria capaz de desenvolver uma estratégia eficaz de negação do uso do mar. Contudo, não há indícios na história em que essa estratégia tenha sido utilizada e que o uso de submarinos para defender o território, frente a uma Força Naval balanceada, tenha sido eficaz.

Sobre a divergência das respostas nos inquéritos, afirmou que o corpo docente da EGN, composto por oficiais com maior conhecimento académico dos conflitos do que seus pares, partilha das mesmas preocupações e advoga pela necessidade do emprego de meios de superfície para o cumprimento da missão constitucional da MB na Defesa da Pátria.

Encerrando-se esta linha de raciocínio para a resposta à pergunta, nos inquéritos aplicados em ambos os grupos, a maioria, cerca de 60% consideram que se MB estiver pronta para se contrapor à uma ameaça estatal, por conseguinte estará pronta para reagir às demais ameaças listadas no PEM2040.

O conjunto das informações acima indica que a composição NAe e Escoltas é a mais apropriada para se contrapor às ameaças Estatais, sendo os Escoltas, pela flexibilidade que possuem, os meios mais presentes nas Operações no Mar. Portanto, percebe-se que, excetuando-se os conflitos urbanos e as ameaças cibernéticas, *i.e*. ameaças desvinculadas da AA, o binómio NAe-Escoltas é o tipo de combinação de meios operativos a ser empregado para se contrapor a todas ameaças vislumbradas no PEM2040.

Um facto marcante da história do Brasil, que reitera a importância dos CT para a MB, foi a Guerra da Lagosta[4]. Mesquita (2021, 33º parágrafo) menciona que os melhores navios da MB à época eram os CT da classe Pará. Estes e outros CT foram deslocados, imediatamente, para a área de operação durante as negociações diplomáticas entre Brasil e França. Ainda que com meios operativos obsoletos, com diversas deficiências, a presença da Força Naval foi suficiente para forçar uma dialética favorável à garantia da soberania do Brasil.

4.4. A capacidade operacional da MB em defender o Brasil até 2040

Para responder a QD4 – *Qual o nível da capacidade operacional da MB em defender o Brasil até 2040?* torna-se imperioso mencionar as respostas das QD

[4] Crise diplomática entre Brasil e França ocorrida na década de 1960 em decorrência da pesca da lagosta no litoral do Brasil (Mesquita, 2021).

precedentes. Referente à QD1, concluiu-se que o MSC é o cenário com maior probabilidade de confronto entre as Forças Navais. Sendo a estratégia de proteção e defesa (A2AD) da RPC similar à proposta estratégica da MB. Esta comparação converte a AA em um *hot-spot*, caso haja conflitos de interesses Estatais.

Quanto à QD2, concluiu-se que, no advento de agressões Estatais, a maior probabilidade de ocorrência é no litoral brasileiro, i.e., na AA, sendo a MB a PLDB.

No que tange à QD3, tendo-se definido o possível local de conflito, as estratégias e os OBEST, concluiu-se que a composição NAe e Escoltas é a mais apropriada para se contrapor às ameaças Estatais, garantindo a soberania brasileira.

Segundo a Enciclopédia Britânica (1963, cit. por Caminha, 1983, p. 42), o Poder Naval procura cinco efeitos desejados: Impedir o inimigo de usar o mar para o transporte de sua força militar, i.e. defendendo o próprio solo, impedir o inimigo de receber pelo mar os bens necessários à continuação da guerra, proteger os navios amigos que executam o tráfego marítimo, bem como a própria força militar, e operar em conjunto ao exército na conquista dos seus objetivos em terra. Naturalmente, o mais importante neste TII é a defesa do próprio solo.

Nesta vertente, norteado pela variável material, o CM (Olsen, 2023) explanou na Câmara dos Deputados que "A defesa naval tem como atividade precípua a garantia da soberania", enfatizando que "[...] atendemos a defesa em 40% da sua demanda, e 60% são negligenciados [...]. Ou seja, naquilo que nos é mais caro, como a defesa e a garantia da soberania, nós atendemos com menos de 50% [...]".

Quanto à CapOpeMB, acrescentou que, devido a obsolescência e restrições severas de orçamento que impediram a manutenção ou *reaparelhamento*[5], terá de desativar 40% dos navios, armamentos e munições até 2028. Salientou que:

> Uma força que não tem a capacidade de causar dano [...], não cumpre efetivamente o seu papel. Força armada precisa ter, por dever, capacidade de causar dano, capacidade de desestimular qualquer ação adversa, no caso da Marinha nas nossas águas, particularmente nas águas jurisdicionais. (Olsen, 2023)

Relativamente aos investimentos que contribuem para o poder de combate da Força Naval, classificou-os como acanhados. Estes investimentos são: o *Sistema de Gerenciamento da Amazônia Azu*l (SisGAAz) (Figura 8), a aquisição de quatro fragatas a serem entregues a partir de 2025 e o desenvolvimento de mísseis antissuperfície.

[5] Reequipamento

Corroborando com a posição do CM, o Comandante em Chefe da Esquadra (Edgar, 2023) afirmou que a quantidade de meios operativos que a Esquadra dispõe não se mostra suficiente para se contrapor às ameaças da atualidade, principalmente considerando as dimensões da AA.

Por ocasião dos inquéritos, 81% dos CMG e 93% dos instrutores consideraram o nível da CapOpeMB, relativo aos meios operativos, regular.

F. L. Vieira (entrevista por *email*, 17 de novembro de 2023) apresentou a debilidade da situação operacional dos navios do seu Esquadrão. Ao assumir o comando em 2021, o Esquadrão era composto por quatro navios. No decorrer do comando, um foi desincorporado da Armada, um ingressou em manutenção preventiva e o outro teve uma avaria grave. Enfatizou ainda que três navios do seu Esquadrão tinham entre 30 e 40 anos de vida operativa. Este facto fora mencionado pelo CM na Câmara dos Deputados.

A capacidade operacional da Marinha em defender a AA abrange outros aspetos além dos meios operativos. As posições estratégicas descritas por Caminha (1983, p. 47), compostas por bases, estações navais e outras posições que venham assumir importância para o apoio logístico às forças de combate da Marinha, i.e., variável infraestrutura, são elementos essenciais a serem explorados na estratégia de defesa. Corroborando com este conceito, a Doutrina de Operações Conjuntas (MD, 2020a) atribui às posições estratégicas a nomenclatura de PIO.

A AA dispõe de diversos PIO, tais como Cabo Frio ou a ilha de Fernando de Noronha, i.e. posições que oferecem uma enorme vantagem ao poder de combate de uma Força Naval, mas que não são exploradas pela MB.

Nos inquéritos, 69% dos CMG e 73% dos instrutores consideraram regular o nível da CapOpeMB relativo ao aproveitamento dos PIO da AA.

A. R. S. Selles (op. cit.) concorda com a perceção mostrada pelas pesquisas de que a CapOpeMB pode ser classificada como regular.

Com os dados e relatos apresentados, é inegável a perceção de que a CapOpeMB em defender o Brasil até 2040 está comprometida, tendo sido avaliada como regular. Há um bom sistema de monitoramento, o SisGAAz, a autonomia na construção de mísseis antissuperfície constitui-se em um fator de força (MD, 2020a, p. 55), mas a não exploração dos PIO da AA e a disponibilidade de poucos meios operativos, sobretudo navios escoltas, degradam a capacidade da MB em defender o Brasil.

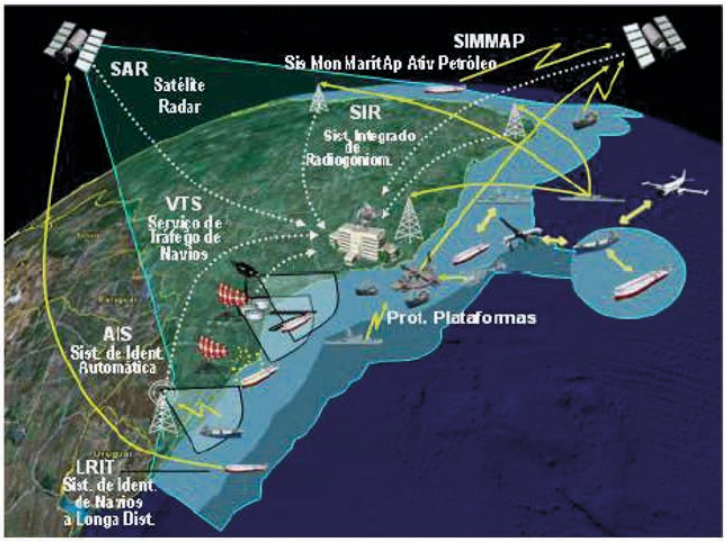

Figura 8 – SisGAAz
Fonte: Disponível em MB (2019).

4.5. A FORMA COMO A MB, POR MEIO DO PBC, PODE DEFENDER O BRASIL

O estratega, quando inicia o planeamento naval, sente o peso do pensamento militar no mais alto nível de decisão do Estado. Sobretudo, partindo de missões atribuídas à Marinha, sem quaisquer hipóteses de conflito (Caminha, 1983, p. 164).

Os OBEST passam a ser a referência para o planeamento militar. Nos inquéritos aplicados aos oficiais da MB, em ambos os grupos, comprovou-se que o binómio plataformas de petróleo/navios aliviadores são os alvos que merecem a maior prioridade de proteção por parte da MB. Entre os instrutores, 80% possuem este entendimento e entre os CMG, 73%. Isto é corroborado por Marroni e Da Silva (2015, p. 149) quando asseveram que mais de 80% da exploração do petróleo brasileiro estão *offshore*.

De entre as CND, destaca-se a capacidade de dissuasão, cujo propósito é desincentivar possíveis agressões. Destarte, conforme proposto por Caminha (1983, p. 168), as avaliações estratégicas são feitas para criar os vetores, *i.e.*, meios operativos e os pontos de apoio de um Poder Naval, i.e., PIO.

Pelo referido à QC – *De que forma a MB, por meio do PBC, pode manter uma capacidade operacional para defender o Brasil?*, construindo a resposta numa

sequência lógica de causa-consequência, primeiramente constatou-se que a capacidade almejada é a dissuasão e as operações navais a serem executadas têm como efeito desejado a garantia da soberania. Em seguida, dentre as variáveis do processo DOPEMAI do PBC, o material e a infraestrutura foram escolhidas por se coadunarem com a proposta de Caminha (1983) anteriormente mencionada. Os meios operativos são os indicadores do material e os PIO são da infraestrutura. Em ambos os casos, estes indicadores mostraram que a CapOpeMB em defender o Brasil até 2040 é regular.

Nesta lógica, para defender os OBEST, propõe-se que a Força Naval se concentre nas seguintes tarefas: defesa de ilhas oceânicas, garantia do uso de linhas de comunicação marítimas estratégicas e defesa das plataformas de petróleo.

Quanto à defesa das ilhas oceânicas e a garantia do uso de linhas de comunicação marítimas estratégicas, destaca-se a interação entre as ilhas e as LCM.

As LCM brasileiras são traçadas nas proximidades do continente e das ilhas pertencentes ao Brasil. A perda da soberania destas ilhas com uma subsequente ocupação por oponentes interferirá diretamente no tráfego marítimo e por sua vez na economia brasileira. O corolário disto é que não é aceitável a hipótese de perder a soberania sobre tais ilhas.

Ainda que, ao longo dos anos, as ilhas não tenham sido observadas pelos chefes de Estado como PIO para defesa do Brasil, sendo, até mesmo, transformadas em área de proteção ambiental, limitando as atividades militares, a MB não pode, sob qualquer circunstância, perder a ideia de que tais ilhas precisam ser transformadas em *hubs* logísticos. Locais, onde uma Força Naval possa realizar reparos e abastecimentos, que possuam aeródromos, com estruturas para manutenção de aeronaves e que sejam armadas com mísseis superfície-ar e superfície-superfície. Assim, propõe-se que sejam estudadas as possibilidades de implementar nas ilhas brasileiras: locais de atracação ou fundeio, aeródromos, hangares, tanques de combustível, depósitos de alimentos e sobressalentes, mísseis, radares e comunicação.

Quanto à defesa das plataformas de petróleo e dos navios aliviadores, os meios operativos são essenciais. A resposta da QD3 indicou que a composição NAe e Escoltas é a mais apropriada para esta tarefa. Entretanto, a resposta da QD4 indicou que o nível da CapOpeMB quanto aos meios operativos é regular. A base da resposta da QD4 foi a análise quantitativa feita por meio dos inquéritos e a qualitativa, em entrevista com o ComEsdE-2 e o CheOpE.

Reiterando a perceção do nível de capacidade operacional, o CM no seu discurso na Câmara dos Deputados enfatizou a sua intenção em retirar do serviço ativo, até 2028, os meios operativos obsoletos e com muitos anos de operação. Esta quantidade representaria cerca de 40% da Armada. Contudo, mencionou que há investimentos em execução, e.g.: a construção de submarinos e quatro fragatas no Brasil, o desenvolvimento e aprimoramento do SisGAAz e do míssil antissuperfície.

O SisGAAz e o míssil antissuperfície de tecnologia brasileira proveem boa vantagem de poder de combate. Propõe-se manter tais investimentos.

Relativamente aos meios operativos, a MB dispõe de um NAe, o Navio Aeródromo Multipropósito Atlântico, adquirido recentemente ao RU. Quanto à construção das fragatas, percebe-se que é imperiosa a incorporação de tais meios na MB. A maioria dos escoltas da MB está em operação desde a década de 1970. É notória a necessidade deste tipo de meio operativo para recompor a capacidade de dissuasão. Desta forma, entre a construção dos submarinos e das fragatas, propõe-se que estas últimas tenham prioridade.

As duas variáveis, *i.*e., material e infraestrutura, são dependentes de outra, a disponibilidade de recursos financeiros. Como a MB não possui o controlo desta variável, o CM tem apresentado veementemente as necessidades da Força. Assim, discursou na Câmara dos deputados:

> [...], é preciso, primeiro, que de facto vinculemos o orçamento da Defesa ao Produto Interno Bruto. Hoje, 1%. Vamos estudar a possibilidade de, gradualmente, elevar isso, de modo que se possibilite o investimento, o reaparelhamento da força e a obtenção de capacidade operacional plena. (Olsen, 2023)

Caso as petições do CM sejam atendidas pelos políticos, propõe-se a aquisição imediata de escoltas de oportunidade de marinhas mais desenvolvidas.

5. CONCLUSÃO

A CF é taxativa ao atribuir a defesa da Pátria como a primeira tarefa das FFAA. A END define que o Atlântico Sul é uma área de interesse geoestratégico para o Brasil, sendo a dissuasão a primeira postura estratégica considerada na defesa dos interesses nacionais. A exploração da AA e a utilização das LCM do Atlântico Sul continuarão a ser vitais para o desenvolvimento do Brasil e, no caso de agressão externa, o País empregará o Poder Nacional, com ênfase na sua expressão militar, na defesa dos seus interesses.

Seguindo os preceitos supracitados, esta investigação teve como *OG propor a forma como a MB, por meio do PBC, pode defender o Brasil*. Foi delimitada nos domínios: temporal, entre 2023 e 2040; espacial, AA; de conteúdo, ao emprego da MB na garantia da soberania, ancorado no PBC.

Neste enquadramento, este estudo teve como meta a resposta da QC – *De que forma a MB, por meio do PBC, pode manter uma capacidade operacional para defender o Brasil?* e quatro QD correlacionadas, que auxiliaram na construção de uma linha de pensamento que consolida a resposta da QC.

Relativamente ao procedimento metodológico, a estratégia de investigação seguiu uma metodologia de raciocínio hipotético-dedutivo, vinculada a uma estratégia de investigação mista, sendo o desenho de pesquisa um estudo de caso. A recolha de dados transcorreu por meio de análise documental de documentos estratégicos brasileiros, dos EUA, do RU, de Espanha e da NATO, Doutrina das Operações Conjuntas do Brasil, manuais táticos do exército dos EUA, conceitos estratégicos e geopolíticos de autores consagrados, artigos de revistas especializadas e notícias de jornais conceituados. Complementou-se com dois inquéritos, cujo público-alvo é especializado no conteúdo proposto e com duas entrevistas semiestruturadas feitas com o CheOpE e o ComEsqdE-2.

Com relação ao público-alvo, os inquéritos foram enviados a 86 oficiais, sendo 23 instrutores da EGN e 63 CMG. Houve a resposta de 15 instrutores e 42 CMG, perfazendo 66% dos inqueridos.

Estruturalmente, esta investigação foi concebida em cinco secções. Apresentou-se o enquadramento conceptual, a descrição do modelo de análise e a metodologia utilizada. Por fim, apresentam-se e propõem-se os resultados alcançados.

Quanto ao OE1, *Identificar as possibilidades de emprego de Forças Navais em cenários de crises ou conflitos até 2040*, em resposta à QD1, constatou-se que o cenário com grande possibilidade de crise ou conflito com o emprego de Forças Navais é o MSC em que há conflitos de interesse entre a RPC e as potências ocidentais. Associado ao cenário em estudo, averiguou-se que a estratégia empregue pela RPC é a A2AD, cuja característica é a defesa. Havendo, portanto, semelhanças com a estratégia proposta pela MB no que se refere à AA.

Referente ao OE2, *Identificar as linhas de defesa do Brasil,* procurando a resposta da QD2, foi apresentada a hipótese de a MB ser a PLDB, através de duas analogias: uma referente à ideia de atribuir às fronteiras francesas o formato

de hexágono e outra, aos EUA, quanto ao conceito de IM. Ao se definir que as fronteiras brasileiras se assemelham a um triângulo, pôde constatar-se que é um Estado naturalmente protegido como uma ilha, e devido à sua grandiosa área seria uma ilha do mundo. Os lados norte e oeste são protegidos pela selva e cordilheira respetivamente, enquanto o lado leste, pelo Atlântico. Destarte, em sendo a característica dos oceanos unir os povos por meio da navegação, este lado torna-se o mais suscetível às agressões de atores Estatais. Esta linha de pensamento indicou que a PLDB é a MB, seguida da FAB e do EB.

No que concerne ao OE3, *Estimar os meios operativos para combater as ameaças vislumbradas no Plano Estratégico da Marinha (PEM) 2040*, concluiu-se que a composição NAe e Escoltas é a mais apropriada para se contrapor às ameaças Estatais, sendo os Escoltas, pela flexibilidade que demonstram, os meios mais presentes nas Operações no Mar. Percebeu-se que, excetuando-se os conflitos urbanos e as ameaças cibernéticas, i.e. ameaças desvinculadas da AA, o tipo de meio operativo a ser empregue contra as ameaças listadas no PEM2040 é o Navio Escolta.

Relativamente ao OE4, *Identificar a capacidade operacional da MB em defender o Brasil até 2040*, considerando que a ameaça adviria de outro Estado, foi feita uma análise das VC associadas aos OBEST a serem protegidas. Definindo-se as VC, a composição dos meios operativos mais apropriada para se contrapor às ameaças de atores Estatais e a condição dos meios operativos e das infraestruturas da MB até 2040, constatou-se que o atual nível de CapOpeMB é regular.

Em face do exposto, no tocante ao OG, *Propor a forma como a MB, por meio do PBC,* pode defender o Brasil, foram feitas as seguintes propostas: definir que as tarefas de defesa de ilhas oceânicas, garantia do uso de linhas de comunicação marítimas estratégicas e defesa das plataformas de petróleo sejam o foco da MB; manter os investimentos no SisGAAz e no míssil antissuperfície; quanto aos meios em construção no Brasil, que seja atribuída prioridade às fragatas; e, caso haja aporte de mais recursos financeiros por parte do governo, que sejam adquiridos Escoltas de oportunidade. As propostas em estudo elevaríam o nível da CapOpeMB. Por ter sido validada a hipótese de que a MB é a PLDB, a adoção das propostas configuraria uma boa gestão estratégica para sanar a problemática apresentada: *O decréscimo da capacidade operacional na defesa do Brasil*.

As limitações à investigação foram: o grau de sigilo dos dados obtidos, sendo todo conteúdo estudado de domínio público; e a ausência de estudos científicos no

mesmo viés. Avalia-se que estas limitações não comprometeram a consistência das análises e das propostas.

Para *estudos futuros,* sugere-se abordar temas relacionados com a manutenção dos meios operativos, como a criação de um Instituto Militar Naval de Engenharia para acumular um corpo de conhecimento técnico e aproximar os engenheiros navais das atividades operativas; a avaliação de ferramentas que mantenham o *savoir-faire* das atividades operativas no mar para as futuras gerações de oficiais da armada, *i.e.*, capacitação de pessoal; e o atual potencial da Guerra de Minas para negar o uso do mar.

REFERÊNCIAS BIBLIOGRÁFICAS

Aron, R. (1962). *Paix et Guerre entre les nations,* Paris: Calmann-Levy.

Beaufre, A. (2012). *Introduction à la stratégie*. Paris: Pluriel.

Brustlein, C. (2019). Five Myths About the Anti-Access/Area Denial Threat. *Revue Défense Nationale*. 85-90. https://www.defnat.com/pdf/cahiers/Le%20Bourget%20EN.pdf

Cadotte, J. (2023, 18 de agosto). *Alaska News Source - USS Ted Stevens will be 'most powerful' warship in the world*. https://www.alaskasnewssource.com/2023/08/18/uss-ted-stevens-will-be-most-powerful-warship-world/

Caiafa, R. (2023, 16 de maio). Marinha do Brasil vai desmantelar 40% de suas instalações até 2028. Infodefensa.com. https://www.infodefensa.com/texto-diario/mostrar/4291806/marinha-do-brasil-devera-desativar-40-seus-meios-ate-2028

Caminha, J. C. G. (1983). Delineamentos da Estratégia, 3v. Rio de Janeiro: Biblioteca do Exército.

Centro Conjunto de Desarrollo de Conceptos. (2022). *Entorno Operativo 2035* (1ª revisão). Madrid: Autor.

Corrêa Silva, R., Pessôa, L. A. M., & Costa, H. G. (2022). Seleção de Navios para parcela de uma Força Expedicionária Anfíbia. *Passadiço* (42ª Ed.), 78-82. https://www.marinha.mil.br/caaml/?q=revista-passadico

Da Silva, A. P. (2013). Os princípios das relações internacionais e os 25 anos da Constituição Federal, *Revista de Informação Legislativa, 200,* 15-32. https://www12.senado.leg.br/ril/edicoes/50/200/ril_v50_n200.pdf

De Melo, R. (2015). Indústria de defesa e desenvolvimento estratégico: estudo comparado França-Brasil. Brasília: Fundação Alexandre de Gusmão [FUNAG].

Department of Defense. (2021). *DoD Strategic Management Plan Fiscal Years 2022-2023*. Washington, D.C.: Autor.

Development, Concepts and Doctrine Centre. (2015). *Future Operating Environment 2035*. Swindon: Autor.

Godoy, M. (2023, 30 de outubro). Comandante da Marinha alerta: Força vai aposentar navios e corte de verba ameaça a segurança do País. Estadão. https://www.estadao.com.br/politica/marcelo-godoy/comandante-da-marinha-alerta-forca-esta-em-crise-e-corte-de-verba-ameaca-a-seguranca-do-brasil/

Hughes Jr., W.P. (1999). *Fleet Tactics and Coastal Combat* (2ª Ed.). Annapolis: Naval Institute Press.

Kimmage, M., & Notte, H. (2023). *The Age of Great-Power Distraction: What Crises in the Middle East and Elsewhere Reveal About the Global Order*. *Foreign Affairs*. https://www.foreignaffairs.com/middle-east/age-great-power-distraction-kimmage-notte

Lei no 9.985/2000, de 18 de julho (2000). *Regulamenta o art. 225, § 1o, incisos I, II, III e VII da Constituição Federal, institui o Sistema Nacional de Unidades de Conservação da Natureza e dá outras providências*. Diário Oficial da União de 19/07/2000, p. 1, col. 1. Brasília: Presidência da República. http://www.planalto.gov.br/ccivil_03/leis/l9985.htm

Louis, F. (2014). Les grands théoriciens de la géopolitique. Paris: Puf.

Marinha do Brasil. (2011). *EMA-134: Manual de Gestão Administrativa da Marinha*. Brasília: Estado Maior da Armada.

Marinha do Brasil. (2020). *EMA-300: Plano Estratégico da Marinha*. Brasília. https://www.marinha.mil.br/pem2040

Marinha do Brasil. (2019). *Política Naval*. Brasília. https://www.marinha.mil.br/politicanaval

Marinha do Brasil. (s.d.). *SisGAAz: proteção e monitoramento das águas jurisdicionais brasileiras* [Online]. https://www.marinha.mil.br/sisgaaz-protecao-e-monitoramento-das-aguas-jurisdicionais-brasileiras

Marroni, E. V. & Da Silva, A. L. R. (2015). Geopolítica do Brasil para o Atlântico Sul: uma revisão de literatura a partir da política pública nacional para o mar. *Revista de Escola de Guerra Naval, periódico especializado em estudos estratégicos, 21*(2), 147-179. https://www.portaldeperiodicos.marinha.mil.br/index.php/revistadaegn/issue/view/693/105

Mesquita J. L. (2021, 15 de fevereiro). Guerra da lagosta, a guerra que não houve. *Estadão*. https://marsemfim.com.br/guerra-da-lagosta-a-guerra-que-nao-houve/

Ministério da Defesa. (2018). 1º SEGAD - Seminário de Gestão e Aquisição de Defesa [Online]. https://www.gov.br/esg/pt-br/composicao/estudos-estrategicos/eventos/1o-segad-seminario-de-gestao-e-aquisicao-de-defesa

Ministério da Defesa. (2015). MD35-G-01: Glossário das Forças Armadas (5ª Ed.). Brasília: Autor. https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf/view

Ministério da Defesa. (2020a). MD30-M-01: Doutrina de Operações Conjuntas (2ª Ed.), 2. Brasília: Autor. https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md30-m-01-vol-2-2a-edicao-2020-dou-178-de-15-set.pdf

Ministério da Defesa. (2020b). *Política Nacional de Defesa e Estratégia Nacional de Defesa*. Brasília: Poder Executivo. https://www.gov.br/defesa/ptbr/ assuntos/copy_of_estado-e-defesa/pnd_end_congresso.pdf

Ministério do Desenvolvimento, Indústria, Comércio e Serviços. (2023). Comércio Exterior. http://comexstat.mdic.gov.br/pt/comex-vis

NATO. (2022). *NATO 2022 Strategic Concept*. Bruxelas: Autor.

Neves, A. N., Nishio J. L. S., Farias Jr., J. L. F., & Franchi T. (2021, 06 de dezembro). Planejamento baseado em capacidades nos documentos de defesa brasileiros. *Hoplos Revista de Estudos Estratégicos e Relações Internacionais, 5*(9), pp.48-69. https://periodicos.uff.br/hoplos/issue/view/2552/673

Olsen, M. S. (2023, maio). Rumos, estratégias, prioridades e desafios da Defesa Nacional. Em: Comissão de Relações Exteriores e de Defesa Nacional. 1ª Sessão Legislativa Ordinária da 57ª Legislatura. Sessão Legislativa organizada pela Câmara dos Deputados, Brasília. https://escriba.camara.leg.br/escriba-servicosweb/html/67595

République Française. (2019). *Que signifie la notion de système international?* [Online]. https://www.vie-publique.fr/fiches/269786-systeme-international-du-modele-westphalien-nos-jours

Robic, M. C. (1989). Sur les formes de l'Hexagone. *Mappemonde, 4*, 18-23. http://www.mgm.fr/PUB/Mappemonde/M489/p18-23.pdf

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

Smith, A. Recherches sur la nature et les causes de la richesse des nations. (G. Garnier, Trad.) Paris.

Soller, M. (2022, 03 de janeiro). Brève histoire de stratégie navale 1/2 – De l'Antiquité aux mondes contemporains. *Conflits*. https://www.revueconflits.com/breve-histoire-de-strategie-navale-1-2-de-lantiquite-aux-mondes-contemporains/

Souza Jr., J.C. (2022). *A atuação da Marinha do Brasil no apoio ao combate de atividades ilícitas no Golfo da Guiné* (TII do CPOG). Instituto Universitário Militar, Lisboa.

US Army. (2020). ATP 3-90.98: *Jungle Operations*. Washington, D.C.: Autor.

US Army. (2000). FM 3-97.6 (90-6): *Mountains Operations*. Washington, D.C.: Autor.

Valladão, A. (2014, 02 de abril). Brésil – une défense sans menaces. *Note nº 04/2014 de la Fondation pour la recherche stratégique*. https://www.frstrategie.org/publications/notes/bresil-une-defense-sans-menaces-2014

Wiltgen, G. (2023, 10 de novembro). Entrevista com o Comandante em Chefe da Esquadra, Vice-Almirante Edgar Luiz Siqueira Barbosa. Defesa Aérea & Naval. https://www.defesaaereanaval.com.br/naval/entrevista-com-o-comandante-em-chefe-da-esquadra-vice-almirante-edgar-luiz-siqueira-barbosa

Zajec, O. (2016). *Introduction à l'analyse géopolitique: histoire, outils, méthodes*. Monaco: Du Rocher.

ESTUDO 2 – CONTRIBUTOS PARA O *DIGITAL BACKBONE* DA MARINHA PORTUGUESA[6]

CONTRIBUTIONS TO THE PORTUGUESE NAVY'S DIGITAL BACKBONE

Paulo Jorge Gonçalves Simões
Capitão-de-mar-e-guerra

José Manuel dos Santos Coelho
Comodoro

RESUMO

As Forças Armadas portuguesas (FFAA) necessitam rapidamente de se adaptar ao contexto tecnológico atual e de alinhar o desenvolvimento digital com os Aliados e com a *North Atlantic Treaty Organization* (NATO). Este estudo visa identificar contributos para o *Digital Backbone* da Marinha Portuguesa, por forma a garantir a interoperabilidade e a condução de *Multi-Domain Operations* com as FFAA, os Aliados e a NATO. Para desenvolver esta investigação adotou-se uma metodologia assente num processo de raciocínio indutivo, recorrendo a uma estratégia qualitativa, baseada num estudo de caso. O estudo identifica diversos desafios a superar como a exiguidade de recursos humanos e de competências digitais, a fragmentação da governação digital e a necessidade de investimento em infraestrutura tecnológica e em novas tecnologias. Analisa as estratégias da NATO e dos aliados, o modelo de segurança *Zero Trust* e a necessidade de transformar as FFAA numa organização orientada a dados. Do conjunto de contributos propostos destaca-se a aposta numa atuação conjunta das FFAA, o desenvolvimento de ecossistemas temáticos e de estratégias digitais, a melhoria da segurança digital e a adoção de práticas de governação robustas.

Palavras-chave: *data-driven*, *digital backbone*, governação, Marinha, transformação digital, *zero trust*

[6] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Promoção a Oficial General (CPOG 2023/2024). A versão integral encontra-se disponível no Centro de Recursos do Conhecimento do IUM.

ABSTRACT

The Portuguese Armed Forces (FFAA) urgently need to adapt to the current technological context and align their digital development with the Allies and the North Atlantic Treaty Organization (NATO). This study aims to identify contributions to the Digital Backbone of the Portuguese Navy to ensure interoperability and the conduct of Multi-Domain Operations within the scope of the FFAA, Allies, and NATO. To carry out this research, a methodology based on inductive reasoning was adopted, using a qualitative approach based on a case study. The study identifies several challenges to overcome, such as the scarcity of human resources and digital skills, fragmentation of digital governance, and the need for investment in technological infrastructure and new technologies. It analyses the Zero Trust security model, which is crucial in an era of increasing cyber threats and emphasizes the need to transform the FFAA into data-driven organizations. From the set of proposed contributions, the commitment for FFAA to act jointly, the development of thematic ecosystems and digital strategies, the improvement of digital security and the adoption of robust governance practices stand out.

***Keywords**: data-driven, digital backbone, governance, navy, digital transformation, zero trust*

1. INTRODUÇÃO

A transformação digital (TD) das organizações é um tema na ordem do dia. Segundo a McKinsey[7] (2020), nos seus processos de TD a maioria das organizações procura implantar rapidamente soluções tecnológicas, cometendo o erro de não alterar os processos, a cultura e a formação dos seus colaboradores. Refere ainda a necessidade da existência de um *Digital Backbone*[8] (DB) atualizado, flexível e suficientemente resiliente para suportar os requisitos da tecnologia em acelerada evolução.

A *North Atlantic Treaty Organization* (NATO) está em processo de edificação do seu DB, para permitir a realização de *Multi-Domain Operations* (MDO), assegurando a interoperabilidade a todos os níveis, na Organização e entre os aliados, de forma a melhorar o conhecimento situacional e a facilitar a tomada de decisão mais ampla e rápida (*Consultation, Command and Control Board* [C3B], 2022).

---

[7] A McKinsey & Company é uma empresa de consultoria empresarial americana que aconselha empresas, governos e outras organizações em consultoria estratégica (www.mckinsey.com).

[8] Combinação de pessoas, processos, dados e tecnologia permitindo uma ligação em tempo real, resiliente entre sensores e plataformas multi-domínio, incluindo através de decisores relevantes (McKinsey, 2020).

As Marinhas aliadas têm emanado diversas estratégias para a sua TD, analisadas pelo CMG Dias Correia (2023). Pretendendo-se dar continuidade à investigação de Correia (2023, pp. 35 a 41), este estudo tem como objeto de estudo a identificação de contributos para o DB da Marinha Portuguesa (MP), contextualizados na realidade digital, interna e externa, sendo necessário limitar no tempo, no espaço e no conteúdo (Santos & Lima, 2019, p. 42). Em termos temporais, a análise a realizar baseia-se no período de novembro de 2023 a 20 de março de 2024, de modo a permitir, em tempo, a conclusão do presente estudo.

Atendendo ao foco dos contributos, no domínio do espaço a investigação desenvolve-se em Portugal, no âmbito da MP, embora se analise a situação das Forças Armadas Portuguesas (FFAA) e se considere os trabalhos em curso na NATO e em organizações civis. Ao nível do conteúdo, restringe-se a investigação à identificação de contributos para um DB da MP, enquadrados nas FFAA, e recorrendo à NATO, aos aliados e a organizações civis.

Tendo em atenção que "a formulação do problema consiste em apresentar de forma explícita, clara, compreensível e operacional a dificuldade que identificamos e que pretendemos resolver" (Santos & Lima, 2019, p. 50), apresenta-se o seguinte problema de investigação: ainda que produza grande quantidade de dados, a MP é uma organização pouco *data-driven* e digitalizada, necessitando de acompanhar a TD dos aliados e das organizações onde se insere, de modo a evoluir no domínio digital.

Assim, o objetivo geral (OG) deste estudo é o de formular contributos para o DB da Marinha Portuguesa, pelo que é definida a seguinte questão central (QC): "Quais os contributos para o *Digital Backbone* da Marinha Portuguesa?". A partir do OG deduziram-se como objetivos específicos (OE): analisar a situação da MP com vista à implementação do *Digital Backbone* e analisar as caraterísticas do DB de organizações externas.

Para descrever a investigação realizada, organizou-se este estudo em seis capítulos. O primeiro apresenta o tema da investigação, o objeto de estudo, os objetivos e as questões de base da investigação. O segundo faz um enquadramento teórico e conceptual da problemática do DB, do *Zero Trust* (ZT) e de organizações orientadas por dados (*data-driven*). O terceiro apresenta a metodologia e o método seguido na investigação. O quarto apresenta os dados adquiridos e processados. O quinto apresenta os resultados, materializando uma proposta de contributos a implementar, e o sexto apresenta as conclusões do trabalho sintetizando os resultados obtidos.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Neste capítulo são apresentados o contexto e as bases conceptuais para a identificação de contributos para o DB da MP.

2.1. Transformação Digital

Na vasta literatura existente não existe uma clara definição de TD, conforme também refere Correia (2023, p. 5). Segundo Tonder (2020), "*there is no universally accepted, robust conceptual framework that can assist businesses and academics to understand the constructs of digital transformation and business model innovation*".

A NATO, na estratégia para a implementação da TD, refere as dimensões **pessoas, processos** e **tecnologia** que, combinando efeitos de modernização, otimização e transformação, incluindo Tecnologias Emergentes e Disruptivas (TED), permitirão atingir os objetivos pretendidos com a TD onde sobressai a condução de MDO (C3Ba, 2023). O *United Kingdom Ministry of Defence* (UK MoD), para além das dimensões referidas, acrescenta a dimensão **dados** ao processo transformacional, em particular para a implementação do DB da Defesa (UK MoD, 2021).

Mais recentemente, a NATO considera que esta última dimensão é um ecossistema de dados, onde os atores interagem e colaboram para encontrar, arquivar, publicar, consumir ou reutilizar dados, bem como promover a inovação e criar valor (NATO CIO, 2023, p. 7).

A MP, na sua Diretiva de Redes, Sistemas de Informação e Transformação Digital (DIRESITD), contempla uma quinta dimensão, a **cultura**, por considerar que terá de a mudar para acomodar a TD pretendida (EMA, 2023). Face à necessidade de efetuar a TD, a diretiva tem subjacente a transformação organizacional de pessoas (estruturas, formação, competências), processos (fluxos de trabalho, rotinas, procedimentos) e cultura (mudança organizacional), de modo que, com recurso à tecnologia (infraestrutura, aplicações) e delimitada no tempo (2026), se acrescente valor (Chefe da Divisão de Redes e Sistemas de Informação [CHDIVREDSI], entrevista presencial, 21 de novembro de 2023). Por outro lado, através da diretiva das TED, a MP identifica a robotização e sistemas autónomos, o *Big Data* e a Inteligência Artificial (IA), sendo estes os pilares prioritários para a transformação no contexto alargado das FFAA (EMAa, 2024).

Importa referir que, no âmbito da investigação de Correia, as FFAA encontram-se num grau de maturidade digital inicial, onde os processos, as perícias e a governação digital são as componentes mais deficitárias (2023, p. 30).

Posto isto, os *Digital Leaders*[9] mencionados por Correia (2023, p. 15) estão na fase de implementação das suas estratégias. Da análise destas estratégias identificam-se, nas referidas cinco dimensões, descritores[10] associados à TD pretendida, definindo o ecossistema[11] que carateriza o DB de uma organização. Neste particular, as tecnologias digitais, em constante desenvolvimento e evolução, são geralmente associadas aos termos SMAC - *Social media, Mobile, Analytics/Big Data, Cloud* - e BRAIDA - *Blockchain, Robotics, Automation of knowledge work/artificial intelligence, Internet of things, Digitisation or Digital fabrication* (3D) e *Augmented Reality (*...) ou ainda outras como a quantum computing, o metaverse e arquiteturas seguras (p.e. ZT) (Willcocks, Hindle, Stanton & Smith, 2024, pp. 119 a 130).

Refira-se ainda que a NATO tem elaborado estratégias, planos de ação e outra documentação em diversas áreas, desde a própria TD, a ciber, o recurso pessoas, a IA, os dados e a implementação de TED, por considerar ser obrigatória a coerência e o alinhamento nesta documentação (CIO NATO, 2023). A necessidade está também patente nos *digital leaders* tendo os EUA, p.e., alinhado nove[12] diferentes estratégias (US DoD, 2022, p. 4).

Segundo Correia (2023, p. 39), "Portugal tem uma estratégia para a TD da Administração Pública, um plano de ação e estratégias setoriais nomeadamente para os dados, *Cloud*, IA, *blockchain*, computação avançada e cibersegurança".

No caso das FFAA não existe qualquer documento estratégico, incluindo para a TD (Correia, 2023, p. 26), com paridade relativamente às identificadas nos aliados e na NATO, apesar de existirem diretivas setoriais no Estado-Maior-General das Forças Armadas (EMGFA) (C. Algarvio, entrevista presencial, 20 de março de 2024) e Ramos que apontam para iniciativas neste âmbito (Correia, 2023, p. 30). No caso dos outros Ramos, para além das respetivas Diretivas Estratégicas, foram identificados no Exército Português o conceito inicial para o desenvolvimento da Robótica e Sistemas Autónomos (Exército, 2023) e a Diretiva para a Investigação, desenvolvimento e Inovação no Exército (Chefe do Estado-Maior do Exército, 2024). No caso da Força

---

[9] Canadá, França, Noruega, Espanha, Estados Unidos da América (EUA), Finlândia e Reino Unido.
[10] Entende-se como descritores, sistemas, ferramentas, processos que os aliados consideram como essenciais para a concretização da TD das suas organizações.
[11] O UK MoD refere que o DB *will be an ecosystem – a combination of people, process, data and technology; it will enable friction-free access to our data, connecting sensors in one domain to platforms in other domains, via decisionmakers at the relevant levels in real time* (2021, p. 14).
[12] Inclui ainda a infraestrutura tecnológica, a modernização C3, a estratégia *Zero Trust* e a estratégia *Cloud*.

Aérea Portuguesa (FAP), releve-se a criação da Divisão de Inovação e Transformação Organizacional (Chefe do Estado-Maior da Força Aérea, 2023).

2.1.1. O *Digital Backbone*

Atualmente, as tecnologias digitais apresentam constantemente novas funcionalidades, que ficam disponíveis para utilização de forma acelerada, dificultando ainda mais a adaptação a um ambiente em constante mudança (Avedillo et al., 2015). Para além de infraestruturas tecnológicas pouco adequadas, a existência de novas tecnologias digitais exige uma capacidade de resposta para a qual essas infraestruturas não estão preparadas (Delmond et al., 2016). Assim, a adaptação da infraestrutura tecnológica por parte das organizações será a base para acomodar a TD em curso (Gampfer, 2018), de modo a manterem-se competitivas (Ross et al., 2016). Portanto, o desafio será a integração de novas tecnologias nas infraestruturas tecnológicas das organizações (Andersson et al., 2012), por forma a melhorar a experiência dos utilizadores ao considerar a centralidade destes (CIO NATO, 2023), sendo necessário transformar essas infraestruturas, quer com a modernização dos sistemas *legacy*[13], quer tornando-as mais flexíveis para acomodar rapidamente novas e inovadoras tecnologias digitais (Furr & Shipilov, 2019).

O termo DB foi introduzido por Ross et al. (2016), tendo-o definido como todos os sistemas de tecnologias de informação e comunicação (TIC) utilizados para uma inovação rápida, essenciais para capturar as inovações digitais, eque garantam uma célere adaptação às mudanças do ambiente tecnológico externo. Paralelamente, definiu o termo de *Operational Backbone* (OB) que incluía os sistemas TI necessários para a manutenção do negócio.

Segundo Löffler (2020, p. 6), existem três princípios fundamentais para a implementação de um OB: o envolver todos os departamentos da organização, deixando a forma de funcionamento em silos, com empenhamento elevado do topo da organização; avaliar continuamente os processos implementados, incluso o uso da tecnologia; incrementar a implementação de serviços partilhados, automatizados e virtualizados de modo a melhorar a eficiência dos colaboradores. A mesma autora refere que o OB é desenvolvido para garantir a confiabilidade

[13] Os sistemas *legacy* (legados) são baseados em tecnologias ultrapassadas, ainda úteis para as operações. Substituí-los por novas tecnologias é um desafio na área dos sistemas de informação (SI). (Gartner, 2023).

e a eficiência, não oferecendo a velocidade e a flexibilidade que as organizações necessitam para a introdução de rápidas inovações digitais (2020, p. 7).

Assim, segundo ela, inúmeras organizações definem um segundo Backbone, o DB, englobando um conjunto de capacidades organizacionais e tecnológicas que permitem não só o rápido desenvolvimento e implementação de inovações digitais, como também não comprometem a confiabilidade do próprio OB (2020, p. 8). Refere ainda que as caraterísticas tecnológicas do DB incluem repositórios de enormes quantidades de dados e ferramentas de análise, serviços modulares (IaaS[14], PaaS[15], SaaS[16]) e equipas flexíveis e ágeis.

Importa ainda referir que para ambos os *backbones* serão necessários diferentes colaboradores, sendo que, este último, exigirá colaboradores com competências digitais inovadoras e diferenciadas, mentalidades e procedimentos ágeis, e uma cultura organizacional de inovação bastante robusta (Andersson, et al., 2012).

Os países aliados encontram-se em diferentes estágios de conceptualização e desenvolvimento da sua TD, e consequentemente de um DB (C3Ba, 2023). Para o UK MoD (2021), o DB será um ecossistema que resulta da combinação de pessoas, processos, dados e tecnologia, que explorará os dados e as TED, e incrementará a colaboração funcional multidomínio com os parceiros civis e militares.

Refere ainda que conectará sensores (*sensors*), sistemas de resposta (*effectors*) e decisores (*deciders*), políticos e militares, garantindo a integração no domínio das operações.

Para a NATO, os elementos-chave do DB incluem redes federadas, computação na nuvem e arquitetura orientada a serviços, pois o DB será "*A federation of networks and systems that provides the technical means for a resilient, scalable, and secure digital service continuum including cloud and edge services*" (NATO's DTIS, 2023). Considera também que um DB deve incorporar de raiz requisitos de segurança da informação e da infraestrutura tecnológica, sendo necessário criar um nível de segurança abrangente e adaptável que proteja dados críticos e mitigue riscos, garantindo uma postura robusta e resiliente num cenário digital cada vez mais complexo (CIO NATO, 2023, p. 12). Assim, a segurança

[14] *Infrastructure as a Service* – acesso a recursos básicos de computação, como servidores e rede.
[15] *Platform as a Service* - permite que os utilizadores acedam a uma variedade de recursos tecnológicos sem a necessidade de implementar e manter sistemas operacionais.
[16] *Software as a Service* - permite que os utilizadores acedam a aplicações prontas para usar.

merecerá atenção pois, como refere o Contra-almirante Gameiro Marques, "não há desenvolvimento sustentado sem segurança, pelo que, se a TD pretende fazer isso através do digital, então tem que haver segurança digital" (2023, cit. por Correia, 2023, p. 16).

2.1.2. O *Zero Trust*

O modelo de rede perimetral[17], que muitas organizações ainda utilizam, protege itens sensíveis através da construção de linhas de defesa que um intruso deve penetrar antes de obter acesso a dados e informação. Contudo, esta abordagem já não é suficiente para garantir a segurança em redes de computadores (Razi Rais, 2023).

O conceito ZT surgiu pela primeira vez em 1994, numa tese de doutoramento intitulada "*Formalizing Trust as a Computational Concept*", de Stephen Paul Marsh, na Universidade de Stirling, nos Estados-Unidos da América, o qual foi continuamente desenvolvido até ao *Jericho Forum,* em 2003, o qual procurou readequar a arquitetura de rede face às evidências de que a maioria dos ataques eram originados dentro da rede (Green-Ortiz et al., 2023).

Em 2009, a consultora Forrester (2023) desenvolveu uma alternativa aos modelos de segurança estáticos, para se focar em políticas de verificação contínua baseada em análise de risco dos utilizadores e dos respetivos dispositivos associados, que denominou de ZT. Em 2014, a Google apresentou uma nova abordagem de segurança corporativa, denominada *BeyondCorp*, ao mover o controlo de acesso do perímetro da rede para os utilizadores (2023). Em 2017, a Gartner introduziu um novo modelo de segurança denominado de *Continuous Adaptive Risk* and Trust Assessment, onde a segurança é adaptável à necessidade de acesso a dados e informação, e monitorizada constantemente, não sendo a gestão do risco da responsabilidade de uma única entidade (Panetta, 2017).

Mais recentemente, o *National Institute of Standards and Technology* (NIST) apresentou normas para a criação de arquiteturas ZT, que se focam na proteção de recursos (sistemas, serviços, processos, contas de rede, etc.), e não segmentos de rede, pois o local da rede deixa de ser a principal componente da segurança do recurso (Scott Rose, 2020).

A NATO desenvolveu uma política de ZT, a qual exigirá mudanças ao nível

[17] Engloba todas as medidas de segurança aplicadas na "periferia" da rede, como *proxies*, *firewalls*, etc.

das pessoas (cultura), dos processos e da tecnologia. Assenta em cinco recursos (utilizadores, dispositivos/sistemas, redes de comunicações, *software* e dados) e três processos (*Visibility & Analytics* - monitorização e análise de eventos, *Orchestration & Automation* – decisão e resposta, *federation* - partilha e interoperabilidade) (NATO Zero Trust Policy, 2023).

Os princípios a que este modelo está associado são os seguintes: assumir que o ambiente pode estar comprometido, acedendo apenas ao essencial; nunca confiar, verificar sempre a ação dos recursos; verificar explicitamente e continuamente todos os acessos; decisões de segurança probabilísticas e explicáveis, baseadas em métricas.

Razi Rais (2023) refere que uma rede ZT é construída com os seguintes pressupostos: a rede é sempre considerada hostil e nela existem ameaças externas e internas; a origem da rede não é suficiente para decidir o nível de confiança; cada dispositivo, utilizador e fluxo de rede é autenticado e autorizado.

O *United States Department of Defense* (US DoD) tem já trabalho desenvolvido nesta área, incluindo o estabelecimento de uma estratégia/plano para a sua implementação, de onde se retira a figura 4 com tarefas a executar (US DoD, 2022).

Apresentado pela *Cybersecurity & Infrastructure Security Agency* (CISA) norte-americana (2023), nesta investigação utilizou-se o modelo de maturidade de ZT, utilizado pelo US DoD por ser aplicável a qualquer organização, sendo empregue no levantamento do nível de segurança digital existente nas FFAA no geral, e na MP em particular.

2.1.3. A organização *data-driven*

Organizações com sistemas legados obsoletos enfrentam desafios na consolidação de dados de diferentes fontes (Huntington & Schrey, 2020). Como as soluções baseadas em análise, IA e a *Internet of Things* (IoT) dependem do acesso irrestrito a dados para gerar informações, uma inadequada espinha dorsal limitará o impacto destas tecnologias (*op cit.*).

Segundo Rashedi (2023), a quantidade de dados disponíveis cresce diariamente e com ela as oportunidades para as organizações gerarem vantagens competitivas, sendo que, a tomada de decisão é caraterizada não só por ter mais parâmetros a considerar, mas também pelo incremento da rapidez com que é tomada. Uma organização orientada por dados (*data-driven*) assenta na construção de ferramentas, competências e, o mais importante, numa cultura que atua sobre

dados (Anderson, 2015), o que é confirmado pelo *Canadian Department of Defense* (CAN DoD), ao referir que uma organização deste tipo terá de efetuar uma alteração cultural significativa (CAN DoD, 2019, p. 20).

Contudo, o termo não colhe total concordância, pois como refere Berkun (2013) "*no team or organization is truly data-driven. Data is not conscious: it is merely a list of inert, dead numbers. Data doesn't have a brain and therefore can't drive or lead anything*". Acrescenta que as organizações querem ser "*data-influenced, where decision makers have good data available that they can use to help answer good questions about what they're doing, how well it's being done and what perhaps they should be doing in the future*". (Berkun, 2013)

Já Knapp (2006) prefere o termo *data-informed*, ao considerar que o termo alarga o âmbito, pois os dados podem ajudar a levantar questões e a informar o que acontece na organização, através de indicadores de desempenho, relatórios e alertas. No presente estudo será mantido o termo *data-driven* por ser o mais difundido[18], como também recomenda Anderson (2015), sendo que o pretendido reflete os três termos.

Para Rashedi (2023) uma organização orientada por dados faz uso dos existentes e da analítica para melhorar as decisões, sendo caraterizada por atributos como a importância, o tipo e âmbito dos dados utilizados, por análises efetuadas com recurso a IA ou *business intelligence*, e pela aptidão de formular recomendações a partir de análises, e ações a partir de recomendações. O modelo de Eckerson (2012) sustenta esta caraterização quando estratifica as componentes que compõem uma organização *data-driven*, as quais se encontram associadas às dimensões consideradas para o presente estudo.

Segundo Anderson (2015, p. 257), a dimensão cultura será a mais exigente em alterar, mas também será a que maior impacto oferecerá na mudança para uma organização *data-driven*, razão pela qual, Rashedi (2023) identifica a necessidade de um objetivo claro e de uma estratégia de dados para fazer face aos desafios e às barreiras existentes nessa mudança.

Segundo Rashedi (2023, p. 35), os estudos sobre esses desafios e barreiras, que se iniciaram em 2011, apontam para as áreas da falta de liderança (inexistência de estratégia e organização em silos), falta de conhecimento sobre o acesso, uso e valor dos

[18] Num pesquisa no Google, efetuada em 07 de abril de 2024, pelas 13:49, os termos surgem referenciados com os seguintes resultados: *data-driven*-3.1 milhões, *data-influenced*-165 mil, *data-informed*-804 mil.

dados (dados em silos) e, insuficiente disponibilidade de competências e de recursos na organização. Refere ainda que a cultura corporativa e a mentalidade individual dos seus colaboradores são igualmente relevantes como barreiras à mudança.

Neste particular, Harkin (2024, p. 13) aponta os seguintes sinais de uma cultura organizacional pouco adaptada para uma organização *data-driven*: política interna e a organização em silos que inibem a colaboração horizontal; receio de falhar, que inibe a inovação e reduz a aceleração nas mudanças; a transformação é vista pelos colaboradores como uma distração; a resistência individual, de equipas ou de funções à implementação da estratégia.

Por fim, no que concerne à tecnologia, importa referir que o CAN DoD identifica um conjunto de TED dependentes[19] do acesso a grande quantidade de dados para operar com a máxima eficácia, que importa considerar para o presente estudo: IA, veículos autónomos, realidade aumentada, realidade virtual/simulação, robots, manufatura aditiva, *intelligence*, IoT e *blockchain* (CAN DoD, 2019, p. 33).

No âmbito do seu modelo de maturidade de exploração de dados, a NATO (NATO - Data Exploitation Working Group, 2021) recomenda modelos específicos para avaliação da qualidade dos dados, da gestão de dados e da analítica[20], que podem ser utilizados para trabalhos futuros das FFAA.

Neste estudo usou-se o modelo de maturidade do *Central Digital and Data Office* do governo inglês (Office, 2023), que supõe a criação de um ecossistema dos dados, o qual foi usado no levantamento do nível de preparação para data-driven das FFAA.

2.2. Modelo de análise

O modelo de análise definido para o presente estudo tem como conceitos enquadrantes o DB, o ZT e Organização *data-driven*. Os dados de base, depois de analisados e selecionados de acordo com as cinco dimensões (cultura, dados, pessoas, processos e tecnologia), e indicadores (dois modelos de maturidade), foram utilizados para categorizar e selecionar contributos para o DB da MP.

De seguida, apresenta-se uma representação esquemática deste modelo de análise:

---

[19] Já para a NATO, as TED incluem IA, biotecnologia, tecnologia de hipervelocidade, tecnologia dos materiais, *Big Data*, tecnologia espacial, computação quântica e sistemas autónomos (C3Ba, 2023)
[20] https://tdwi.org/pages/research/maturity-models-and-assessments.aspx, acedido em 20Mar24.

Quadro 1 – Modelo de Análise

Objetivo Geral	Formular contributos para o *Digital Backbone* da Marinha Portuguesa				
Questão Central	Quais os contributos para o *Digital Backbone* da Marinha Portuguesa?				
Objetivos Específicos	**Questões Derivadas**	**Conceitos Enquadrantes**	**Dimensões**	**Indicadores**	**Técnica de recolha de dados**
OE1: Analisar a situação da Marinha Portuguesa com vista à implementação do *Digital Backbone*	QD1: Qual a situação da Marinha Portuguesa com vista à implementação do *Digital Backbone*?	*Digital Backbone* *Zero Trust* Organização *data-driven*	Cultura Dados Pessoas Processos Tecnologia	Nível de maturidade de *data-driven* Nível de maturidade de *Zero Trust*	Análise documental Entrevistas semiestruturadas
OE2: Analisar as caraterísticas do *Digital Backbone* de organizações externas	QD2: Quais as caraterísticas do *Digital Backbone* de organizações externas?				

3. METODOLOGIA E MÉTODO

O presente estudo foi apoiado no estudo de caso que, assentando em múltiplas fontes de evidência, enquadradas por uma lógica de construção de conhecimento, permite estabelecer uma base de aplicação de soluções para responder à Questão Central (Santos & Lima, 2019, pp. 22-37).

No caso particular deste estudo, a investigação terá por base a revisão da literatura, as estratégias particulares de várias organizações e o enquadramento conceptual, sendo que, através da análise documental e de entrevistas semiestruturadas, tirar-se-ão as devidas conclusões.

No que se refere às entrevistas semiestruturadas, foram identificadas duas entidades na Marinha (Almirante Chefe do Estado-Maior da Armada; Superintendente da Informação), uma no Exército (Chefe do Gabinete do Vice-Chefe do Estado-Maior), uma na FAP (Chefe da Divisão de Comunicações e Sistemas de Informação do Estado-Maior), duas no EMGFA (Chefe da Divisão de Inovação e Transformação; Chefe do Departamento de Planeamento, Projetos e Segurança do Centro de Comunicações e Informação, Ciberespaço e Espaço), uma na Secretaria-Geral do Ministério da Defesa Nacional (SG-MDN) (Secretário-Geral Adjunto da SG-MDN) e uma na Delegação de Portugal junto da NATO (DELNATO - Conselheiro da Delegação), cuja autoridade técnica e funcional, e conhecimento, se consideram relevantes para o estudo.

Estas entrevistas foram realizadas de forma presencial ou à distância, de acordo com a disponibilidade dos entrevistados. Os guiões das entrevistas, limitados no número de perguntas e diferenciados entre os entrevistados, focaram-se na área dos conceitos estruturantes. Para a elaboração destes, foi tida em conta a metodologia apresentada por Manuela Sarmento (2013, pp. 29-66). Importa referir que, em complemento às entrevistas, foi solicitado individualmente o preenchimento de dois questionários, por forma a determinar o nível de maturidade, dos dados e do ZT, das organizações a que pertencem.

Os principais instrumentos de recolha de dados compreenderam a análise documental e a realização de entrevistas complementadas com o preenchimento de dois questionários por parte de alguns entrevistados. A análise documental contemplou documentos de referência de outros países e da NATO, relativos à implementação do DB associado à TD. As entrevistas foram direcionadas a militares com cargos nos três Ramos, no EMGFA, na SG-MDN e na NATO, de modo a identificar, analisar e caraterizar o DB nas cinco dimensões apresentadas (pessoas, processos, tecnologias, dados e cultura). Com os questionários pretendeu-se aferir o nível de maturidade da SG-MDN, do EMGFA e dos Ramos. Para o data-driven os indicadores decorrem de cinco níveis do modelo de maturidade dos dados, adaptado do governo do Reino Unido, e para o ZT os indicadores decorrem de quatro níveis do modelo de maturidade da CISA. As transcrições das entrevistas foram alvo de análise interpretativa para enquadramento, categorização e identificação de dados relevantes para a investigação.

A documentação da NATO e dos aliados com informação para a investigação foi analisada tematicamente e os dados relevantes para o objeto desta investigação foram selecionados atento a sua classificação e importância para o objeto de estudo. A análise temática das estratégias e orientações de organizações congéneres permitiu trabalhar sobre uma amostra homogénea tendo-se identificado tendências generalizadas de contributos. Com base na análise interpretativa do conteúdo das entrevistas (lacunas e contributos) e nas análises temáticas anteriores, foi realizada uma análise SWOT para determinar os objetivos a perseguir. Como resultado, da conjugação racional da análise documental e das entrevistas, foram identificados diversos contributos aplicáveis ao DB da MP, bem como uma proposta de modelo de governação. A validação das propostas apresentadas foi efetuada com recurso às provas da estratégia, tendo sido consultados diversos especialistas.

4. APRESENTAÇÃO DOS DADOS

Neste capítulo são apresentados os dados selecionados por forma a responder às duas questões derivadas da presente investigação.

4.1. As Forças Armadas Portuguesas

"As FFAA são complexas na perspetiva tecnológica (…) chamadas a cumprir missões entre si e com outras Forças Armadas, devendo operar no conjunto e no combinado em missões distintas e de diferente duração, sendo a interoperabilidade um requisito obrigatório" (DN, 2024). "A posição de Portugal como coprodutor de segurança internacional (…) prioritariamente, no quadro da NATO (…) [sendo que] a modernização das Forças Armadas portuguesas resulta a integração de Portugal na Aliança Atlântica" (Governo de Portugal, 2013, p. 22). "A Defesa Nacional (DN), constituída por diversos organismos (…) está integrado numa rede de organizações, como outros organismos do Estado e forças de segurança, indústria de defesa e meio académico diverso" (DN, 2024).

4.1.1. Secretaria-Geral do Ministério da Defesa Nacional

Cabe à SG-MDN a implementação de uma política integradora para os SI e TIC no universo da DN, incluindo a gestão de informação em apoio à tomada de decisão (DN, 2024).

Neste particular, o Secretário-Geral Adjunto do MDN refere que no âmbito da TD das FFAA será necessário "estabelecer uma estratégia conjunta e comum, (…) onde os processos devem ser governados por uma entidade (…) [o que] não quer dizer que os Ramos não tenham respaldo nesse órgão de governação" (A. Francisco, entrevista presencial, 05 de março de 2024).

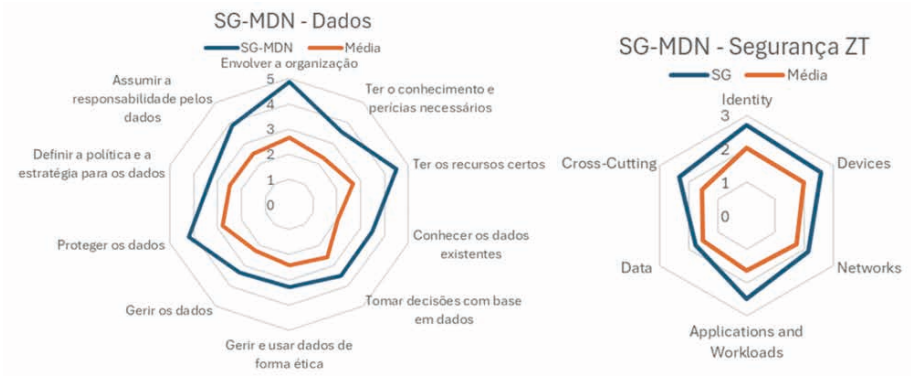

Figura 1 – Nível de maturidade da SG-MDN quanto aos dados e segurança ZT

Da sua avaliação (Figura 1), o nível de maturidade dos dados varia entre a aprendizagem (nível 3) e o desenvolvimento (nível 4), e o nível de maturidade da segurança (ZT) implementada varia entre o inicial (nível 2) e o avançado (nível 3), ambos acima da média na Defesa. Verifica-se, como principal necessidade, a **criação de uma estratégia para a gestão e governação dos dados**, que decorra da implementação de um processo que sistematize e promova a **governação digital** (A. Francisco, op. cit.). Estão em vias de serem implementadas ferramentas de IA como o CoPilot da Microsoft e outras de analítica, que muito auxiliarão o processo de tomada de decisão (op. cit.). Ao nível da literacia e da cibersegurança, o grau de maturidade na SG-MDN não é uniforme, razão pela qual não estar preparada em pleno para incorporar e explorar novas tecnologias (op. cit.).

4.1.2. Estado-Maior-General das Forças Armadas

A Diretiva Setorial do Centro de Comunicações e Informação, Ciberespaço e Espaço e a Diretiva Setorial da Ciberdefesa, identificam Iniciativas Setoriais que materializam os Objetivos Estratégicos da Diretiva Estratégica do EMGFA 2023|2026, cujo propósito de evolução está parcialmente alinhado com os Objetivos Estratégicos da NATO (EMGFA-CCICE, 2024). Contudo, **não existe uma estratégia definida para a TD** (C. Algarvio, op. cit) que contemple as dimensões Pessoas, Cultura, Dados, Processos e Tecnologia (D. Vaz, entrevista presencial, 27 de fevereiro de 2024) **ou um modelo de Governação** inclusivo, com uma liderança forte, apoiada por elementos de reconhecida competência técnica (op. cit.).

Da avaliação (Figura 2), o nível de maturidade dos dados situa-se essencialmente no nível inicial (nível 1) próximo do emergente (nível 2), abaixo da média na Defesa, e o nível de maturidade da segurança implementada varia entre o tradicional (nível 1) e o inicial (nível 2), próximo ou acima da média na Defesa.

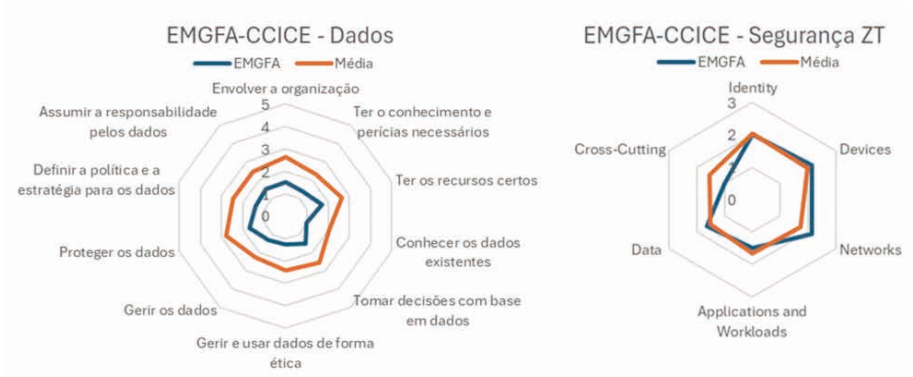

Figura 2 – Nível de maturidade do EMGFA quanto aos dados e segurança ZT

4.1.3. A Força Aérea Portuguesa

Segundo Figueiredo (entrevista presencial, 07 de março de 2024), a FAP "não se encontra pronta para, de uma forma imediata incorporar e explorar as novas tecnologias necessárias à evolução para uma organização centrada em dados". Acrescentou que tal facto resulta por a infraestrutura tecnológica estar desatualizada e carecer de um forte investimento, persistindo a utilização de numerosas aplicações *legacy*, bem como inúmeras aplicações desenvolvidas *ad-hoc* e processos manuais e em papel. A carência de recursos, a dificuldade de recrutamento e/ou contratação de colaboradores com competências específicas nas áreas tecnológicas, perante as condições de atratividade atuais, foram fatores igualmente apontados. Apresentou soluções para mitigar estas fragilidades, como promover a criação de estratégia da TD, garantir o alinhamento da organização, investir na formação e em competências, consultar especialistas e estabelecer parcerias.

Da sua avaliação (Figura 3), o nível de maturidade dos dados situa-se essencialmente no nível emergente (nível 2) e na aprendizagem (nível 3), acima da média na Defesa, e o nível de maturidade da segurança implementada varia entre o tradicional (nível 1) e o inicial (nível 2), ainda assim acima da média na Defesa.

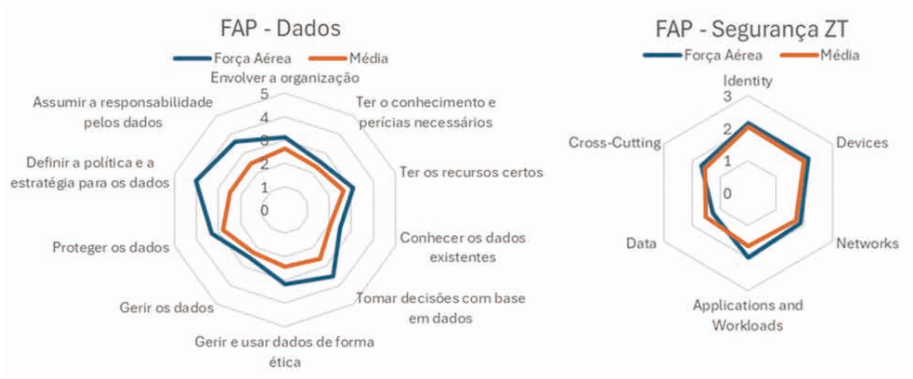

Figura 3 – Nível de maturidade da FAP quanto aos dados e segurança ZT

4.1.4. A Força Aérea Portuguesa

Segundo Barroso (entrevista por *MsTeams*, 08 de março de 2024), a maturidade digital nas FFAA é insipiente com uma cultura pouco conjunta pois atua-se muito sectorialmente. Existe iliteracia ao nível da liderança, um problema de governação e um *déficit* tremendo de especialistas, o qual depende da atrição que o mercado permitir. Refere ainda que não existe uma estratégia de dados. Apresentou algumas soluções como a contratação de consultores para auxiliar na definição das estratégias, promover a atração para a inovação, contratar serviços especializados e edificar um *data set* único da Defesa. Segundo ele não existe falta de financiamento, mas sim de prioridades. Mencionou que a Diretiva Estratégica do Ramo no âmbito da inovação prevê, até 2026, a continuação da desmaterialização e da digitização, estando a ser criada uma estrutura para promover a atração para a inovação e para incorporar e explorar convenientemente novas tecnologias.

Da sua avaliação (Figura 4), o nível de maturidade dos dados situa-se essencialmente no nível emergente (nível 2), acima da média na Defesa no que se refere à gestão e proteção dos dados, e o nível de maturidade da segurança implementada encontra--se no nível tradicional (nível 1) próximo do nível inicial (nível 2), somente acima da média na Defesa no que se refere aos dados e governação (*Cross-Cutting*).

Figura 4 – Nível de maturidade do Exército quanto aos dados e segurança ZT

4.1.5. A Marinha Portuguesa

Segundo o CHDIVREDSI, constata-se que a arquitetura das TIC da MP não acompanhou o desenvolvimento tecnológico na área, apresentando-se não só insuficiente para a atual velocidade requerida à tomada de decisão, como também com vulnerabilidades ao nível da segurança da infraestrutura, das aplicações e dos dados. O núcleo tecnológico apresenta-se fragmentado, frágil e pouco moderno face às necessidades atuais, os dados residem em silos, de complicado acesso, dificultando a sua integração, o conhecimento para os tratar é reduzido e que a MP necessita de ter os seus macroprocessos reduzidos e digitalizados. Acrescenta que as TED ainda não são exploradas em profundidade (op. cit.).

Acresce que, conforme se observa na figura 5, o universo do que é administrado é demasiado grande para os talentos técnicos existentes, quer pessoas quer tempo e conhecimento (Marinha - Superintendente da Informação, email, 12 de março de 2024).

Figura 5 – Universo da administração de TI na Marinha
Fonte: Marinha – Superintendente da Informação (2024).

A governação associada ao processo da DIRESITD apresenta objetivos específicos e linhas de desenvolvimento a perseguir até 2026 (CHDIVREDSI, op. cit.), algumas das quais terão de ser reanalisadas periodicamente dada a exigência na sua implementação num contexto exíguo de talentos e de financiamento (Superintendente da Informação, entrevista presencial, 26 de fevereiro de 2024). Com a aprovação da Diretiva das TED, verifica-se também uma clara intenção de transformação organizacional em torno da digitalização e de uma organização *data-driven* para potenciar as capacidades das TED (Figura 6).

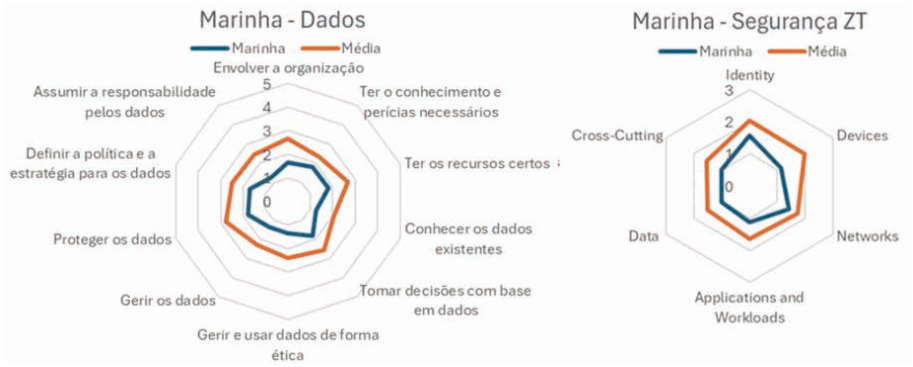

Figura 6 – Nível de maturidade da Marinha quanto aos dados e segurança ZT

Com a aprovação de duas diretivas específicas, a MP está a trabalhar para incorporar rapidamente e explorar convenientemente novas tecnologias (G. e Melo, entrevista presencial, 21 de fevereiro de 2024). Da avaliação, o nível de maturidade dos dados situa-se no nível inicial (nível 1) próximo do emergente (nível 2), e o nível de maturidade da segurança varia entre o tradicional (nível 1) e o inicial (nível 2), ambos abaixo da média.

4.2. Síntese conclusiva e resposta à QD1

A análise documental e as entrevistas permitiram apurar que **a MP não se pode dissociar do contexto militar nacional onde se insere**. Pelo observado, **as instituições das FFAA** analisadas **atravessam o mesmo tipo de contrariedades** para efetivar a TD, implementar o DB e acomodar a introdução de novas tecnologias. Com base em raciocínio lógico e a partir do conhecimento acumulado e, da análise das entrevistas, obteve-se um conjunto alargado de

lacunas (*Gap Analysis*) e de contributos (*Inputs*), correlacionados com as dimensões do estudo, os quais podem contribuir para a elaboração de uma estratégia conjunta. A MP, para a implementação do DB, carece de atenção nessas dimensões, encontrando-se em melhoria contínua (transição digital) (Correia, 2023, p. 29). Pela análise identificaram-se as seguintes potencialidades (Tabela 1):

Tabela 1 – Potencialidades

Potencialidades		Procedência
P1	Motivação da estrutura de topo	(G. Melo. *op. cit.*)
P2	Promoção de uma cultura de inovação	Todos os entrevistados
P3	Reconhecimento da importância do digital	Todos os entrevistados
P4	Existência de diretivas internas	Marinha, Exército
P5	Existência de centros de inovação e experimentação	(G. Melo. *op. cit.*)
P6	Quadro legislativo favorável no EMGFA-CCICE	(D. Vaz, *op. cit.*)
P7	Integração na NATO	(F. Carvalho, *op. cit.)*, (Governo de Portugal, 2013).

Por outro lado, ao nível das vulnerabilidades internas das FFAA, identifica-se (Tabela 2):

Tabela 2 – Vulnerabilidades

Vulnerabilidades		Procedência
V1	Governação digital fragmentada	Todos os entrevistados
V2	Iliteracia digital generalizada	Todos os entrevistados
V3	Organização em silos e dados pouco estruturados	(C. Algarvio, *op. cit.*), (D. Vaz, *op. cit.*)
V4	Predominância de sistemas legados	(A. Figueiredo, *op. cit.*)
V5	Maturidade digital insipiente	(C. Algarvio, *op. cit.*), (Marinha – SI, *op. cit.*), (J. Barroso, *op. cit.*)
V6	Capacidade limitada de talentos técnicos	(Marinha – SI, *op. cit.*)

4.3. A NATO e as Forças Armadas de países de referência

4.1.3. A Força Aérea Portuguesa

No âmbito da aplicação transversal da TD na NATO, surge no final de 2023 a intenção de alinhamento da Organização através da introdução do conceito de empresa (*enterprise*[21]), contemplando 57 diferentes entidades, incluindo, entre

[21] A NATO, em dezembro último, apresentou o contexto de uma organização única (NATO CIO, 2023).

outros, centros de decisão em terra e embarcados, representações nos aliados e infraestruturas de treino e formação (CIO NATO, 2023). Existem estudos que apoiam este pensamento como facilitador da TD, como os elaborados por Peter Brook (2015) e por Fabian Gampfer (2018). Segundo Carvalho (entrevista *online*, 10 de março de 2024), esta mudança de paradigma facilita o processo de TD ao olhar a organização como um todo, **contudo, ainda não está disponível um modelo de governação que permita monitorizar todo o processo**. Esta aproximação é igualmente seguida pelo Reino Unido com a criação do modelo *One Defence*, onde o DB e o centro de competências digitais são únicos na Defesa (UK MoD, 2021, pp. 22 a 28).

Segundo Carvalho (op. cit.), a NATO ainda não tem medidas para auxiliar países menos capacitados na TD. Existe, contudo, um conjunto de *use cases* a serem implementados, que permitirão orientar os aliados para o desenvolvimento de capacidades úteis à TD nas respetivas organizações. Referiu ainda que o recente plano de ação para a TD contempla medidas específicas para as três dimensões consideradas pela NATO (pessoas, processos e tecnologia), incluindo medidas para tornar a organização *data-driven*. Refira-se que o pilar Pessoas é colocado no centro da TD (*human-centric*) ao se garantir que a tecnologia serve as pessoas e que estas servem a organização.

Através da estratégia de implementação dessa transformação, a NATO estabelece como fundamental (EMGFA-CCICE, 2024): a interoperabilidade quer a resultante das relações inter-organizacionais quer a oferecida pela iniciativa[22] da *Federated Mission Networking* (FMN); o alinhamento de programas digitais, incluindo os aspetos de segurança ciber; a existência de programas de formação para o desenvolvimento de uma força de trabalho preparada para o digital; o fornecimento por parte dos aliados de forças de combate adequadas com capacidades modernizadas e pessoal treinado em operações multidomínio; uma arquitetura de governação centrada em dados e serviços digitais disponíveis; a definição e redesenho de processos em diversas áreas para refletir a evolução dos requisitos das TED, pela centralização dos dados e ZT; garantir sistemas

[22] Esta iniciativa contempla o *Coalition Warrior Interoperability eXploration, eXperimentation, eXamination, eXercise* (CWIX), que é o maior exercício de interoperabilidade da NATO (www.act.nato.int).

digitais interligados e centrados em dados através de um núcleo digital (DB), cujos componentes incluem redes federadas, *cloud* e uma arquitetura orientada aos serviços; garantir um ecossistema de partilha de dados da NATO.

4.3.2. As Forças Armadas congéneres

Segundo o UK MoD (2021), o digital está omnipresente e a mudar o caráter da guerra e da política, à medida que as capacidades baseadas em dados mudam a forma como as Forças Armadas comunicam, trabalham e operam (...) para se transformarem e explorarem novas formas de trabalhar, e tiveram de abordar questões legadas como: dados em silos internos, difíceis de aceder e integrar; núcleos tecnológicos fragmentados, frágeis, inseguros e obsoletos; lacunas críticas de competências digitais e de dados em todas as estruturas; processos e cultura ainda da era industrial.

Para concretizarem as respetivas transformações, os países aliados adotaram novas abordagens para aproveitar a oportunidade da tecnologia disruptiva, as quais plasmaram em estratégias diversificadas (Correia, 2023). Dessas estratégias foi elaborada de entre um grupo representativo de aliados, a matriz com contributos a considerar num DB.

São vários os Aliados, como os EUA (US DoD, 2022, p. 4), a implementarem tecnologias consideradas como prioritárias e para as quais existem estratégias dedicadas. De entre essas tecnologias releva-se a IA, cuja aplicabilidade em ecossistema será útil explorar.

No âmbito do ZT, e atento os desenvolvimentos efetuados pelo CISA, o DoD norte-americano utiliza o conceito associando-o à edificação de capacidades[23] (US DoD, 2022), sendo adequado analisar e, eventualmente, implementar nas FFAA.

4.4. Tendências Empresariais

4.4.1. As principais tecnologias

Segundo os entrevistados, as tecnologias centrais a implementar na TD da organização são a gestão de mega dados, IA e Computação na nuvem. Shivakumar (2024, p. 18) acrescenta ainda a IoT. A convergência de tecnologias inovadoras, como p.e., a integração de IA, *Big Data* e IoT em soluções holísticas, pode criar

[23] DOTMLPI(P)–Doutrina| Organização| Treino| Material| Liderança| Pessoal| Infraestruturas| Política.

plataformas estáveis que servem como base para futuras inovações, para além de gerarem sinergias e poupanças de recursos (Moore, 2001).

Com efeito, com o desenvolvimento da IA e do *Machine Learning,* outras tecnologias com potencial utilização militar evoluíram como o reconhecimento de imagem, o processamento de linguagem natural, a robótica e os sistemas autónomos, a análise preditiva, etc., as quais, quando combinadas, têm potencial para permitir um amplo espectro de aplicações, como a mineração e análise de grandes volumes de dados, assistentes de voz de IA e recolha de informação e análise (Johnson, 2023, p. 24).

Importa relevar a importância da IA no contexto ciber, ao ser usada como força multiplicadora para ações cibernéticas defensivas e ofensivas, o que terá um impacto na cibersegurança, podendo reconhecer anomalias numa rede e alterações a padrões de comportamento, e identificar vulnerabilidades no *software* (Johnson, 2021, p. 150).

Segundo Huntington & Schrey (2020), para melhorar o impacto das tecnologias será necessário definir uma adequada arquitetura de sistemas, melhorar a gestão dos dados, do seu armazenamento e da analítica, criar um ecossistema de *application programmable interfaces* para também integrar sistemas legados, aplicar metodologias *agile* na estrutura organizacional e nos processos, garantir um ambiente seguro para proteger dados, redes e tecnologias e, criar uma estrutura de governação para a transformação necessária.

Importa ainda referir a necessidade de a organização ter os talentos necessários não só para conduzir a TD da organização, como também para implementar as tecnologias acima identificadas. Segundo Rashedi (2023, pp. 107 - 109), só para implementar uma organização *data-driven* são necessárias quatro especialidades[24] diferentes dependendo da estrutura organizacional existente, da dimensão da organização, da sua maturidade em relação aos dados e do nível e complexidade do produto final exigido. Refere ainda que a organização pode treinar o seu pessoal para exercer essas competências, ou recrutar especialistas, ainda que a escassez de talentos seja cada vez mais visível no mercado.

4.4.2. A estrutura de governação

Para ter sucesso no mundo digital, as organizações devem constantemente

[24] *Data Engineer, Data Scientist, Data Analyst* e *Business Analyst*.

desenvolver as suas estruturas internas e construir uma cultura forte em torno da inovação, onde a mudança não deve ser vista como uma exceção, mas como um padrão organizacional (Berg & Josefsson, 2019, p. 17). Com efeito, perante um contexto externo em constante mudança, para realizar a TD a organização necessita de uma estratégia digital clara, de líderes que promovam uma cultura inovadora e assumam riscos (Schwertner, 2017, p. 389). Contudo, apesar de não existir uma fórmula linear que garanta a correta liderança de todo o processo, diversos autores procuram delinear modelos de governação para auxiliar o processo da TD.

O modelo de Jacobi e Brenner (2017) consiste em **três áreas** principais e **interdependentes**, cada qual com fatores críticos de sucesso a atingir ((a) a (i)): **liderança e visão**: Os líderes devem ter conhecimento profundo sobre TD, sentido de urgência, coragem para mudar a organização e combater a resistência à mudança (Parviainen et al., 2017, p. 65). Para tal, devem (a) formular estratégias com objetivos claros; (b) demonstrar o envolvimento total por parte da estrutura de topo da organização; (c) identificar um responsável pela implementação da estratégia; **cultura e pessoas**: Um dos fatores de sucesso para efetuar a mudança é minimizar a resistência dos colaboradores, priorizando a TD de modo a ser relevante (Schwertner, 2017, p. 388). Deve-se privilegiar por (d) uma cultura inovadora, aberta e não adversa ao risco; (e) descentralizar pelos colaboradores a estratégia a implementar, recolhendo contributos individuais; (f) manter e desenvolver conhecimento digital na organização, incluindo a presença em estruturas externas; **processos e estrutura organizacional**: A TD requer a mudança da estrutura organizacional de modo a melhorar o fluxo de informação e permitir a existência de equipas ágeis (Matt et al., 2015, p. 339). Assim, deve-se (g) desenvolver ecossistemas e incorporar a estrutura digital na organização; (h) implementar funcionalmente equipas ágeis interdependentes; (i) desenvolver parcerias externas, alinhadas com as estratégias digitais.

Debruçando-se sobre o referido modelo, Berg e Josefsson (2019, pp. 70-73) estudaram as relações entre os fatores críticos de sucesso, concluindo que os fatores afetam e são afetados entre eles e os que já se encontram implementados influenciam a forma como os restantes são executados. Concluem ainda que, com este modelo, a organização terá uma melhor perspetiva onde deve centrar a sua atenção, obtendo maior benefício de cada um dos fatores críticos e, corrigir eventuais desalinhamentos ou atrasos de implementação.

Esta proposta **procura responder à situação de governação digital deficitária** mencionada por Correia (2023, p. 30). Sendo projetado para garantir que a estratégia digital seja implementada de maneira coesa, com clareza nas responsabilidades de liderança, promovendo a integração e a colaboração em toda a DN, este modelo assegura que os investimentos e as iniciativas digitais estejam alinhadas com as metas estratégicas mais amplas da Defesa e que haja uma gestão eficaz dos recursos.

Teece (2007) refere que o nível aferir é uma atividade que resulta na identificação, desenvolvimento e avaliação de oportunidades tecnológicas em relação às necessidades da organização, pois, saber quais e quando efetuar mudanças é crucial para a TD; o nível consolidar representa a captura de valor resultante da implementação ou inovação introduzidas; o nível reconfigurar refere-se à continuada renovação e transformação dos processos e rotinas da organização, o que, quando associado à transformação de estruturas e meios da organização, revela constante crescimento do valor resultante.

Como referem Ribeiro e Pinto (2022, p. 185), para tirar proveito do processo estratégico será necessário garantir o alinhamento de todos os processos de gestão com a estratégia da organização. Tal só é possível com uma estrutura central, que forneça orientação e coordenação. É neste sentido que o modelo de governação proposto pressupõe um fórum de governação ao nível do EMGFA e MDN, e uma série de fóruns de governação ao nível dos Ramos[25], assegurando a direção estratégica e a tomada de decisão coletiva.

4.5. Síntese conclusiva e resposta à QD2

A análise documental permitiu apurar que a MP não se pode dissociar do contexto internacional onde se insere para a edificação do seu DB. Pelo observado, a NATO e aliados encontram-se a efetuar a TD numa perspetiva *enterprise* de modo a olhar as suas organizações como um todo. No caso da NATO, **ainda não existe um modelo de governação implementado** e identificou-se a necessidade de apostar numa aproximação *human-centric*, em exercícios de interoperabilidade e em tecnologias consideradas de base como a IA, o *Big Data* e a *Cloud*. Dos aliados obtiveram-se contributos, enquadrados nas dimensões em estudo. Do tecido não militar, identificou-se a necessidade de desenvolver ecossistemas temáticos e

[25] A DIREDSITD tem um objetivo específico para a criação de um grupo de governação da TD na MP.

outras tecnologias úteis na edificação de um DB, o que está em linha com a posição de alguns dos entrevistados. Identificou-se igualmente uma proposta de modelo de governação, o qual foi adaptada ao contexto do presente estudo.

Assim, foi possível identificar as seguintes potenciais oportunidades externas (Tabela 3):

Tabela 3 – Oportunidades

Oportunidades		Procedência
O1	Disponibilidade de programas e use cases para edificação de capacidades na NATO	(F. Carvalho, *op. cit.*)
O2	Possibilidade de *benchmarking* de estratégias dos aliados	(Correia, 2023)
O3	Transformação da NATO em *data-driven*	(F. Carvalho, *op. cit.*)
O4	Existência de um plano de ação da NATO para a transformação digital	(NATO CIO, 2023)
O5	Realização na NATO de exercícios de redes de missão federadas	(EMGFA-CCICE, 2024)
O6	Desenvolvimento de tecnologias IA, *Big Data* e *Cloud* em franca expansão	(Shivakumar, 2024)
O7	Alinhamento da Organização como *Enterprise*	(NATO CIO, 2023)

Por outro lado, identificam-se os fatores externos que afetam negativamente as FFAA (Tabela 4):

Tabela 4 – Ameaças

Ameaças		Procedência
A1	Rápida evolução tecnológica	(Johnson, 2021)
A2	Diversas especialidades associadas a tecnologias	Literatura diversa
A3	Escassez de especialistas nas áreas do digital	(UK MoD, 2021); Entrevistas
A4	Redes inseguras com inclusão de novas tecnologias	(Johnson, 2021)
A5	Tecnologia *legacy* implementada nas organizações	(UK MoD, 2021)
A6	Impacto da inclusão combinada de tecnologias	(Johnson, 2021)

5. DISCUSSÃO DOS RESULTADOS

Neste capítulo, apresentam-se contributos em resposta à QC da investigação.

5.1. Matriz SWOT

A partir das Potencialidades (*Strengths*), Vulnerabilidades (*Weaknesses*), Oportunidades (*Opportunities*) e Ameaças (*Threats*) identificadas, desenvolveu-

-se uma análise SWOT (Apêndice A), a qual permite entender a relação entre os fatores internos e externos, resultando na identificação dos objetivos estratégicos (Ribeiro, 2020, pp. 150-152). Com este mapeamento consideraram-se quatro formas inovadoras de ação estratégica[26] (Ribeiro & Pinto, 2022, p. 46) instituídas em outras análises estratégicas do EMGFA, cada qual com dois objetivos estratégicos a concretizar.

Assim, atento a matriz SWOT no Apêndice A, os objetivos estratégicos a atingir são: (i) crescimento - OE1 - Fomentar a interoperabilidade através da participação em eventos de experimentação, testes e exercícios, nacionais e internacionais, como o exercício CWIX da NATO; OE2 - Garantir presença, na representação estratégica-política na NATO, de um especialista militar para acompanhar o processo de implementação do DB daquela Organização; (ii) focalização - OE3 - formular, operacionalizar e monitorizar, na estrutura de topo das FFAA e MDN, todo o processo da TD e da implementação do DB. A existência de uma estrutura de governação e de gestão terá essa responsabilidade; OE4 - centralizar no EMGFA e MDN a responsabilidade da edificação genética, estrutural e operacional do núcleo *data-driven* das FFAA; (iii) diversificação - OE5 - criar ecossistemas temáticos associados à transformação conjunta das Forças Armadas, privilegiando a partilha de especialistas e de dados. O planeamento e integração de TED nas FFAA é otimizado com a criação de ecossistemas; OE6 - assegurar o compromisso da liderança de topo das FFAA na aquisição, partilha e promoção da literacia digital; (iv) defesa - OE7 - desenvolver a resiliência do DB através da concretização do conceito de desconfiança total (ZT) no acesso a redes, dados e sistemas. A avaliação e implementação do trabalho desenvolvido pelo CISA acelera esse desiderato; OE8 - diligenciar, ao nível do conjunto, a criação de estratégias para as FFAA quer para a TD quer para as TED como a inteligência artificial, dados, IoT e *cloud computing,* alinhadas com a Administração Pública.

5.2. Outros contributos

Da presente investigação resultaram outros contributos para o DB, nomeadamente: Identificação de modelos de maturidade (propostos e em utilização pela NATO e aliados); levantamento do estado de situação das FFAA,

[26] Crescimento (potencialidades com oportunidades), Focalização (vulnerabilidades com oportunidades), Diversificação (potencialidades com ameaças) e Defesa (vulnerabilidades com ameaças).

tarefa realizada através de representantes participantes, com recurso a entrevistas e levantamentos de maturidade. Padece de atuação conjunta e estruturada entre os Ramos; contributos para a elaboração de estratégias, compilação de propostas identificadas nas entrevistas, enquadradas pelas dimensões em análise, as quais afigura-se ser de analisar para a elaboração das estratégias a implementar nas FFAA, quer da TD quer das TED, num total de 18 lacunas a mitigar e 29 oportunidades a explorar; identificação de contributos das estratégias dos Aliados, enquadrados pelas dimensões em análise, foram identificadas tecnologias e processos a considerar, assim como, documentos estratégicos elaborados pelos aliados; apresentação de um modelo de governação, proposta de modelo para suprir uma lacuna identificada na implementação e operacionalização da TD.

5.3. Validação dos Objetivos Estratégicos

As propostas apresentadas, com recurso às provas da estratégia[27], segundo a caraterização de Ribeiro (2009). Realça-se que estas mereceram algumas reservas por considerarem que existe uma governação limitada ao nível do conjunto e falta de pessoal em quantidade e qualificação. Houve ainda referência à necessidade de mudança de culturas institucionais, que podem levar algum tempo a consolidar, e a necessidade de financiamento para operacionalizar a TD. Todos os especialistas consideram que aprenderam com este estudo e que é útil para desenvolver as FFAA no âmbito digital.

5.4. Síntese conclusiva e resposta à QC

Com base nas respostas às QD foi efetuada uma análise SWOT, que permitiu identificar oito objetivos estratégicos como contributos para a edificação de um DB. Como corolário da investigação efetuada, foram igualmente apresentados outros contributos das entrevistas, das estratégias dos Aliados e da análise documental de autores civis e de organizações externas para análise de implementação. Identificou-se igualmente modelos de maturidade, em uso na NATO e nos aliados, e de governação que, atento as necessidades levantadas nas entrevistas, consideram-se úteis para análise de aplicabilidade.

Fica assim respondida a QC - Quais os contributos para o *Digital Backbone*

[27] Adequabilidade (permite atingir os objetivos?), Exequibilidade (possível executar com os meios disponíveis?) e Aceitabilidade (custos aceitáveis face aos objetivos desejados?).

da Marinha Portuguesa?, concretizando o OG desta investigação - Formular contributos para o *Digital Backbone* da Marinha Portuguesa.

6. CONCLUSÕES

A TD das organizações é um processo contínuo e dinâmico, sem uma data de término específica, devido à natureza evolutiva da tecnologia e às constantes mudanças nas exigências do mercado e nas expectativas dos utilizadores. À medida que novas tecnologias emergem e se desenvolvem, as organizações precisam de se adaptar e inovar continuamente para manter a sua competitividade, eficiência e relevância.

São diversos os fatores que influenciam ao longo do tempo o ritmo e a natureza dessa transformação, assentando, entre outros, na rapidez com que se atinge a maturidade digital, quer das organizações, quer das próprias tecnologias.

As FFAA, organizações profundamente tecnológicas, estão sujeitas a estes fatores de influência, pelo que importa avaliar continuamente a sua maturidade digital, a qual depende não apenas de tecnologia, mas também de pessoas, da cultura organizacional, dos processos implementados e da organização orientada a dados.

A partir do problema identificado, que reflete que a MP é uma organização pouco *data-driven* e pouco digital, considerou-se que, perante o insuficiente nível de capacitação digital das FFAA e os desafios comuns que atravessam, os resultados devem ser enquadrados e sincronizados entre as estruturas da DN analisadas, através de um processo sob a mesma governação, de modo a garantir a adoção de soluções comuns visando a geração de benefícios mútuos por razão de escala, eficácia e uniformidade de ação.

O procedimento metodológico seguido consistiu num processo de raciocínio indutivo, recorrendo a uma estratégia qualitativa assente em entrevistas e análise documental, baseado no estudo de caso.

De forma a dar resposta às QD, é efetuada diversa leitura e análise documental, e foram efetuadas entrevistas a especialistas de todas as estruturas visadas da DN, as quais contribuíram para o *gap analysis* efetuado sobre as FFAA,

Essa avaliação apurou que a MP não se encontra totalmente preparada para implementar um DB e efetuar a TD. Os constrangimentos identificados são semelhantes em todos os ramos, nomeadamente escassez de pessoal e material, pessoal pouco qualificado e baixa literacia digital. Embora a MP reconheça

a importância do digital e esteja motivada para a inovação, enfrenta desafios significativos incluindo governação digital fragmentada e dependência de sistemas legados. Acresce que a ausência de talentos nas áreas dos dados e das novas tecnologias é um enorme desafio para a implementação de um DB das FFAA.

Por outro lado, refira-se que a NATO estabeleceu orientações para que a sua TD e a implementação do correspondente DB ocorresse num contexto de uma organização única (*enterprise*).

Os resultados obtidos por esta investigação, baseados numa avaliação do estado atual das FFAA em termos de capacidades digitais, bem como nas tendências e práticas de organizações congéneres e do setor empresarial, conduziram a uma série de recomendações e objetivos estratégicos, destinados a promover a implementação do DB nas FFAA, no geral, e na MP em particular.

Quanto ao OG e em resposta à QC, os objetivos estratégicos identificados na análise SWOT incluem a promoção de uma cultura de inovação e a integração de tecnologias emergentes, como a IA, *Big Data* e *cloud*, para melhorar a eficiência operacional e a segurança cibernética. É enfatizada a necessidade de estratégias digitais conjuntas, a melhoria da literacia digital e a implementação de segurança robusta em toda a infraestrutura.

No caso da elaboração das estratégias, devem ser tido em consideração necessidades de alinhamento com a TD da Administração Pública.

Além disso, a adoção de práticas de governança e de segurança robustas são essenciais para a proteção de dados, redes e sistemas, numa era de crescentes ameaças cibernéticas. Neste particular, a implementação de um modelo de ZT é considerada fundamental para a segurança da TD das FFAA, atento a que estas devem ser orientadas a dados de modo a aproveitar o potencial das tecnologias digitais.

Para superar esses desafios e aproveitar as oportunidades identificadas, a investigação recomenda a implementação de uma iniciativa conjunta e comum nas FFAA, e o desenvolvimento de competências digitais e de estratégias diversificadas, alinhado com o que os aliados enveredam atualmente. É igualmente enfatizada a importância de acompanhar todo o processo de desenvolvimento da NATO e de criar ecossistemas para a DN, relacionados com as TED e os dados, e de promover não só uma cultura de inovação, mas também de estabelecer parcerias estratégicas.

Não foram identificadas limitações ao desenvolvimento do estudo, mas verificou-se que é um assunto intrincado pois afeta as organizações nas cinco dimensões abordadas.

No que concerne a estudos futuros no âmbito do Instituto Universitário Militar, considera-se o desenvolvimento das diferentes estratégias a implementar, tendo como referência os aliados e a NATO.

Concluindo, o presente estudo propõe uma abordagem holística para a criação do DB das FFAA, destacando a necessidade de enquadramento com a restante DN, de adaptação cultural, de trabalho conjunto e de desenvolvimento de competências, de investimento em tecnologias emergentes e da implementação de práticas de governança e segurança robustas. Essas medidas visam não apenas melhorar a eficiência em MDO, mas também de assegurar a capacidade de permanente adaptação ao contexto externo num ambiente cada vez mais célere, digitalizado e interconectado.

REFERÊNCIAS BIBLIOGRÁFICAS

Alford, J. (2023). *Intelligent Digital Ecosystems - How rethinking technology will expand your mind and change your world*. [ISBN 978-1-7779796-3-8 (eBook)]. eBook. https://intelligentdigitalecosystems.com/

Anderson, C. (2015). *Creating a Data-Driven Organization*. USA - Boston: O'Reilly.

Andersson, H., Kaplan, J., & Smolinski, B. (2012, 01 de outubro). Capturing value from IT infrastructure innovation. *Business Technology Office, Mckinsey Digital*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/capturing-value-from-it-infrastructure-innovation#/

Avedillo, J. G., Begonha, D., & Peyracchia, A. (2015). T*wo ways to modernize IT systems for the digital era*. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/two-ways-to-modernize-it-systems-for-the-digital-era#/

Berg, E., & Josefsson, C. (2019, 31 de maio). Enabling Digital Transformation - A Dynamic Capabilities Approach. Sweden: LINKÖPING UNIVERSITY. https://liu.diva-portal.org/smash/get/diva2:1321862/FULLTEXT01.pdf

Berkun, S. (2013). scottberkun.com. https://scottberkun.com/2013/danger-of-faith-in-data/

Brook, P. (2015). *Enterprise and the Technology Environment*. STO-EN-SCI-276. S&TO - Science & Technology Organization. https://www.sto.nato.int/publications/pages/results.aspx?k=STO-EN-SCI-276&s=Search%20All%20STO%20Reports

C3Ba. (2023). *NATO's Digital Transformation implementation Strategy*. NATO.

CAN DoD. (2019). *Data Strategy*. Canadian Armed Forces. p. 33. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/data-strategy.html

Chefe do Estado-Maior da Força Aérea. (2023). *Criação da Divisão de Inovação e Transformação Organizacional do estado-Maior da Força Aérea*. Força Aérea. Despacho.

Chefe do Estado-Maior do Exército. (2024). *Diretiva para a Investigação, Desenvolvimento e Inovação no Exército*. Exército Português.

CIO NATO. (2023). *NEDTAP - NATO Enterprise Digital Transformation Action Plan*. Bruxelas: NATO.

CISA. (2023). Cybersecurity & Infrastructure Security Agency. https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-209a

Correia, A. D. (2023). *A transformação digital nas Forças Armadas Portuguesas*. Lisboa: IUM. http://hdl.handle.net/10400.26/46767

Delmond, M., Coelho, F., Keravel, A., & Mahl, R. (2016, 01 de janeiro). How Information Systems Enable Digital Transformation: A focus on Business Models and Value Co-production. *HEC Paris Research Paper No. MOSI-2016-1161,* SSRN - Elsevier. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2806887

DN. (2024). Portal da Defesa Nacional (DN). https://www.defesa.gov.pt/

DTIS NATO. (2023). *NATO's DTIS*. PO(2023)0191 (INV). NATO. DTIS - Digital Transformation Implementation Strategy.

Eckerson, W. (2012). *Secrets of Analytical Leaders*. http://download.101com.com/pub/tdwi/files/SecretsofAnalyticalLeaders.pdf

EMAa. (2024). *Diretiva para as Tecnologias Emergentes e Disruptivas*. Lisboa: Marinha - Estado-Maior da Armada.

EMGFA-CCICE. (2024). *Correspondência entre as Diretivas setorias do CCICE e CoCIBER e a Diretiva Estratégica para a Implementação da Transformação Digital na NATO*. Relatório nº EMGFA-REL-2024-000008. EMGFA. Lisboa:

Estado-Maior da Armada. (2023). *Diretiva de Redes, Sistemas de Informação e Transformação Digital*. Lisboa: Marinha.

Exército, D. D. P. D. F.-E.-M. D. (2023). *Robótica e Sistemas Autónomos (RAS) - Conceito Inicial*. Exército Português. Informação. Lisboa: Exército.

Forrester research, inc. (2023). Forrester. forrester.com. https://www.forrester.com/zero-trust/

Furr, N., & Shipilov, A. (2019). Digital Doesn't Have to Be Disruptive. The best results can come from adaptation rather than reinvention. *Magazine*, Harvard Business Review. https://hbr.org/2019/07/digital-doesnt-have-to-be-disruptive

Gampfer, F. (2018, 17-20 de junho). Managing Complexity of Digital Transformation with Enterprise *Architecture*. *31st Bled EConference: Digital Transformation: Meeting The Challenges*, pp. 635-642. . Bled, Slovenia: University of Maribor Press. http://press.um.si/index.php/ump/catalog/book/343

Gartner. (2023, 30 de janeiro). Gartner Glossary. Retirado de https://www.gartner.com/en/information-technology/glossary/legacy-application-or-system

Google. (2023, 1 de dezembro). BeyondCorp. cloud.google.com. https://cloud.google.com/beyondcorp?hl=pt-br

Governo de Portugal. (2013). *Conceito Estratégico de Defesa Nacional*. Lisboa. https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/Conceito-Estrategico-de-Defesa-Nacional.pdf

Green-Ortiz, C., Fowler, B., Houck, D., Hensel, H., Lloyd, P., McDonald, A., & Frazier, J. (2023). *Zero Trust Architetcure*. Vol. Networking Technology: Security series. San Jose: Cisco Press. https://www.ciscopress.com/store/zero-trust-architecture-9780137899739

Harkin, B. (2024). *Evolving form Digital Transformation to Digital Acceleration*. Using the Galapagos Framework. Taylor & Francis Group. https:/doi.org/10.1201/9781003404217

Huntington, M., & Schrey, C. (2020, 23 de janeiro). *McKinsey Digital*. www.mckinsey.com. https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/enhancing-the-tech-backbone

Jacobi, R., & Brenner, E. (2017, 15 de setembro). How Large Corporations Survive Digitalization. *Digital Marketplaces Unleashed*, pp. 83-97. Berlin: Springer.

Johnson, J. (2021). *Artificial Intelligence and the future of warfare - The USA, China, and strategic stability*. Manchester, UK: Manchester University Press.

Johnson, J. (2023). *AI and the Bomb - Nuclear Strategy and Risk in the Digital Age*. New York: Oxford University Press.

Knapp, M. S., Swinnerton, J. A., Copland, M. A., & Monpas-Huber, J. (2006). https://www.education.uw.edu/ctp/sites/default/files/ctpmail/PDFs/DataInformed-Nov1.pdf

Löffler, K. (2020). Literature Review on Operational vs. Digital Backbone: Successfully Transforming IT Infrastructure. *Transforming IT Infrastructure - Seminar IT-Management in the Digital Age*. Wedel, Germany: fhwedel - University of Applied Sciences.

Lopez, C. T. (2022). *DOD Releases Path to Cyber Security Through Zero Trust Architecture*. https://www.defense.gov/News/News-Stories/Article/Article/3229211/dod-releases-path-to-cyber-security-through-zero-trust-architecture/

Matt, C., Hess, T., & Benlian, A. (2015, 04 de agosto). Digital Transformation Strategies. Business and Information. 57, 339–343. Springer. https://link.springer.com/article/10.1007/s12599-015-0401-5

McKinsey. (2020). Enhancing the tech backbone. McKinsey & Company. https://www.mckinsey.com/industries/industrials-and-electronics/our-insights/enhancing-the-tech-backbone#/

Mezzetta, S. (2023). P*rinciples of Data Fabric - Become a data-driven organization by implementing Data Fabric solutions efficiently* (1ª Ed.). Birmingham, Uk: PacktPublishing Ltd.

Moore, G. A. (2001). *Crossing the Chasm*. New York: Perfectbound.

NATO - Data Exploitation Working Group. (2021). *Approval for NATO's Data Exploitation Framework Policy*. Data Exploitation Working Group. Bruxelas: NATO.

NATO. (2023). *NATO Zero Trust Policy*. NATO. Working paper.

NATO CIO. (2023). *NATO Enterprise Digital Transformation Action Plan* (NEDTAP). NATO. Chief Information Officer. Bruxelas: NATO.

Office, C. D. A. D. (2023). *Data Maturity model*. https://www.gov.uk/government/collections/data-maturity-assessment-for-government

Panetta, K. (2017). The Gartner IT Security Approach for the Digital Age. gartner.com. https://www.gartner.com/smarterwithgartner/the-gartner-it-secutity-approach-for-the-digital-age

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017, 13 de março). Tackling the digitalization challenge: how to benefit from digitalization in practice. International Journal of Information Systems and Project Management. https://revistas.uminho.pt/index.php/ijispm/article/view/3856/3909

Rashedi, J. (2023). *The Data-driven Organization*. Using Data for the Success of Your Company. Switzerland: Springer.

Razi Rais, C. M. E. G. A. D. B. (2023). *Zero Trust Networks* (2ª edição Ed.). Vol. Building Secure Systems in Untrusted Network. Boston, USA: O'Reilly.

Ribeiro, A. S. (2009). *Teoria Geral da Estratégia: O essencial ao processo estratégico*. Coimbra: Almedina.

Ribeiro, A. S. (2020). *Modelos do processo estratégico* (Coleção Estudos Políticos e Sociais Ed.). Lisboa: Universidade de Lisboa.

Ribeiro, A. S., & Pinto, S. D. S. (2022). *O processo de gestão estratégica no EMGFA*. Lisboa: Instituto Universitário Militar.

Ross, J. W., Sebastian, I. M., Beath, C., Mocker, M., Moloney, K. G., & Fonstad, N. O. (2016). *Designing and executing Digital Strategies*. Artigo apresentado na *Thirty Seventh International Conference on Information Systems*. Dublin.

Santos, L. A. B. D., & Lima, J. M. M. D. V. (2019). *Orientações Metodológicas para Elaboração de trabalhos de investigação* (2.ª Ed., revista e atualizada). Lisboa: Instituto Universitário Militar. https://www.ium.pt/pub/107

Sarmento, M. (2013). *Metodologia Científica para a elaboração, escrita e apresentação de teses* (Coleção Manuais Ed.). Lisboa: Universidade Lusíada. http://editora.lis.ulusiada.pt

Schwertner, K. (2017). Digital Transformation of Business. https://pdfs.semanticscholar.org/51bb/4fd609d174438fb8911f283d48d34ef1e894.pdf

Scott Rose, O. B. S. M. S. C. (2020). *Zero Trust Architecture*. Vol. Special Publication 800-207. NIST - National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Shivakumar, S. K. (2024). *Elements of Digital Transformation*. Londres: CRC Press, Taylor & Francis Group.

Teece, D. J. (2007, 07 de August). Explicating Dynamic Capabilities: The Nature and Microfoundations of enterprise performance. (28) , 1319-1350. Strategic Management Journal. https://onlinelibrary.wiley.com/doi/abs/10.1002/smj.640

Tonder, C. V., Schachtebeck, C., Nieuwenhuizen, C., & Bossink, B. (2020). A framework for Digital Transformation and Business Model Innovation. *Journal article*, . South Africa: The University of Johannesburg Institutional Repository (UJ IR). https://ujcontent.uj.ac.za/esploro/outputs/journalArticle/A-framework-for-digital-transformation-and/9912165207691

UK GOV. (2023). www.gov.uk. Data Maturity Assessment for Government. https://www.gov.uk/government/collections/data-maturity-assessment-for-government

UK MoD. (2021). *Digital Strategy for Defence*. Delivering the Digital Backbone and unleashing the power of Defence's data. Ministry of Defence. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/990114/20210421_-_MOD_Digital_Strategy_-_Update_-_Final.pdf

US DoD. (2022). *DoD Zero Trust Strategy*. Department of Defense. Washington, D.C.: U.S. Department of Defense. https://dodcio.defense.gov/Library/

Willcocks, L., Hindle, J., Stanton, M., & Smith, J. (2024). *Maximizing value with automation and digital transformation*. Switzerland: palgrave macmillan.

APÊNDICE A – Análise SWOT

Quadro 2 – Análise SWOT

	POTENCIALIDADES	VULNERABILIDADES
	P1 – Motivação da estrutura de topo P2 – Promoção de uma cultura de inovação P3 – Reconhecimento da importância do digital P4 – Existência de Diretivas internas P5 - Existência de centros de inovação e experimentação P6 – Existência de quadro legislativo no CCICE P7 – Integração na NATO	V1 – Governação digital fragmentada V2 – Iliteracia digital generalizada V3 – Organização em silos e dados pouco estruturados V4 – Predominância sistemas legados (*legacy*) V5 – Maturidade digital insipiente V6 – Capacidade limitada de talentos técnicos
OPORTUNIDADES	**CRESCIMENTO**	**FOCALIZAÇÃO**
O1 – Disponibilidade de programas e use cases para edificação de capacidades na NATO O2 – Possibilidade de benchmarking de estratégias dos aliados O3 – Transformação da NATO em *data-driven* O4 – Existência de um plano de ação da NATO para a transformação digital O5 – Realização na NATO de exercícios de redes de missão federadas O6 – Desenvolvimento de tecnologias IA, *Big Data*, IoT e *Cloud* em franca expansão O7 – Alinhamento da Organização como *Enterprise*	**FOMENTAR** a interoperabilidade através da participação em eventos de experimentação, testes e exercícios, nacionais e internacionais. (P1,P2,P3,P4,P5,P7)x(O1,O2,O3,O4,O5) **GARANTIR**, na representação estratégica-política na NATO, um especialista militar para acompanhar o processo de implementação do DB da Organização. (P1,P2,P3,P4,P7)x(O1,O2,O4,O5,O6)	**FORMULAR, OPERACIONALIZAR e MONITORIZAR**, na estrutura de topo das FFAA e MDN, todo o processo da TD e da implementação do DB. (V1,V2,V3,V4,V5,V6)x(O2,O3,O4,O6,O7) **CENTRALIZAR** no EMGFA e MDN a responsabilidade da edificação genética, estrutural e operacional das Forças Armadas *data-driven*. (V1,V2,V3,V4,V5,V6)x(O1,O2,O3,O4,O5,O6,O7)
AMEAÇAS	**DIVERSIFICAÇÃO**	**DEFESA**
A1 – Rápida evolução tecnológica A2 – Diversas especialidades associadas a tecnologias A3 - Escassez de especialistas FFAA nas áreas do digital A4 – Redes inseguras com inclusão de novas tecnologias A5 – Tecnologia *legacy* implementada nas organizações A6 – Impacto da inclusão combinada de tecnologias	**CRIAR** ecossistemas temáticos associados à transformação conjunta das Forças Armadas, privilegiando a partilha de especialistas e de dados. (P1,P2,P3,P4,P5,P6,P7)x(A1,A2,A3,A4,A5,A6) **ASSEGURAR** o compromisso da liderança de topo da organização na aquisição, partilha e promoção da literacia digital. (P1,P2,P3,P4,P6,P7)x(A1,A2,A3,A4)	**PROMOVER** a resiliência do DB através da implementação do conceito de desconfiança total (*Zero Trust*) no acesso a redes, dados e sistemas. (V1,V3,V4)x(A1,A2,A3,A4,A5,A6) **DILIGENCIAR**, ao nível do conjunto, a criação de estratégias para as FFAA quer para a TD quer para domínios como a inteligência artificial, dados e *cloud*. (V1,V2,V3,V5,V6)x(A1,A2,A4,A5,A6)

ESTUDO 3 – *INTELLIGENCE-LED POLICING*: CONTRIBUTOS PARA SUA IMPLEMENTAÇÃO NA GNR[28]

INTELLIGENCE-LED POLICING: CONTRIBUTIONS TO ITS IMPLEMENTATION IN THE GNR

Paulo Jorge Macedo Gonçalves
Coronel GNR de Infantaria

Mário José Machado Guedelha
Brigadeiro-general GNR

RESUMO

Esta investigação tem por objeto de estudo o modelo *Intelligence-Led Policing* (ILP) que se apresenta como uma abordagem mais proativa colocando as informações no epicentro do processo de planeamento e decisão operacional. Partindo da tese inicial que o ILP se constitui uma mais-valia complementar para o policiamento da GNR, define-se como objetivo geral propor contributos para a implementação deste modelo na organização. A metodologia baseia-se numa combinação de estratégias quantitativas e qualitativas. Os principais instrumentos de recolha de dados compreendem a análise documental, entrevistas semiestruturadas e inquérito por questionário. A amostra inclui oficiais de todos os níveis de decisão da GNR. Os resultados indicam que, embora o ILP não esteja totalmente implementado na GNR, reconhece-se a sua relevância e complementaridade com outros modelos de policiamento. A implementação do ILP depende da melhoria da capacidade analítica, através da integração de tecnologia avançada de análise de dados. O processo de decisão requer a integração sistemática de informações a todos os níveis de decisão. A formação específica em ILP é fundamental, assim como a autonomização da estrutura de informações ao nível tático. O envolvimento e compromisso das lideranças são fatores críticos de sucesso para superar a resistência à mudança e implementar efetivamente o ILP.

Palavras-chave: GNR, *intelligence-led policing,* Informações, policiamento

[28] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Promoção a Oficial General (CPOG 2023/2024). A versão integral encontra-se disponível nos Repositórios Científicos de Acesso Aberto de Portugal (https://www.rcaap.pt/).

ABSTRACT

This research focuses on the Intelligence-Led Policing (ILP) model, which represents a more proactive approach by placing information at the center of operational planning and decision-making processes. Starting from the initial thesis that ILP constitutes an additional value for the policing of the GNR, the main objective is defined as proposing contributions for the implementation of this model within the organization. The methodology is based on a combination of quantitative and qualitative strategies. The main data collection tools include document analysis, semi-structured interviews, and surveys. The sample includes officers from all decision-making levels within GNR. The results indicate that, although ILP is not fully implemented in the GNR, its relevance and complementarity with other policing models are recognized. The implementation of ILP depends on improving analytical capacity through the integration of advanced data analysis technology. The decision-making process requires the systematic integration of information at all levels of decision. Specific training in ILP is essential, as well as the empowerment of the information structure at the tactical level. The involvement and commitment of leadership are critical success factors to overcome resistance to change and effectively implement ILP.

***Keywords**: GNR, intelligence-led policing, intelligence, policing*

1. INTRODUÇÃO

A segurança, como pilar fundamental do Estado de Direito Democrático, desempenha um papel crucial na garantia das liberdades individuais e coletivas, bem como na preservação do bem-estar social. Neste contexto, as forças policiais emergem como instituições centrais, cuja missão primordial é assegurar a ordem pública, a segurança dos cidadãos e a proteção dos direitos fundamentais.

Em termos globais, tem-se assistido a uma diversificação das formas de criminalidade, evidenciando a natureza dinâmica e complexa dos desafios de segurança que se colocam às sociedades contemporâneas. O aumento significativo dos cibercrimes, que englobam desde fraudes financeiras, ataques a infraestruturas críticas, até violações de dados pessoais, ressalta a vulnerabilidade dos espaços digitais e a necessidade de reforçar as capacidades de cibersegurança. Paralelamente, formas tradicionais de criminalidade continuam a afetar diversas comunidades, muitas vezes reinventando-se ao incorporar a utilização de novas tecnologias no seu *modus operandi*. Adicionalmente, a globalização e o desenvolvimento tecnológico acelerado contribuem para a complexidade

do cenário de segurança, ao constituir-se como um elemento facilitador da operação transnacional de redes criminosas.

A resposta a estes desafios requer cada vez mais uma abordagem holística por parte das forças policiais e um esforço contínuo de inovação e adaptação às novas realidades tecnológicas e sociais, visando não apenas combater as manifestações atuais da criminalidade, mas também antecipar e mitigar as ameaças emergentes.

A Guarda Nacional Republicana (GNR), enquanto força de segurança de natureza militar, ocupa uma posição fundamental no espectro da segurança pública e na salvaguarda do Estado de Direito Democrático. Operando num contexto caracterizado pela complexidade e pela constante evolução dos desafios à segurança, a GNR enfrenta a necessidade premente de adaptar e atualizar continuamente as suas estratégias e modelos de atuação.

O modelo de policiamento *Intelligence-Led Policing* (ILP), vulgo Policiamento Orientado pelas Informações, tem ganho alguma proeminência como uma estratégia inovadora na área da segurança pública e no combate à criminalidade. Esta abordagem, que coloca as informações no cerne do processo de tomada de decisão das forças policiais, representa um paradigma significativamente diferente em relação aos modelos tradicionais de policiamento.

A Estratégia da Guarda 2025, bem como os subsequentes pelos Planos de Atividade, reforçam a necessidade de se proceder à melhoria do Sistema de Informações que concorra para uma melhor avaliação das tendências criminais e fenómenos criminais (Guarda Nacional Republicana [GNR], p. 105), no sentido de capacitar a Guarda para a adoção de um policiamento mais proativo, segundo os princípios subjacentes ao ILP (GNR, 2021, p. 113) e adotar as estratégicas mais eficazes no combate à criminalidade (GNR, 2022, p. 15).

Este modelo de policiamento está alinhado com as tendências contemporâneas de modernização e inovação no setor da segurança pública. A GNR, ao incorporar tais práticas, não apenas se coloca na vanguarda das estratégias policiais modernas, mas também demonstra um compromisso com a evolução contínua e com a busca de métodos mais eficientes e eficazes para garantir a segurança da comunidade.

A atualidade e abrangência do tema encerra em si uma complexidade intrínseca que fundamenta a necessidade de uma investigação mais aprofundada. O interesse neste tema justifica-se não apenas pela sua atualidade e relevância no contexto da segurança interna, mas também pela necessidade de compreender

como esta abordagem pode ser eficazmente integrada nas práticas de policiamento existentes na GNR.

O argumento central da investigação é fundado no pressuposto de que o ILP pode constituir-se como uma mais-valia complementar nas estratégias globais de policiamento da GNR. Este paradigma representa uma mudança significativa em relação às abordagens tradicionais, enfatizando a utilização das informações como alicerce fundamental para apoiar o processo de tomada de decisão no âmbito das atividades de policiamento.

A presente investigação tem por objeto de estudo o modelo de policiamento ILP, constituindo-se como o elemento central e a variável dependente. O objetivo geral (OG) da investigação é propor contributos para a implementação do ILP na GNR e deste foram deduzidos os seguintes objetivos específicos: OE1 – identificar as fragilidades e potencialidades do ILP; OE2 – analisar os modelos de policiamento da GNR; OE3 – analisar a influência dos fatores críticos na implementação do ILP na GNR.

A questão central (QC) do trabalho, ou seja, problema da investigação como o elemento orientador de todo o percurso pré-estabelecido, consiste em saber de que forma pode o ILP ser implementado na GNR.

A investigação está organizada em cinco capítulos, desdobrados em secções e subsecções. O primeiro capítulo é dedicado à introdução, que inclui o enquadramento, justificação e delimitação do tema, definição do objeto, dos objetivos e das questões de investigação. O segundo capítulo dá corpo ao enquadramento teórico e conceptual, onde se integra o estado da arte e o modelo de análise. O terceiro capítulo descreve a metodologia e o método, onde se caracterizam os participantes no trabalho de campo e as técnicas de recolha e de análise de dados. Os resultados do trabalho empírico – entrevistas e inquérito por questionário - são apresentados e discutidos no quarto capítulo, para encerrar a parte textual da investigação com as conclusões, que constituem o quinto capítulo.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

No presente capítulo procede-se a uma análise de três aspetos fundamentais que constituem a base conceptual deste trabalho de investigação.

2.1. Informações

Ao longo da sua história, as forças policiais têm integrado as informações no âmbito do desenvolvimento das suas atividades. Todavia, importa salientar

que o conceito de informações é passível de ser interpretado através de diversas definições, as quais exibem variações consideráveis, tendo em conta o contexto, as culturas, os idiomas e as tradições inerentes a cada sociedade.

Especificamente em Portugal, constata-se uma preferência marcada pelo emprego do termo "Informações", em contraposição ao termo "Inteligência", este último mais adotado em contextos anglo-saxónicos, mas também por outras nações como é o caso da França, de Espanha e do Brasil.

As definições tradicionais de informações, apontam para estas como o resultado do processo de análise de notícias. De acordo com o acervo doutrinário da GNR, as informações são definidas como o produto resultante da pesquisa, estudo e interpretação das notícias que aumenta o conhecimento sobre determinado assunto (Escola da Guarda, 2008, p. 3).

A noção de que "notícias + análise = informações" fornece, de facto, uma perspetiva simples que não reflete a complexidade subjacente ao processo de produção de informações. Embora esta fórmula capte a essência básica de que as informações são geradas pela recolha e subsequente análise de dados (notícias), acaba por não refletir a verdadeira essência do processo de produção de conhecimento que servirá de base para a tomada de decisão.

Ratcliffe (2016, p. 71), apoiando-se na abordagem de Davenport (1997), vem propor um *continuum* entre "dados", "informação", "conhecimento" e "informações", conforme se ilustra na figura seguinte.

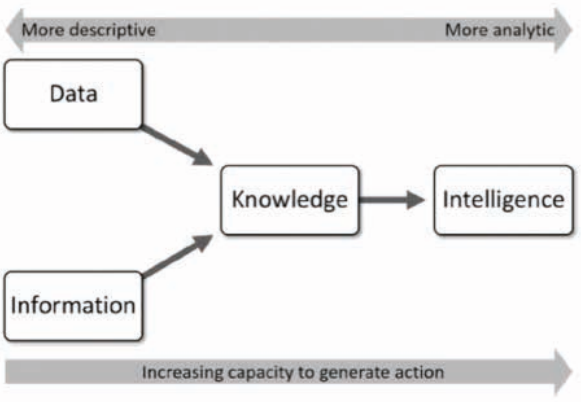

Figura 1 – DIKI (*Data, Information, Knowledge, Intelligence) Continuum*
Fonte: Ratcliffe (2016).

Assim, de acordo com Ractcliffe (2016, p. 71), os **dados** correspondem a observações e medições não interpretadas, incluindo aspetos quantificáveis como relatórios e estatísticas que foram filtrados e categorizados. A **informação** traduz-se em dados contextualizados e dotados de significado, que depois submetidos a técnicas de análise e interpretação, produzem o **conhecimento** sobre um determinado contexto. Este conhecimento servirá de alicerce para a produção de **inteligência** que tem por finalidade apoiar a processo de tomada de decisão.

Tendo em consideração o *continuum* proposto, adotamos para a presente investigação a definição (adaptada) avançada pelo *National Centre for Policing Excellence* (NCPE) do Reino Unido, que vem definir "informações policiais" como o produto final de um processo de produção de conhecimento sobre um determinado contexto, resultante da análise de dados e informações que tem por finalidade apoiar o processo de tomada decisão operacional das forças policiais (NCPE, 2005, p. 196).

2.2. Modelos de policiamento

A fundação da Polícia Metropolitana de Londres por Sir Robert Peel, em 1829, é usualmente apontada pela academia como um marco fundamental na evolução do policiamento moderno, tendo estabelecido a base para as práticas contemporâneas de segurança pública (Dempsey, 2019, p. 4). Referenciado como os "Princípios Peelianos", o policiamento moderno destacou a premissa de que a eficácia policial depende da aceitação pública da autoridade das forças policiais, o que requer não apenas o respeito pelas leis, mas também a aderência a princípios éticos e morais dos agentes da lei no exercício de suas funções.

Os modelos de policiamento podem ser entendidos como abordagens que orientam as forças policiais nos seus esforços para manter a segurança pública, prevenir o crime e promover as suas relações com a comunidade (Rowe, 2013, p. 5). Cada modelo reflete um conjunto de princípios, estratégias e práticas que moldam a forma como a polícia desenvolve as suas atividades e interage com a comunidade.

Os estudos e a literatura especializada em segurança pública tendem a categorizar as abordagens policiais em cinco modelos principais: o policiamento tradicional, o policiamento comunitário ou de proximidade, o COMPSTAT (estatísticas computacionais e estatísticas comparativas), policiamento orientado para o problema e o policiamento orientado pelas informações. Apesar de cada um destes modelos ser delineado por objetivos estratégicos distintos, é amplamente

reconhecido que podem ser eficazmente complementares entre si, quando implementados de forma simultânea e integrada (OSCE, 2017, p. 14).

O modelo de **policiamento tradicional** é indiscutivelmente o mais reconhecido entre os diversos modelos de policiamento, configurando-se como o paradigma padrão na maioria das organizações policiais. Segundo Weisburd e Eck (2004, p. 44), o policiamento tradicional privilegia a visibilidade policial como um mecanismo dissuasório, adotando uma estratégia centrada na identificação e na detenção dos agentes dos crimes cometidos.

De acordo com Ratcliffe (2003, p. 2), os modelos tradicionais, muito centrados na reação, têm-se demonstrado incapazes de conter o aumento dos índices de criminalidade. São frequentemente descritos como modelos de "policiamento orientado para incidentes", pois a força policial tem por finalidade resolver incidentes individualmente considerados, em vez de tentar resolver fenómenos de criminalidade recorrentes (Braga, 2008, p. 9).

Este modelo é fundamentado na convicção de que uma presença policial robusta e a aplicação intransigente da lei contribuem significativamente para a manutenção da ordem pública e para a segurança da comunidade. As estratégias são usualmente reativas e incluem o aumento e a concentração do efetivo policial, patrulhamento ostensivo e uma resposta célere às ocorrências.

O **policiamento comunitário ou de proximidade** emerge como uma das inovações mais significativas e amplamente implementadas no campo da segurança pública ao longo das últimas décadas (Weisburd & Eck, 2004, p. 46). Apesar da sua adoção generalizada, é extremamente difícil encontrar uma definição universal para este modelo.

Moleirinho (2009, p. 26) refere que a dificuldade em encontrar uma definição única para este modelo, emerge dos diversos enquadramentos sociais, organizacionais e culturais. Enquanto a expressão *Community-oriented policing* é predominantemente adotada em contextos anglo-saxónicos, nos países do sul da Europa predomina o termo policiamento comunitário ou de proximidade, que deriva da expressão francesa *Police de proximité* (Moleirinho, 2009, p. 26) ou mesmo, *Policía de Barrio* (Polícia de Bairro), como é designado em Espanha (Romero, 2019, p. 16).

Este modelo de policiamento surge na década de 1970, no Reino Unido, como forma de dar resposta às crescentes preocupações sobre a eficácia dos métodos tradicionais de policiamento (Weisburd & Eck, 2004, p. 46). As suas origens refletem uma mudança no sentido de uma abordagem mais holística, integrada e

cooperativa, centrando-se na construção de relações fortes baseadas na confiança entre a polícia e a comunidade.

As estratégias de policiamento comunitário envolvem frequentemente uma interação regular (muitas vezes para além do contexto de resposta ao crime) entre as forças policiais e a comunidade (Ratcliffe, 2016, p. 50). Estas interações abrangem a implementação de parcerias, que se constituem como um elemento central na promoção de um diálogo construtivo sobre as preocupações comuns relativas às questões relacionadas com a segurança da comunidade (Organização para a Segurança e Cooperação na Europa [OSCE], p. 15). Ao facilitar uma comunicação aberta e contínua, estes fóruns desempenham um papel crucial na construção da confiança mútua e no fortalecimento das relações entre a polícia e a comunidade.

O modelo de policiamento **COMPSTAT** emerge como um ponto de viragem nas práticas de policiamento modernas (Police Executive Forum, 2013, p. 3). O termo resulta da fusão das designações "estatísticas computacionais" e "estatísticas comparativas" e emergiu como um pilar central na estratégia de policiamento de Nova York sob a administração do então "*Mayor*" Rudolph Giuliani (James, 2011, p. 44).

O COMPSTAT baseia-se, essencialmente, num modelo de gestão orientado por dados, o qual enfatiza a importância de recolher, analisar e empregar o resultado de estudos estatísticos para determinar a forma de alocar os recursos policiais. Este modelo envolve representações espaciais do crime em determinadas áreas específicas (Hengsen, 2011, p. 27) e visa assegurar que os esforços de policiamento sejam concentrados nas áreas e nos problemas mais críticos, permitindo alcançar um impacto imediato na redução da criminalidade e na promoção rápida de um ambiente comunitário mais seguro.

O conceito de **Policiamento Orientado para o Problema** (POP) foi inicialmente apresentado por Herman Goldstein em 1979. Este conceito representa uma abordagem inovadora na qual as forças policiais adotam uma postura mais proativa na identificação, análise e abordagem dos problemas da comunidade (Hengsen, 2011, p. 21). Este modelo sugeria uma reorientação estratégica da atuação policial, enfatizando a necessidade de uma abordagem mais focada em resolver as reais causas dos problemas, ao invés de apenas reagir aos seus sintomas (Romero, 2019, p. 17).

Para Weiburd e Eck (2004, p. 46), o POP transcende o paradigma convencional de policiamento, traduzindo-se numa abordagem que se concentra na identificação e resolução sistemática de problemas específicos que contribuem para a ocorrência do crime, desordem social e sentimento de insegurança na comunidade. De acordo com os mesmos autores, tal abordagem evidencia a importância da interdisciplinaridade e da cooperação interagências no contexto da segurança pública, reconhecendo que as soluções para os desafios de segurança transcendem as capacidades e competências tradicionais das forças policiais.

O modelo conceptual do POP é habitualmente sistematizado numa metodologia que se denomina por "SARA Model", um acrónimo para: *Scanning* (identificação dos problemas da comunidade), *Analysis* (análise e compreensão dos problemas), *Response* (desenvolvimento e implementação de respostas operacionais) e *Assessment* (avaliação do impacto das ações implementadas).

De acordo com a perspetiva de Hengsen (2011, p. 23), o POP pode ser considerado como um precursor do ILP, pela adoção sistemática de uma perspetiva analítica como uma componente essencial no processo de identificação, análise e resolução de problemas emergentes.

2.3. *Intelligence-Led Policing*

A utilização das informações pelas forças policiais não é um fenómeno novo. Segundo Schreier (2009, p. 60), esta abordagem ganhou particular destaque no Reino Unido, após o reconhecimento das limitações do modelo de policiamento tradicional, que se mostrou insuficiente perante o aumento da criminalidade.

O modelo de policiamento ILP surgiu inicialmente na Polícia de Kent, no Reino Unido, como uma resposta direta ao aumento da criminalidade contra a propriedade e à crescente exigência da comunidade face à atuação policial (Bureau of Justice Assistance, 2005, p. 9).

O denominado *Kent Police Model*, reconhecido como a primeira aplicação prática do ILP, constituiu um avanço significativo na estratégia de combate ao crime, introduzindo uma nova filosofia focada na antecipação de atividades criminosas por meio de técnicas avançadas de análise criminal. Segundo Mallory (2007, p. 6), a implementação desta abordagem teve como resultado uma redução considerável dos crimes contra a propriedade em Kent, contribuindo ainda para a alocação mais eficiente de recursos policiais.

Apesar do crescente interesse pelo ILP na esfera académica, constata-se a ausência de uma definição consensual que seja universalmente adotada pelos diversos autores.

Schreier (2009, p. 61) afirma que o princípio fundamental do ILP se consubstancia na recolha e análise de informação para produzir um produto de inteligência que é concebido para informar o processo de tomada de decisão.

Para Fuentes (2006, p. 3) o ILP pode ser definido como uma filosofia colaborativa que permite uma melhor compreensão do ambiente operacional, apoiar os decisores no processo de tomada de decisão na formulação de estratégias e/ou definição de ações operacionais de controlo do crime, bem como contribuir para uma maior eficiência na alocação de recursos.

Carter (2009, p. 80) define ILP como o processo de recolha e análise de informações relacionadas com crime e com as condições que contribuem para a ocorrência do crime, resultando num produto de inteligência destinado a auxiliar as forças policiais no desenvolvimento de respostas táticas contra as ameaças e/ou no planeamento estratégico para fazer face às ameaças emergentes.

Para Ratcliffe (2016, p. 66), o ILP enfatiza a importância das informações como ferramenta fundamental para um processo de decisão objetivo, não como um fim em si mesmo, mas como um meio para prevenir e reprimir a criminalidade.

Numa tentativa de sistematizar esta abordagem policial, Ratcliffe (2016, p. 83) sugere o Modelo 4-i (conforme se ilustra na figura seguinte), no qual o autor pretendeu explicar os papéis e a relação entre as principais componentes do conceito de ILP, conforme se ilustra na figura seguinte.

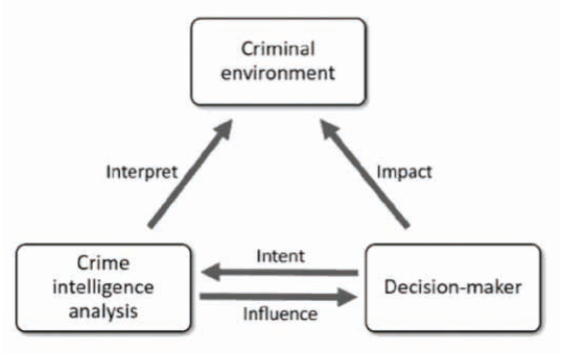

Figura 2 – Modelo 4i ou Modelo de Ratcliffe
Fonte: Ratcliffe (2016).

O Modelo 4-i evoluiu a partir do seu modelo original, o Modelo 3i, ao adicionar a "intenção" por forma a refletir a importância da orientação estratégica para o processo de produção de informações, para que as informações produzidas estejam alinhadas com as prioridades da organização policial. De acordo com Ratcliffe (2016, p. 83), o decisor policial passa a ter um papel mais ativo no sistema, sendo que a sua experiência em contexto de ILP desempenha um papel fundamental na otimização do processo de produção de informações e consequente eficácia deste modelo de policiamento.

De acordo com Ratcliffe (2016, p. 82), o **ambiente criminal** é um elemento dinâmico e refere-se ao conjunto composto pelo espaço físico e pelas condições sociais que moldam a natureza e a extensão da criminalidade, devendo a sua análise ser contextualizada em função do nível de decisão - local, regional ou nacional.

A **análise de inteligência criminal,** conforme descrita por Ratcliffe (2016, p. 82), é um processo sistemático que envolve a produção de informações sobre uma realidade específica do ambiente criminal, com o objetivo de apoiar o processo de tomada de decisão operacional. Esta análise procura uma compreensão detalhada dos padrões e tendências da criminalidade, assim como das condições subjacentes que contribuem para os problemas de segurança de uma determinada comunidade.

Os **decisores policiais**, tipicamente os comandantes operacionais, constituem-se como elementos-chave, pois compete-lhe a decisão sobre as estratégias a implementar para criar um impacto positivo no ambiente operacional (Ratcliffe, 2003, p. 4).

O Modelo 4i realça ainda, a interação entre os quatro elementos principais: intenção, interpretação, influência e impacto (Ratcliffe, 2016, pp. 82-83). A "**intenção**" refere-se à definição de objetivos estratégicos que guiam a produção de informações. A "**interpretação**" é o processo de análise crítica das informações para entender os problemas de segurança que afetam um determinado ambiente operacional. A "**influência**" diz respeito à capacidade das informações de orientar a tomada de decisão na antecipação dos desafios e na formulação das melhores estratégias para debelar os problemas de segurança da comunidade. E por fim, o "**impacto**" que se traduz na avaliação dos efeitos produzidos pelas estratégias implementadas sobre o ambiente criminal.

Para Ratcliffe (2016, p. 67), este modelo é ainda capaz de incorporar áreas de atuação policial que não estão diretamente relacionadas com a criminalidade, mas que ainda assim constituem problemas para a comunidade e para as forças policiais.

Assim, este paradigma coloca as informações no epicentro de praticamente todas as áreas de atuação das forças policiais, enfatizando a importância de uma colaboração estreita e contínua entre o órgão de produção de informações e os decisores policiais (OSCE, 2017, p. 19).

Neste sentido, para efeitos do presente estudo, adotamos a definição de ILP apresentada por Ratcliffe na sua versão mais abrangente, ou seja, considerando que a aplicação deste modelo não se esgota no campo da criminalidade, podendo ser aplicado a todas as áreas de atuação policial.

Assim, define-se ILP como uma abordagem policial que se traduz na aplicação da análise de informações como uma ferramenta objetiva do processo de decisão para a formulação de estratégias de prevenção e antecipação dos problemas operacionais que afetam as forças policiais e as comunidades que servem.

2.4. Modelo de análise

No quadro seguinte apresenta-se o modelo de análise.

Quadro 1 – Modelo de Análise

<table>
<tr><td>Objetivo Geral</td><td colspan="5">Propor contributos para a implementação do Intelligence-Led Policing (ILP) na GNR</td></tr>
<tr><td rowspan="2">Objetivos Específicos</td><td>Questão Central</td><td colspan="4">De que forma podem ser implementados na GNR os contributos do ILP?</td></tr>
<tr><td>Questões Derivadas</td><td>Conceitos</td><td>Dimensões</td><td>Indicadores</td><td>Técnica de recolha de dados</td></tr>
<tr><td>OE1
Identificar as fragilidades e potencialidades do ILP</td><td>QD1
Quais as principais fragilidades e potencialidades do ILP</td><td>ILP</td><td rowspan="3">Estratégica

Operacional

Tática</td><td>Apoio à decisão
Atuação direcionada
Alocação de recursos
Prevenção/ Antecipação
Proteção dados pessoais
Princípios éticos</td><td rowspan="3">Entrevistas exploratórias

Entrevistas semiestruturadas

Inquérito por questionários</td></tr>
<tr><td>OE2
Analisar os modelos de policiamento da GNR</td><td>QD2
Como se caracterizam os modelos de policiamento da GNR?</td><td>modelos de policiamento</td><td>Modelo tradicional
Comunitário & próximidade
COMSTAT
Orientado para o problema</td></tr>
<tr><td>OE3
Analisar a influência dos fatores críticos na implementação do ILP na GNR</td><td>QD3
De que forma os fatores críticos influenciam a implementação do ILP na GNR?</td><td>ILP</td><td>Capacidade analítica Tecnologia
Processo de decisão Formação
Lideranças
Cultura organizacional</td></tr>
</table>

3. METODOLOGIA E MÉTODO

Opta-se pela combinação de "estratégias quantitativas e qualitativas, de modo a capitalizar as potencialidades e a colmatar as vulnerabilidades de cada uma delas" (Santos & Lima, 2019, p. 30), seguindo uma estratégica mista, através da utilização de várias técnicas de recolha de dados. Adota-se como *Research Design* o estudo de caso, porque com a investigação procura-se "recolher informação detalhada sobre uma única unidade de estudo, podendo essa unidade ser o indivíduo, a comunidade ou até mesmo a nação" (Santos & Lima, 2019, p. 36), no caso concreto a unidade de estudo é a Guarda Nacional Republicana num estudo transversal. São variáveis independentes os "modelos de policiais", as "informações (capacidade analítica)", a "tecnologia", o "processo-decisão" e a "formação" OSCE (2017, pp. 42-43) e por Pascal Gemke (2017, pp. 26-32).

Elegeu-se a população e, dentre esta, optou-se por uma amostra não probabilística recorrendo-se a especialistas para obtenção da informação, como se apresenta no quadro 2.

Quadro 2 – Participantes e procedimento

Nível de Decisão	População / Participantes	Estratégia de Investigação	Técnicas de Recolha de Dados
Estratégico	Comandante-geral 2º Comandante-geral	Qualitativa	Entrevistas semiestruturadas
Operacional	Comandante operacional Chefe do departamento de operações Diretor de Informações Diretor da Investigação Criminal Oficiais do Comando Operacional		
Tático	Comandantes de Comando Territorial 2.º Comandante de Comando Territorial Chefes da Secção de Operações, Treino e Relações-públicas Chefes das Secções de Informações e Investigação Criminal Chefes das Secções SEPNA	Quantitativa	Inquérito por questionário

Os principais instrumentos de recolha de dados compreenderam a análise documental, a realização de entrevistas semiestruturadas e a realização de um inquérito por questionário. A análise documental baseou-se em obras e artigos científicos de referência sobre a temática em estudo. Foram elaboradas entrevistas exploratórias, como elementos preliminares e de rutura. Posteriormente foram

elaborados dois guiões de entrevista que foram aplicados a uma amostra-teste, durante o mês de fevereiro de 2024, tendo por finalidade a sua validação para aplicação à amostra definitiva. As entrevistas foram realizadas durantes os meses de fevereiro e março de 2024.

O questionário foi elaborado no *Google Forms*, que depois de validado numa amostra reduzida, foi aplicado, durante o mês de março de 2024, a oficiais dos 18 Comandos Territoriais do Continente, mais concretamente aos Comandantes, 2º Comandantes, Chefes das Secções de Operações Treino e Relações-Públicas, Chefes das Secções de Informações e Investigação Criminal e Chefes das Secções de SEPNA. O questionário é constituído por 60 questões (58 questões fechadas e duas questões abertas), distribuídas por quatro partes, conforme se ilustra no quadro 4. A percentagem de respostas ao inquérito por questionário cifrou-se nos 85% dos 82 oficiais inquiridos.

Quadro 3– Organização do questionário

Partes	Questões	Totais
Caracterização da amostra	6 Questões (idade, género, habilitações literárias, posto, função e tempo na função)	6
Modelos de Policiamento no Dispositivo Territorial	1-7	7
Potencialidades e Fragilidades do ILP	8-21	14
ILP no Dispositivo Territorial	22-53	33

Para o tratamento das entrevistas utilizou-se a técnica de análise de conteúdo, percorrendo as fases de análise, codificação e categorização. Para o efeito, constituiu-se um quadro resumo de análise, no qual se identificam os principais segmentos dos indicadores, presenças e percentagens.

Na análise do inquérito por questionário utilizou-se o software IBM *Statistical Package for the Social Sciences* (SPSS) para obtenção das estatísticas mais comuns, nomeadamente médias, desvios, modas e correlações, representadas por quadros e gráficos.

Ao longo do processo de análise de dados, foram sinalizados pontos fortes, pontos fracos, ameaças e oportunidades que serviram de base para uma posterior análise SWOT, com a finalidade de deduzir possíveis medidas/estratégias para a efetiva implementação do ILP na GNR.

4. APRESENTAÇÃO DOS DADOS E DISCUSSÃO DOS RESULTADOS

Neste capítulo apresentam-se os dados, a análise e discussão dos resultados.

4.1. Potencialidades e fragilidades do ILP

Neste subcapítulo apresentam-se os dados relativos ao estudo da variável dependente, mais concretamente no que concerne às potencialidades e fragilidades do ILP para as operações policiais.

Da análise às entrevistas resulta que todos os entrevistados concordam que o ILP se traduz numa abordagem policial adequada para fazer face aos desafios operacionais da atualidade sendo apontadas como principais potencialidades pela maioria dos entrevistados e inquiridos o aumento da eficiência e eficácia policial; a otimização na alocação dos recursos operacionais; o apoio ao processo de tomada de decisão, permitindo a diminuição da incerteza e uma atuação mais direcionada para fazer face aos principais problemas operacionais; o incremento da capacidade de antecipação e prevenção dos problemas operacionais, pela identificação prévia das principais tendências e fenómenos criminais.

Como principais fragilidades, os entrevistados e inquiridos referenciaram: a necessidade de incrementar a capacidade analítica da estrutura de informações da Guarda; a necessidade de tecnologia avançada para a análise de grande volume de dados e os custos associados à aquisição dessa tecnologia.

Relativamente à fragilidade relacionada com eventuais violações dos direitos, liberdades e garantias, bem como a não observância das normas relacionadas com a proteção de dados pessoais, pela implementação do modelo, constata-se uma discordância nos resultados obtidos na entrevista quando comparados com os resultados do questionário.

Esta tendência discordante é também evidente relativamente ao risco de distorções de julgamento ou preconceitos relativamente a determinados indivíduos ou grupos de indivíduos.

Decorrente da análise e em resposta à QD1, conclui-se que o modelo ILP é considerado uma abordagem policial adequada para os desafios operacionais contemporâneos, contribuindo para uma maior eficácia e eficiência operacionais, através da otimização na alocação de recursos operacionais e do apoio incontornável ao processo de tomada de decisão para uma maior capacidade de antecipação

e prevenção dos problemas operacionais. Contudo, constatam-se algumas fragilidades, como a necessidade de melhorar a capacidade analítica associada ao processamento de análise de grandes volumes de dados, bem como os custos associados à aquisição de ferramentas tecnológicas. Apesar de ter sido revelada uma discordância entre os resultados das entrevistas e do questionário, inferem-se algumas preocupações com possíveis violações de direitos individuais, relacionadas com a proteção de dados pessoais e o risco de distorções de julgamento sobre determinados grupos ou comunidades.

4.2. Modelos de policiamento na GNR

Neste subcapítulo apresentam-se os dados relativos aos modelos de policiamento da GNR (variável independente). Pretendeu-se com as questões da entrevista e do questionário identificar a proeminência dos modelos de policiamento descritos no subcapítulo 2.2.

Da análise podemos constatar que a maioria (n=9) dos entrevistados caracteriza o modelo de policiamento da GNR como um modelo eminentemente reativo. De acordo com o B. Rocha (entrevista por email, 30 de março de 2024), "[...] existe muita predominância de um modelo mais reativo [...] caracterizando-se, no essencial, nas respostas operacionais da Guarda às ocorrências inopinadas [...]".

O modelo comunitário e de proximidade é também referido por 90% dos entrevistados, sendo que dois dos entrevistados referem que existem claras orientações políticas para o desenvolvimento deste modelo. R. Veloso (entrevista por email, 14 de março de 2024) refere que "[...] este modelo é consubstanciado numa base pró-ativa, alicerçada no reforço da presença policial com vista à aproximação ao cidadão".

Relativamente ao POP, é referenciado por 60% dos entrevistados. O modelo COMPSTAT é referido (indiretamente) apenas por P. Silvério (entrevista por *email*, 15 de março de 2024), ao afirmar que a Guarda "[...] analisa os dados, identifica tendências, períodos do dia de maior probabilidade de ocorrências e "zonas quentes" da criminalidade [...] para a priorização e emprego de forças".

Apesar de se inferir da maioria das entrevistas que o ILP ainda não está efetivamente implementado, 60% dos entrevistados reconhece que a Guarda desenvolve este modelo de forma complementar a outros modelos. De acordo com o R. Veloso (*op. cit.*), "[...] o ILP constitui uma abordagem complementar a outros modelos de policiamento, configurando, na sua génese [...] a identificação

de fenómenos emergentes, sobre os quais impende uma necessidade de resposta operacional multinível [...] em conjugação com outros modelos de policiamento".

Pese embora resultar uma discordância dos inquiridos relativamente ao facto de o patrulhamento ser efetuados por patrulhas aleatórias, sem um foco específico pré-definido (M=2), podemos constatar que cerca de 43% dos inquiridos considera que a Unidade adota uma abordagem reativa às ocorrências (M=4), que se constitui como um dos elementos caracterizadores do policiamento tradicional.

Esta concordância é ainda confirmada pela análise das respostas, da qual resulta a concordância que o sucesso das atividades de policiamento da unidade ser determinado, quer pelo aumento crimes participados e detenções efetuadas (M=4), quer pela reação tempestiva às ocorrências (M=4).

Assume ainda especial relevo o policiamento comunitário e de proximidade, na medida em que cerca 87% dos inquiridos concorda que se privilegia a construção de laços de colaboração com as comunidades locais, promovendo o estabelecimento de parcerias para a resolução de problemas que afetam essas comunidades. Tal tendência é ainda confirmada pela análise da questão.

No que concerne ao policiamento orientado para o problema, verifica-se que, no desenvolvimento da atividade operacional, se assume uma estratégia proativa centrada na identificação e análise dos principais problemas operacionais, no sentido de implementar as melhores medidas para a sua resolução (M=4). Esta concordância generalizada é ainda confirmada pelos resultados obtidos na análise.

Tal tendência concordante verifica-se também, no que refere ao modelo COMPSTAT (M=4), na qual 54,3% dos inquiridos concorda que o policiamento é caracterizado por uma abordagem essencialmente orientada por dados estatísticos para identificar os locais com maior concentração de ilícitos criminais, tendo em vista a redução rápida dos índices de criminalidade (M=4)

Relativamente ao ILP e como resulta da análise, a maioria dos inquiridos concorda (61,4%) que se enfatiza a análise de informações para planear e orientar as atividades operacionais, garantindo-se uma intervenção direcionada e uma alocação de recursos mais eficiente.

Da análise dos resultados e em resposta à QD2, conclui-se a predominância do modelo de policiamento reativo na GNR, pese embora o modelo de policiamento comunitário assuma especial relevo, ao ser referenciado pela esmagadora maioria dos entrevistados e inquiridos. O modelo POP e o modelo COMPSTAT foram menos mencionados, mas reconhecidos por alguns entrevistados como uma abordagem

policial proativa em determinadas situações. Concluiu-se ainda que o modelo ILP, embora não totalmente implementado, é adotado de forma complementar aos outros modelos, destacando-se a sua importância na identificação e resposta a tendências e fenómenos criminais emergentes. Em resumo, a GNR tende a equilibrar modelos reativos e proativos, com uma crescente aposta na análise de informações e envolvimento das comunidades.

4.3. Fatores críticos para a implementação do ILP

Neste subcapítulo apresentam-se os dados relativos ao estudo dos fatores críticos para a implementação do ILP na GNR.

4.3.1. As informações e a capacidade analítica

Seguidamente, apresentam-se os dados obtidos e discutem-se os resultados da análise das entrevistas e do questionário no que concerne à variável independente informações e a capacidade analítica.

Da análise resulta que a maioria dos entrevistados (n=7) considera que a atual capacidade analítica da estrutura de informações tem respondido às necessidades gerais de informações.

Importa realçar a referência ao desenvolvimento em curso do Sistema de B*usiness Intelligence* Policial, que segundo o B. Baraças (entrevista por *email*, 27 de março de 2024), "[...] assentará na ligação automática dos dados dos sistemas de informações operacionais a um *software* de análise (já adquirido), que congrega as capacidades de retrospetiva, predição e cenarização.

Da análise dos resultados, resulta que 92,9% dos inquiridos demonstra concordância relativamente ao facto de as decisões, quando baseadas em informações, produzirem melhores efeitos na resolução dos problemas operacionais que afetam a Unidade.

Apesar da maioria dos inquiridos considerar que as informações são determinantes para o desenvolvimento da atividade operacional, apenas 32,9% dos inquiridos concorda que as Secções de Informações e Investigação Criminal (SIIC) possuem capacidade analítica para produzirem informações de qualidade sobre os fenómenos criminais.

Pode ainda inferir-se que as SIIC não têm capacidade para produzir informações sobre todas as áreas de atuação da Unidade (M=2) e que a maioria dos seus recursos está dedicada a produzir informações no âmbito de processos de inquérito criminais atribuídos. Neste sentido, importa ainda referir que a maioria dos inquiridos considera que efetiva implementação do ILP requer um aumento do número de militares especializados em análise de dados e informações (M=4).

4.3.2. A tecnologia

De seguida, apresentam-se os dados obtidos e discutem-se os resultados da análise das entrevistas e do questionário no que concerne à variável independente tecnologia. Dos resultados da entrevista, resulta que 40% dos entrevistados considera que a estrutura das informações se encontra tecnologicamente preparada para a implementação do ILP, ainda que se seja necessário um investimento adicional em ferramentas aplicacionais de análise, acompanhada da respetiva formação especializada.

Destaca-se que 90% dos entrevistados considera que a integração da inteligência artificial pode potenciar a implementação do ILP, pois como refere P. Silvério (op. cit) "[...] com a integração da Inteligência Artificial surgem novas capacidades preditivas resultantes da rápida análise de *Big Data*".

Da análise pode inferir-se que que a maioria dos inquiridos considera que existe a necessidade de introduzir novas ferramentas tecnológicas, para melhorar o processo de produção de informações das SIIC. Os inquiridos tendem a discordar com a adequação e eficácia das ferramentas tecnológicas disponíveis na análise e processamento de grandes volumes de dados.

Importa ainda referir que a maioria dos inquiridos considera que a implementação dos vários sistemas de informação da Guarda tem contribuído para uma melhoria na produção de informações no dispositivo territorial.

4.3.3. O processo de decisão

Seguidamente, apresentam-se os dados obtidos e discutem-se os resultados da análise das entrevistas e do questionário no que concerne à variável independente processo de decisão.

Resulta da análise das entrevistas que os produtos de informações são integrados, quer na formulação estratégica (n=2), quer no âmbito do planeamento de operações, através da integração do anexo de informações em todas as diretivas

operacionais, de avaliações de segurança e risco ou de relatórios de notícia ou informação.

As necessidades de informações são regularmente transmitidas de forma descendente em razão da matéria. Segundo R. Veloso (op. cit), "[...] as questões relacionadas com os fenómenos emergentes são remetidas ao Comando Operacional para apresentar os respetivos produtos informacionais". De acordo com mesmo entrevistado, "[...] no âmbito das atividades correntes, releva a importância a monitorização da atividade operacional efetuada diariamente pelo Centro Integrado Nacional de Gestão de Operações [...]", sendo que "[...] as necessidades de informação, quando se mostre necessário, são transmitidas no *briefing* diário, tendo em vista a sua integração no processo de tomada de decisão".

Em termos gerais, podemos inferir que as informações são integradas no processo de decisão operacional. A maioria dos inquiridos concorda que o comando da Unidade transmite regularmente as suas necessidades de informações e estas têm a capacidade de influenciar positivamente o processo de decisão operacional.

A SIIC é normalmente envolvida no processo de planeamento de operações da Unidade, sendo este envolvimento determinante para o desenvolvimento da atividade operacional.

A maioria dos inquiridos (61,4% concorda e 30% concorda totalmente) considera que a integração das informações no processo de decisão contribui para a alocação mais eficiente dos recursos operacionais.

4.3.4. A formação

De seguida, apresentam-se os dados obtidos e discutem-se os resultados da análise das entrevistas e do questionário no que concerne à variável independente formação.

Da análise decorre que a formação assume um papel importante para a implementação do ILP. A maioria dos entrevistados considera que devem ser desenvolvidas ações de formação transversais a todas as categorias profissionais da Guarda, devendo ser integrados conteúdos programáticos de ILP nos cursos de formação, promoção e qualificação. Como refere P. Silvério (op. cit.), a efetiva implementação do ILP implica um "[...] investimento nos recursos humanos através da formação [...]" e, de acordo com R. Veloso (op. cit), passa pelo desenvolvimento de "[...] processos de formação específicos nos Planos Anuais de Formação [...]".

Os resultados apontam para uma concordância generaliza sobre a necessidade de melhorar a formação em ILP.

A maioria dos inquiridos considera que a falta de formação em ILP limita a eficácia deste modelo , sendo que 77,2% dos inquiridos concorda que esta formação deve ser uma prioridade para todos os níveis e 84,3% defende que a integração da formação em ILP nos currículos de formação base e de progressão é fundamental para promover a efetiva implementação do ILP.

4.3.5. Estrutura, envolvimento das lideranças e cultura organizacional

Seguidamente, apresentam-se os dados obtidos e discutem-se os resultados da análise a outros aspetos relevantes, no que concerne à estrutura, o envolvimento das lideranças e à cultura organizacional atinentes para efetiva implementação da abordagem ILP.

A maioria dos entrevistados considera que as informações deverão ter uma estrutura autónoma ao nível tático, à semelhança do que acontece ao nível operacional. De acordo com R. Bailote (entrevista por *email*, 27 de março de 2024) quando se refere a junção das informações com a investigação criminal na mesma estrutura, afirma que tal facto "[...] reduz a papel das informações à investigação criminal". Para alguns dos entrevistados, esta autonomização pode ser conseguida "[...] dividindo os atuais Núcleos de Análise de Informações e Informação Criminal em dois núcleos diferenciados", como refere B. Baraças (op. cit.).

Pode-se ainda verificar, que 60% dos entrevistados considera que a criação de um *Fusion Centre* ao nível operacional, se traduz numa mais-valia para a implementação do ILP, por permitir a integração das informações provenientes das várias valências de atuação.

Pode-se ainda inferir-se que a maioria dos entrevistados considera que envolvimento das lideranças é determinante para a efetiva implementação do ILP, sendo necessário que o modelo seja assumido em toda a estrutura da Guarda.

Quanto à cultura organizacional, alguns dos entrevistados consideram que tem sido potenciada uma "cultura de informações" no seio da Guarda, e que a atual cultura organizacional facilita a implementação do modelo, existindo, no entanto, a necessidade de uma clara aposta na divulgação da importância do modelo no âmbito dos processos de comunicação interna.

Da análise às questões do questionário, importa realçar que, apesar das posições estarem muito divididas ao nível tático, 27,1% dos inquiridos discorda e 25,7% discorda totalmente que a estrutura atual das SIIC favorece o desenvolvimento do ILP em todas as áreas de atuação operacional da Unidade. Esta tendência é confirmada pelo facto de a maioria dos inquiridos concordar que as componentes de informações e investigação criminal deveriam estar organicamente separadas para evitar o foco excessivo na resolução de casos criminais específicos.

Relativamente ao envolvimento das lideranças, releva-se que cerca de 88% dos inquiridos manifesta a sua concordância com o facto de o sucesso na implementação do ILP estar substancialmente dependente do apoio e comprometimento das lideranças a todos os níveis da organização.

Quanto à cultura organizacional, a maioria dos inquiridos concorda que a efetiva implementação do ILP requer mudanças na cultura organizacional da Unidade, particularmente na valorização das informações como eixo central do planeamento e do processo de decisão operacional e que a resistência à mudança se constitui um desafio para a efetiva implementação do ILP.

4.4. Análise SWOT

Como referido anteriormente, da revisão bibliográfica e da análise dos resultados das entrevistas e do questionário, extraíram-se alguns elementos para a sistematização de uma análise SWOT, nomeadamente os que resultam da análise do ambiente interno - pontos fortes (S) e pontos fracos (W) - e os que decorrem do ambiente externo - ameaças (T) e oportunidades (O). Nos quadros seguintes, apresenta-se a sistematização desses elementos nos quadrantes da matriz SWOT, que servirão de base para a formulação das Linhas de Orientação Estratégica (LOE) para a efetiva implementação do ILP na Guarda.

4.4.1. Análise do ambiente interno

Na tabela seguinte, apresentam-se os principais pontos fortes e pontos fracos identificados durante a investigação.

Tabela 4 – Ambiente interno

Pontos fortes (S)	Pontos fracos (W)
S1 - Ampla cobertura territorial	W1 - Capacitação analítica limitada
S2 - Diversas áreas de atuação	W2 - Estrutura de informações com baixo nível de integração do conhecimento e limitado interfacd entre as diferentes valências
S3 - Estrutura hierarquizada e disciplina organizacional	W3 - Estrutura de informações dimensionada para a análise de informação criminal ao nível tático
S4 - Estrutura das informaçºoes transversal a yodos os níveis de decisão	W4 - Sistemas de informação com limitada capacidade de análise e sem capacidade preditiva
S5 - Presença de uma "cultura de informações" organizacional aberta à mudança decorrente de diversas transformações organizacionais anteriores	W5 - Quantidade e qualidade de dados insuficiente nos sistemas de informação
S6 - Capacidades crescentes dos sistemas de informação	W6 - Limitada afetação de recursos humanos à estrutura de informações
S7 - Compromisso com a inovação e modernização	W7 - Carência de formaçºao de ILP em todos os níveis de organização
S8 - Valorização da formação e capacitação contínuas	W8 - Insuficiente formação especializada em ferramentas de análise
S9 - Proximidade e forte ligação à comunidade	W9 - Resisitência à mudança
S10 - Cooperação permanente em congéneres e outras agências policiais internacionais	W10 - Constrangimentos orçamentais

4.4.2. Análise do ambiente externo

As principais oportunidades e ameaças identificadas são apresentadas na tabela seguinte.

Tabela 5 – Ambiente externo

Oportunidades (O)	Ameaças (T)
O1 - A natureza global do crime facilita a colaboração internacional e oferece uma oportunidade para expandir parcerias internacionais na partilha de informações	T1 - Complexidade do ambiente de segurança, com assimetrias sociais, evolução demográfica e progressiva urbanização da área de atuação da Guarda
O2 - A emergência de novos desafios de segurança, como o cibercrime e criminalidade transacional, pode ser uma oportunidade para a a GNR desenvolver e implementar soluções de ILP	T2 - Fenómenos criminais associados às novas tecnologias
O3 - Os avanços tecnológicos e o desenvolvimento de novas tecnologias de análise de informações, especialmente na análise de Big Data	T3 - A dependência crescente de sistemas de informação e bases de dados expões as operaçõespoliciais a riscos de ataques cibermétícos e violações de dados
O4 - Mudança de paradigmas associados ao crescente desenvolvimento da inteligência artificial	T4 - Âmbito de atuação alargado a outras dimensões operacionais - controlo de fronteiras

[Cont.]

O5 - Exploração dos domínios subjacentes à utilização do espaço aéreo, marítimo, terrestre e ciberespaço	T5 - Deficiente interoperabilidade entre os sistemas de informação
O6 - Crescente reconhecimento do valor das informações na segurança pública	T6 - Limitações éticas e legais podem limitar a capacidade e a eficácia do ILP
O7 - Crescente consciencialização pública sobre segurança	T8 - Escrutínio externo permanenge face à atuação operacional
O8 - Cooperação sobre o setor privado e com a academia	T9 - Limitações orçamentais
O10 - Acesso a fundos estruturais de investimento	

4.4.3. Linhas de orientação estratégica

Da análise do ambiente interno e externo, deduziram-se as seguintes linhas de orientação estratégica, para maximizar as pontos fortes e oportunidades e para mitigar os pontos fracos e ameaças associadas efetiva implementação do ILP: **LOE 1 - Investimento em tecnologia e análise de dados** - investir em tecnologia de ponta para melhorar a capacidade de análise, incluindo ferramentas com capacidade preditiva e de análise de *Big Data;* implementar soluções de Inteligência Artificial com capacidade de grande volume de dados, para a identificação proativa de padrões e tendências de criminalidade, bem como outros riscos e ameaças à segurança; garantir a qualidade dos dados, através da implementação de procedimentos e protocolos rigorosos, que garantam a precisão, a integridade e a atualidade dos dados introduzidos nos sistemas de informação. **LOE 2 - Desenvolvimento de competências e capacitação** - implementar programas de formação especializada contínua para desenvolver as capacidades analíticas na estrutura de informações; introdução de conteúdos programáticos sobre ILP nos cursos de formação de base, de promoção e de especialização; criação de um *Fusion Centre* dedicado à avaliação contínua de ameaças em todas as áreas de atuação da Guarda e à adaptação das estratégias de ILP; autonomização das Informações ao nível tático, sem prejuízo da sua ligação à estrutura investigação criminal. **LOE 3 - Cibersegurança e gestão da privacidade -** implementar medidas de cibersegurança para garantir a integridade e privacidade das informações contra os ataques cibernéticos externos; estabelecer políticas claras e mecanismos de supervisão para o uso de dados, assegurando a conformidade com a legislação de proteção de dados e com os princípios éticos-policiais. **LOE 4 - Fomentar a Colaboração e as Parcerias** - incrementar a colaboração

com outras agências e fortalecer a colaboração, tanto a nível nacional quanto internacional, para a partilha de informações e desenvolvimento de uma resposta coordenada e integrada, face às ameaças transnacionais; estabelecer parcerias com instituições académicas, empresas de tecnologia e outras organizações para o desenvolvimento e melhoria das ferramentas tecnológicas de análise; fortalecer a relação com a comunidade para melhorar a perceção pública da atividade policial e incentivar a cooperação na partilha tempestiva de informações. **LOE 5 - Adaptação estratégica e flexibilidade** - estabelecer sistemas de monitorização e avaliação permanente para ajustar estratégias e táticas baseadas no *feedback* operacional e nas mudanças no ambiente operacional; selecionar áreas específicas para implementação inicial de projetos piloto de ILP, permitindo vencer a resistência à mudança e demonstrar gradualmente as potencialidades do ILP; explorar oportunidades de financiamento externo, incluindo parcerias público-privadas e fundos da União Europeia, para apoiar projetos decorrentes da implementação do ILP; assegurar o envolvimento das lideranças em todos os níveis da organização, através da demonstração de um compromisso claro com os princípios e práticas do ILP.

4.4.4. Síntese conclusiva

Da análise efetuada e em resposta à QD3, pode-se concluir que as informações estão cada vez mais presentes no planeamento da atividade operacional, com a consequente influência positiva na melhoria das decisões operacionais. No entanto, conclui-se que subsistem desafios significativos relacionados com a capacidade analítica da estrutura de informações, que carecem desta capacidade para abordar a totalidade das áreas de atuação da GNR, relevando-se a necessidade de reforçar esta estrutura com recursos humanos especializados em análise de informações para a implementação efetiva do ILP.

Embora se reconheçam os avanços em termos de tecnologia e sistemas de informação operacional, conclui-se que se torna imperioso um investimento adicional em novas ferramentas tecnológicas e formação especializada para potencializar a eficácia na análise de grandes volumes de dados e melhorar a produção de informações.

Pode ainda concluir-se que as informações são integradas no processo de decisão estratégico, operacional e tático, sendo largamente reconhecido o seu valor para uma atuação direcionada e para uma alocação de recursos mais eficiente.

Quanto à formação, conclui-se pela necessidade crítica de melhorar a formação em ILP, em todas as categorias profissionais da Guarda, relevando-se a importância da integração de conteúdos programáticos de ILP para a efetiva implementação do modelo.

Conclui-se ainda, que existe a necessidade de reformar a estrutura organizacional das SIIC, destacando-se a importância de uma separação funcional entre as informações e investigação criminal no sentido de promover a efetiva implementação do ILP. O envolvimento das lideranças em todos os níveis de decisão torna-se fundamental, bem como a promoção de uma cultura organizacional que valorize as informações, no planeamento e no processo de decisão operacional, para superar algumas resistências à mudança e para a efetiva implementação do modelo.

A análise SWOT conduziu à formulação de Linhas de Orientação Estratégica (LOE) para a implementação do ILP na Guarda, visando capitalizar pontos fortes e oportunidades enquanto mitiga pontos fracos e ameaças. As LOE consubstanciam a resposta à QC e incluem o investimento em tecnologia avançada de análise de informações, desenvolvimento de competências através de formação contínua, reforço da cibersegurança e salvaguarda dos direitos de privacidade, promoção de colaborações e parcerias nacionais e internacionais, e a adaptação estratégica com flexibilidade, selecionando áreas específicas para implementação inicial de projetos piloto de ILP.

5. CONCLUSÕES

No contexto atual, as forças policiais deparam-se com desafios de segurança cada vez mais complexos, resultantes de um ambiente de segurança cada vez mais volátil, incerto, complexo e ambíguo. A globalização e os avanços tecnológicos têm facilitado a expansão das atividades criminosas que, muitas vezes, ultrapassam fronteiras nacionais e desafiam as capacidades convencionais de aplicação da lei.

A generalizada livre circulação de pessoas e bens na União Europeia, apesar dos seus inegáveis benefícios para os estados-membros, facilita igualmente a operação transnacional de redes criminosas. Portugal, com a sua localização periférica na Europa e com as extensas fronteiras marítimas, enfrenta desafios muito específicos, incluindo o tráfico de drogas e a imigração ilegal, para além de questões de segurança interna comuns a todo o espaço europeu.

Para abordar eficazmente estes desafios, torna-se imperioso que as forças de segurança adotem metodologias inovadoras que transcendam os modelos

tradicionais policiamento que se têm demonstrado desajustados para debelar eficientemente estas novas ameaças. A adoção de estratégias que integrem tecnologias avançadas, a partilha e análise de informações, possibilita uma resposta mais efetiva aos fenómenos criminais, para além de contribuir para a sua prevenção e antecipação.

Neste contexto, destaca-se o modelo de ILP, que coloca a utilização das informações como pilar central para todas as atividades policiais. Ao contrário do policiamento tradicional, que frequentemente reage aos eventos post factum, o ILP procura antecipar e prevenir a criminalidade e os demais problemas operacionais, através da compreensão mais abrangente das causas que lhe estão subjacentes, bem como através da identificação de padrões e da antecipação de tendências de ameaças potenciais.

A investigação foi desenvolvida com o objetivo de propor contributos para a implementação do modelo ILP na GNR, tendo por base o argumento que este modelo constitui uma abordagem complementar que pode trazer mais-valias ao desenvolvimento da atividade operacional da organização.

O procedimento metodológico adotado baseou-se numa articulada combinação de técnicas de recolha e análise de dados, concorrentes para os objetivos do estudo e com a finalidade de dar resposta ao problema e às questões da investigação.

A amostra foi definida para abranger diversos níveis de decisão, ganhando corpo no Comando da Guarda (nível estratégico), em oficiais do Comando Operacional nas áreas de operações, informações e investigação criminal (nível operacional) e nos oficiais do dispositivo territorial do Continente (nível tático).

Os instrumentos de recolha de dados incluíram a análise documental, entrevistas semiestruturadas e inquéritos por questionário. As técnicas de análise de dados englobaram a análise de conteúdo para as entrevistas e a aplicação do *software IBM SPSS* para a análise os questionários, que garantiram rigor e cientificidade aos resultados obtidos.

Durante o processo de análise foram ainda identificados aspetos relevantes, que constituíram a base para uma análise SWOT, que serviu de alicerce para formular potenciais linhas de orientação estratégica, conducentes à implementação bem-sucedida do ILP na GNR.

Em termos de resultados obtidos, importa relevar as potencialidades do modelo ILP no que concerne à capacidade de otimizar a alocação de recursos operacionais e de apoiar a tomada de decisão estratégica e operacional em contexto

de segurança pública. Esta abordagem proativa, que integra as informações no processo decisão policial, torna-se particularmente relevante nos ambientes operacionais contemporâneos, onde a capacidade de antecipação e prevenção de problemas operacionais se constitui um imperativo.

No entanto, a implementação do ILP não está isenta de desafios. A necessidade de reforçar a capacidade analítica para gerir e interpretar grandes volumes de dados é uma fragilidade que necessita ser considerada. Os custos associados à aquisição e manutenção de tecnologias avançadas representam outro importante desafio, exigindo um investimento considerável, que pode limitar a sua adoção, especialmente em contextos de restrições orçamentais.

Além dos desafios operacionais e financeiros, o modelo ILP pode estar também associado a questões legais e éticas que importa ressalvar, particularmente no que diz respeito à proteção de dados pessoais. O risco de distorções no julgamento, potenciado pela excessiva dependência de dados quantitativos, sublinha a necessidade de desenvolver mecanismos robustos de governança, que garantam o estrito cumprimento dos normativos legais, bem como a garantia da integridade e da ética na utilização das informações no desenvolvimento da atividade operacional.

No que concerne aos modelos policiamento, a GNR reflete uma dinâmica interessante entre abordagens tradicionais e abordagens modernas de policiamento. A predominância do policiamento reativo, caracterizado por uma resposta direta a incidentes e crimes ocorridos, continua a ser a prática mais comum. Contudo, o modelo de policiamento comunitário e de proximidade evidencia um esforço significativo para transcender as metodologias convencionais. Debaixo de uma forte orientação política, a GNR tem vindo a desenvolver diversos programas especiais que têm promovido a construção de laços robustos com a comunidade e tem contribuído para uma compreensão mais aprofundada das necessidades e preocupações da comunidade, bem como para o desenvolvimento de uma comunicação mais efetiva com o cidadão.

Por outro lado, modelos como COMPSTAT e o POP são exemplos de abordagens policiais mais proativas que, embora esses modelos sejam aplicados de forma menos extensiva na organização, a sua utilização em situações pontuais demonstra o reconhecimento institucional da necessidade de abordagens mais flexíveis e adaptadas ao ambiente operacional. A aplicação de COMPSTAT e POP em circunstâncias específicas, além de aumentar a eficácia das operações policiais,

pode servir como catalisador para a sua adoção mais ampla, à medida que seus benefícios se tornem evidentes, através de sucessos operacionais concretos. A continuidade na integração destes modelos no âmbito da estratégia global de policiamento poderá fortalecer as capacidades de prevenção e resposta da GNR, alinhando-se com as melhores práticas de segurança pública contemporâneas.

O ILP, apesar de não estar totalmente implementado, desempenha um papel complementar fundamental no processo de planeamento da GNR. A adoção plena deste modelo depende de um conjunto de fatores críticos que podem potenciar a sua efetiva implementação.

A capacidade analítica é fundamental para a efetiva implementação do ILP. Apesar de ser reconhecido o valor das informações, subsistem, contudo, alguns desafios no que concerne à capacidade analítica da estrutura de informações, que se mostra insuficiente para abordar integralmente as diversas áreas de atuação da GNR. No entanto, a implementação do Sistema de *Business Intelligence* Policial promete melhorar significativamente a capacidade analítica, ao proporcionar as capacidades de retrospetiva, predição e cenarização, com base na análise dos dados existentes nos sistemas de informação operacionais.

A tecnologia é um pilar indispensável para a implementação do ILP. Pese embora os progressos alcançados no desenvolvimento de tecnologias e sistemas de informação operacional, ressalta-se a urgência de investimentos adicionais em novas ferramentas tecnológicas e a integração da inteligência artificial, para ampliar a capacidade de análise de grandes volumes de dados e aumentar a capacidade preditiva do sistema de informações da GNR.

O processo de decisão em contexto ILP é manifestamente suportado pela integração das informações. Esta abordagem destaca-se pela sua capacidade de influenciar decisões estratégicas, operacionais e táticas, através da integração de informações no processo de planeamento de operações. Apesar de se ter concluído que as informações são integradas no processo de decisão estratégico, operacional e tático, esta integração é efetuada de forma pontual e muitas vezes de forma *ad hoc*, em resposta às necessidades imediatas, carecendo de um processo sistematizado que concorra para a prevenção e antecipação dos problemas operacionais e, para o reconhecimento atempado das tendências emergentes.

Melhorar esses aspetos torna-se fundamental para uma resposta mais direcionada e proativa aos desafios operacionais, garantindo que o processo de decisão se constitua um pilar decisivo na implementação do ILP. Neste sentido,

torna-se necessária a sistematização de um modelo que transcenda a resposta a circunstâncias imediatas e se foque numa visão estratégica de antecipação, que permita agir de forma mais eficaz num ambiente operacional cada vez mais dinâmico.

A formação desempenha um papel crucial para implementação do ILP. A integração de conteúdos específicos de ILP nos planos de formação, tanto na formação base como nos cursos de promoção e qualificação de todas as categorias profissionais, é imperativa para assegurar a eficácia e a implementação efetiva do modelo. Esta integração curricular deve ser considerada como uma prioridade estratégica, pois constitui-se como fator crítico de sucesso para o desenvolvimento de competências necessárias à aplicação prática dos princípios subjacentes ao ILP.

A estrutura organizacional necessita de ajustes para favorecer a implementação do ILP. A autonomização das informações em relação a estrutura de investigação criminal é recomendada, para evitar a predominância de abordagens reativas e concentradas na resolução de casos específicos de processos de inquérito criminais. A criação de um *Fusion Centre* ao nível operacional poderia integrar diversas valências de atuação e promover a análise de informações mais abrangente, quer ao nível estratégico, quer ao operacional. Essas mudanças na estrutura tornam-se fundamentais para alinhar a estrutura das informações com os princípios do ILP, facilitando a efetiva implementação do modelo a todos os níveis de decisão da organização.

O envolvimento ativo das lideranças é primordial para a efetiva implementação do ILP. As lideranças devem estar comprometidas em promover uma cultura que valorize a análise de informações e a tomada de decisão baseada em informações. O sucesso na implementação do ILP depende substancialmente do apoio e do comprometimento das lideranças em todos os níveis da organização, desde o processo de formulação estratégica até a execução prática dos planos e ordens operacionais.

Este envolvimento não deve ser percebido apenas como uma formalidade administrativa, mas como um compromisso estratégico contínuo e visível, capaz de vencer a resistência organizacional e capaz de promover uma verdadeira "cultura de informações" como epicentro do planeamento e do processo de decisão operacional.

Este trabalho de investigação oferece contribuições importantes para o conhecimento nas áreas de segurança pública e administração policial.

Um dos principais contributos deste estudo são as propostas de linhas de orientação estratégia que podem potenciar implementação bem-sucedida do ILP no seio da GNR. O estudo também contribui para o conhecimento existente ao confirmar e expandir os conceitos teóricos do ILP com dados empíricos específicos referentes ao contexto da GNR, fornecendo um modelo de análise que pode ser adaptado ou replicado por outras forças policiais.

Como limitação ao presente trabalho de investigação, releva-se o facto de não ter sido possível efetuar um estudo comparado sobre a implementação do Modelo de ILP, nas forças de gendarmerie congéneres, nomeadamente na *Guardia Civil* da Espanha, na *Gendarmerie Nationale* da França e na *Arma dei Carabinieri* da Itália. Esta limitação traduziu-se na dificuldade em recolher a informação necessária dessas forças, restringindo, assim, a capacidade de comparar as práticas de implementação e os resultados alcançados pelo modelo de ILP naquelas organizações. A ausência de dados detalhados impediu uma avaliação da eficácia e das adaptações do modelo ILP em diferentes contextos institucionais e culturais, limitando a extensão das conclusões à escala internacional.

Para investigações futuras, recomenda-se o estudo sobre a integração da inteligência artificial nos sistemas de informação operacionais da GNR, no sentido de melhorar e incrementar as capacidades analíticas e preditivas da organização, contribuindo assim para uma resposta mais eficaz aos desafios futuros.

Neste trabalho de investigação, resultante na análise SWOT, extraem-se algumas recomendações consubstanciadas em linhas de orientação estratégica, que visam otimizar os fatores críticos identificados, no sentido de facilitar a efetiva implementação deste modelo policial pela GNR. Propõe-se ainda, um modelo sistematizado para a implementação do ILP na GNR. Este modelo fundamenta-se no Modelo 4i de Ratcliffe, que articula as dimensões de "*Intent*", "*Interpret*", *Influence*" e *Impact*", proporcionando um quadro estratégico para a integração das informações nas operações policiais.

Em conclusão, enquanto Portugal e a GNR navegam por um ambiente de segurança global cada vez mais complexo, a adoção do ILP, além de ser uma opção, é uma necessidade imperativa. A efetiva implementação desse modelo promete melhorar a segurança pública e a eficiência operacional, mas também posicionar a GNR na vanguarda das práticas policiais modernas, para enfrentar os desafios de segurança do século XXI.

REFERÊNCIAS BIBLIOGRÁFICAS

Association of Chief of Police Officers. (1975). *Report of the ACPO Subcommittee on Criminal Intelligence*. London: Association of Chief of Police Officers.

Bandeira, M. (s/d). *Validade interna e externa de uma pesquisa*. São João del-Rei: Departamento de Psicologia – UFSJ.

Bispo, A. J. (2004). *A Função de Informar*. Estudos em Honra do General Pedro Cardoso. Lisboa: Prefácio.

Bolas, J. (2021). *Estrutura das Informações na Guarda (Trabalho de Investigação Individual)*. Lisboa: Instituto Universitário Militar.

Braga, A. A. (2008). *Problem-oriented policing and crime prevention* (2nd Ed.). New York: Criminal Justice Press.

Bureau of Justice Assistance . (2005). *Intelligence-Led Policing: the new intelligence architeture* [versão PDF]. https://www.ojp.gov/pdffiles1/bja/210681.pdf

Camacho, J. (2015). *A mobilidade da informação na Polícia de Segurança Pública (Tese de Dissertação de Mestrado em Estratégia)*. Lisboa: Instituto Superior de Ciências Sociais e Políticas .

Carter, D. L. (2008). *The concept and development of Intelligence-Led Policing*. Michigan: Michigan State University.

Carter, D. L. (2009). *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies (2nd Ed.)*. Michigan: Michigan State University.

Clemente, P. (2012). *Políticas de Segurança - Desafios e Rumos*. Lisboa: Pactor.

Davenport, T. H. (1997). *Information Ecology: Mastering the Information and Knowledge Environment*. New York: Oxford University Press.

Dempsey, F. &. (2019). *An introduction to Policing (9th Ed.)*. Boston: Cengage Learning Inc.

Escola da Guarda. (2008). *Manual de Informações*. Queluz: Escola da Guarda

Fernandes, L. (2014). *Intelligence e Segurança Interna*. Lisboa: ISCPSI.

Fortin, M. (2003). *O Processo de Investigação*. Portugal: Lusociência.

Fuentes, J. R. (2006). *Pratical guide to Intelligence-Led Policing*. New Jersey: New Jersey State Police.

Gemke, P. (2017). *Organizational factors enabling Intelligence-Led Policing in Dutch Police Force (Master thesis in Systems Engeneering, Policy Analysis and Management*. Haia: Faculty of Technology - Policy Management.

Guarda Nacional Republicana. (2020). *Plano de Atividades*. Lisboa: Comando Geral.

Guarda Nacional Republicana. (2021). *Plano de Atividades*. Lisboa: Comando Geral.

Guarda Nacional Repubicana. (2022). *Plano de Atividades*. Lisboa: Comando Geral

Guedelha, M. (Coord.). (2020). *Estratégia da Guarda 2025, uma estratégia centrada nas pessoas*. Lisboa: Comando Geral.

Hengsen, T. (2011). *Toward Intelligence-Led Policing: A qualitative study and assessment of how the critical factors of Intelligence-Led Policing are perceived by Chicago Police Department's Organized Crime Division*. Chicago: Loyola University Chicago.

International Association of Law Enforcement Association Analysts. (2012). *Law Enforcement Analytic Standards (2nd Ed.)* https://www.ojp.gov/ncjrs/virtual-library/abstracts/law-enforcement-analytic-standards-2nd-edition

James, A. (2011). *The Influence od Intelligence-Led Policing Models on Investigative Policing and Practice in Mainstream Policing 1993-2007: Division, Resitance and Investigative Orthodoxy*. Department of Social Policy. London: London School of Economics and Political Science.

Mallory, S. L. (Setembro de 2007). T*he concept of asymmetrical policing* [versão PDF]. Retirado de https://www.dcaf.ch/sites/default/files/publications/documents/WPS_No12_new.pdf

Maroco. (2007). *Análise estatística com utilização do SPSS*. Lisboa: Edições Sílabo.

Moleirinho, P. (2009). *Da Polícia de Proximidade ao Policiamento Orientado pelas Informações*. Dissertação de Mestrado em Direito e Segurança, Faculdade Nova de Lisboa, Lisboa.

Moloeznik, M. P. & Balcázar V. M. (2013). Aproximación a la inteligencia policial. *Revista Criminalidad*, 131-151.

National Centre for Policing Excellence. (2005). *Guidance on the National Intelligence Model*. Wyboston, UK: National Centre for Policing Excellence.

Office Community-Oriented Policing Services. (2012). *Community-oriented policing defined*. https://portal.cops.usdoj.gov/resourcecenter/RIC/Publications/cops-p157-pub.pdf

Organização para a Segurança e Cooperação na Europa. (2017). *OSCE Guidebook Intelligence-Led Policing*. Vienna: OSCE Secretariat Transnational Threats Department Strategic Police Matters Unit.

Police Executive Research Forum. (2000). *Excellence in Problem-Oriented Policing: the 2000 Herman Goldstein Award Winners*. https://www.ojp.gov/library/publications/excellence-problem-oriented-policing-2000-herman-goldstein-award-winners

Police Executive Forum. (2013). *COMPSTAT: Its origins, evolution, and future in Law Enforcement Agencies*. https://www.ojp.gov/ncjrs/virtual-library/abstracts/compstat-its-origins-evolution-and-future-law-enforcement-agencies

Ratcliffe, J. H. (2003). Intelligence-Led Policing. *Trends & Issues in crime and criminal justice*. https://www.aic.gov.au/sites/default/files/2020-05/tandi248.pdf

Ratcliffe, J. H. (2016). *Intelligence-Led Policing (2nd Ed.)*. New York: Routledge.

Romero, A. B. (2019). *Modelos Policiales Comparados*. Valência: Univeritat Jaume I.

Rowe, M. (2013). *Introduction to policing (2nd Ed.)*. London: Sage Publishing.

Santos, L. A., & Lima, J. V. (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação*. Cadernos do IUM N.º 8 (2.ª ed., revista e atualizada).

Schreier, F. (2009). Fighting the pre-eminent threat with intelligence-led operations. *Occasional Paper n.16*.https://www.files.ethz.ch/isn/99600/occasional_16.pdf

United Nations Office on Drugs and Crime. (2011). *Criminal Intelligence - Manual for Analysts*. Vienna: United Nations Office on Drugs and Crime.

Weisburd & Eck. (May de 2004). What can Police do to reduce crime, disorder and fear? *The annals of the American Academy of Political and Social Science 593*, 42-65.

ESTUDO 4 – A *IDENTITY INTELLIGENCE* ENQUANTO INSTRUMENTO CONTRIBUINTE PARA AS OPERAÇÕES MILITARES: DESAFIOS FACE AO AMBIENTE CONTEMPORÂNEO[29]

IDENTITY INTELLIGENCE AS AN INSTRUMENT CONTRIBUTING TO MILITARY OPERATIONS: CHALLENGES IN THE FACE OF THE CONTEMPORARY ENVIRONMENT

André Miguel Farinha Bento
Major, Infantaria

Rui Pedro Gomes de Aguiar Cardoso
Major, Infantaria

RESUMO

Esta investigação tem como objeto de estudo a *Identity Intelligence*, nomeadamente, no seu contributo como ferramenta no processo de produção de Informações no apoio oportuno a uma tomada de decisão eficaz em operações militares no atual ambiente operacional. Para tal, adotou-se uma metodologia consubstanciada num raciocínio indutivo e numa estratégia de investigação qualitativa, assente num estudo de caso, com recurso a análise documental e entrevistas semiestruturadas, de modo a proporcionar um aprofundamento significativo sobre a interação entre a tecnologia de identificação e as necessidades operacionais das Forças Armadas Portuguesas. Após se ter avaliado como pode a *Identity Intelligence* otimizar a conduta das operações militares, os principais resultados obtidos destacam a eficácia da *Identity Intelligence* em proporcionar informações precisas e oportunas que potenciam a tomada de decisão em cenários complexos e voláteis. Foi possível demonstrar que a *Identity Intelligence*, através da combinação de dados biométricos e análise de redes humanas, otimiza a capacidade de prever e reagir a ameaças, aumentando assim a eficiência das operações militares. As conclusões realçam o recrudescimento indelével da relevância da *Identity Intelligence* em adaptar-se e evoluir no seio das estruturas de informações militares, de modo a fazer face aos desafios impostos pela constante inovação tecnológica.

Palavras-chave: análise de informações, ambiente operacional contemporâneo, Forças Armadas Portuguesas, *identity intelligence*, operações militares, tecnologia de identificação

[29] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto (CEMC 2023/2024). A versão integral encontra-se disponível nos Repositórios Científicos de Acesso Aberto de Portugal (https://www.rcaap.pt/).

ABSTRACT

This research focuses on Identity Intelligence, particularly its contribution as a tool in the information production process supporting timely and effective decision-making in military operations within the current operational environment. An inductive reasoning methodology was adopted alongside a qualitative research strategy, grounded on a case study involving documentary analysis and semi-structured interviews, to significantly deepen the understanding of the interaction between identification technology and the operational needs of the Portuguese Armed Forces. After evaluating how Identity Intelligence can optimize the conduct of military operations, the key findings underscore the effectiveness of Identity Intelligence in providing precise and timely information that enhances decision-making in complex and volatile scenarios. It has been demonstrated that Identity Intelligence, through the combination of biometric data and human network analysis, optimizes the ability to predict and respond to threats, thereby increasing the efficiency of military operations. The conclusions highlight the indelible intensification of the relevance of Identity Intelligence in adapting and evolving within military information structures, in order to meet the challenges posed by constant technological innovation.

***Keywords**: information analysis, contemporary operational environment, portuguese Armed Forces, identity intelligence, military operations, identification technology*

1. INTRODUÇÃO

A natureza da guerra, embora imutável na sua essência, tem visto o seu caráter evoluir de forma acelerada pelo ritmo vertiginoso da disponibilidade de informação, bem como pelas constantes mudanças tecnológicas. Neste contexto, é essencial fornecer informações de qualidade para apoiar a tomada de decisão (UK Ministry Of Defense, 2023, p. 3).

É neste panorama dinâmico que as Informações se procuram renovar e adaptar, com o objetivo de gerar vantagem e de contribuir para o processo de tomada de decisão em operações militares (OM) (Silva, 2023, pp. 23-25).

A evolução tecnológica tem facilitado o desenvolvimento de ferramentas de recolha de dados, essenciais para a produção de Informações. Nesta conformidade é crucial ponderar sobre como as Informações e as suas atividades se constituem como instrumento fundamental na redução da incerteza. Reside nesta precisão o grande desafio para a área das Informações, intensificado pela globalização que se tem manifestado desde o término do século XX, onde a capacidade de obtenção de informações se encontra em constante evolução, sendo realmente importante para uma decisão adequada (UK Ministry of Defense, 2023, pp. 6-10).

Por conseguinte, identifica-se a premência de analisar, no atual contexto a tecnologia, enquanto ferramenta potenciadora de dinamização e desenvolvimento de capacidades na conduta de OM, sem nunca desconsiderar o elemento humano, em virtude deste ser a única variável movida por intencionalidade e imprevisibilidade.

É perante este contexto que a "*Identity Intelligence*" (I2), enquanto instrumento de apoio à conduta das OM, se constitui como uma abordagem inovadora de recolha e análise de informações, para que a informação crucial possa ser capitalizada e consequente, assegurando o apoio esclarecido ao decisor, nomeadamente no seu processo de decisão militar.

Assim, este trabalho pretende avaliar como pode a I2 otimizar a conduta das OM, oferecendo contributos para fazer face a ambientes complexos e incertos, nos quais indelevelmente estamos inseridos. Assim, a relevância deste estudo estabelece-se na sua contribuição para compreender melhor as dinâmicas das Informações Militares (IM), associadas à aplicabilidade prática deste instrumento, fundamentais para o sucesso das OM na era contemporânea.

Deste modo, a pertinência deste tema de investigação advém da necessidade de adaptação e inovação contínua por parte das Forças Armadas (FFAA) em utilizar novas capacidades tecnológicas, que possam contribuir para uma produção de informações mais eficiente, e consequentemente, a um apoio à tomada de decisão mais célere e esclarecido, mitigando as limitações das IM no que diz respeito à informação incompleta (NATO, 2016). Esta investigação tem como objeto de estudo a I2 em OM, com especial foco no seu contributo como ferramenta no processo de produção de Informações no apoio oportuno a uma tomada de decisão eficaz em operações no atual ambiente.

O Objetivo Geral (OG) da investigação é avaliar de que modo a I2 pode otimizar a conduta das OM face ao atual Ambiente Operacional (AO). Para cumprir o OG da investigação, foram formulados dois objetivos específicos (OE): OE1 – Analisar os desafios das OM face ao atual ambiente operacional; OE2 – Analisar o impacto da I2 nas OM. De forma a atingir o OG definido, foi formulada uma questão central (QC), e respetivas questões derivadas (QD). Assim a QC desta investigação é: *Como pode a I2 contribuir para a otimização da conduta das Operações Militares no atual ambiente operacional,* sendo as questões derivadas as seguintes: QD1 – Quais os desafios das OM face ao atual AO? QD2 – Qual o impacto da I2 nas OM?

No respeitante à organização, a presente investigação está estruturada sob a forma de artigo científico (Norma de Execução Permanente de Investigação [NEP/INV] - 001, 2020), encontrando-se organizada em cinco capítulos, sendo o primeiro a presente introdução. No segundo é efetuado o estado da arte, com especial enfoque, nos conceitos estruturantes, culminando nesta parte, com o modelo de análise adotado. No terceiro capítulo é abordada a metodologia e o método seguido na investigação. No quarto capítulo são apresentados e analisados os resultados, dando-se resposta às QD, encetando-se a proposta de contributos, da qual resulta a resposta à QC. No quinto e último capítulo são traçadas as conclusões, efetuando-se uma súmula dos resultados e identificação de limitações, aditando-se igualmente, contributos para o conhecimento, proposta de estudos futuros e recomendações de ordem prática.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

As OM constituem o fulcro das atividades das FFAA e são uma série de ações táticas executadas por forças de combate, que podem incluir múltiplos componentes, sendo meticulosamente coordenadas temporalmente e espacialmente, com o propósito de alcançar objetivos operacionais e, por vezes, estratégicos (IUM, 2019, p. 4). Desta forma, o comandante e o seu estado-maior são responsáveis por planear pormenorizadamente todas as ações para se atingirem os efeitos desejados tendo em consideração não só um qualquer tipo de terreno, como também, a própria multidimensionalidade do ambiente envolvente. Atualmente, o espaço onde as OM ocorrem está em permanente mutação e evolução, sendo caraterizado por uma série de condições e influências que impactam a utilização das FFAA e moldam as decisões dos líderes militares (EME, 2012, p. 1-1).

As decisões estratégicas, operacionais ou táticas devem ser enformadas por informações adquiridas de forma oportuna, representando desta forma, um recurso de significativa influência devido ao seu potencial de assegurar uma superioridade tática contra forças opositoras. Tal vantagem informacional é um contribuinte crítico para o êxito de OM. Independentemente da tipologia de operação, o acesso a informações pertinentes e atualizadas é indispensável para o exercício de comando, possibilitando uma tomada de decisão informada, ágil e atempada, garantindo, quando possível, a preservação da iniciativa – um axioma central da arte da guerra (Silva, 2019).

Como Burton (2005) aponta, a capacidade de detetar ações, padrões ou procedimentos hostis através de meios tecnológicos não se traduz na habilidade de discernir as verdadeiras intenções da ameaça. Assim, deduz-se que o ambiente contemporâneo e a natureza da ameaça possuem caraterísticas únicas, influenciadas por variáveis como por exemplo a localização, cultura e objetivos específicos, variáveis intrinsecamente ligadas ao fator humano.

Cardoso (2004, pp. 150-151) afirma que "as atividades de Informação implicam um processo complexo que abarca a pesquisa, a avaliação, a integração e a interpretação das informações [...], as quais para serem eficazes necessitam ser precisas e oportunas".

No entanto, as OM contemporâneas já não se limitam aos campos de batalha tradicionais; transcendem-se para múltiplos domínios – terra, ar, mar, espaço e ciberespaço – (Manolache, 2023, pp. 164-168) exigindo, desta forma, uma capacidade de recolha e análise robusta.

Neste desiderato, a I2 poderá constituir-se como uma ferramenta de extrema importância para identificar, analisar e prever comportamentos de entidades de interesse (Baber et al., 2020), onde é premente perceber quem são os adversários neste ambiente complexo, em que as ameaças se caracterizam pela sua fluidez e imprevisibilidade (Lind, 2004). A I2, devido ao emprego de uma abordagem integrada, utiliza tecnologias avançadas tais como biometria, análise forense e comportamental, de forma a poder capacitar as forças militares a operar com maior precisão, como por exemplo, através da identificação precisa de indivíduos que representem ameaças. Concomitantemente, analisa as redes onde estes se encontram inseridos, bem como os seus padrões comportamentais, assentindo uma necessária antecipação de forma a garantir uma resposta mais ágil e informada das ameaças emergentes, robustecendo também a segurança das próprias forças militares, prevenindo acessos não autorizados a instalações militares.

Atualmente, existem pequenos núcleos de especialização em I2, que se encontram em desenvolvimento entre as nações e parceiros da *North Atlantic Treaty Organization* (NATO). Ao fundir os processos, poder-se-á capitalizar a negação de anonimato à ameaça; fornecer às forças da NATO produtos de informação relativos a ameaças e a sua identificação positiva; auxiliar na proteção da força para identificar tentativas adversárias de usar falsas identidades para obter acesso a instalações (NATO, 2017a).

De modo a contribuir para a conduta das OM, a I2 proporciona um nível mais profundo de compreensão, conforme indica a Figura 1. Desta forma, através da I2, é possível compreender o contexto sobre uma pessoa de interesse numa determinada área.

De acordo com as referências identificadas é possível verificar a importância que tem sido dada a esta temática, onde já foram iniciadas formações e especializações associada aos conceitos doutrinários elencados, sendo necessário continuar a desenvolver-se a sua base concetual e doutrinária, bem como aplicações práticas em operações reais, para que a I2 se possa considerar um produto especializado de informações de referência, em que o presente trabalho poderá contribuir para esse desiderato.

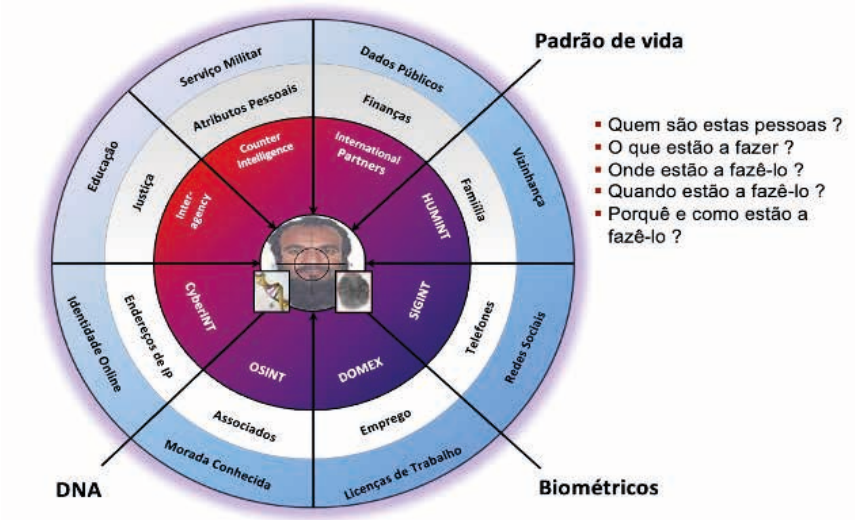

Figura 1 – Integração da I2 com todas as fontes disponíveis
Fonte: Adaptado de Garrett e Jones, (2023).

2.1. Ambiente Operacional Contemporâneo

O atual AO é caracterizado por um conjunto de condições, circunstâncias e fatores influenciadores que afetam o emprego de Forças militares e influenciam as decisões do comandante (EME, 2012, p. 1-1). O AO contemporâneo exige um entendimento profundo das mudanças e dinâmicas emanadas de uma sociedade cada vez mais integrada e complexa nas suas múltiplas facetas de análise (Greer,

2023). Segundo Silva (2023) observou-se, nos últimos três anos, uma transição de um ambiente volátil, incerto, complexo e ambíguo (VUCA) para uma realidade caraterizada por ser frágil, incompreensível, não linear e ansiosa (BANI). Segundo o autor, esta transformação tornou-se particularmente evidente no rescaldo da pandemia da COVID-19 e dos recentes conflitos na Ucrânia e no Médio Oriente. A fragilidade baseia-se numa perceção ilusória de segurança e estabilidade, oriunda de um ecossistema interconectado que se presume como robusto e coeso. Paralelamente, a ansiedade emerge do paradoxo inerente à globalização, com o acesso a um volume avassalador de informação e desinformação, representando um desafio contínuo para quem tem a responsabilidade de tomar decisões ou de aconselhar decisores, gerando uma sensação de inquietude perante potenciais detalhes negligenciados. A não linearidade do ambiente contemporâneo é também premente, uma vez que o previsível cedeu lugar ao inexplicável, desafiando os padrões históricos como garantia contra a imprevisibilidade dos acontecimentos. Este fator está intimamente ligado ao caráter ininteligível do ambiente atual, onde a crença num conhecimento capaz de elucidar os fenómenos emergentes se dissipou (Silva, 2023, pp. 22-25).

Não obstante a caracterização do ambiente BANI, Cascio (2021) sublinha que o conceito de VUCA não se extinguiu. Na mesma referência, Cascio menciona que os aumentos da volatilidade, da crise climática global, bem como o aparecimento de sistemas de inteligência artificial (IA), ultrapassam a incerteza ou simples ambiguidade, interferindo de forma incisiva na capacidade de planear o futuro.

O modelo BANI não é uma ferramenta para transformar organizações por si só, mas uma linguagem para descrever o caos no ambiente onde a humanidade está inserida, que poderá ajudar a decompor questões complexas, permitindo uma melhor compreensão do mundo, naquilo que são os eventos e as ameaças recentes embora não tivesse sido desenvolvido para se tornar um conceito global (Cascio, 2021).

Nesta conformidade pode inferir-se que o AO contemporâneo poderá continuar a ser caracterizado como VUCA, e o conceito de BANI corresponderá a uma extensão da descrição do mesmo, não havendo lugar a uma efetiva transição, mas sim a uma maior complexidade do ambiente onde estamos inseridos.

É perante este panorama dinâmico que as informações se procuram renovar, adaptar e alinhar, com o objetivo de gerar vantagem estratégica e operacional e de contribuir para o processo de tomada de decisão em OM.

2.2. Operações Militares

Até à queda do muro de Berlim em 1989 a guerra era considerada um fenómeno estatal, com regras e procedimentos. Com o fim da guerra fria e a entrada na última década do século XX, surgem outros focos de agitação regionais e desenvolvimento de múltiplos radicalismos, passando a guerra a não ser exclusivamente conduzida entre estados, dando origem a que as OM se desenvolvam num mundo díspar com grandes desproporções qualitativas e como um fenómeno social (Telo, 2002 cit. por Rodrigues, p. 7) (Santos, 2012, cit. por Rodrigues, p. 7).

As guerras em curso demonstram que os avanços tecnológicos têm sido importantes, continuando, no entanto, a ser difícil de prever os efeitos na consecução dos objetivos militares (Maathuis & Chockalingam, 2023, p. 276). Apesar desta imprevisibilidade, o processo de decisão militar estará no cerne deste fenómeno geral que é a guerra (NATO, 2022). De acordo com o Regulamento de Campanha e Operações (2005) as OM são ações militares necessárias para o cumprimento de uma missão estratégica, operacional e tática, para atingir os objetivos de qualquer empenhamento, batalha, operação de campanha ou de grande envergadura.

Por outro lado, devido à complexidade do AO contemporâneo a definição anterior, mais vocacionada para operações de combate, onde a capitulação da força opositora terminava com a consecução dos objetivos militares, atualmente os objetivos militares estão interligados com a criação de um ambiente seguro e estável, onde a preponderância das operações de estabilização assumem um papel tão importante como as operações ofensivas e defensivas, tornando-se comum a expressão de "operações militares em todo o espetro do conflito"(EME, 2012, p. 2).

Deste modo e relacionando os dois conceitos é possível definir as OM como atividades realizadas pelas FFAA com o objetivo de atingir objetivos estratégicos ou táticos específicos, onde a tipologia de operação (Ofensiva, Defensiva, de Estabilização ou de Apoio Civil) irá definir, no seu planeamento (Processo de Decisão Militar), que meios e recursos serão necessários para a condução das mesmas (Maathuis & Chockalingam, 2023, p. 276).

A condução de OM em todo o espectro do conflito pelas FFAA requer uma preparação adequada e uma constante adaptação à evolução do ambiente em que ocorrem, especialmente no seio da população, em que a compreensão dos adversários e das ameaças é uma mudança significativa. Assim, a adaptabilidade e integração de novas técnicas e procedimentos são fundamentais (Lind, 2004, pp. 12-16).

De acordo com o exposto pode inferir-se que o conceito contemporâneo de OM é o de um conjunto complexo de ações realizadas pelas FFAA caracterizadas pela integração e pela adaptabilidade, que requerem um planeamento que considere para além do emprego da força, o estabelecimento de condições para uma paz duradoura e o bem-estar da população, sendo o sucesso das OM, medido pela capacidade de atingir objetivos com o mínimo de danos colaterais.

2.3. Informações Militares

Historicamente, as informações têm determinado as capacidades de um adversário pelo tamanho, forma e qualidade do seu aparelho militar e pelo desempenho do seu equipamento, tendo sido sempre excecionalmente difícil determinar as suas intenções. Nos ambientes operacionais contemporâneos e futuros, onde o tamanho da capacidade militar de um oponente pode ser menos relevante devido a táticas não convencionais ou híbridas, os elementos afetos à área das Informações devem assegurar que os comandantes compreendam que determinar as capacidades dos adversários, o seu centro de gravidade, as suas redes e intenções já não se limita à pura força física, sendo necessário considerar habilidades não militares e capacidades não físicas (NATO, 2020).

De acordo com Alessandro Scheffler e Jan-Hendrik Dietrich (2023, pp. 1047-1049), as IM estão nos dias de hoje mal definidas, tornando-se árduo diferir, neste complexo AO contemporâneo, aquilo que são IM e Informações "civis". Se no passado as informações tratavam de recolher informação sobre o inimigo no contexto de guerra, o mesmo não acontece atualmente, onde por vezes se torna difícil destrinçar aquilo que são as IM das restantes, perante o atual mundo globalizado.

Estes autores argumentam que as IM são analisadas como uma rede de atores e instituições, ao invés de uma única organização, com uma variedade de abordagens e definições, que variam de acordo com os países e suas estruturas de informações nacionais (Scheffler & Dietrich, 2023, pp. 1052-1055).

Não obstante, a NATO define as Informações como um produto resultante da recolha direcionada e do processamento de informação, sobre um determinado ambiente e sobre as capacidades e intenções dos atores, a fim de identificar ameaças e oferecer oportunidades para tomada de decisão aos comandantes militares (NATO, 2022, pp. 2-1). Estas são categorizadas, em consonância com os níveis da guerra, em Informações Estratégicas, Operacionais e Táticas (NATO, 2022).

Assim, considera-se que as IM são um processo sistemático de recolha, processamento, análise e disseminação de um produto de apoio à decisão, que pode ou não ter sido identificado pelos decisores e que são de interesse para o meio militar (Silva & Ribeiro, 2018, p. 180).

Desta forma poderá asseverar-se que as Informações conduzem as operações, considerando que as IM detêm uma importância primordial em todo o processo de planeamento e tomada de decisão, bem como na condução das OM. No âmbito do desenvolvimento das suas atividades as IM fundamentam-se no tratamento das informações através do CPI, que engloba a fase de orientação do esforço de pesquisa, a fase de pesquisa, a fase de processamento e a fase de disseminação da informação (Sousa, 2020, p. 6).

Num contexto militar, a determinação do objeto das IM é iniciada no nível político, com a identificação dos objetivos nacionais a serem alcançados e dos obstáculos que se opõem ou desafiam esses interesses (Silva & Ribeiro, 2018, pp. 180-181). Os referidos autores elucida que, mediante a análise das atividades, atitudes, intenções, sistemas de poder e a sua aplicabilidade, pode deduzir-se que o objeto das IM engloba as ameaças militares, efetivas e potenciais, caracterizadas por uma mutabilidade constante (Silva & Ribeiro, 2018). Do mesmo modo, Gomez (2005, cit. por Silva & Ribeiro, 2018, p. 180) sustenta que as IM são essenciais ao esforço militar de um país, como meio para atingir o objetivo de apoiar a decisão política na prevenção de conflitos, assegurando, em última instância, forças militares eficientes para a salvaguarda da soberania nacional.

De acordo com o CEDN, as IM devem desempenhar um papel significativo para "consolidar Portugal como coprodutor de segurança internacional. Os meios militares representam um elemento vital para a segurança do Estado e um fator de projeção do prestígio internacional de Portugal" (CEDN, 2013, p. 9). Face ao exposto, infere-se que as IM são caracterizadas pela sua capacidade de apoiar a decisão política, relativamente às suas componentes do instrumento militar nos seus vetores de emprego e nos demais instrumentos de poder (Silva & Ribeiro, 2018, p. 199), utilizando as suas capacidades, meios e instrumentos para a prossecução desse objetivo na conduta das OM levadas a cabo pelas FFAA.

Para os propósitos deste estudo, a definição de IM a considerar é o processo constante de recolha, processamento, análise e disseminação de um produto de apoio à decisão, emergente de um interesse prévio e de necessidades identificadas pelos decisores com relevância militar (Silva & Ribeiro, 2018).

2.4. *Identity Intelligence*

Como se pôde constatar anteriormente, o AO contemporâneo onde as OM se desenvolvem é complexo e composto por diversos fatores interligados. A intenção por detrás do elemento humano que desencadeia e perpetra as ameaças são um desígnio das IM. O fator humano associado a este ambiente é composto por terroristas, insurgentes, líderes com capacidade de influenciar e grupos financiados por estados clandestinamente que se confundem com a população (Fernandes, 2023).

Com o intuito de capacitar as IM na obtenção de informações oportunas, a I2 poderá perspetivar-se como uma ferramenta contribuinte para analisar e compreender toda a rede, identificando o indivíduo que se poderá caracterizar como ameaça (Fernandes, 2023).

Segundo o conceito NATO (2017a, p. 3) a I2 é definida como as Informações resultantes do processamento de atributos de identidade relativos a indivíduos, grupos, redes ou populações de interesse.

Os atributos de identidade podem ser dados biométricos, biográficos que incluem dados contextuais (incluindo comportamentais), recolhidos de todas as disciplinas de informações que podem ser utilizados isoladamente ou em conjunto, para identificar um indivíduo, conforme demonstrado na Figura 2:

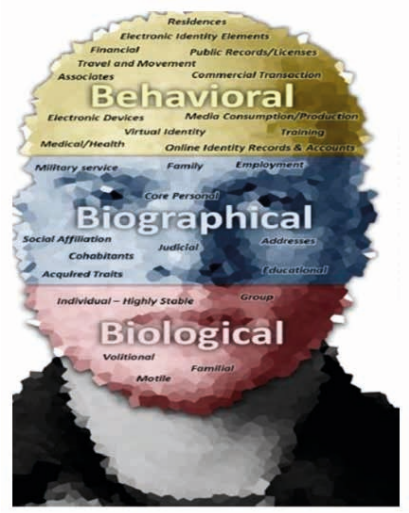

Figura 2 – Atributos e tipos de Identidade
Fonte: Adaptado de NATO (2017a).

A identidade é o conjunto total de dados e informações exclusivas de um indivíduo. Ao efetuar a pesquisa e processamento da informação recolhida, a I2 proporciona a capacidade de identificar a existência de identidades de ameaças anteriormente desconhecidas, associar a informação de identidade a uma pessoa específica, analisar o padrão de vida do indivíduo e conectá-lo a outras pessoas, locais, materiais ou eventos, caracterizando o indivíduo e a potencial ameaça dos seus associados (NATO, 2017a).

O objetivo da I2 é preencher as lacunas entre a Biometria e a Análise de Redes Humanas (HNA[30]) ao proporcionar ligações a grupos hostis, analisando as fontes disponíveis e relacionando-as com os atributos de identidade disponíveis para permitir a sua identificação positiva (NATO, 2017a).

Desta forma pode considerar-se que a I2 é uma ferramenta analítica especializada e transversal que melhora a análise de todas as fontes e proporciona uma compreensão das identidades e das suas redes em OM. A análise aprofundada do ambiente humano permite descobrir as verdadeiras identidades, as suas associações e intenções, o que acrescenta valor às IM (NATO, 2017a, pp. 4-6).

Assim, a I2 torna-se num instrumento importante nas OM, no atual AO, onde a complexidade só pode ser ultrapassada com abordagens inovadoras para fazer face às ameaças que se podem manifestar através de táticas convencionais, irregulares e cibernéticas, neste mundo globalizado (Baber et al., 2020, p. 24).

A análise e previsão de comportamentos, baseadas em tecnologias como biometria, análise forense e comportamental, permitem uma resposta mais rápida e eficaz às ameaças emergentes. Os autores sublinham também a importância da eficiência na pesquisa e análise de informações, assim como a disseminação em tempo oportuno, considerando-os elementos fundamentais para o sucesso em OM (Baber et al., 2020, pp. 24-27).

Não obstante, é importante referir os desafios éticos, legais e de privacidade relacionados ao uso do I2, propondo diretrizes para uma implementação responsável que respeite os direitos individuais (NATO, 2017a, p. 5).

2.5. Modelo de análise

Após a revisão da literatura prévia, elaborou-se o modelo de análise, onde são apresentados os conceitos e dimensões que estruturaram a realização do presente trabalho.

[30] HNA – Sigla em inglês: *Human Network Analysis*

Quadro 1 – Modelo de Análise

Objetivo Geral	Avaliar como pode a I2 otimizar a conduta das operações militares face ao atual ambiente operacional			
Questão Central	Como pode a I2 contribuir para a otimização na conduta das Operações Militares no atual ambiente operacional?			
Objetivos Específicos	**Questões Derivadas**	**Conceitos**	**Dimensões**	**Técnicas de Recolha**
OE1: Analisar os desafios das Operações Militares face ao atual ambiente operacional	**QD1**: Quais os desafios das Operações Militares face ao atual ambiente operacional?	Ambiente Operacional Contemporâneo Operações Militares	Política Económica Social Informacional Militar Tecnológica	Análise documental Entrevistas semiestruturadas
OE2: Analisar o impacto da I2 nas Operações Militares.	**QD2**: Qual o impacto da I2 nas Operações Militares?	I2 Informações Militares	Inovação Tecnológica Eficácia Eficiência	Análise documental Entrevistas semiestruturadas

3. METODOLOGIA E MÉTODO

O raciocínio que norteou a pesquisa foi a de um raciocínio indutivo, uma vez que se pretendeu uma compreensão do contexto da pesquisa, tendo sido realizadas uma série de observações particulares relativas à I2, às OM, ao atual ambiente operacional e às IM, partindo-se das circunstâncias especificas destes conceitos no AO contemporâneo, para estabelecer contributos sobre a forma como a ferramenta I2 pode otimizar a conduta das OM. A estratégia de investigação adotada foi a qualitativa, visto que o conhecimento resultou da interpretação e atribuição de significado de um conjunto de militares com experiência comprovada no âmbito do modelo de I2. Assim, através de entrevistas, estes especialistas forneceram uma visão realista que permitiu analisar o AO e avaliar como a ferramenta I2 pode otimizar a conduta das OM.

O desenho de pesquisa aplicado baseou-se no estudo de caso através do qual se descreveu e verificou o contributo da I2 na conduta das OM, no atual AO, efetuando assim o estudo apenas a uma única unidade de estudo, descrevendo-a sem a intenção de manipular variáveis (Santos & Lima, 2019).

A investigação empregou o horizonte temporal transversal, uma vez que abrangeu o período desde 2021 até à atualidade, analisando-se interações que a I2 tem vindo a desenvolver na contribuição para a conduta das OM, nomeadamente na contribuição para o processo de decisão militar no atual AO.

Para o presente estudo, recorreu-se à análise de diferentes fontes bibliográficas e a entrevistas semiestruturadas para entender a atual dinâmica, bem como encontrar padrões que permitam criar indicadores para avaliar a I2, considerando as dimensões Política, Informacional, Militar e Tecnológica, permitindo desta forma analisar a integração da I2 na produção de IM, analisando os desafios presentes, bem como as limitações existentes. Para se responder às QD e à QC, recorreu-se à análise documental e à realização de entrevistas semiestruturadas a especialistas na área de IM, procedendo- se depois à realização de uma matriz SWOT de modo a responder à QC.

Efetuaram-se entrevistas de acordo com o guião no apêndice C a elementos que desempenharam funções em FND, de modo a identificar as limitações, desafios e as necessidades de desenvolvimento para um melhor contributo das IM para as OM. Por outro lado, entrevistaram-se também especialistas em IM que já tiveram contacto com a ferramenta de I2 para se poder analisar a possibilidade do seu contributo efetivo para a otimização das OM.

A amostra é não probabilística por conveniência (Hill & Hill, 2005) que espelhou a experiência de especialistas militares e civis. Contudo, apenas os especialistas militares participaram no estudo. Assim, procurou-se alcançar o intervalo de amostra proposto por Morse (2000), que é de seis a dez indivíduos, dos quais os mesmos obedecem aos critérios de terem exercido funções na área das IM nos últimos anos. Dada a complexidade do tema investigado, conseguiu-se identificar nove especialistas, decidindo-se prosseguir com o método preconizado por Sarmento. Confirmou-se a obtenção de saturação conceptual, uma vez que as respostas coligidas evidenciaram uma tendência para a convergência.

Relativamente à recolha de dados, foi utilizado o instrumento da análise documental para enquadrar concetualmente a ferramenta I2, através de fontes e origens diversas. Como complemento à análise documental, foi efetuada a realização de entrevistas semi-estruturadas, em que na primeira parte foram colocadas questões relativas aos desafios do AO, de forma a responder à QD 1, e na segunda parte foram colocadas questões referentes à I2 de modo a analisar o seu contributo e impacto para responder à QD 2. As entrevistas tiveram lugar presencialmente e por *email*, tendo sido autorizado o uso da informação coligida para o desenvolvimento do presente trabalho.

A análise das entrevistas foi efetuada mediante a aplicação do método de análise categorial, seguindo a metodologia científica definida por Sarmento (2013,

pp. 53-66). Esta análise de conteúdo baseia-se numa técnica metódica que agrupa e simplifica o volume de palavras textuais em categorias distintas, fundamentando-se numa abordagem científica rigorosa com regras de codificação bem definidas (Sarmento, 2013, p. 53).

4. APRESENTAÇÃO DOS DADOS E DISCUSSÃO DE RESULTADOS

Neste capítulo são apresentados os dados e a discussão dos resultados, que permitiram dar respostas às QD1, QD2 e QC, nos subcapítulos, 4.1, 4.2 e 4.3, respetivamente.

4.1. O Ambiente Operacional Contemporâneo e as Operações Militares

O denominado AO onde as OM decorrem é complexo e pode ser composto por forças convencionais, por ameaças assimétricas ou por grupos de crime organizado, sendo certo que o fator humano estará sempre presente neste contexto, onde é manifestada a intenção de efetivar uma ação.

Desta forma, é de extrema importância os comandantes responsáveis por planear e desenvolver as OM estarem cientes que é necessário compreender o ambiente o melhor possível para alcançar o sucesso nas operações (NATO, 2020).

4.1.1. Dimensão Política

A dimensão política é complexa e abrangente, estando cada mais ligada às dimensões económica e social. Deste modo, a nível político o incremento da segurança do AO, através de relações multilaterais, associado a uma resiliência (militar e civil), para o controlo de armamento e a não proliferação de armas de destruição maciça será um dos desafios que o atual AO contemporâneo se debate. Por outro lado, e por forma a melhorar o ambiente securitário, a nível político existirão os desafios de melhorar e otimizar as regras de Direito Internacional em todo os domínios, para que este seja cumprido e respeitado (*Allied Command Transformation* ACT, 2023). Da análise das entrevistas realizadas, foi possível identificar, que nesta dimensão e associado aos desafios do AO contemporâneo, a **Perceção da Ameaça Existente e a Dinâmica Contemporânea** são críticas para a capacidade de resposta e prevenção neste nível.

Observa-se que a perceção desigual da ameaça por diferentes elementos das estruturas superiores do Estado pode, de acordo com Fernandes (entrevista presencial, 05 de fevereiro de 2024)"limitar a realização de atividades e a inserção em projetos", indicando que a visão comum é fundamental para a visão e coesão estratégica, onde a limitação dos decisores em apoiar a capacitação de uma ferramenta pode ser crucial.

A dinâmica contemporânea, nas palavras de Cavaco (entrevista presencial, 28 de fevereiro de 2024), demonstra que "as operações militares têm que lidar com um ambiente cada vez mais complexo, com múltiplos atores, onde o nível político também tem interferência, não podendo ser descurado", demonstrando que a complexidade operacional não está apenas refletida naquilo que são as OM única e exclusivamente, tendo a dimensão política impacto direto nas operações fazendo parte do atual AO desafiante.

A esta dimensão política está também associada a parte económica, onde segundo Silva (entrevista presencial, 15 de março de 2024), "os desafios passam indelevelmente também por uma consciencialização nos vetores políticos e consequentemente económicos para uma adaptabilidade e eficácia do emprego militar face ao ambiente volátil, incerto, complexo e extremamente frágil que atualmente se vive", bem como a pressão social onde se verifica "que a guerra da informação e de desinformação, enquanto instrumento de manipulação de vontades e opiniões assume relevância nas tomadas de decisão política em prol da pressão social."(Silva, op.cit.)

4.1.2. Dimensão Informacional

Nesta continuidade a parte informacional releva-se de elevada importância no AO contemporâneo, onde as OM terão lugar num ambiente extremamente congestionado a nível informacional e onde a abundância de narrativas irão impactar o sucesso das operações. Adicionalmente, a tecnologia com a IA irá aumentar a quantidade e até a qualidade de efeitos a produzir no ambiente informacional, contribuindo para uma maior dificuldade de deteção dos elementos que tentarão corromper e destabilizar o Sistema Internacional, onde o fator humano (primordial na intenção de efetuar estas ações) também será o mais afetado por outro lado, onde poderá ser corrompido mesmo em tempo de paz através de redes sociais ou através de plataformas que consiga mover massas populacionais (ACT, 2023).

De acordo com os especialistas o atual AO, ao nível informacional tem vindo a sofrer constantes mudanças, sendo que a **Evolução da Ameaça e a Capacidade Técnica** se encontra patente nesta dimensão, conforme demonstrado na figura 4.

De acordo com Borges (Entrevista presencial, 22 de fevereiro de 2024), a proliferação de "notícias falsas e manipuladoras de forças hostis nas redes sociais", exemplificadas pelo grupo Wagner, no teatro de Operações (TO) da Républica Centro-Africana (RCA) são exemplos desta evolução da ameaça, capazes de gerar desinformação, que necessitam de um alerta constante na análise de informações.

Neste contexto, a Guerra Híbrida representa também uma evolução alarmante, que segundo Fernandes (op. cit.) se constitui num campo de batalha "híbrido, complexo e disperso por inúmeras organizações". A atual conjuntura na Ucrânia catalisou esta transformação, onde a guerra não é apenas travada com armamento, mas também através da manipulação de informações e da velocidade de propagação de mensagens nas redes sociais (Marques, entrevista por *email*, 20 de fevereiro de 2024).

De acordo com Cavaco (op. cit.), o elevado volume e complexidade de informação disponível no atual AO também se constituem como um desafio informacional, visto ser necessário possuir capacidades técnicas para "garantir que as FFAA estejam adequadamente preparadas para lidar com este volume e complexidade de informação" onde, segundo Baleia (Entrevista presencial, 12 de março de 2024), o "mundo virtual e o aumento das ameaças *cyber*, e de tudo o que é utilizado pelas redes sociais e meios virtuais, colocam em causa toda a segurança e o desenvolvimento da utilização de fontes abertas para apoio da aquisição de informação correta no apoio às OM".

4.1.3. Dimensão Militar

Ao nível militar, será cada vez mais importante identificar as ameaças através da otimização do processo de *targeting* onde as IM contribuem sobremaneira, podendo utilizar novos sistemas e plataformas, bem como operações de deceção. O atual AO caracterizado por se desenvolver num ambiente multidomínio (terra, mar, ar espaço, e ciberespaço) acarreta novos meios para desenvolver as ações militares, dificultando a credibilidade e identidade, no mundo virtual onde a informação circula, moldando a coesão das forças que desenvolvem OM no espaço físico, impactando o seu domínio cognitivo (ACT, 2023).

A capacidade militar no ambiente multidimensional será moldada por mudanças de paradigma e de *mindset*, aliados a alterações estruturais, devido à capacidade adversária abrangente, associadas ao desenvolvimento tecnológico. Esta aceleração da tecnologia aumentará a complexidade no AO e consequentemente no ambiente securitário, onde a intenção, característica essencial de uma ameaça, se tornará cada vez mais complexa e difícil de percecionar, em que as forças militares terão de procurar rapidamente adaptar-se, tornando o processo de decisão militar mais ágil e célere. Neste particular a integração de sistemas de IA e de sensores capazes de responder mais rapidamente, que serão usados em todos os domínios, aumentando a capacidade de deteção e a identificação da ameaça naquilo que são as suas tipologias (Terrorismo, Espionagem, Subversão, Sabotagem e Crime Organizado - TESSOC), contribuem para um processo de decisão mais rápido, com um maior alcance e precisão. Adaptar a força militar para teatros com condições adversas, implicará a utilização de novas capacidades, apoiadas pela tecnologia em constante desenvolvimento, que trará novos conceitos operacionais. Ainda assim, a capacidade humana será de extrema importância, onde uma cooperação entre entidades governamentais e não governamentais será necessária, tendo em conta que as capacidades de um estado são finitas e necessitam de apoio para responder militarmente, não o conseguindo efetuar eficazmente num ambiente multidimensional (ACT, 2023).

Da análise de entrevistas, é possível apresentar os desafios referentes à dimensão Militar no AO contemporâneo, evidenciada nas respostas dos especialistas. **A Segurança, Capacidade Técnica, a Interoperabilidade, a Dinâmica Contemporânea e o Fator Humano** são indicadores valiosos que refletem preocupações e obstáculos específicos da dimensão militar.

A Segurança da Informação é essencial para o sucesso das OM segundo Cavaco (*op.cit.*), pois encontram-se continuamente "sujeitas a ameaças cibernéticas, espionagem e sabotagem". A disseminação da informação é outra preocupação de acordo com Croce (entrevista por *email*, 12 de março de 2024), em que "a disseminação de aplicativos e soluções com "*backdoors*", ou seja, que possibilitam o acesso sem o consentimento ou a consciência do operador" põe em causa a fiabilidade, classificação de segurança e utilidade da informação, essencial ao sucesso das OM.Em relação à Capacidade Técnica, Borges (op. cit.) salienta que um "elevado volume de dados disponíveis no TO" e um "número reduzido de analistas disponíveis", impõem desafios significativos, exigindo "um esforço contínuo" para processar e analisar dados eficazmente. Para Monteiro (entrevista presencial, em

23 de fevereiro de 2024), a necessidade de lidar com "ameaças diversificadas como terrorismo, ciberataques, guerras híbridas e crises humanitárias" neste contexto de recursos limitados exige uma gestão e formação técnica exemplares.

A Interoperabilidade reflete a capacidade de diferentes sistemas e entidades colaborarem efetivamente. De acordo com Borges (op. cit.), "a disseminação de informações atempadamente por parte das forças dos setores", ilustram os desafios de sincronização em tempo real porquanto a partilha de informações é apresentada por Fernandes (op. cit.), como como essencial, especialmente no âmbito de projetos como o *Joint Intelligence, Surveillance and Reconnaissance* (JISR), que promovem a mudança de paradigma de "necessidade de saber" para "necessidade de partilhar".

A Dinâmica Contemporânea é evidenciada por Monteiro (op. cit.) nesta dimensão, através da mudança em curso, onde "mudanças significativas no AO, caracterizadas por imprevisibilidade, surpresa, incerteza e mudanças contínuas" são necessárias para a adaptação ao AO, associado às inovações tecnológicas.

4.1.4. Dimensão Tecnológica

De acordo com o exposto pode inferir-se que o atual ambiente contemporâneo é marcado por uma constante mudança, onde a dimensão tecnológica está interligada com as restantes dimensões referidas anteriormente, evidenciado através das entrevistas com especialistas. **O Fator Humano e a Evolução Tecnológica** emergiram como indicadores desta dimensão.

O Fator Humano molda o AO, em que a capacidade de acessibilidade de informação e de influenciar atores se apresenta como essencial, não obstante o elevado desenvolvimento tecnológico, o fator humano continuará presente de acordo com Fernandes (op. cit.) pois "as forças da NATO irão operar no futuro num AO, que apesar de certamente complexo, mal definido, será de natureza centrada no ser humano". O campo de batalha do futuro será constituído por uma rede de relações e influências mútuas, através da participação ativa em redes de estruturas civis e militares, ligadas entre si com acesso à tecnologia (Marques, op. cit.). Baleia (op. cit.) reconhece a capacidade das forças de "influenciar atores e de gerar informações valiosas no terreno, pois "cada soldado é um elemento vital na recolha de informações", onde a habilidade de comunicar eficazmente com a população local transforma-se numa ferramenta para operações bem-sucedidas.

Deste modo, a Evolução Tecnológica surge como um catalisador de mudança no atual ambiente, em que de acordo com Cavaco (op. cit.) "a introdução

de drones, IA, e capacidades de ciberataques" redefinem o que é possível no TO. O desenvolvimento destas tecnologias para além de incremental, é disruptivo, exigindo uma reinterpretação da dissuasão e uma restruturação dos procedimentos operacionais. Estas inovações desdobram-se numa compreensão mais profunda do AO e permitem uma análise mais célere e informada das ameaças (Croce, op. cit.).

A imprevisibilidade e a surpresa, desafiam a integridade da tomada de decisão militar e exigem uma abordagem holística que abrange as diversas dimensões do ambiente de operações (Monteiro, op. cit.), onde a inclusão de *Unmanned Aircraft System* (UAS) para recolha de informação, ou a utilização de dados biométricos no acesso a áreas classificadas já contribuem para esse tipo de abordagem (Silva, op. cit.).

4.1.5. Síntese conclusiva

De acordo com os dados apresentados e em resposta à QD 1, fica patente a complexidade e amplitude dos desafios mencionados pelos especialistas no atual AO. A capacidade técnica não se limita apenas à posse de ferramentas adequadas, englobando também a habilidade de gerir eficazmente o volume de informação e de recursos humanos disponíveis. Simultaneamente, a segurança da informação emerge como um pilar fundamental, onde a luta contra a desinformação e a garantia da integridade dos dados são de importância capital.

Sublinha-se também a necessidade premente de abordagens inovadoras para superar os obstáculos identificados, onde a cooperação e a partilha de conhecimento podem contribuir para a mitigação destes desafios, promovendo um ambiente mais seguro e eficiente na análise de informações.

Assim, este panorama de mudança, oferece igualmente um terreno fértil para a investigação e para a exploração de novas estratégias que possam contribuir para uma maior eficácia das OM.

Numa sociedade contemporânea em que se vive o paradoxo do aumento das liberdades gerais e específicas e simultaneamente a intolerância ao respeito das diferentes ideologias, verifica-se que a probabilidade de descontrolo e difusidade social tem significativa margem de evolução.

Os desafios presentes nas dimensões apresentadas, intrinsecamente ligados à pressão social e económica, associados à globalização e à crescente tecnologização traduz-se em desafios à perceção real do ambiente securitário.

4.2. A *Identity Intelligence* como instrumento na produção de Informações Militares

Conforme referido anteriormente, o AO terá inúmero desafios, onde os Comandantes terão de estar preparados para compreender profundamente o ambiente que os rodeia para poderem decidir eficazmente no tempo disponível. Por conseguinte, as Informações são primordiais para desenvolver essa compreensão e melhorar o processo de decisão.

Para uma compreensão holística, é necessária uma aquisição e um desenvolvimento de conhecimento de modo a poder desenvolver a resposta a uma determinada situação num determinado momento (*insight*), bem como identificar e prever o que vai acontecer a seguir (*foresight*) (NATO, 2020). Deste modo, as IM contribuem para a contínua compreensão do AO, identificando as condições necessárias para atingir os objetivos desejados, evitando efeitos não desejados e avaliando o impacto nos atores adversários, amigos ou neutrais (NATO, 2020).

De acordo com as entrevistas realizadas, no atual AO, onde as ameaças são difusas, o elemento humano continua a ser primordial, no que diz respeito à prossecução de ações, ou da sua intenção de as perpetrar (Marques, op. cit.).

Os desafios globais atuais, como aponta Fernandes (op. cit.), carecem de "novas formas de pensar e reagir ao mundo" e na forma como influenciamos a tomada de decisões. A capacidade de ligar ameaças a indivíduos ou grupos, fundamentada em dados biométricos e na análise de redes humanas, capacita os comandantes com o conhecimento necessário para efetuarem ações precisas e até mesmo para neutralizar ameaças antes destas se materializarem. Perante cenários globalizantes de transnacionalidade criminosa e terrorista, tem sido feito um elevado esforço na criação de sistemas interoperáveis securitários assentes nos biométricos.

4.2.1. Eficácia e Eficiência

A Eficácia e Eficiência das IM moldam a capacidade de atuação das FFAA nas OM. De acordo com a análise de conteúdo das entrevistas, os indicadores identificados como a **Oportunidade da Informação e Qualidade da Informação,** são de extrema importância de onde se retiram contributos que ilustram como a I2 é crucial no contexto contemporâneo em OM.

A oportunidade da informação, associada à capacidade preventiva como Fernandes (op. cit.) refere, está intrinsecamente ligada à análise de redes humanas e ao *targeting*, transformando-se numa ferramenta imprescindível. Esta permite

"prevenir ataques ou planear operações com precisão" (Fernandes, op. cit.), minimizando danos colaterais através da capacidade de identificar, entender e antecipar comportamentos. A previsibilidade referida para além de reforçar a segurança, incrementa a capacidade de decisão para intervenções pontuais associadas à celeridade da informação.

A qualidade da informação, associada às informações detalhadas para a tomada de decisão, são um catalisador para decisões informadas para a conduta das OM. Conforme relata Marques (op. cit.), a utilização da tecnologia I2 "requer a manutenção de relações, processos e tecnologias" que integram dados atualizados e relevantes para responder aos *Critical Commander's Information Requirements* (CCIR), incrementando assim a qualidade da informação disponível.

A I2 destaca-se pela capacidade de "oferecer enorme eficácia nas avaliações e garantir a eficiência" de acordo com Marques (op. cit.). Esta eficiência decorre da capacidade de entender ameaças complexas e fornecer uma compreensão abrangente do AO, permitindo aos comandantes agir com confiança fundamentada em dados concretos e análises rigorosas, precipitando para, de acordo com as palavras de Silva (op. cit.), "um necessário ajustamento de técnicas, táticas e procedimentos até aqui utilizadas, procurando otimizar recursos e tornar o seu emprego eficaz e eficiente" permitindo desta forma uma compreensão abrangente do AO.

4.2.2. Inovação Tecnológica

O AO contemporâneo é dinâmico e pleno de oportunidades que quando associada à inovação tecnológica, podem contribuir positivamente para o futuro das FFAA e de forças de segurança.

As entrevistas realizadas apontam os indicadores, **Desenvolvimento Tecnológico, Adaptação e as atividades de Contrainformação**, como possibilidades para novas capacidades e abordagens, onde a I2 poderá contribuir significativamente para a condução de OM, nomeadamente na produção de IM.

Na produção de IM é necessário ter em conta, a tentativa de identificar os elementos que se poderão perfilar como ameaça, onde a identidade é um fator primordial no processo de tomada de decisão de um comandante (Fernandes, op. cit..).

O desenvolvimento tecnológico, conforme Cavaco (op. cit.) destaca, é crucial perante a crescente "complexidade das informações militares", exigindo "investimentos em tecnologia e capacitação". Esta é uma área em que as forças devem continuamente evoluir para manter a eficiência na tomada de decisão.

Para Monteiro, a Adaptação ao AO constitui-se como uma constante renovação, como a melhoria das "capacidades e tecnologias militares" (op. cit.), sendo também caracterizado pela abertura para "um mundo de pesquisa e descoberta" proporcionado pelo avanço tecnológico de acordo com Baleia (op. cit.).

Na produção de IM, utiliza-se o CPI, que de uma forma muito sucinta, é uma sequência de atividades, onde, através da obtenção de determinados dados, após uma análise cuidada é convertida em informações (conhecimento) para depois ser disseminada pelas entidades competentes (NATO, 2016).

Os analistas de Informações, utilizando a I2, iniciam o processo através de atributos de identidade conhecidos (dados biométricos), de modo a explorar os indivíduos e a rede onde estão inseridos. Para tal utilizam as assinaturas biométricas que estão disponíveis, integrando os dados biográficos ou situacionais de determinado indivíduo ou rede de indivíduos, cruzando a informação obtida com a *Human Network Analysis in Support to Targeting* (HNAT), conforme a figura seguinte:

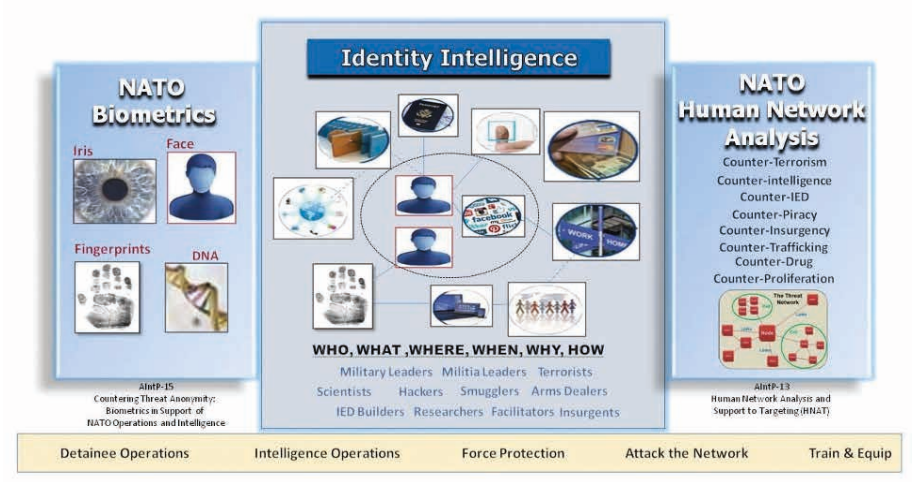

Figura 3 – Relação entre Biometria, HNAT e I2
Fonte: Adaptado de NATO (2017a).

Como se pode deduzir, as informações com a I2 revelam-se de extrema importância, permitindo fornecer aos comandantes na tomada de decisão, a identificação dos perpetradores de uma possível ameaça, de que forma a poderão executar, bem como a sua localização, fornecendo um conhecimento abrangente do AO envolvente (NATO, 2017a).

Nesta conformidade a Adaptação surge como necessidade premente, em que, de acordo com Borges (op. cit.), a recolha de informações via UAS e o desenvolvimento de "sistemas de armas avançados e de maior precisão" melhoram a capacidade operacional e a segurança dos soldados no terreno. A interação com civis, o uso de UAS e a identificação de indivíduos ou grupos através de dados biométricos em apoio a operações demonstram como a adaptação é imprescindível para as forças em OM, em que segundo Fernandes (*op. cit.*) "a NATO avançou para uma capacidade moderna de identificação de ameaças para enfrentar coletivamente os desafios do anonimato em ambientes assimétricos e conflito híbridos através da biometria".

Nesta senda, as atividades de Contrainformação, nomeadamente na identificação de ameaças, será incrementada pela I2 de acordo com Marques (op. cit.), pois eliminará a anonimidade e proporcionará contributos mais precisos para o *targeting*. Para Croce (op. cit.), este desenvolvimento contribui significativamente para a "proteção da força" e permite uma análise mais incisiva das ameaças, evidenciando a importância da contrainformação, na identificação e posterior neutralização de ameaças, assim como na identificação de vulnerabilidades.

4.2.3. Limitações

Independentemente dos aspetos positivos anteriormente elencados, importa destacar que a I2 apresenta algumas limitações, referentes ao **enquadramento legal** que representa um obstáculo considerável, sobretudo no concernente à impossibilidade de recolha de dados biométricos fora da área de operações e referentes a questões **organizacionais**, de acordo com as entrevistas efetuadas. Nas palavras de Fernandes (op. cit.), as restrições legais referentes à proteção de dados e a falta de regulamentação internacional são desafios que limitam a partilha de informações vitais para o planeamento e execução das OM.

No enquadramento legal, a aplicação de políticas de proteção de dados coloca limitações na recolha e uso de informações pessoais, vitais para a I2, de acordo com Fernandes (op. cit.), em que "ao nível NATO esta ferramenta serve

apenas para operar dentro da área de operações, não podendo ser recolhida, sem autorização, informações de cidadãos nacionais e partilhá-la naquilo que é base de dados de I2 da NATO".

As OM, ao cruzarem fronteiras jurisdicionais, confrontam-se com a incompatibilidade regulamentar, o que pode atrasar ou até impedir ações e decisões militares. Adicionalmente, a necessidade de consentimento, muitas vezes inalcançável em teatros de operações, coloca obstáculos éticos e práticos ao recolher dados tal como Reis (entrevista presencial, 15 de fevereiro de 2024) indica "as pessoas não são obrigadas a participarem na recolha de dados biométricos e pessoais".

Em termos organizacionais, a especialização torna-se um requisito incontornável. Pessoal qualificado em I2 é essencial para interpretar dados complexos e assegurar a sua aplicabilidade operacional, pois tal como Fernandes (op. cit.) indica "a I2 requer a manutenção de relações, processos e tecnologias para fornecer informações atempadas que apoiam os CCIR".

As infraestruturas precisam de ser robustas e seguras para processar e armazenar informações sensíveis, sendo necessário para Fernandes (op. cit.) "a criação de um espaço dedicado a esta ferramenta". Por fim, a atualização constante de dados é crucial; a validade da I2 depende da precisão e atualidade da informação, exigindo um compromisso com a manutenção contínua de bases de dados, onde "é necessário um investimento monetário e de pessoal dedicado a esta área" (Fernandes, op. cit.).

4.2.4. Síntese Conclusiva

Como se pode constatar, a I2 torna-se um instrumento vital para compreender e mitigar as ameaças de forma célere e eficaz. Em resposta à QD 2, poderá afirmar-se que a ferramenta I2, oferece uma visão holística que transcende o simples armazenamento de dados, proporcionando uma capacidade de antecipação e prevenção na conduta das OM, permitindo uma tomada de decisão mais eficaz. O empenhamento e o emprego eficiente de recursos operacionais dependem da capacidade de discernir, com precisão, quem, quando e como se interage no AO.

Estas oportunidades, refletidas no discurso dos entrevistados, desdobram-se em vários indicadores. Evidencia-se que a inovação e adaptação tecnológica, alinhados com uma gestão das relações humanas e uma abordagem proativa da contrainformação, são os pilares para transformar desafios do atual AO em

vantagens, onde a I2 impactará as OM. As FFAA, munidas desta ferramenta, estarão mais preparadas para enfrentar os desafios do futuro, garantindo segurança e vantagem operacional num AO que se transforma rapidamente.

No contexto policial a utilização de biometria já é um facto consolidado, sendo que num futuro próximo, as vertentes policiais e militares indubitavelmente terão de se cruzar face à multidimensionalidade do espetro da ameaça. Neste sentido, a inclusão doutrinária da I2 é expectável assim como a sua implementação gradual de acordo com o risco e ameaça (Silva, op. cit.).

4.3. Contributos da *Identity Intelligence* para a conduta das Operações Militares nas Forças Armadas Portuguesas em Forças Nacionais Destacadas

O processo de *targeting* conduzido por informações concisas e fidedignas, permitirá aos comandantes os detalhes necessários para atingir determinado efeito, bem como a audiência, onde a I2 através da identificação positiva o permite efetuar (NATO, 2020).

No que diz respeito às FFAA portuguesas e à condução de OM em FND, a utilização desta ferramenta ainda é escassa, estando as FFAA portuguesas a dar os primeiros passos em formação de operadores para utilização desta ferramenta (Marques, op. cit.).

De acordo com as entrevistas realizadas, o contributo das IM para as OM, nomeadamente na RCA, foi referido um conjunto de oportunidades de melhoria, relativos aos **recursos humanos, a necessidade de desenvolvimento tecnológico** associados às suas **missões operacionais**, conforme figura seguinte:

Assim, segundo os entrevistados, os indicadores identificados constituem os pilares desta análise, refletindo as barreiras que as FFAA portuguesas enfrentam, delineando por outro lado áreas críticas para o desenvolvimento e a inovação, onde a I2 poderá contribuir sobremaneira.

As limitações nos recursos humanos são explanadas pela necessidade de formação e experiência. Como revelado por Borges (op. cit.), a formação das FND nas áreas das informações é frequentemente breve e superficial, destacando a lacuna no desenvolvimento das competências essenciais, como a falta de familiaridade prévia com funções especializadas, que podem comprometer a execução das missões.

A necessidade de desenvolvimento tecnológico é realçada pelas limitações técnicas aparentes, tais como a falta de *software* avançado capaz de garantir a segurança e a integração eficiente das informações, bem como ferramentas para criar um quadro operacional unificado (Borges, op. cit.). A situação é exacerbada por bases de dados rudimentares, onde a organização de informações ainda depende de sistemas como o *Excel*, evidenciando a necessidade de otimização no processamento de dados (Borges, op. cit.).

No que concerne à missão operacional, a dependência externa para recolha de informações surge como um ponto de fragilidade, onde as FND em estudo dependem excessivamente de informações oriundas de redes locais, tais como estruturas políticas locais, o que pode afetar a autonomia e a veracidade dos dados recolhidos (Monteiro, op. cit.). De modo a responder à QC do presente trabalho poderá observar-se a matriz SWOT apresentada na figura 4, onde é possível verificar a análise do Impacto da I2 nas OM, demonstrando que esta ferramenta pode otimizar a forma como as operações podem ser efetuadas, naquilo que são as suas vantagens (Forças e Oportunidades), bem como naquilo que são as suas limitações (Fraquezas e Ameaças) no ambiente interno e externo.

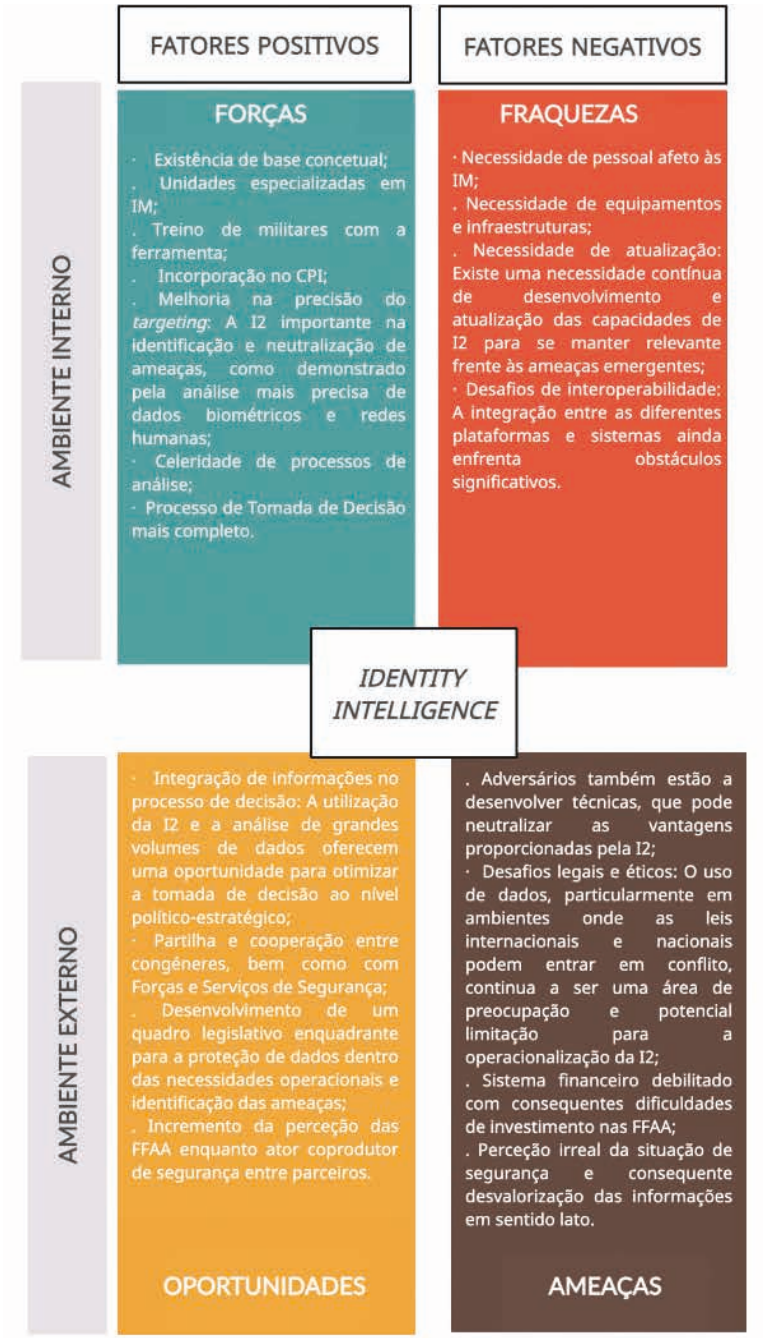

Figura 4 – Matriz SWOT para "Impacto da I2 nas Operações Militares"

Torna-se evidente que capacitando as FFAA portuguesas com a I2, a identificação das ameaças tornar-se-á mais célere, oferecendo uma oportunidade de melhorar e antecipar a tomada de decisão, no atual AO, contribuindo para a otimização da condução das OM.

A compreensão holística e a capacidade de identificar os atores humanos, a adaptação às evoluções da ameaça e o domínio das novas tecnologias são agora indissociáveis da excelência operacional, tendo sido os fatores que todos os especialistas entrevistados ressalvaram. Neste contexto, a análise de informações e a inovação tecnológica não são meros complementos à condução de OM, fazem parte dos seus alicerces fundamentais.

A capacidade de antecipar e responder de forma eficaz às transformações do AO é uma das marcas distintivas das FFAA que pretendem liderar a vanguarda no seu campo de atuação, em que a I2 poderá contribuir sobremaneira para esse desiderato.

5. CONCLUSÕES

O AO atual necessita de uma compreensão holística das transformações e dinâmicas oriundas de uma sociedade progressivamente integrada e complexa, muito devido à evolução tecnológica emergente. Neste cenário, as Informações procuram uma constante renovação, adaptação e alinhamento, visando contribuir decisivamente para a tomada de decisão em OM (Silva, 2023, pp. 23-25).

A inovação tecnológica tem sido uma aliada na criação de métodos avançados de recolha e análise de dados, cruciais para o processamento de Informações. A análise de informações e o avanço tecnológico não são apenas complementares às OM; constituem o seu fundamento.

Neste desiderato a I2 emerge como um recurso valioso na conduta de OM, justificada pela imperiosa necessidade de métodos inovadores, visto que as FFAA contemporâneas são desafiadas não apenas por adversários convencionais, mas por uma miríade de ameaças que se camuflam na constante evolução do AO. Face ao caudal avassalador de dados que permeiam o AO, é fundamental extrair a informação decisiva para a tomada de decisões com a maior brevidade possível, onde a I2 permitirá identificar de forma mais célere as ameaças, permitindo, no limite, a sua neutralização antes destas se efetivarem, contribuindo com um produto especializado de informações.

O procedimento metodológico adotado neste estudo baseou-se numa abordagem qualitativa, ancorada em entrevistas semiestruturadas a especialistas na área das informações e em I2, bem como numa análise documental, de modo a responder às questões de investigação. Este processo permitiu a identificação de dados e perspetivas diversas, essenciais para compreender as possibilidades da I2 dentro do AO contemporâneo e a sua relevância na produção de IM, contribuindo para alimentar o CPI, permitindo também a sua confrontação com as exigências práticas das OM e a sua influência na tomada de decisão.

Os resultados alcançados, expostos no capítulo 4 'Apresentação dos dados e Discussão de Resultados' refletem uma clara correlação entre a integração da I2 e a otimização da conduta das OM destacando-se contributos essenciais que permitiram atingir o OG: Avaliar como pode a I2 otimizar a conduta das OM face ao atual AO.

Assim, observou-se que a I2, ao integrar dados precisos e atualizados, possibilita a tomada de decisões mais informadas, contribuindo significativamente para a proatividade das ações militares, incrementando em geral a capacidade preventiva e a eficiência no *targeting*. Particularmente, ressalva-se a capacidade da I2 em acrescentar valor ao processo de tomada de decisão através da identificação e análise de padrões comportamentais e respetivas ligações a indivíduos ou grupos de interesse.

As análises dos especialistas apontam para a relevância do desenvolvimento tecnológico aliada a uma postura ativa contra a desinformação, estabelecendo assim as bases para converter os desafios contemporâneos em oportunidades. Possuindo ferramentas como a I2, as forças militares encontram-se numa posição privilegiada para lidar com os desafios emergentes, assegurando proteção operacional num contexto global em constante transformação. Os desafios sociais associados à globalização e à crescente tecnologização e dependência social, económica e informacional traz enormes potencialidades e desafios à perceção real do que é a segurança, verificando-se que, perante cenários globalizantes de transnacionalidade criminosa e terrorista, tem sido feito um elevado esforço na criação de sistemas interoperáveis securitários assentes nos biométricos.

Desta forma, a resposta à QC: "Como pode a I2 contribuir para a otimização na conduta das Operações Militares no atual ambiente operacional?" é concretizada, na medida em que, caso as FFAA disponham desta ferramenta, incorporando o seu produto final no CPI, a deteção de ameaças e a melhoria na tomada de decisões

tornam-se mais exequíveis e consequentemente céleres, potenciando a eficiência operacional no AO atual, capacitando as FFAA para antever e reagir com eficácia às mudanças no AO, característica distintiva das FFAA naquilo que é o seu core.

O presente estudo expandiu o conhecimento existente ao elucidar como a I2 pode ser operacionalizada dentro do paradigma das OM, destacando a sua aplicabilidade prática, naquilo que foi a identificação de indicadores. Evidencia-se desta forma, a relevância da I2 nas OM das FFAA Portuguesas, percebendo-se que esta ferramenta poderá ser útil, oferecendo outro tipo de capacidades à realidade altamente complexa das operações contemporâneas, tendo sido o pilar desta investigação a forma como a I2 pode ser utilizada para melhorar a condução operacional das OM. Destaca-se ainda a I2 como uma ferramenta importante na arquitetura das informações contemporâneas. A existência de uma base concetual sólida, unidades especializadas em IM, bem como o treino e especialização nesta ferramenta são também fatores positivos que sustentam a sua integração na produção de IM. Por outro lado, a partilha de IM com FFAA congéneres são também oportunidades que as FFAA portuguesas devem assimilar e aproveitar. Contudo é importante ressalvar que associados aos fatores positivos, existem desafios que devem ser ultrapassados, onde a necessidade de pessoal afeto às IM é sobremaneira importante. A necessidade de infraestruturas e de equipamentos interoperáveis na sua plenitude, também são obstáculos que as FFAA devem ultrapassar para conseguir operacionalizar esta ferramenta e melhorar o produto de IM. Em todo o caso, ressalva-se que estes obstáculos estão intimamente ligados ao ambiente externo, onde para além dos desafios legais e éticos associados à recolha de dados biométricos, a falta de investimento como um todo nas FFAA pode colocar em causa o desenvolvimento e utilização da I2, onde conforme foi evidenciado, uma falsa perceção de segurança na sociedade em geral, tem impacto nas decisões políticas nesse âmbito.

Apesar dos contributos significativos obtidos, o estudo reconhece limitações, incluindo a concentração geográfica nas FFAA Portuguesas e a ausência de um estudo de caso empírico que exemplificasse a I2 numa ação real. A limitada variedade de especialistas consultados pode ter influenciado a abrangência das perspetivas sobre o tema, bem como o facto de determinados dados serem de carácter classificado.

Para futuras investigações, recomenda-se a incluir um leque mais amplo de OM internacionais e a implementação de estudos de caso detalhados que ilustrem o impacto direto da I2, tendo em conta os indicadores identificados por esta

investigação, em cenários operacionais específicos. Adicionalmente, seria frutífero explorar as ligações éticas e legais inerentes à recolha e análise de dados na I2, bem como as implicações para a privacidade e direitos humanos.

Na ordem prática, aconselha-se a adoção de políticas de formação contínua especializada, o investimento em infraestruturas de dados robustas, e a criação de protocolos claros para a atualização e partilha constante de informação. Sugerem-se também parcerias estratégicas para o desenvolvimento de tecnologias de I2, e a implementação de mecanismos de revisão e *feedback* que assegurem a sua adequação contínua num AO em evolução.

As recomendações fornecidas por esta pesquisa estimulam uma compreensão mais aprofundada do papel da I2 e facilitam a progressão para a consolidação das capacidades defensivas nacionais no âmbito das OM, interagências e multidimensionais.

REFERÊNCIAS BIBLIOGRÁFICAS

Allenby, B. R. (2000). Environmental Security: Concept and Implementation. International Politic*al Science Review / Revue Internationale de Science Politique, 21*(1), 5–21. http://www.jstor.org/stable/1601426

Baber, P., Baker, P., & Dotson, M. (2020). Identity Intelligence contributes to Multi-Domain Operations. *Military Intelligence*, 24-28. https://www.ikn.army.mil/apps/MIPBW/MIPB_Features/Baber.pdf

Burton, F. (2005). *The Problem of HUMINT*. Stratfor. https://worldview.stratfor.com/article/article/problem-humint

Cascio, J. (2021). Criador do termo BANI explica como sobreviver na era do caos. *Você RH*. https://vocerh.abril.com.br/futurodotrabalho/criador-do-termo-bani- explica-como-sobreviver-na-era-do-caos/

Chiavenato, I. (1994). *Recursos humanos na Empresa: pessoas, organizações e sistemas*. São Paulo: Atlas.

Clausewitz, C. V. (1832). *Da Guerra,* 2ª edição. Mem-Martins: Europa-América.

Exército Português. (2012). *PDE 3-00 Operações*. Lisboa: Exército Português.

Fernandes, José. (2023, novembro). Taxionomia e Produto das Informações. Em Instituto Universitário Militar, *Pós Graduação em Informações Militares*. Organizado pelo Instituto Universitário Militar.

Gabinete do Chefe de Estado-Maior-General das Forças Armadas. (2021). *Diretiva Estratégica do EMGFA 2021-2023*, Lisboa: Autor.

Garrett, D & Jones, R. (2023, fevereiro). *Attribute Collection, PED, Data Flow/ Analysis. Em NATO Maritime Interdiction Operational Training Centre, Nato Identity Intelligence Analyst in a complex environment course*. Organizado pela NATO Maritime Interdiction Operational Training Centre.

Gomez, C., 2005. Cooperación Internacional en Matéria de Inteligencia Militar. *Cuadernos de Estratégia* No. 130.

Governo de Portugal. (2013). *Conceito Estratégico de Defesa Nacional*. https://www.defesa.gov.pt/pt/pdefesa/estrategia/CEDN/Paginas/default.aspx

Greer, K. B., James K. (2023, maio 1). *War in 2050: The Army's Operating Concept After Next*. Modern War Institute. https://mwi.westpoint.edu/war-in-2050-the-armys-operating-concept-after-next/

Hill, M & Hill, A. (2005). *Investigação por Questionário (2.aEd.)*. Lisboa: Edições Sílabos IUM. (2019). *Manual Escolar, Planeamento de Operações Conjuntas e Combinadas, Nível Estratégico e Nível Operacional*. Instituto Universitário Militar.

Lind, W. S. (2004). Understanding Fourth Generation War. *MILITARY REVIEW*.

Maathuis, C., & Chockalingam, S. (2023). Tackling Uncertainty Through Probabilistic Modelling of Proportionality in Military Operations. *Proceedings of the European Conference on Cyber Warfare & Security*, 276–284. https://search.ebscohost.com/login.aspx?direct=true&db=tsh&AN=164740825&lang=pt-pt&site=ehost-live

Manolache, I. C. (2023). The Role of Multi-Domain Operations in Modern Warfare. *Land Forces Academy Review, 28*(3), 163–170. https://doi.org/10.2478/raft-2023-0020

Ministério da Defesa Nacional, (2005). *Regulamento de Campanha Operações*. Lisboa: Exército Português.

Morse, J. M. (2000). Determining Sample Size. *Qualitative Health Research, 10*(1), 3–5. https://doi.org/10.1177/104973200129118183

Narciso, T. (2010). Interoperabilidade Organizacional na Administração Pública, Universidade de Aveiro.

NATO (2016). *NATO Standard AIntP-15 Countering Threat Anonymity: Biometrics in Support of Nato Operations and Intelligence*. NATO Standardization Office.

NATO (2017a). *Annex to PO (2017) 0407 - Concept for Identity Intelligence*. NATO Standardization Office.

NATO (2017b). *NATO Standard AIntP-13 Human Network Analysis and Support to Targeting (HNAT)*. NATO Standardization Office.

NATO (2020). *NATO Standard AJP-2 Allied Joint Doctrine for Intelligence, Counterintelligence and Security*. NATO Standardization Office.

NATO (2021). *NATO Standard AJP-3.9 Allied Joint Doctrine for Joint Targeting*. NATO Standardization Office.

NATO (2022). *NATO Standard AJP-2.1 Allied Joint Doctrine for Intelligence Procedures*. NATO Standardization Office.

NEP/INV-001. (2020). *Procedimentos relativos à elaboração de trabalhos de investigação realizados no âmbito de cursos que não atribuem grau académico*. Lisboa: Instituto Universitário Militar.

Priberam. (sem data). Definição de Eficiência. https://dicionario.priberam.org/efici%C3%AAncia

Rodrigues, L. (2013). *Operações Militares Modernas: Adaptabilidade um requisito de Liderança Pedrouços Instituto Universitário Militar*. https://comum.rcaap.pt/bitstream/10400.26/10005/1/TII_OPERA%c3%a7%c3%b5es%20militares%20modernas_adaptabilidade%20um%20requisito%20de%20lideran%c3%a7a_final_revisto.pdf

Santos, C. A. G. D., 2012. *Emprego do Poder Militar na Atualidade e Cultura Organizacional das Instituições Militares – Reflexões*. Rio de Janeiro, Brasil, ECEME

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

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

Scheffler, A., & Dietrich, J.-H. (2023). Military Intelligence: Ill-Defined and Understudied. *Internacional Journal of Intelligence and Counterintelligence, 36*(4). Retirado de https://www.tandfonline.com/doi/epdf/10.1080/08850607.2023.2187190?

Silva, C. (2023). As informações Militares no Exército Português—Perspetivas e Desafios. *Jornal do Exército, 726,* 22–25.

Silva, C. M. C. R. M. (Coord.) (2019). *Informações, Contrainformação e Segurança enquanto instrumentos Militares Contribuintes para a Segurança e Defesa Nacional*. Coleção "ARES", 33. Lisboa. Instituto Universitário Militar.

Silva, C., & Ribeiro, F. (2018). Military Intelligence: A Tool of National Security and Defence. *Revista de Ciências Militares, VI*(2), 177–205. http://comum.rcaap.pt/bitstream/10400.26/34630/2/Military%20intelligence%20...%20%28ing%29_Carlos%20Silva%20%26%20Fernando%20Ribeiro.pdf

Sousa, S. J. M. (2020). *No Planeamento e Condução de Operações Militares*. Instituto Universitário Militar, Lisboa.

Telo, A. J., 2002. Reflexões sobre a Revolução Militar em Curso. In: *Nação e Defesa* Nº103 Outono-Inverno 2002 2ª Série. Lisboa: Academia Militar – CINAMIL (Centro de Investigação da Academia Militar), 211-249.

UK Ministry Of Defense. (2023). *Joint Doctrine Publication 2-00*.

Viana, C. (2010). O Princípio da eficiência: A eficiente eficácia da administração pública. *Revista da Faculdade de Direito da Universidade do Porto,* VII , 301–311.

ESTUDO 5 – OS CONTRIBUTOS DA BASE TECNOLÓGICA E INDUSTRIAL DE DEFESA PARA O DESENVOLVIMENTO DAS CAPACIDADES DAS FORÇAS ARMADAS[31]

THE CONTRIBUTIONS OF THE DEFENSE TECHNOLOGICAL AND INDUSTRIAL BASE TO THE DEVELOPMENT OF THE ARMED FORCES' CAPABILITIES

José Manuel Figueiredo Moreira
Coronel de Infantaria

Paulo Jorge Barbosa Rodrigues
Capitão-de-mar-e-guerra EN-MEC

RESUMO

O regresso à Europa da guerra de alta intensidade evidenciou as debilidades do setor industrial europeu de defesa para providenciar às Forças Armadas as capacidades necessárias para enfrentar esta tipologia de conflitos. Portugal, em 2023, e a UE, em 2024, aprovaram estratégias para desenvolver a indústria de defesa, considerada um pilar fundamental para garantir uma autonomia estratégica em setores-chave dos Estados. Para formular orientações que promovam um maior contributo da base tecnológica e industrial de defesa para o desenvolvimento das capacidades das Forças Armadas, a investigação decorreu sob três perspetivas de análise relacionadas com a estratégia, as interações organizacionais e o processo de planeamento de defesa. Concluiu-se que a estratégia aprovada é adequada para alcançar os objetivos, mas necessita de instrumentos jurídicos e financeiros para sua implementação. Embora haja entendimento entre as entidades do ecossistema e a IdD Portugal Defence tenha um papel central como interlocutora entre Forças Armadas e indústria, ainda há problemas nos processos, recursos e competências. Além disso, o planeamento de defesa e a execução da lei de programação militar são áreas que mais precisam de ajustes e decisões para aumentar a participação da indústria em projetos militares.

Palavras-chave: base tecnológica, capacidades, ciclo de planeamento, defesa nacional, estratégia, Forças Armadas, idd Portugal *Defence*, indústria de defesa, programação militar

[31] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto (CEMC 2023/2024). A versão integral encontra-se disponível no Centro de Recursos do Conhecimento do Instituto Universitário Militar.

ABSTRACT

The return of high-intensity warfare to Europe has highlighted the weaknesses of the European defense industrial sector in providing the Armed Forces with the necessary capabilities to face this type of conflict. Portugal, in 2023, and the EU, in 2024, approved strategies to develop the defense industry, considered a fundamental pillar to guarantee strategic autonomy in key sectors of states. In order to formulate guidelines that promote a greater contribution from the defence technological and industrial base to the development of the Armed Forces' capabilities, the research was carried out from three perspectives of analysis related to strategy, organizational interactions and the defence planning process. It was concluded that the approved strategy is suitable for achieving the objectives but needs legal and financial instruments for its implementation. Although there is understanding between the entities in the ecosystem and IoD Portugal Defence has a central role as an interlocutor between the Armed Forces and industry, there are still problems with processes, resources and competencies. In addition, defense planning and the execution of the military programming law are areas that most need adjustments and decisions to increase industry participation in military projects.

***Keywords**: technological base, capabilities, planning cycle, national defense, strategy, Armed Forces, idd portugal defence, defense industry, military programming*

1. INTRODUÇÃO

O reaparecimento de conflitos armados no flanco Este da Europa, relançou a discussão ao nível da sociedade, em geral, e dos decisores políticos, em particular, sobre a necessidade de uma maior autonomia estratégica e de um maior investimento em Capacidades Militares (CM) (Monteiro, 2023, p. 1). Para esta autonomia estratégica, o setor industrial de defesa assume um papel crucial na obtenção dos objetivos políticos, com a economia de defesa a ter cada vez mais peso na economia nacional dos países. Reconhecendo que a capacidade de defesa da Europa, assenta numa Indústria de Defesa (ID) forte e reativa, a Comissão Europeia (CE) aprovou em março de 2024, a primeira Estratégia Industrial de Defesa Europeia (EIDE) com um programa de implementação e um conjunto de medidas promotoras de mais e melhor investimento em CM e de duplo-uso europeias (CE, 2024, p. 2).

Portugal tem acompanhado a tendência europeia e da Aliança Atlântica, tendo promulgado em 2010, a primeira Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa (EDBTID), numa lógica de alinhar "[…] o esforço de racionalização e eficiência a nível nacional com os princípios e objetivos da Estratégia […] Europeia, subscrita em maio de 2007, pelos Estados Membros

da Agência Europeia de Defesa" (Resolução do Conselho de Ministros [RCM] nº 35/2010 de 6 de maio, 2010, p. 1600).

A inadequabilidade desta estratégia para potenciar a Base Tecnológica e Industrial de Defesa (BTID) num contexto de profundas alterações geopolíticas e geoestratégicas, requereu a aprovação, 13 anos depois, de uma nova EDBTID[32], na qual Portugal enseja ter uma ID inovadora e competitiva, imprescindível para reforçar a autonomia estratégica e a capacidade de resposta das Forças Armadas (FFAA) portuguesas (RCM52, 2023, p. 26). É uma estratégia que ambiciona mitigar a fraca participação da ID nacional na edificação de CM. Este problema, para ser ultrapassado, exigirá um esforço coletivo e o envolvimento de "todos os intervenientes com responsabilidades na promoção, dinamização e consolidação das competências, capacidades, oportunidades e desafios que se colocam à BTID" (RCM52, 2023, p. 38).

Surge assim, uma estratégia cuja operacionalização dependerá da concretização dos objetivos delineados no Plano de Ação Estratégico (PAE) recentemente aprovado[33]. O sucesso deste plano assenta no contributo de um conjunto de entidades vinculadas entre si por um esforço de trabalho participativo e colaborativo. O espaço que este assunto ocupa na atual agenda política nacional e europeia, torna a temática, pela sua tempestividade, num fator de interesse e oportunidade significativos na elaboração deste trabalho, que se propõe formular orientações que potenciem o contributo da BTID no desenvolvimento das capacidades das FFAA e, ainda, para adequar o planeamento estratégico militar à satisfação dos objetivos da Defesa (Ribeiro, 2006, p. 7).

O objeto de investigação deste trabalho é o ecossistema do Setor da Defesa (SD), constituído pelas entidades que enformam a Estrutura Superior de Defesa Nacional (ESDN), a empresa IdD Portugal *Defence* S.A. (IdD) e a BTID. O Objetivo Geral (OG) desta investigação é formular orientações para, dentro do ecossistema do SD, otimizar a contribuição da ID nacional para o desenvolvimento das capacidades das FFAA portuguesas. Para atingir o objetivo geral e melhor enquadrar o processo de investigação definiram-se os seguintes Objetivos Específicos (OE): OE 1: analisar a adequabilidade da EDTBID para potenciar a participação da ID no desenvolvimento das capacidades das FFAA; OE 2: analisar as interações entre

[32] Aprovada pela RCM n.º 52/2023 de 5 de junho de 2023.
[33] Aprovado por Despacho do Secretário de Estado da Defesa Nacional de 16 de fevereiro de 2024

as entidades da ESDN, a IdD e a ID, enquanto responsáveis pela *governance* do desenvolvimento de CM; OE 3: avaliar o nível de participação da IdD/ID no CPD.

Para uma melhor orientação do processo de investigação, identificou-se uma Questão Central (QC) à qual o trabalho, no seu todo, pretende dar resposta: De que forma o ecossistema do SD pode otimizar a contribuição da ID nacional para o desenvolvimento das capacidades das FFAA portuguesas?

Este trabalho desenvolve-se ao longo de seis capítulos, com esta introdução a materializar o primeiro e as conclusões o último. O segundo capítulo compreende os aspetos essenciais à investigação relacionados com a revisão da literatura, os conceitos estruturantes, o Modelo de Análise e a metodologia e método de investigação. O terceiro capítulo debruça-se sobre a EDBTID, iniciando-se com a análise do atual contexto interno e externo do setor industrial de defesa para, após uma caraterização da estratégia, inferir da adequabilidade e conformidade da mesma face aos objetivos que se propõe atingir. O quarto capítulo assenta na análise às entidades do ecossistema do SD para, através das suas interações, dos mecanismos implementados e dos processos instituídos, se aferir o grau de maturidade das sinergias criadas e a expressão do trabalho colaborativo praticado entre essas entidades. No quinto capítulo é feita a avaliação do nível de participação da IdD/ID no CPD e, também, da relevância da Lei de Programação Militar (LPM) para capacitar a ID. O capítulo das conclusões compreende uma súmula dos resultados da investigação com resposta à QC do TII e do seu contributo para o conhecimento científico. Refere ainda as limitações da investigação e apresenta recomendações e sugestões para futuros trabalhos.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Ao introduzir a noção de competitividade, Couto (2004), p. 215) apresenta um conceito de estratégia evolutiva e adaptável ao meio empresarial e que permite enquadrar a EDBTID como: "ciência e arte de, à luz dos fins de uma organização, estabelecer e hierarquizar os objetivos, e gerar, estruturar e utilizar os recursos, tangíveis e intangíveis, a fim de se atingirem aqueles objetivos num ambiente admitido como conflitual ou competitivo".

O sucesso da participação da ID no desenvolvimento das capacidades das FFAA muito dependerá do desempenho das entidades do ecossistema e da sua capacidade de interoperarem a nível organizacional. Para a CE (2017, p. 24) a interoperabilidade organizacional refere-se à forma como as administrações

públicas alinham os seus processos empresariais, responsabilidades e expectativas para atingir objetivos acordados em comum e mutuamente benéficos.

Designa-se planeamento estratégico, o processo para estabelecer e hierarquizar os objetivos, que segundo Ribeiro (2006, p. 1) consiste em "articular com coerência os meios nacionais de natureza política, económica, psicossocial e militar, no espaço e no tempo de ação para, em situações de disputa internacional, materializar os objetivos nacionais".

Da pesquisa bibliográfica efetuada, foi possível constatar que as principais fontes literárias sobre esta temática foram formuladas num contexto geoestratégico mundial sem crises pandémicas, conflitos estatais e guerras de alta densidade e, portanto, sem ameaças aos interesses vitais dos estados que menosprezaram as suas capacidades de defesa desinvestindo nas indústrias de defesa (Conselho da União Europeia [CUE], 2022, p. 24).

Outro aspeto verificado foi a relação direta entre o volume e qualidade de artigos científicos produzidos e os momentos de importantes alterações normativas no setor que afetaram o relacionamento da ID com as FFAA. Foi o caso da aprovação da EDBTID em 2010, com a investigação científica sobre os investimentos na Defesa e a BTID a ganhar novo fulgor.

Em 2016, a nível europeu, surgem dois documentos estruturantes no âmbito da economia de defesa: A Estratégia Global da UE e o Plano de Ação Europeu. Esta legislação alterou significativamente o pensamento sobre a importância da autonomia estratégica e do desenvolvimento da ID (RCM52, 2023, p. 26).

Em termos nacionais, a restruturação da IdD em 2020 determina uma nova fase para a investigação científica face ao papel preponderante desta empresa na implementação da atual EDBTID. A responsabilidade que lhe está acometida de elaborar o PAE da EDBITD traduz num novo desafio ao status quo vigente entre as entidades do ecossistema do SD (RCM52, 2023, p. 28).

Por último, a nova EDBTID aprovada em 2023 e a EIDE em 2024 assumem-se como principais catalisadores para uma profunda reforma dos modelos de planeamento e de desenvolvimento de CM, com a ID a assumir-se como um elemento ativo e determinante na capacitação dos Estados como garantes da segurança e defesa dos respetivos territórios (CE, 2024, p. 1).

Da investigação realizada sobre a ID conclui-se que o desenvolvimento de capacidades para as FFAA tem tido um impacto pouco significativo na economia do sector industrial de defesa (Ferreira, 2013, p. 4). Basicamente, só a partir de

2016 se denota na Europa uma lenta consciencialização para a necessidade de uma maior autonomia estratégica face aos Estados Unidos da América, orientada para a edificação de capacidades ligadas à defesa e segurança, com uma aposta clara do desenvolvimento de uma BTID Europeia "inovadora, competitiva e resiliente", inserida no conceito de uma "Europa de Defesa" (RCM52, 2023, p. 26).

Circunscrevendo o estado da arte à relação entre a BTID e as FFAA, identificaram-se dois trabalhos com particular interesse para o desenvolvimento desta investigação. Machado (2021, pp. 27-30) que estudou o posicionamento de Portugal perante o Fundo Europeu de Defesa (FED) e os contributos que daí podem advir para as capacidades das FFAA. Este estudo focou-se nas oportunidades para a BTID e para o Sistema Científico e Tecnológico Nacional (SCTN), decorrentes desta fonte de financiamento europeu, para suprir as lacunas do sistema de forças nacional. Num estudo mais recente sobre os investimentos da defesa, Monteiro (2023, pp. 27-30), centrou a sua pesquisa na interação entre as entidades do SD, da indústria e dos atores externos às FFAA, apontando um conjunto de elementos de ação potenciadores de uma melhor concretização dos projetos inscritos na LPM.

Um aspeto relevante que o estado da arte permitiu inferir, foi a inexistência de investigação quanto ao objeto de estudo deste TII, particularmente sobre as dimensões em que se articula o seu MA. Importa agora aditar à sua originalidade um novo e tangível conhecimento.

2.1. Modelo de análise

O Quadro 1 esquematiza a forma como a partir do OG e da QC se identificaram três OE e levantaram as respetivas Questões Derivadas (QD).

O tratamento dos dados provenientes da análise documental e das entrevistas semiestruturadas efetuadas, permitiu, com base nos indicadores definidos, abordar a problemática do estudo nas três dimensões em que foi investigado cada um dos OE. Na dimensão legislativa, centra-se o estudo na EDBTID para deduzir sobre a sua adequabilidade. Na dimensão estrutural/organizacional procura-se conhecer a predisposição das organizações para se tornarem interoperáveis. Na dimensão operacional, avalia-se, num processo de planeamento em concreto, a efetiva interação entre os colaboradores.

Quadro 1 – Modelo de Análise

Objetivo Geral	Formular orientações para, dentro do ecossistema do setor da defesa, otimizar a contribuição da indústria de defesa nacional para o desenvolvimento das capacidades das FFAA portuguesas.			
Questão Central	De que forma o ecossistema do setor da defesa pode otimizar a contribuição da indústria de defesa nacional para o desenvolvimento das capacidades das FFAA portuguesas?			
Objetivos Específicos	**Questões Derivadas**	**Conceitos**	**Dimensões**	**Indicadores**
OE1 - Analisar a adequabilidade da EDTBID para potenciar a participação da ID no desenvolvimento das capacidades das FFAA.	**QD 1** - Em que medida a EDBTID estabelece as orientações e as medidas necessárias para uma efetiva contribuição da ID para o desenvolvimento das capacidades das FFAA?	Estratégia de Desenvolvimento da Base Tecnológica, Industrial de Defesa	Legislativa	Alinhamento da EDBTID Adequabilidade Mecanismos colaboração Nível de ambição
OE2 - Analisar as interações entre as entidades da ESDN, a IdD *Portugal Defence* e a ID, enquanto responsáveis pela *governance* do desenvolvimento de capacidades militares	**QD 2** - De que forma interagem as entidades da ESDN, a IdD *Portugal Defence* e a ID, enquanto responsáveis pela *governance* do desenvolvimento de capacidades militares?	Interoperabilidade organizacional	Estrutural Organizacional	Órgãos / estruturadas criadas Plataformas STIC Adequabilidade de competências Tempo na função Mecanismos de colaboração Processos implementados
OE 3 - Avaliar o nível de participação da IdD *Portugal Defence* S.A. e da ID no Ciclo de Planeamento de Defesa	**QD 3** - Qual o nível de participação da IdD *Portugal Defence* S.A. e da ID no Ciclo de Planeamento de Defesa?	Planeamento Estratégico	Operacional	Conhecimento do CPD Participação das empresas Tipo e periodicidade das interações Ações de comunicação e divulgação Eventos planeados

3. METODOLOGIA

Considerando o objeto da investigação e os objetivos definidos será aplicada uma estratégia qualitativa procurando-se compreender o fenómeno da pesquisa através de uma ação determinante na recolha de dados com recurso a entrevistas semiestruturadas e análise documental (Santos & Lima, 2019, p. 28). O desenho de pesquisa é sustentado num estudo de caso, atendendo a que se procura recolher informação detalhada sobre a dinâmica do ecossistema do SD, enquanto fenómeno

particular e específico, assente numa perspetiva pragmática quanto aos resultados que conduzam a uma maior participação da ID na edificação de capacidades das FFAA (Santos & Lima, 2019, p. 37).

Considerando o objeto de estudo, foi necessário recolher o máximo de contributos das entidades que enformam o ecossistema do SD, constituído por dois grupos principais: o da ESDN e o da IdD/ID. No grupo da ESDN, foram escolhidas as entidades com responsabilidades diretas no planeamento e desenvolvimentos das capacidades das FFAA. Ao nível do MDN foram entrevistadas as lideranças de topo da Direção-Geral de Planeamento de Defesa Nacional (DGPDN) e da Direção-Geral de Recursos da Defesa Nacional (DGRDN). No EMGFA, o intento focou-se na Divisão de Planeamento Estratégico Militar (DIPLAEM) e na Divisão de Inovação e Transformação (DIT). Nos Ramos, diligenciou-se obter contributos dos responsáveis pelos trabalhos dos Estados-Maiores e dos chefes das respetivas divisões de planeamento militar. Adicionalmente, foi possível colher os aportes do Chefe de Estado-Maior da Armada e do Comandante das Forças terrestres.

Para a IdD/ID utilizou-se o mesmo guião de entrevista, apesar da primeira ter, no contexto desta investigação, responsabilidades únicas e distintas. Atendendo ao momento atual da IdD, considerou-se pertinente ouvir a presidente cessante e o novo presidente para recolher dados sólidos sobre esta empresa. Na ID procurou-se diversificar a tipologia de entidades, auscultando empresas participadas pelo Estado, empresas sucursais de multinacionais e empresas que, não estando inseridas na BTID, cooperam com as FFAA.

Para evitar uma análise inconclusiva perante as respostas obtidas destes dois grupos, entrevistou-se um leque de especialistas e académicos, possibilitando obter uma visão externa sobre o assunto e sustentar os contributos recebidos dos dois grupos anteriores.

As entrevistas foram coordenadas diretamente com os entrevistados, com prévio envio dos guiões. Todos os entrevistados autorizaram a sua identificação e citação durante o trabalho, sempre que tal for entendido por conveniente.

Na recolha de informação, adotou-se uma estratégia de investigação qualitativa ou intensiva com primazia pela análise documental e pela realização de entrevistas semiestruturadas como principais instrumentos captativos. A análise documental incidiu sobre as estruturas organizacionais das entidades do SD, os normativos e legislação que enquadram essas organizações, as competências atribuídas aos seus líderes, a expertise dos seus quadros, os processos de

planeamento e os modelos de participação. Para as entrevistas, optou-se por um formato semiestruturado que possibilitou a recolha de dados resultantes da experiência pessoal e do contexto social e organizacional em que o entrevistado se insere. O formato do questionário foi organizado em três grandes blocos de questões para permitir recolher dados em cada uma das dimensões de análise.

Na análise documental, utilizou-se a técnica da análise de conteúdos nas suas três etapas de redução de dados, apresentação/organização e validação dos mesmos. (Santos & Lima, 2019, p. 118). Para as entrevistas, os dados obtidos das questões abertas colocadas aos entrevistados foram tratados com recurso à análise categorial, segundo método apresentado por Sarmento (2013, p. 53). Considerando a natureza dos grupos de entrevistados, adaptou-se a técnica de análise para permitir inferências sobre as condições de produção estabelecidas (Vala, 1986, p. 104, cit. por Santos & Lima, 2019, p. 118). Neste sentido, para melhor aferir as conclusões obtidas em cada questão, na matriz de análise de conteúdos foram introduzidos, totais parciais por grupo.

4. ESTRATÉGIA DE DESENVOLVIMENTO DA BASE TECNOLÓGICA E INDUSTRIAL DE DEFESA 2023-2033

Neste capítulo pretende-se analisar a EDBTID para inferir das suas potencialidades e adequabilidade em corresponder aos desafios do desenvolvimento da BTID. Para tal, é importante efetuar uma análise ao contexto atual do setor da ID a nível europeu e nacional e caracterizar a estratégia para, assim, se deduzir a sua adequabilidade.

4.1. O CONTEXTO EUROPEU PARA O DESENVOLVIMENTO DA INDÚSTRIA DE DEFESA

4.1.1. Da estratégia global à bússola estratégica

Desde 2016 que a UE, através da sua estratégia global, ambiciona robustecer a sua posição como ator global influente, nomeadamente na área da segurança e defesa (União Europeia [UE], 2016a, pp. 3-5).

O Plano de Ação Europeu no domínio da defesa, aprovado nesse mesmo ano, tem como principal objetivo atuar em três pilares principais: (1) o lançamento de um FED; (2) a promoção de investimentos nas cadeias de fornecimento no SD; (3) o reforço do mercado único da defesa (CE, 2016, p. 6). A figura 1 permite visualizar

a evolução das fontes de financiamento que a UE implementou até à formalização final do FED em 2021.

O reconhecimento da Estratégia Global sobre a necessidade de uma maior coordenação e investimento em defesa, levou à criação em 2017 da Cooperação Estruturada Permanente com o objetivo de desenvolver capacidades de defesa conjuntas e torná-las disponíveis para operações militares da UE (CUE, 2017, p. 57).

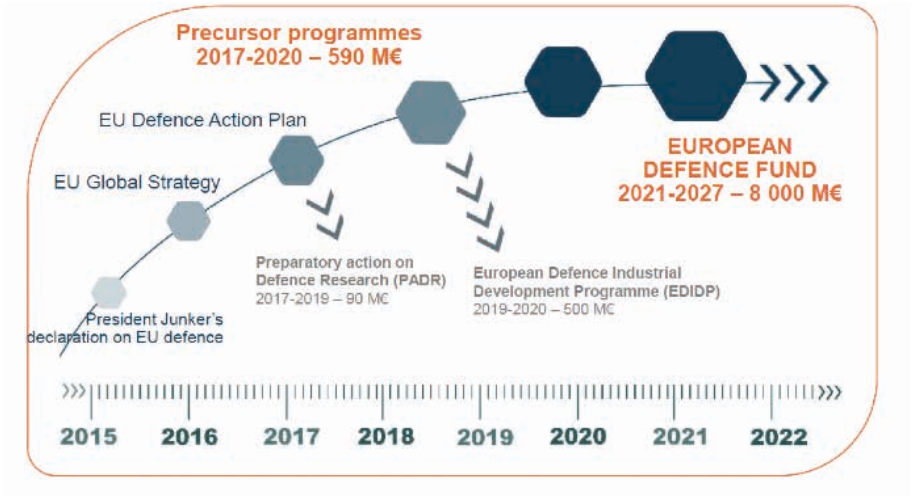

Figura 1 – Evolução do investimento no setor da defesa na EU
Fonte: Comissão Europeia (2023).

Por sua vez, em 2018 é estabelecido o Programa Europeu de Desenvolvimento Industrial no domínio da defesa destinado a apoiar a cooperação entre empresas do SD em toda a UE, reconhecendo-se a importância de potenciar as Pequenas e Médias Empresas (PME) (Parlamento e Conselho da UE [PCUE], 2018, pp. 30-34).

O FED, aprovado em 2019, começou a funcionar em 2021 com um orçamento para o período de 2021-2027 de 8 mil milhões de euros, passando a ser um importante instrumento de financiamento da UE para apoiar o investimento na investigação e no desenvolvimento conjunto de equipamentos e tecnologias de defesa, incentivando a aquisição e manutenção conjunta (PCUE, 2021, p. 149).

Em 2022 é aprovada a Bússola Estratégica (BE) como o principal documento orientador da UE no domínio da segurança e defesa (CUE, 2022, pp. 2-3).

4.1.2. A nova estratégia industrial de defesa europeia

Nos finais de 2023, os líderes europeus apelaram à definição de uma estratégia industrial de defesa europeia para reforçar a BTID, aumentar o investimento na defesa e o desenvolvimento de capacidades (Conselho Europeu, 2023, p. 7).

Em março de 2024 a CE (2024, pp. 1-2), apresenta a primeira EIDE e o novo programa para a ID, com a ambição de "alavancar e suportar o esforço dos Estados Membros para investirem mais e melhor numa indústria de defesa forte, como pré-requisito essencial para atingir a prontidão defensiva".

Para a implementação da estratégia é proposto um conjunto de medidas de apoio onde se destaca o programa da ID europeia. Este programa, a par do FED, destina-se a fortalecer o pilar industrial de defesa da UE com financiamento a longo prazo, para além do atual quadro financeiro plurianual 2021-2027 (CE, 2024, p. 1).

4.2. O CONTEXTO NACIONAL PARA O DESENVOLVIMENTO DA INDÚSTRIA DE DEFESA

Por força da sua Lei Orgânica (Decreto-Lei n.º 183/2014, de 29 de dezembro, 2014, p. 2), compete ao MDN a responsabilidade de "conceber, desenvolver, coordenar e executar a política relativa à promoção da base tecnológica e industrial de defesa". Política essa que no programa do XXIII governo constitucional (2022, p. 60), refere a ID como "crucial para a efetiva autonomia e capacidade de cumprimento das missões das Forças Armadas".

A primeira estratégia de desenvolvimento da BTID em Portugal é aprovada pela RCM n.º 35/2010 que, juridicamente, a enquadra de forma detalhada, procurando consolidar e reforçar uma ID competente e competitiva que, em consonância com as iniciativas da UE, fosse capaz de satisfazer requisitos e capacidades das FFAA (RCM35, 2010, p. 1599).

A preocupação com um elevado nível tecnológico no SD, como condição essencial para melhorar a operacionalidade das FFAA, também está bem enfatizada no Conceito Estratégico de Defesa Nacional, apontando os setores das tecnologias da informação, da aeronáutica e da construção naval, como polos potencialmente dinâmicos "da produção, consumo, difusão e demonstração da inovação e da tecnologia dos portugueses." (RCM n.º 19/2013 de 5 de abril, 2013, p. 1995).

A forma vertiginosa como o mundo se alterou nestes últimos anos, provocou uma mudança significativa nos conceitos de segurança e defesa individual e coletiva. Os efeitos da pandemia (COVID-19), as alterações climáticas, o regresso das rivalidades entre as grandes potências e o conflito armado na Ucrânia,

revelaram a inadequabilidade da estratégia de 2010 para adaptar a indústria da defesa às recentes e profundas transformações tecnológicas e geoestratégicas. Neste contexto é aprovada, em junho de 2023, a EDBTID (RCM52, 2023, pp. 26-27).

4.3. Caracterização da estratégia de desenvolvimento da base tecnológica e industrial de defesa 2023-2033

Na perspetiva do planeamento estratégico militar onde, segundo Ribeiro (2020, p. 63), se procura "o equilíbrio entre modernizar as forças existentes para aumentar a sua prontidão atual e edificar novas forças para aumentar a capacidade futura", a EDBTID estabelece novas linhas de orientação que têm em conta a necessidade de desenvolver uma ID capaz de criar emprego altamente qualificado, de reforçar a capacidade nacional em áreas tecnológicas de elevado valor acrescentado e de responder aos desafios associados aos novos domínios (ciberespaço e espaço) e às emergências sanitárias e ambientais, cada vez mais complexas (RCM52, 2023, p. 26).

Conceptualmente a EDBTID, segundo a classificação do General André Beaufre (1966, p.45), assume-se como uma estratégia total, considerando que ao exigir uma "[…] efetiva articulação das entidades com responsabilidade nas áreas da defesa nacional, segurança, economia, inovação, ciência e tecnologia, ambiente, digitalização e modernização administrativa", (RCM52, 2023, p. 27), corresponde às competências que Couto (1988, p. 228) atribuiu a esta estratégia: "o desenvolvimento harmonioso e a utilização dos recursos morais e materiais, com vista à oportuna prevenção ou superação de ameaças e à consecução de determinados objetivos políticos".

Sendo um documento orientador, com um horizonte de implementação a dez anos (sujeito a atualizações), a EDBTID apresenta um alinhamento multifacetado com um conjunto de estratégias ligadas a outros setores do Estado e com documentos estruturantes de organizações internacionais como o conceito estratégico da Organização do Tratado do Atlântico Norte (OTAN) e a bússola estratégica da UE (RCM52, 2023, pp. 26-27).

Como elementos principais, a estratégia apresenta uma visão com quatro objetivos estratégicos, quatro Eixos de Intervenção (EI) e um modelo de governança, monitorização, avaliação e revisão. Identifica ainda, os setores industriais-chave e as áreas tecnológicas prioritárias a nível europeu, na OTAN e no contexto da Defesa Nacional (DN) (RCM52, 2023, pp. 34-38).

Quanto ao modelo de gestão, a estratégia não define claramente um órgão de direção e deixa a sua coordenação, monitorização e execução numa partilha de responsabilidades entre o MDN, através da DGRDN, e a IdD. À DGRDN compete a responsabilidade de monitorizar a execução da EDBTID em estreita coordenação e articulação com a IdD (RCM52, 2023, p. 28). À IdD cabe a responsabilidade de elaborar o PAE, de executá-lo e de coordenar a ação das entidades nele envolvidas (RCM52, 2023, p. 38).

Apesar da determinação política para elaborar e aprovar o PAE no prazo de 90 dias após a entrada em vigor da estratégia (05 de junho 2023), este somente foi aprovado em fevereiro de 2024.\

4.4. A adequabilidade da estratégia

Para Ribeiro, (2007, p. 160) a adequabilidade é um critério que se utiliza dentro do contexto de formulação de estratégia, "destinado a avaliar se uma modalidade de ação contempla as circunstâncias em que o Estado atua e tem possibilidades de desenvolvimento" e que serve para testar a sua eficácia em termos de custo e valor acrescido. As questões que Ribeiro (2008, B-34) define como o teste de adequabilidade foram abordadas, no aplicável, nas respostas dos entrevistados.

Com a recente aprovação do PAE completou-se o processo da gestão estratégica composto por quatro fases básicas: análise do ambiente, formulação, operacionalização e controlo (Ribeiro, 2020, p. 130). Desta forma, mitigou-se a principal lacuna quanto à operacionalização da EBTID.

Perante o desafio do esforço coletivo que a EDBTID coloca às entidades dos ecossistemas do SD, os dados recolhidos das respostas à primeira questão (Quadro 2) são inequívocos: 88% dos inquiridos afirmaram que o sucesso desse esforço passa pela implementação de mecanismos de coordenação e de articulação entre as entidades a que Nunes et al. (2023, p. 5) designa por "tripla hélice", ou seja, o governo, aqui representado pela ESDN, a indústria, que neste caso inclui a IdD mais a ID, e o SCTN.

Quadro 2 – Relação dos eixos de intervenção com os objetivos estratégicos

	VISÃO: Desenvolver BTID que seja criadora de valor acrescentado para a Defesa e para a economia nacional, sustentável e competitiva, tanto a nível nacional quanto internacional.			
	OE 1 - Afirmar e Reforçar a BTID	OE 2 - Assumir Portugal como produtor e exportador de tecnologia e serviços no âmbito da Economia de Defesa	OE 3 - Fomentar e dinamizar a participação em redes internacionais de cooperação	OE 4 - Incentivar a investigação, desenvolvimento e inovação
EI 1 - Capacidades e setores industriais-chave	X	X		
EI 2 - Capacidades e competências da BTID	X	X		
EI 3 - Cooperação nacional e internacional	X		X	
EI 4 - Investigação, desenvolvimento e inovação	X	X	X	X

Fonte: Comissão Europeia (2023).

Da opinião generalizada sobre a necessidade de implementar processos colaborativos, melhorar a comunicação e a capacidade de diálogo para envolver mais ativamente a IdD/ID nos processos de planeamento e desenvolvimento das capacidades. Ou seja, aquilo a que Macedo (entrevista presencial, 28 de fevereiro de 2024) designa como "sincronismo e coordenação na definição e no planeamento; coerência na ação".

Atendendo ao seu conteúdo e, em particular, às orientações estratégicas emanadas, 81% dos entrevistados partilham a opinião de que estas se baseiam numa lógica coerente e adequada aos objetivos a atingir e que, no geral, a EDBTID apresenta um equilíbrio entre as atuais debilidades da BTID e os EI elencados para as mitigar.

Não obstante a apreciação da estratégia ser bastante favorável, foram indicadas algumas medidas que deveriam ter sido contempladas para potenciar e desenvolver a BTID, (Figura 2). Para além da necessidade de ser aprovado um PAE coerente e eficaz, 77% dos entrevistados consideram que a EDBTID, à semelhança da estratégia europeia, deveria incorporar incentivos fiscais e financeiros de apoio às empresas. A existência de um fundo de financiamento nacional com as características do FED, possibilitaria às PME da ID participarem em projetos associados às novas tecnologias e inovação e, dessa forma, robustecerem os seus tecidos empresariais e capacidade de produção.

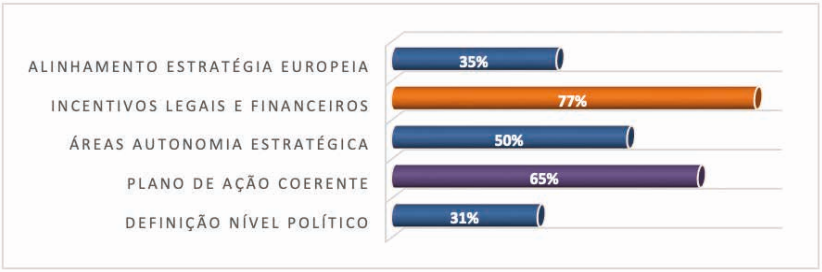

Figura 2 – Identificação de lacunas à EDBTID

4.5. Síntese conclusiva

Iniciou-se o capítulo analisando a importância da ID a nível europeu onde, pela primeira vez, foi aprovada uma EIDE, com diversos instrumentos de apoio e de financiamento, em particular para as PME. A nível nacional, constatou-se, dentro do domínio da Defesa, existir um edifício normativo abrangente e conducente à promoção e desenvolvimento da ID nacional. A aprovação da EDBTID em 2023 enquadra-se e está em consonância com a vontade, politicamente expressa, de fortalecer a ID e de modernizar as FFAA. Sendo uma estratégia para 10 anos, a EDBTID define orientações e identifica objetivos estratégicos para reforçar a capacidade nacional em setores industriais chave e áreas tecnológicas prioritárias. O atraso na aprovação do seu PAE impossibilitou a sua desejada operacionalização e a implementação de medidas concretas e eficazes.

Os dados obtidos nas entrevistas possibilitaram concluir que a EDBTID está bem formulada e que estabelece as condições necessárias para uma maior colaboração e cooperação entre as FFAA e a ID, desde logo, pela importância do "triplo-hélice" para o esforço coletivo que a gestão da estratégia exige.

Como principais lacunas foram identificadas a inexistência do PAE, entretanto aprovado, e a falta de mecanismos legais e financeiros como fonte de investimento para a ID. A revisão do atual normativo jurídico-financeiro e a promoção de uma cultura e liderança vocacionada para a criação de redes de confiança, são dois outros instrumentos que, conjuntamente com a EDBTID, possibilitarão uma maior e melhor contribuição da ID para o desenvolvimento das capacidades das FFAA.

5. PERSPETIVA DA INTEROPERABILIDADE ORGANIZACIONAL DENTRO DO SETOR DA DEFESA

Para analisar a forma como interagem as entidades do ecossistema do SD, importa inferir das condições inerentes à IO para, após caraterização do ecossistema, verificar se as atuais interações proporcionam condições de sucesso para a *governance* do desenvolvimento das capacidades das FFAA.

5.1. A INTEROPERABILIDADE DAS ORGANIZAÇÕES

É fundamental que as organizações do ecossistema do SD tenham capacidade para interagirem na prossecução de objetivos comuns. Isto implica, obrigatoriamente, a partilha de conhecimento e de informações, através de processos administrativos de suporte e intercâmbio de dados entre os respetivos sistemas de Tecnologias de Informação e Comunicação (TIC) (Parlamento e Conselho Europeu, 2009, p. 23).

Segundo a CE (2010, p. 21) o modelo de interoperabilidade assenta em quatro níveis claramente definidos na Figura 3. A integração destes níveis é imprescindível à sua implementação. A primeira condição para as organizações serem interoperáveis, é estarem de acordo e em consonância na forma como se vão relacionar, alinhar processos e responsabilidades em prol de benefícios comuns.

Figura 3 – Níveis de interoperabilidade
Fonte: Adaptado a partir da Comissão Europeia (2010).

A cada entidade do ecossistema do SD (Figura 3) coloca-se o desafio de prover a criação de condições endógenas e exógenas para implementar a interoperabilidade necessária a uma execução ágil e eficiente do PAE da EDBTID e, com uma forte participação da ID, a gestão eficaz dos projetos de desenvolvimento das capacidades das FFAA.

5.2. Caraterização do ecossistema do setor da defesa

5.2.1. A estrutura superior da Defesa Nacional

O MDN é responsável pela definição e condução da política de DN e das FFAA. Na sua orgânica evidenciam-se duas entidades com responsabilidades acrescidas no processo de planeamento de forças e de edificação de capacidades: A DGPDN que "tem por missão apoiar a formulação, coordenação e execução da política de defesa nacional, do planeamento estratégico e das relações externas de defesa […]" (n.º 1 do art.º 2.º do Decreto Regulamentar n.º 14/2015 de 31 de julho), e a DGRDN, responsável por "Conceber, desenvolver, coordenar e executar as políticas de armamento, bens, equipamentos, infraestruturas e investigação e desenvolvimento necessárias às Forças Armadas e à defesa nacional" do n.º 2 do art.º 2.º do Decreto Regulamentar n.º 8/2015 de 31 de julho).

Na estrutura do EMGFA, a DIPLAEM é o órgão primariamente responsável pelo planeamento estratégico militar e pela programação militar, recebendo a colaboração da DIT e da Divisão de Recursos.

5.2.2. A IdD Portugal *Defence* S.A.

A IdD foi criada em 2020 (Despacho conjunto n.º 786/2020, de 30 de dezembro de 2019) num processo de restruturação da anterior IdD - Plataforma das Indústrias de Defesa Nacionais e atribuição dos ativos que resultaram da extinção da EMPORDEF, nomeadamente as participações sociais que esta empresa detinha (IdD, 2023, p. 3).

Tem como missão executar políticas sectoriais da Defesa, através da consolidação de um centro público de decisão empresarial e detém, entre outras, as seguintes responsabilidades (IdD, 2023, pp. 4-13): a gestão das participações sociais do Estado nas empresas do SD, (Figura 4); a gestão da BTID, incluindo a representação na UE, na OTAN e em fóruns internacionais relevantes para a economia de defesa.

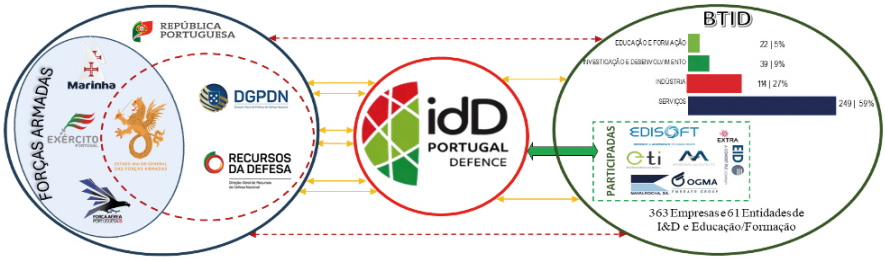

Figura 4 – Ecossistema do setor da Defesa

Com a responsabilidade atribuída pela EDBTID, de elaborar um PAE para implementar a estratégia, a IdD passa a desempenhar o papel de principal interlocutor e "de interface entre a Defesa e a Economia, competindo-lhe ser o canal de comunicação privilegiado entre o MDN e a BTID" (IdD, 2024, p. 6)

5.2.3. A indústria de defesa nacional

As indústrias de defesa assumem um papel central no âmbito da DN e são de importância estratégica para um Estado (Rodrigues, 2020, p. 78). Contudo, o desinvestimento verificado nas últimas duas décadas reflete-se no atual estado da ID nacional que, assente maioritariamente em PME, é muito heterogénea, com pouca competitividade a nível internacional e voltada essencialmente para a oferta de serviços (Nunes & Alves, 2022, p. 24). Esta situação coloca a ID numa posição de subcontratação pelos principais atores económicos internacionais e com um papel submisso de fornecimento de bens e serviços, por vezes de baixa intensidade económica (M. Ferreira, 2017, p. 16).

Não obstante, Nunes et al. (2023, p. 32) consideram existir condições para promover e potenciar a ID, lapidando o "diamante[34]" das PME portuguesas. A confirmá-lo, está o crescimento de quase 50% no número de entidades que integraram a BTID nos últimos sete anos, num total de 363 empresas, organizadas em 21 clusters, com atuação em 40 setores de atividade distintos (RCM52, 2023, p. 30).

[34] Nunes et al (2023, p. 32) identifica um conjunto de facetas da ID nacional a que chamou de "diamante".

Esta diversidade de competências e o caráter de duplo-uso da ID portuguesa, cria as condições desejáveis para uma fácil integração em consórcios internacionais, particularmente em áreas ligadas à aeronáutica, à construção naval, aos têxteis técnicos, aos sistemas autónomos, à cibersegurança e ao espaço (RCM52, 2023, p. 30).

Quando comparadas com outras empresas, as da ID apresentam significativas vantagens ao nível da produtividade por trabalhador (55% superior), das remunerações auferidas (praticamente o dobro da média), do investimento em investigação e desenvolvimento e da afetação de pessoal a esta área, da qualificação do capital humano e do seu forte pendor tecnológico (Nunes & Alves, 2022, pp. 34-51).

A IdD na sua página oficial da *internet* mantém atualizados os dados estatísticos mais relevantes da BTID portuguesa, conforme Figura 5.

Figura 5 – Dados sobre a BTID
Fonte: IdD (s.d.).

5.3. Análise das interações entre as entidades do ecossistema do setor da defesa

Para esta análise, colocaram-se dez questões do guião aos entrevistados. As respostas permitiram gerar subcategorias associadas aos indicadores do MA (Sarmento, 2013, p. 55). Apresentam-se os dados por subcategorias para facilitar a compreensão dos resultados obtidos.

5.3.1. Subcategoria dos processos

Pela análise, deduz-se que, sempre que necessário e pontualmente, as instituições dispõem de mecanismos para interagirem, ainda que estes não assentem em processos de colaboração sistematizados. Contudo, a perceção da ID sobre estes mecanismos não coincide com a da ESDN. Apenas um dos cincos entrevistados da indústria reconheceu a existência dos mesmos. A justificação resulta da ESDN considerar que consegue contatar a ID sempre que necessita,

enquanto esta tem dificuldade de acesso à ESDN pela falta de conhecimento da organização e estrutura militar e dos seus processos de planeamento. Ao desenvolverem esta questão, os entrevistados transmitiram, quase unanimemente, que a IdD para além de interface deve ser um veículo informacional junto da ID.

Com o propósito de trazer informação internacional para a ID, a DGPDN tem em curso uma iniciativa que J. Gorgulho (entrevista presencial, 16 de fevereiro de 2024) denomina de "Diplomacia Económica para a ID". Neste processo, a IdD constitui-se como ponto único de gestão desta diplomacia entre a Defesa e a indústria.

5.3.2. Subcategoria do conhecimento

A pergunta, apesar de elementar, fornece um dado fundamental para o estabelecimento de qualquer modelo de cooperação. A interoperabilidade só será exequível se existir um conhecimento mútuo entre pessoas e organizações.

Os dados revelam um total de 100% de conhecimento sobre a ID e suas principais áreas de atividade. Apenas dois entrevistados do lado da ID afirmaram desconhecer os órgãos da ESDN responsáveis pelo planeamento e desenvolvimento de capacidades, apesar de conhecerem os seus pontos de contato.

5.3.3. Subcategoria dos recursos

Foi considerado fundamental existirem órgãos e pessoas dedicadas em exclusivo ao planeamento e desenvolvimento de capacidades. Neste sentido, H. Macedo (op. cit.) alerta que a redução de efetivos que se verifica nas FFAA deve ser mitigada com a transformação digital e a automatização dos processos, sob o risco da "menor capacidade de processar informação e consequente dificuldade de resposta das organizações".

Todas as entidades da ESDN, excetuando a DGRDN, afirmam possuir órgãos e pessoas focadas no planeamento de capacidades, verificando-se um crescente dinamismo com a criação de órgãos dedicados à investigação, desenvolvimento e inovação que potenciam a interação das FFAA com a ID.

Do lado da IdD/ID regista-se o facto da IdD não dispor, nem de órgãos, nem de pessoas em exclusividade. O seu Presidente C. Félix (entrevista presencial, 22 de março de 2024) reconhece que "a IdD não tem, *in-house*, competências de planeamento e desenvolvimento de capacidades, sendo uma lacuna estrutural que está a ser trabalhada".

A preocupação mais premente sobre os recursos humanos na área do planeamento relaciona-se, em particular dentro das FFAA, com a curta permanência dos militares nestas funções. Para F. Vaz (entrevista presencial, 23 de fevereiro de 2024) e N. Ávila (op. cit.) a rotação dos militares em ciclos de dois, três anos, prejudica a consolidação de conhecimentos e dificulta a construção da relação de mútua confiança necessária à criação uma cultura de colaboração e cooperação.

Outro aspeto importante foi mencionado por C. Félix, (op. cit.) que propõe a implementação de um projeto, designado de "Base Tecnológica de Peritos de Defesa assente numa *pool*, instituída formalmente, de peritos militares e civis com formação em diversas áreas tecnológicas e científicas". Para além da disponibilização de recursos humanos para colmatar insuficiências conjunturais, pode também apoiar tecnicamente qualquer uma das entidades nas diferentes fases do processo de planeamento.

No entanto, para reduzir a insuficiência de militares e a sua rotação, a solução mais viável, apresentada por 81% dos entrevistados, reside na inclusão de civis nos órgãos de planeamento das FFAA, ou ainda, no recurso a militares na reserva, à semelhança do que já fazem os órgãos do MDN.

Nesta subcategoria obteve-se outro dado importante que indica a inexistência de representantes permanentes entre as entidades. Verifica-se, contudo, que há uma rede consolidada de pontos de contato facilitadora da comunicação interorganizacional.

Apesar da maioria dos entrevistados (54%) concordar com a existência de representantes militares na IdD, é na ESDN que a ideia acolhe menor aceitação, justificada pela capacidade dos Ramos se fazerem representar no EMGFA e este no MDN. Por seu lado, tanto o atual presidente como todos os ex-presidentes da IdD admitem que deveriam existir representantes militares na empresa para aproximar o cliente (FFAA) do fornecedor (ID) e garantir o alinhamento do desenvolvimento dos projetos com as necessidades militares.

5.3.4. Subcategoria das Plataformas

A existência de plataformas informáticas para partilha de dados enquadra-se no nível da interoperabilidade técnica, atrás mencionado. A plataforma *SmartDefence,* concebida pela IdD, é pouco conhecida e usada pela ESDN. Os entrevistados alegam ser necessário reformular a plataforma, tornando-a acessível e funcional. A ID reconhece-a como um mecanismo capaz de promover

uma maior interação, mas alerta que a qualidade da informação a divulgar deve proporcionar a criação de valor empresarial, ou seja, a concretização de negócios (Barbedo, entrevista presencial, 26 de fevereiro de 2024).

5.3.5. Subcategoria das competências

Mais de 70% das respostas revelam ser vantajoso que, a nível nacional, exista um órgão consultivo com características semelhantes ao NATO *Industrial Advisory Group*[35] (NIAG) para a "ID ser capaz de expressar cada vez mais a sua opinião, influenciar positivamente e ajudar as FFAA" (J. Neves, entrevista presencial, 4 de março de 2024).

A empresa IdD, que representa Portugal no NIAG, é considerada como a mais competente, capaz e a mais vocacionada para liderar ou coordenar as atividades desse órgão consultivo. Contudo, nem todos os grupos de entrevistados partilham desta opinião. Na ESDN, menos de metade concorda que assim seja.

Face ao protagonismo atribuído pela nova EDBTID à IdD na coordenação, implementação e monitorização da estratégia, impunha-se saber a opinião dos entrevistados sobre a capacidade desta empresa, gestora de empresas da BTID, para cumprir, eficazmente, a missão de principal interface entre as FFAA e a ID.

O Quadro 9 mostra, em mais de 60% das respostas obtidas, que num setor vital para a soberania do País, o superior interesse do Estado não pode colocar em causa a capacidade da IdD de defender sempre o desígnio nacional de obtenção de autonomia estratégica em setores industriais chave e de satisfazer as necessidades operacionais das FFAA, dotando-as de novas capacidades tecnologicamente evoluídas.

5.3.6. Subcategoria da comunicação

Apenas quatro entidades confirmaram possuir um Plano Estratégico de Comunicação (PEC) e destas, apenas duas incluem nos seus planos, objetivos voltados para a colaboração institucional com as demais entidades do ecossistema.

A inexistência de um PEC não invalida que não haja divulgação e partilha de informação ao nível das lideranças de topo. Dos entrevistados, 90% assumem

[35] O NIAG é um órgão consultivo e de assessoria da OTAN que estabelece a ligação com as indústrias de defesa dos países membros com o propósito de incluir o ponto de vista industrial e o desenvolvimento da tecnologia nos trabalhos da Aliança. (NATO, 2018, pp. 7-11)

praticar uma comunicação estratégica dirigida às demais entidades com a finalidade de promover a interação e potenciar a participação coletiva no desenvolvimento do setor industrial de defesa.

Para os académicos, o PEC é um documento fundamental para promover a cultura da organização, colocar a Defesa na agenda política e informar a sociedade sobre os assuntos de soberania nacional, contribuindo para um maior sentido cívico do cidadão.

5.4. Síntese conclusiva

Com o OE de analisar as interações entre as entidades do ecossistema do SD, através das relações que desenvolvem entre si, iniciou-se este capítulo com uma abordagem à IO e respetivos níveis de interdependência existentes.

Na caracterização do ecossistema do SD identificaram-se os órgãos da ESDN com responsabilidades no planeamento e desenvolvimento de capacidades. No MDN, a DGPDN e a DGRDN são os órgãos centrais a quem compete desenvolver políticas e implementar medidas atinentes a um maior contributo da ID no desenvolvimento de capacidades das FFAA. Ao nível do EMGFA, a responsabilidade primária do planeamento de defesa recai sobre a DIPLAEM com a DIREC e a DIT a participarem também neste processo. Por sua vez, a IdD, a quem foi atribuída a responsabilidade de elaborar o PAE que irá implementar a EDBTID, aparece neste novo contexto como um elemento preponderante na ligação entre as FFAA e a ID. Quanto à ID, malgrado a sua pequena dimensão e fragmentação, apresenta alguns pontos fortes para se adaptar facilmente a novos desafios e ganhar preponderância em determinados nichos de mercado.

As entrevistas efetuadas possibilitaram identificar cinco subcategorias que, no seu todo, respondem à QD levantada. Assim, ao nível dos processos, não obstante estes serem pontuais e poucos sistematizados, constata-se existirem mecanismos implementados para, sempre que necessário, tomar decisões concertadas.

Confirmou-se existir um conhecimento situacional alargado do ecossistema do SD e das especificidades da ID, fruto da existência na ESDN de órgãos e pessoas dedicadas em exclusivo ao planeamento de defesa. Nesta matéria a preocupação incide na curta permanência dos militares nas funções de planeamento, vulnerabilidade esta que pode ser colmatada recorrendo a pessoal civil, ou a militares na reserva.

Quanto à existência de representantes permanentes, esta só fará sentido pela presença de militares na IdD, porquanto a rede de pontos de contato existente demonstra ser suficiente para suprir as necessidades de ligação entre as entidades. A plataforma *SmartDefence*, criada pela IdD, ainda é pouco conhecida, necessitando de uma reformulação para se converter no principal portal colaborativo entre todas as entidades. De uma forma geral, é reconhecida a missão e o papel de interface da IdD, entendendo-se que poderia liderar um órgão consultivo nacional semelhante do NIAG. Não se registaram objeções face ao seu interesse comercial nas ID participadas pelo Estado.

Por último, constatou-se que, apesar da falta de um PEC, as entidades dispõem de uma comunicação estratégica que lhes permite atingir os objetivos de cooperação desejados.

As conclusões supra permitem assim responder à QD 2.

6. O CICLO DE PLANEAMENTO DE DEFESA[36]

Neste capítulo, após uma breve caraterização do CPD, procede-se à avaliação da participação da IdD e da ID neste ciclo para, de seguida, se inferir a importância da LPM para a ID nacional, por se tratar da principal fonte de investimento das FFAA.

6.1. Caracterização do Ciclo de Planeamento de Defesa

Para um melhor entendimento, a Figura 6 demonstra o modelo de planeamento.

[36] Conhecido também por Ciclo de Planeamento de Defesa Militar. No Despacho n.º 25/MDN/2022, que promulgou a Diretiva Ministerial Orientadora, passou a designar, apenas, de Planeamento de Defesa.

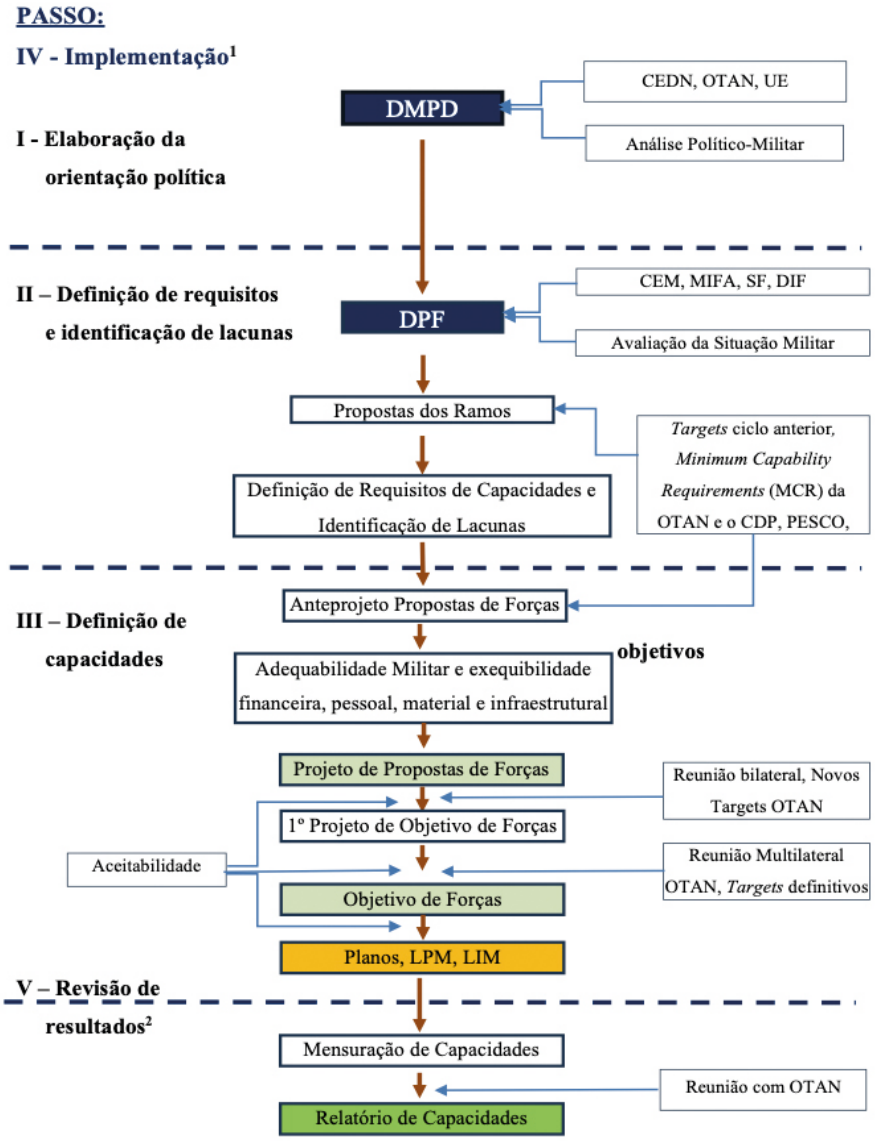

Figura 6 – Modelo de Planeamento de Defesa
Fonte: Adaptado a partir de Despacho n.º 25/MDN (2022).

O CPD tem a duração de quatro anos e desenvolve-se em cinco passos sucessivos enformando o Modelo de Planeamento de Defesa. A sua coordenação é da competência do Grupo de Articulação do Planeamento de Defesa[37] (GAPD), presidido pelo Diretor-Geral de Política de DN. As orientações para todo o processo advêm da Diretiva Ministerial de Planeamento de Defesa (DMPD), que fornece a "orientação política e transmite o conjunto de finalidades e objetivos que devem ser alcançados no âmbito do planeamento de defesa" (Despacho n.º 25/MDN/2022 de 23 de junho, p. 5).

O CPD é um processo contínuo de planeamento que possibilita uma tomada de decisão coordenada e integrada sobre as CM a serem edificadas, estruturadas e empregues no espaço e no tempo (Ribeiro, 2010, p. 152). A sustentação financeira deste planeamento é obtida pela LPM, enquanto principal instrumento de gestão, controlo e investimento das FFAA (Despacho n.º 25/MDN, 2022, p. 2).

O CPD preconiza uma permanente e estreita ligação com a ID para potenciar a sua participação no desenvolvimento das capacidades necessárias à modernização das FFAA, maximizando o contributo da economia de defesa para a economia nacional (Despacho n.º 25/MDN, 2022, p. 8).

Relativamente ao desenvolvimento do ciclo de planeamento de defesa, de acordo com o Despacho n.º 25/MDN (2022, p. 5), os cinco passos que constituem o CPD são: I - Elaboração da orientação política; II - Definição dos requisitos de capacidades e identificação de lacunas; III - Definição dos objetivos de capacidades; IV – Implementação e V – Revisão dos resultados.

A DMPD marca o início formal do CPD e constitui-se como uma fonte única de informação, definindo as prioridades da política de DN a partir da análise de toda a documentação estruturante a nível interno e externo[38]. O passo II inicia-se com a Diretiva de Planeamento de Forças emitida pelo CEMGFA, a partir da qual todas as entidades elaboram as propostas das necessidades específicas e procedem à identificação de lacunas em termos de capacidades a edificar (EMGFA, 2020, pp. 3-11). O terceiro passo decorre ao longo de dois anos e é o mais moroso e complexo. A sua finalidade é selecionar as CM para as quais devem ser atribuídos recursos financeiros, culminando com o projeto de proposta de forças e com as Diretivas

[37] Integram também o GAPD: Chefe do Estado-Maior-General das Forças Armadas (CEMGFA), Chefes de Estado-Maior dos Ramos, Diretor-Geral de Recursos da DN e Secretário-geral do MDN

[38] Orientações internacionais provenientes das *Political Guidance* da OTAN e da Estratégia Global da UE (Despacho n.º 25/MDN, 2022, p. 6).

do MDN e do EMGFA para a revisão da LPM e da Lei de Infraestruturas Militares (LIM), (EMGFA, 2020, pp. 5-13).

A implementação dos planos e a execução da LPM e LIM tem uma natureza contínua, uma vez que a edificação de capacidades decorre de forma ininterrupta ao longo de todo o CPD (EMGFA, 2020, pp. 3-17). A revisão dos resultados é fundamental para todo o processo no qual o Relatório de Capacidades se constitui como um instrumento essencial de controlo e de apoio ao início do CPD seguinte (Despacho n.º 25/MDN, 2022, p. 9).

6.2. Participação da IdD / indústria de defesa no Ciclo de Planeamento de Defesa

No processo do CPD foram identificados os momentos[39] em que a interação da ID com as FFAA poderia ser mais decisiva, sugerindo-se a criação de uma estrutura de coordenação na qual a DIPLAEM e a IdD assumiriam um papel de relevo na criação de sinergias para potenciar a participação da ID no CPD (EMGFA, 2020, pp. 6-10).

Perante as respostas dadas percebe-se que há um longo caminho a percorrer para colocar a ID dentro do CDP: metade dos inquiridos desconhecem o CPD e 38% tê um conhecimento, apenas, muito vago do mesmo. Existe a opinião generalizada (85%) de que a IdD/ID devem participar no CPD. Para 69% dos inquiridos da ESDN, essa participação deve ocorrer de uma forma condicionada e/ou com a IdD/ID a ter, somente, visibilidade do processo.

Para M. Almeida (entrevista presencial, 8 de fevereiro de 2024), a participação da ID no CPD possibilitaria desenvolver ideias para responder cabalmente às necessidades das FFAA e também apoiar o planeamento com as tendências da evolução tecnológica a incorporar nas capacidades a desenvolver.

Por sua vez, C. Félix (op.cit.) considera que Portugal tem um tecido científico muito competitivo capaz de contribuir para o ciclo de vida de desenvolvimento de capacidades, já que estas resultam das ideias e da sua transformação.

Sobre a possibilidade da IdD integrar o GAPD, os entrevistados da ESDN não partilham da opinião dos demais. Como justificação, salientam que os termos

[39] Imediatamente após: (1) a identificação de lacunas; (2) a avaliação da adequabilidade militar; (3) o projeto de proposta de forças; (4) o objetivo de forças e (5) a publicação da LPM (EMGFA, 2020, pp. 6-10-6-12).

de referência do GAPD incluem a possibilidade de serem convidadas outras entidades para participarem no processo. Este recurso legal permite, no critério da necessidade de saber, incluir a IdD no GAPD.

6.3. A importância da Lei de Programação Militar para a indústria de defesa

Das várias políticas públicas na área da defesa, a LPM, aprovada pela Lei Orgânica n.º 1/2023 de 17 de agosto (2023, p. 2), constitui o principal instrumento financeiro na edificação de capacidades para a DN, tendo como objetivo a programação do investimento público das FFAA em matéria de armamento e equipamento. Ao promover projetos com integração de novas tecnologias nos sistemas de defesa, a LPM funciona como uma alavanca para o desenvolvimento da BTID, potenciando a capacidade industrial nacional. Na EDBTID, a preocupação de enquadrar a participação da ID na LPM é um dos EI da estratégia "de forma a identificar os domínios nos quais a BTID poderá ter capacidade para se envolver" (RCM52, 2023, p. 35).

6.3.1. Subcategoria dos processos

Os dados evidenciam um quase total desconhecimento por parte da IdD/ID do processo de elaboração da LPM. Todos os entrevistados destas instituições afirmaram não existirem mecanismos implementados para receber os seus contributos e que estes são dados de forma pontual. A. Pessanha (entrevista presencial, 21 de fevereiro de 2024) identifica uma enorme vulnerabilidade neste processo, enfatizando que o total alheamento da IdD do processo da principal lei de investimento nas FFAA não se coaduna com as responsabilidades atribuídas a esta entidade na promoção e potenciação da ID. Por este motivo, C. Nunes (entrevista online, 01 de março de 2024) propõe a criação de uma unidade de missão que serviria de mecanismo de coordenação entre todas as entidades para todas as matérias, em particular para a efetiva execução da LPM.

6.3.2. Subcategoria do conhecimento

Na opinião de 80% dos entrevistados, o conhecimento pela IdD/ID dos projetos e subprojectos da LPM somente no lançamento dos concursos públicos, prejudica a ID nacional face às grandes empresas internacionais, impossibilitando

a definição atempada de estratégias de negócio para obter vantagens competitivas. Para L. Policarpo (entrevista presencial, 23 de fevereiro de 2024) urge desmitificar o tabu da informação sensível para continuar a excluir a ID da LPM. É possível fazer a sanitização da informação e credenciar as empresas da ID para terem acesso.

Esta incipiente partilha de informação sobre a LPM está bem patente no Quadro 12, mostrando que 88% das entidades possuem planos de atividade anuais com interações programadas, mas que, apenas 23% desses planos possuem iniciativas específicas sobre a LPM. Como medida mitigadora, 73% dos inquiridos sugerem a organização de *industry days* específicos para a LPM.

6.3.3. Subcategoria da execução

A avaliação efetuada nesta subcategoria procurou averiguar a existência de mecanismos de proteção à ID nacional para incrementar a sua participação na execução da LPM e o papel que a IdD poderá assumir na fase do *Procurement* (contratação/aquisição) das capacidades.

Há uma opinião generalizada que devem existir mecanismos de proteção, à semelhança do que alguns países europeus fazem para as suas ID. Vários entrevistados apontaram Espanha como um dos países com forte proteção da ID. A preocupação com este aspeto, levou a IdD a constituir um grupo de trabalho para analisar as práticas implementadas nesses países e de que forma poderão ser transpostas para o normativo jurídico nacional (C. Félix, op.cit.).

G. Melo (entrevista presencial, 14 de fevereiro de 2024), corroborado por demais inquiridos, afirma que o sucesso de toda a EDBTID passa, primária e fundamentalmente, por uma vontade política em definir qual o nível de ambição nacional para a ID. É necessário priorizar as áreas ligadas à Defesa nas quais o País deve possuir autonomia estratégia para depois implementar um conjunto de incentivos fiscais, financeiros e legislativos que possibilitem a promoção da ID nacional no desenvolvimento dos projetos em sede de LPM. Com efeito, 88% das respostas apontam para a necessidade de rever esses normativos.

A proteção / promoção da ID passa também por uma revisão dos mecanismos da contratação pública para o SD com a criação de quadros legais de exceção (C. Nunes, op. cit). Para J. Neves, (op. cit) a frequente impugnação de concursos no atual quadro jurídico português, remete as FFAA para a procura de soluções

no âmbito da NATO *Support and Procurement Agency*[40] (NSPA), o que prejudica, sobremaneira, os interesses da ID nacional.

Dentro dos mecanismos existentes, mas não aplicados, foi referida a prerrogativa que decorre da alínea b) do nº 1 do Artº 346 do Tratado de Funcionamento da UE (TFUE) que permite derrogar os princípios da concorrência do mercado na aquisição de produtos destinados a fins especificamente militares (UE, 2016b). Este é um dos instrumentos legais que a EDBTID (RCM52, 2023, p. 33) pretende explorar para "alavancar as capacidades competitivas e distintivas da indústria nacional e melhor posicionar as empresas portuguesas em determinados segmentos do mercado".

Quanto ao papel que a IdD, à semelhança da NSPA, pode ou deve ter na fase do *Procurement*, os dados evidenciam uma reação negativa à possibilidade da IdD se assumir como uma central de compras da Defesa.

Segundo G. Melo (*op.cit.*) o *Procurement*, conceptualmente, deveria ser centralizado, porém a realidade demonstra que apenas a contratação distribuída permite implementar mecanismos mais ágeis, expeditos e eficazes. Ainda assim, a existir um procedimento centralizado, G. Melo considera que seria uma atribuição da DGRDN e não da IdD.

Para 92% dos entrevistados da ESDN e 50% da IdD/ID, a IdD pode desempenhar um papel importante em ações de assessoria e *coaching* (V. Hilário, entrevista escrita, 4 de abril de 2024), na agilização dos processos administrativos, por norma burocráticos, e no apoio as FFAA para a elaboração de cadernos de encargos tecnicamente capazes (M. Almeida, *op. cit.*).

Quase todos os entrevistados, favoráveis a uma central de compras nacional para a Defesa, referem a necessidade da IdD ser restruturada organizacional e estatutariamente para exercer essa função. Para C. Félix (*op. cit.*) tratar-se-ia de um processo a médio e longo prazo, dependente da vontade política e do reconhecimento da IdD pelos seus pares da Defesa. A curto prazo, a IdD deve ter uma componente consultiva, através do seu projeto da base tecnológica de peritos de defesa.

[40] A NSPA é a principal agência fornecedora de serviços da OTAN, fornecendo um vasto leque de capacidades integradas à Aliança, aos seus países membros e parceiros (NATO, s.d.).

6.3.4. Síntese conclusiva

Caracterizado o CPD, procedeu-se à avaliação da participação e contributos da IdD/ID neste ciclo, considerando que já estão identificados os momentos em que estas entidades podem participar. Os resultados das entrevistas mostram que, fora da ESDN, o CPD é um processo desconhecido, ou vagamente conhecido. A sua importância, requer que sejam criadas condições para a IdD/ID participarem, pelo menos, como observadores.

Relativamente à integração da IdD no GAPD, surgiu uma demarcação nos grupos de entrevistados, com os elementos da ESDN a considerarem não ser essencial a IdD tornar-se membro efetivo deste grupo. No que se refere à LPM, à semelhança do que acontece com o CPD, a ID não conhece o seu processo de elaboração e os eventuais contributos dados, resultam de pedidos *ad-hoc* da ESDN.

A importância da LPM para a ID requer que esta tenha capacidade de conhecer, a priori, os seus projetos e subprojectos para, atempadamente, se preparar para a fase dos concursos públicos, implementando as estratégias empresariais necessárias ao negócio. A realização de *industry days* específicos para os projetos LPM é considerada uma boa ferramenta para atenuar a atual falta de conhecimento e potenciar a interação.

Na execução da LPM há uniformidade de opiniões referente à necessidade de implementar medidas de proteção/promoção da ID nacional, tentando-se compreender os mecanismos empregues por outros países na proteção das suas ID.

A nível interno, o caminho passa por se definirem as áreas prioritárias para uma autonomia estratégica nacional, para posteriormente, se criarem os mecanismos jurídicos e financeiros para potenciar a ID no desenvolvimento das capacidades das FFAA.

É sobejamente reconhecida a dificuldade das FFAA em concluírem os seus concursos públicos a nível nacional, devendo, por isso, ser revisto o mecanismo da contratação pública no SD tornando o processo mais ágil, evitando-se, assim, o recurso à NSPA, o que prejudica a ID portuguesa. O mecanismo previsto no TFUE deve também ser mais explorado na fase do *Procurement*.

Nesta fase, a IdD pode desempenhar, fundamentalmente, um papel de consultadoria técnica e de *coaching* empresarial, pois ainda não está dimensionada, nem estruturalmente preparada, para assumir-se como central de compras, à semelhança da NSPA. Para a IdD atingir este patamar, será necessário existir vontade política e um clima de confiança entre todas as entidades do ecossistema do SD.

7. CONCLUSÕES

No atual contexto geopolítico, com ameaças cada vez mais concretas à segurança da Europa, a UE e os seus Estados Membros deparam-se com a urgente necessidade de garantirem uma prontidão defensiva sustentada por uma ID robusta e competitiva, capacitada para proporcionar a autonomia estratégica em áreas vitais como as da segurança e defesa dos seus cidadãos e reposicionar a Europa como um ator preponderante e um garante de paz na nova ordem internacional que se perfila.

A implementação de políticas para reforçar e promover uma maior integração e cooperação na defesa, à escala europeia e nacional, tem subjacente o investimento numa BTID resiliente e inovadora que disponibilize tecnologias críticas para reduzir as dependências estratégicas da Europa e a vulnerabilidade das suas cadeias de valor no fornecimento de CM indispensáveis à modernização das FFAA.

A aprovação da primeira EIDE em março deste ano, revela a importância do setor industrial de defesa no fortalecimento da posição política e militar da UE. Em questões de defesa, ao promover uma maior cooperação entre os Estados Membros, a estratégia incentiva a colaboração em projetos transnacionais e a partilha de tecnologias e capacidades, enquanto fatores imprescindíveis à manutenção das soberanias nacionais, ao desenvolvimento económico, à inovação e criação de emprego qualificado.

Portugal, em consonância com esta visão e partilhando as preocupações europeias, aprovou várias estratégias no domínio da Defesa, criando um edifício normativo abrangente com o fim de promover e desenvolver a ID nacional.

A aprovação da EDBTID em 2023, está enquadrada e em concordância com a vontade politicamente expressa de fortalecer a ID e modernizar as FFAA, reconhecendo-se a ID como um pilar estratégico essencial para a execução de políticas de defesa eficazes para a soberania nacional e para a integração de Portugal nas dinâmicas de defesa europeias e da OTAN.

Caracterizada por uma composição heterogénea, dominada por PME, a ID nacional debate-se com um problema de competitividade face à sua dimensão e à do mercado português, num setor de atividade em que os Estados são simultaneamente os únicos investidores e compradores de CM. O apoio governamental é assim vital para assegurar que a ID possa, não apenas aumentar a sua capacidade produtiva, mas também desenvolver-se com sucesso num ambiente competitivo global, maximizando a sua participação em mercados externos.

O reforço da capacidade nacional em áreas tecnológicas de alto valor conducentes a uma maior participação da ID, requer políticas governamentais e mecanismos de ação estratégica que promovam a confiança e a cooperação entre todas as entidades do ecossistema do SD. É o caso da EDBTID, cuja gestão e implementação vai exigir um esforço coletivo e interdependência profunda para se criarem as condições necessárias a uma maior colaboração entre a ID e as FFAA,

A inevitabilidade desta interação organizacional para o sucesso da EDBTID e consequente reforço da autonomia estratégica nacional e da capacidade de ação das FFAA, motivou a questão central deste trabalho para saber como o ecossistema do SD pode otimizar a contribuição da ID nacional para o desenvolvimento das capacidades das FFAA.

Para responder eficazmente, estabeleceu-se um procedimento metodológico de investigação baseado num estudo de caso e num raciocínio dedutivo que, a partir da conceção geral do ecossistema, desenvolveu uma análise detalhada das interações e fatores correlacionais entre as entidades. Adotando uma estratégia de investigação qualitativa foi possível, através da análise documental e das entrevistas semiestruturadas, deduzir as evidências científicas que permitiram cumprir o objetivo geral deste trabalho.

O MA indicado possibilitou mensurar o OG recorrendo a três OE desenvolvidos individualmente nos capítulos anteriores. Com base nas respetivas sínteses conclusivas, apresentam-se as conclusões gerais deduzidas e que materializam o principal propósito desta investigação.

O momento atual é ímpar para a ID aproveitar as oportunidades que, a nível europeu e nacional, estão a ser colocadas à sua disposição sob o desígnio de uma autonomia estratégica, assente num setor industrial forte e competitivo. Neste sentido, compete à ID explorar os mecanismos de financiamento que a EIDE disponibiliza, em particular para as PME que caracterizam o setor industrial de defesa português.

No contexto nacional, a EDBTID, estabelecida para uma década, específica diretrizes e objetivos estratégicos para ampliar a capacidade nacional em setores industriais chave e áreas tecnológicas prioritárias. Pese embora o atraso na aprovação do PAE, constata-se haver dinamismo necessário para a sua eficaz implementação.

Trata-se, portanto, de uma EDBTID adequada que contempla as condições necessárias para uma efetiva colaboração e cooperação entre as FFAA e a ID

enfatizando a importância do "triplo-hélice" para o sucesso coletivo desta gestão estratégica.

As principais lacunas identificadas na EDBTID foram a ausência inicial do PAE, entretanto aprovado, e a inexistência de suportes legais e financeiros adequados para fomentar investimentos na ID. A revisão do seu modelo de financiamento e a implementação de uma cultura e liderança promotoras de redes de confiança, são encaradas como medidas cruciais necessárias que, em conjunto com a EDBTID, possibilitarão, de forma decisiva, uma maior contribuição da ID para o desenvolvimento das capacidades das FFAA.

No que respeita à IO e às relações desenvolvidas entre as entidades, constata-se que existe um perfeito conhecimento e uma consciência situacional do ecossistema do SD, condição fundamental para se atingirem níveis de desempenho mais elevados.

A existência de órgãos e pessoas dedicadas, em exclusivo, ao planeamento e desenvolvimento de capacidades, tem possibilitado, através da atual rede contatos, manter a ligação entre as instituições. As principais vulnerabilidades prendem-se com a falta de processos sistematizados e a grande rotatividade dos militares, mitigável com a inclusão de pessoal civil ou militares na reserva.

Assiste-se ainda, a um maior protagonismo da IdD que, assumindo um papel fundamental na execução e controlo da EDBTID, detém uma ação preponderante no desenvolvimento de uma ID nacional que, embora, pequena e fragmentada, demonstra possuir capacidades adaptativas para enfrentar os desafios e impor a sua posição em nichos específicos do mercado.

Porém, a aceitação e o reconhecimento, sem objeções, das novas atribuições da IdD está também dependente da sua capacidade: para dinamizar a plataforma *SmartDefence*, tornando-a funcional, relevante e colaborativa; para liderar um órgão nacional consultivo tipo NIAG; e agilidade em dotar a sua estrutura com representantes permanentes das FFAA para facilitar a aproximação do cliente (as FFAA) ao fornecedor (a ID), assegurando o desenvolvimento de capacidades customizadas.

Quanto ao CPD, não obstante a sua importância para a ID, verificou-se que é praticamente desconhecido fora da ESDN. Esta situação impede a ID de se ajustar e desenvolver estratégias de negócio em conformidade com as opções tomadas para o futuro das FFAA. É opinião comum que o processo do CPD deve ter maior visibilidade junto da ID, sugerindo-se que, no mínimo, a IdD possa

participar nele como observadora. Contudo, a integração da IdD no GAPD é controversa. Alguns membros da ESDN argumentam não ser essencial a sua inclusão como membro efetivo, podendo ser convidada ao abrigo dos estatutos na base da necessidade de saber.

Relativamente à LPM, a ID não está familiarizada com o seu processo de elaboração e, principalmente, com os seus projetos e subprojectos. Esta situação coloca a ID numa posição de vulnerabilidade, impossibilitando-a de se preparar para competir nos concursos públicos com empresas mais robustas. Para melhorar o conhecimento da ID sobre a LPM é sugerida a realização de eventos específicos, tipo *industry days*, a fim de divulgar a lei e os seus projetos.

Verifica-se, ainda, uma inequívoca necessidade de proteger e promover a ID nacional recomendando-se que, à semelhança de outros países europeus, se desenvolvam mecanismos jurídicos e financeiros que a privilegiem na fase do *Procurement*. A revisão dos processos de contratação pública é, também, considerada essencial para aumentar a percentagem de êxito de concursos públicos a nível nacional, reduzindo-se a dependência de organizações externas, como a NSPA, prejudiciais ao desenvolvimento da ID nacional.

Face ao exposto, estão reunidas as condições para responder à QC, formulando-se as seguintes orientações para otimizar a contribuição da ID nacional para o desenvolvimento das capacidades das FFAA: aprovar instrumentos legais e financeiros que possibilitem novos modelos de financiamento da ID; fomentar uma cultura e liderança assentes no diálogo e vontade de partilhar para promover redes de confiança; implementar processos de trabalho sistematizados, com canais de comunicação bem definidos, que conduzam a uma maior colaboração e cooperação; manter mais tempo os recursos humanos nas funções de planeamento alocando civis ou militares na reserva para uma melhor gestão do conhecimento e memória organizacional; dotar o ecossistema com um órgão de consulta novo ou adaptado sob coordenação da IdD e reforçar esta empresa com quadros militares para agilizar a interface entre as FFAA e a ID; dinamizar e operacionalizar a plataforma *SmartDefence*, tornando-a no portal colaborativo para os investimentos na Defesa; garantir, pelo menos como observadores, a participação da IdD/ID no CPD; permitir à IdD/ID ter visibilidade sobre o processo de elaboração da LPM; permitir, atempadamente, o acesso da IdD/ID às fichas de projeto e subprojectos; divulgar a LPM através de iniciativas inseridas nos planos de atividades; implementar medidas de proteção/promoção da ID nacional na fase do *Procurement*; rever normativos da

contratação pública nacional e explorar prerrogativa do TFUE para evitar o recurso das FFAA à NSPA; reforçar o papel da IdD como agência de consultadoria e de *coaching* empresarial no apoio à ID.

Com este estudo abordou-se a problemática da participação da BTID no desenvolvimento das capacidades para a FFAA numa ótica diferente que aportou novo conhecimento relacionado com a construção social que o ecossistema do SD pode instituir para melhorar a sua interdependência, em prol de um objetivo de interesse comum que, simultaneamente, é um desígnio nacional.

Durante o trabalho, as principais limitações encontradas estão associadas à aprovação do PAE e da EIDE numa fase já adiantada da investigação. Este facto inviabilizou a análise documental de dois documentos estruturantes e de enorme relevância para os propósitos deste estudo. Consequentemente, à luz destes novos normativos, importa rever as conclusões aqui apresentadas.

Recomenda-se, por isso, a continuação deste estudo para aferir o impacto dos dois documentos, ora citados, nas conclusões deste trabalho, pois é possível que tragam novas perspetivas de análise a equacionar. A existência de normativos jurídicos mais protecionistas da ID em alguns países da UE merece também ser objeto de estudo para estabelecer-se o comparativo e propor as devidas alterações à legislação nacional e aos procedimentos da contratação em vigor. Por outro lado, demonstrada a relevância da IdD nesta temática, justifica-se um estudo que investigue a adequabilidade da sua estrutura, organização e estatutos às responsabilidades legalmente atribuídas e àquelas que neste estudo foram deduzidas.

REFERÊNCIAS BIBLIOGRÁFICAS

Beaufre, André. (1966). *Introduction a la Stratégie*. ArmandColin, Paris.

Comissão Europeia (2003). *Governança e Desenvolvimento*. Bruxelas. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2003:0615:FIN:PT:PDF

Comissão Europeia (2010). *Annex 2 to the Communication: Towards interoperability for European public services*. Bruxelas. https://ec.europa.eu/isa2/sites/default/files/isa_annex_ii_eif_en.pdf

Comissão Europeia (2016). Plano de Ação Europeu no Domínio da Defesa. Bruxelas. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/uri=CELEX:52016DC0950

Comissão Europeia (2017). *Annex to the European Interoperability Framework – Implementation Strategy*. Bruxelas. https://eur-lex.europa.eu/%20resource.html?uri=cellar:2c2f2554-0faf-11e7%208a3501aa75ed71a1.0017.02/DOC_3&%20format=PDF

Comissão Europeia (2023). *EDF Presentation at the 54th Paris Air Show 2023*. Bruxelas: Directorate General for Defense, Industry, and Space. https://defence-industry-space.ec.europa.eu/document/download/bd6586e4-db60-45a5-a5d0-20bc1d98e259_en?filename=2023-06-19to25%20-%20Slides%20DEFIS%20presentation%20at%20Paris%20Air%20Show%20-%20EDF%202023%20%2B%20latest%20developments.pdf

Comissão Europeia (2024). E*uropean Defence Industrial Strategy: Joint Communication*. Bruxelas. https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en?filename=DIS%20Joint%20%20Communication.pdf

Conselho da União Europeia (2017). *Decisão (PESCO) 2017/2315 do Conselho que estabelece uma cooperação estruturada permanente (CEP) e determina a lista de Estados-Membros participantes*. Bruxelas: Jornal Oficial da UE. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32017D2315

Conselho da União Europeia (2022). *Bússola Estratégica para a Segurança e a Defesa*. Bruxelas. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf

Conselho Europeu (2023). *Reunião do Conselho Europeu (14 e 15 de dezembro de 2023) – Conclusões*. Bruxelas. https://www.consilium.europa.eu/media/68990/europeancouncilconclusions-14-15-12-2023-pt.pdf

Couto, A. C. (1988). *Elementos de Estratégia: Apontamentos para um Curso*. Lisboa: Instituto de Altos Estudos Militares.

Couto, A. C. (2004). *"Posfácio" em António Horta Fernandes e Francisco Abreu, Pensar a Estratégia: do Político-militar ao Empresarial*. Lisboa: Sílabo.

Decreto-Lei nº 183/2014, de 29 de dezembro (2014). *Lei Orgânica do Ministério da Defesa Nacional*. Diário da República n.º 250/2014, Série I de 2014-12-29. Lisboa: Ministério da Defesa Nacional.

Decreto-Lei n.º 249/2015, de 28 de outubro, (2015). A*prova a orgânica do ensino superior militar e consagra as suas especificidades no contexto do ensino superior*. Diário da República, 1.ª série, 211, 9298-9304. Lisboa: Presidência do Conselho de Ministros.

Decreto Regulamentar n.º 8/2015 de 31 de julho (2015). *Aprova a orgânica da DGRDN*. Diário da República, 1.ª série, 148, 5195-5197. Lisboa: Ministério da Defesa Nacional.

Decreto Regulamentar n.º 14/2015 de 31 de julho (2015). *Aprova a orgânica da DGPDN*. Diário da República, 1.ª série, 148, 5295-5297. Lisboa: Ministério da Defesa Nacional.

Despacho n.º 25/MDN/2022, de 23 de junho (2022). *Diretiva Ministerial Orientadora do Ciclo de Planeamento de Defesa*. Lisboa: Ministério da Defesa Nacional.

Despacho conjunto n.º 786/2020, de 30 de dezembro (2019). L*iquidação da EMPORDEF SGPS — Reestruturação das Participações Públicas na Economia de Defesa*. Diário da República, 2.ª série, 14, 38-40. Lisboa: Gabinetes do Ministro da Defesa Nacional e do Secretário de Estado do Tesouro.

EMGFA (2020). *Planeamento Estratégico Militar*. Lisboa: Divisão de Planeamento Estratégico Militar.

Ferreira, J. A. B. (2013). *Indústria Nacional na edificação de Capacidades da Defesa. Contributos do Desenvolvimento Sustentado das capacidades das Forças Armadas para a Economia nacional*. Lisboa: Instituto de Estudos Superiores Militares. TII CPOG 2012-2013.

Ferreira, M. C. (2017). *Economia da Defesa Nacional*. IDN cadernos. Lisboa. https://comum.rcaap.pt/bitstream/10400.26/22880/1/idncadernos_27.pdf

Ferreira, Vanessa M. (2017). *A Boa Governança Pública e o seu reflexo na pobreza*. Dissertação de Mestrado. Porto: Faculdade de Direito da Universidade do Porto.

Governo Constitucional (2022). *Programa do XXIII Governo Constitucional*. Lisboa. https://www.portugal.gov.pt/gc23/programa-do-governo-xviii/programa-do-governo-xviii-pdf.aspx?v=%C2%ABmlkvi%C2%BB=54f1146c-05ee-4f3a-be5c-b10f524d8cec

IdD Portugal Defence S. A. (2022). *Relatório e Contas Consolidado 2022*. https://www.iddportugal.pt/wp-content/uploads/2023/09/IDD-RGC-CONSOLIDADO-2022.pdf

IdD Portugal *Defence* S. A. (2023). *Plano de Atividades e Orçamento (PAO) 2023*. https://www.iddportugal.pt/wp-content/uploads/2023/10/idD-Portugal-Defence_Plano-Atividades-e-Orcamento-2023-2025-Incl.-Parecer-CF-e-ROC.10.11.2022_Signed.pdf

IdD Portugal *Defence* S. A. (2024). *Plano de Ação da Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa 2023-2033*. Lisboa: IdD Portugal Defence.

IdD Portugal *Defence* S. A. (s.d.). *Base Tecnológica e Industrial de Defesa*. https://www.iddportugal.pt/

Lei n.º 49/2009, de 5 de agosto (2009). *Regula as condições de acesso e exercício das atividades de comércio e indústria de bens e tecnologias militares*. Diário da República, 1.ª série, 150, 5065-5072. Lisboa: Assembleia da República.

Lei Orgânica n. º1, de 17 de agosto (2023). *Lei de Programação Militar*. Diário da República, 1.ª Série, 159, 2-8. Lisboa: Assembleia da República.

Machado, Francisco M. R. (2021). *Fundo Europeu de Defesa: Posicionamento de Portugal e Contributos para as Capacidades Militares*. Lisboa. Instituto de Estudos Superiores Militares. TII CPOSFA 2020-2021.

Mascarenhas, E., coord. (2014). *Indústrias e Tecnologias de Segurança e Defesa - Desafios e Oportunidades*. Cadernos N.º 6. Lisboa: Centro de Estudos Euro Defense.

Monteiro, F. J. T. T. M. (2023). *Restabelecimento dos Investimentos na Defesa*. Lisboa: Instituto Universitário Militar. TII CPOG 2022-2023.

NATO. (2018). *The Voice of Industry in NATO to inform Capability Development*. NIAG. https://diweb.hq.nato.int/niag/Documents/1524-18_BROCHURE50ans_NIAG-LR.pdf

NATO. (s.d.). *NATO Support and Procurement Agency (NSPA)* [Online]. https://www.nato.int/cps/en/natohq/topics_88734.htm

NEP / INV — 003 (A3) (2020). *Estrutura e regras de citação e referenciação de trabalhos escritos a realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.

Nunes C. & Alves R. P. (2022). *A Economia de Defesa em Portugal: A Caminhar Em Direção ao Futuro*. https://www.iddportugal.pt/economia-defesa/economia-defesa-numeros/

Nunes, I., Hartley, K., Ferraz, R., Venema, A., Szego, E., Olsson, P., Lopes, A., Nunes, C., Mendonça, J., & Simões, P. (2023). *Economia de Defesa—Um Conceito e uma Prática* (IDN E-Briefing Papers). Lisboa: Instituto da Defesa Nacional. http://hdl.handle.net/10400.26/46182

Parlamento e Conselho da UE (2018). *Regulamento (UE) 2018/ 1092 - Programa Europeu de Desenvolvimento Industrial no domínio da Defesa*. Bruxelas:

Jornal Oficial da EU. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32018R1092

Parlamento e Conselho da UE (2021). Regulamento (UE) 2021/697 - cria o Fundo Europeu de Defesa e revoga o Regulamento (UE) 2018/1092. Bruxelas: Jornal Oficial da EU.

Parlamento e Conselho Europeu (2009). Decisão nº 922/2009/CE sobre soluções de interoperabilidade para as administrações públicas europeias (ISA). Bruxelas: Jornal Oficial da UE. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009: 260:0020:0027:PT:PDF

Resolução do Conselho de Ministros n.º 35/2010 de 06 de maio (2010). *Aprova a Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa*. Diário da República, 1.ª Série, 88, 1599-1606. Lisboa: Presidência do Conselho de Ministros.

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

Resolução do Conselho de Ministros n.º 52/2023, de 05 de junho (2023). *Aprova a Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa*. Diário da República, 1.ª Série, 108, 26-39. Lisboa: Presidência do Conselho de Ministros.

Ribeiro, A. S. (2006). *Planeamento Estratégico e de Forças*. Revista Militar n.º 2457 – outubro de 2006, pp. 1019 -0. Lisboa. https://www.revistamilitar.pt/artigopdf/136

Ribeiro, A. S. (2007). *Elaboração da Estratégia de Defesa Militar: Contributos para um Novo Modelo*. Lisboa: Instituto Superior de Ciências Sociais e Políticas [ISCSP].

Ribeiro, A. S. (2008). *Processo de Formulação da Estratégia de Defesa Nacional*. Lisboa: Instituto de Estudos Superiores Militares. TII CPOG 2007-2008.

Ribeiro, A. S. (2010). *Teoria Geral da Estratégia: O Essencial ao processo Estratégico*. Coimbra: Almedina.

Ribeiro, A. S. (2020). *Modelos do Processo Estratégico*. Lisboa: Instituto Superior de Ciências Sociais e Políticas.

Rodrigues, C. (2020). *Made in Portugal: A Indústria de Defesa Nacional durante a Guerra Colonial (1961-1974)*. Revista de Ciências Militares, novembro, VIII (2), 73-92. https://www.ium.pt/?page_id=5714

Santos, Loureiro dos (2011). *Despacho do Presidente da Academia de Ciências de Lisboa sobre a aceitação da Definição/Conceito de Ciências Militares e a respetiva integração no conjunto dos domínios científicos reconhecidos por aquela Instituição*. Lisboa: Academia das Ciências.

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

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

União Europeia (2016a). *A Global Strategy for the European Union's Foreign And Security Policy*. Bruxelas. https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

União Europeia (2016b). *Tratado sobre o Funcionamento da União Europeia (versão consolidada)*. Bruxelas: Jornal Oficial da União Europeia. https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF

ESTUDO 6 – CONTRIBUTOS PARA A IMPLEMENTAÇÃO DA ESTRATÉGIA DE DESENVOLVIMENTO DA BASE TECNOLÓGICA INDUSTRIAL DE DEFESA 2023-2033[41]

CONTRIBUTIONS TO THE IMPLEMENTATION OF THE STRATEGY FOR THE DEVELOPMENT OF THE DEFENSE INDUSTRIAL TECHNOLOGY BASE 2023-2033

Pedro Mário Ferreira Fontes
Major de Administração Militar

Paulo Jorge do Nascimento Fernandes
Coronel de Material

Sofia Vitoriano Saldanha Junceiro
Capitão-de-fragata

RESUMO

A necessidade de fortalecer a indústria de defesa revela-se essencial para responder aos desafios de segurança atuais. Após um período marcado por baixos investimentos em defesa e uma crescente dependência de tecnologia externa, torna-se imperativo desenvolver a Base Tecnológica e Industrial de Defesa (BTID) para garantir a autonomia e a eficácia operacional das Forças Armadas. Neste contexto, é pertinente analisar os contributos que promovam uma transição eficaz para a Indústria 4.0, que se caracteriza pela adoção de tecnologias avançadas e pela automação e interligação de processos. A metodologia utilizada baseou-se num raciocínio indutivo a partir de um estudo de caso com uma abordagem mista, que incluiu análise documental e entrevistas semiestruturadas. Este estudo envolveu 17 entidades relevantes da BTID, permitindo obter uma visão abrangente sobre os desafios e sucessos da digitalização. Os resultados revelam uma integração significativa das tecnologias da Indústria 4.0 na BTID, embora se verifiquem diferenças entre os diversos setores. Apesar da BTID demonstrar um nível de maturidade tecnológica superior à média das empresas nacionais, enfrenta desafios como a necessidade de atualização contínua de competências e a integração de sistemas na era da transformação digital.

Palavras-chave: Base Tecnológica e Industrial de Defesa, Forças Armadas, indústria 4.0, transformação digital

[41] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto (CEMC 2023/2024). A versão integral encontra-se disponível no Centro de Recursos do Conhecimento do Instituto Universitário Militar

ABSTRACT

The necessity to strengthen the defense industry emerges as crucial in addressing current security challenges. Following a period characterized by minimal investment in defense and increasing reliance on external technology, it becomes imperative to develop the Defense Technological and Industrial Base (DTIB) to ensure operational autonomy and effectiveness of the Armed Forces. In this context, it is pertinent to examine contributions that facilitate an effective transition to Industry 4.0, characterized by the adoption of advanced technologies and the automation and interconnection of processes. The methodology employed involved inductive reasoning based on a mixed-approach case study, which included document analysis and semi-structured interviews. This study engaged 17 relevant entities within the DTIB, providing a comprehensive perspective on the challenges and successes of digitalization. The findings reveal significant integration of Industry 4.0 technologies within the DTIB, though variations exist across different sectors. Despite the DTIB demonstrating a technological maturity level above the national average, it faces challenges such as the need for continuous skill updating and system integration in the era of digital transformation.

***Keywords**: Defense Technological and Industrial Base, Armed Forces, industry 4.0, digital transformation*

1. INTRODUÇÃO

Com o fim da Guerra Fria, a Europa mergulhou numa sensação generalizada de segurança, provocando uma crescente despreocupação com os assuntos de defesa, tanto a nível político como social. A bolha de segurança que se foi criando, juntamente com a narrativa de uma paz duradoura na Europa, conduziu a uma constante redução dos investimentos em defesa, sendo estes canalizados para outras áreas consideradas prioritárias (Conselho da União Europeia, 2009, p. 27).

O desinvestimento em defesa, aliado ao desinteresse generalizado pelos assuntos de defesa, fez com que os Estados europeus não sentissem a necessidade de controlar a indústria de defesa, deixando assim de assumir a despesa associada, a qual se tornava cada vez mais difícil de justificar perante a sociedade (Chin, 2019, p. 770).

Esta conjuntura provocou o desaparecimento da indústria de defesa ou a sua passagem para entidades privadas. Como facilmente se compreende, a indústria privatizada, tendo o lucro como principal objetivo, teve de se reinventar. Passou por processos de transformação industrial para não se limitar à produção exclusiva para a defesa, desenvolvendo produtos que pudessem alcançar outros mercados

e clientes, nomeadamente através de bens comerciais de utilização civil (Antunes, 2013).

Após a tomada de consciência política e económica de que a indústria de defesa não representava apenas um custo associado aos Estados beligerantes, mas sim um setor industrial de utilidade pública, desde logo pelos postos de trabalho e pela contribuição para a economia nacional, os Estados-membros da União Europeia (UE) acordaram, em 2007, desenvolver a Base Tecnológica e Industrial de Defesa Europeia (BTIDE). Esta iniciativa visava estabelecer uma base industrial de defesa comum, mais integrada e com menos duplicações, para aumentar a autonomia industrial de defesa europeia (Comissão Europeia, 2007). Para alcançar esta meta, revelava-se essencial uma coordenação eficaz, a integração e o investimento nas bases industriais de defesa nacionais dos Estados-membros (Briani et al., 2013).

Em 2010, e por forma a alinhar os esforços nacionais com os princípios e objetivos da BTIDE, foi criada a Base Tecnológica e Industrial de Defesa (BTID) nacional, aprovada pela Resolução do Conselho de Ministros (RCM) n.º 35/2010, de 6 de maio. Esta estratégia nacional apela à inovação e à colaboração entre o meio civil e as Forças Armadas (FFAA), por forma a estimular o desenvolvimento de tecnologias de duplo uso, ou seja, tecnologias que podem ser empregues por militares, mas também tem utilização no meio civil (RCM nº 35/2010).

Da mesma forma, o Conceito Estratégico de Defesa Nacional (CEDN) de 2013, ainda em vigor, realça a importância de garantir um nível tecnológico elevado no setor da defesa, promovendo a Investigação, Desenvolvimento e Inovação (ID&I), para potenciar o produto operacional das FFAA. Refere também a necessidade da integração da BTID num Plano Nacional de Inovação mais amplo, por forma a desenvolver tanto a economia portuguesa como a manter o alinhamento com a ambição europeia (RCM n.º 19/2013, de 5 de abril, 2013, p. 1995).

A recente tensão geopolítica e o conflito entre a Rússia e a Ucrânia de 2022, destacaram a importância de uma defesa europeia comum e aceleraram a adoção de novas políticas de defesa europeias, para fazer face aos desafios emergentes do atual contexto internacional. Entre elas, destaca-se a bússola estratégica de segurança e defesa da UE, de 21 de março de 2022, que incita os Estados-membros a adotarem uma abordagem estratégica de defesa comum, indicando o caminho para se alcançar a soberania tecnológica europeia, a redução de dependências externas e o fortalecimento da BTIDE (European Union, 2022, pp. 47–48).

Neste novo quadro internacional, foi revista a estratégia de desenvolvimento da BTID nacional para o período 2023-2033, aprovada a 5 de junho de 2023. Incorporando uma visão mais ampla e integrada da defesa, esta estratégia foca-se na modernização e inovação da indústria de defesa portuguesa e menciona a importância da colaboração internacional, sobretudo com a UE e com a *North Atlantic Treaty Organization* (NATO), além da necessidade de se promover uma indústria moderna e preparada para se adaptar aos desafios emergentes, com destaque para os domínios do ciberespaço e espaço, e das emergências complexas, incluindo as sanitárias e ambientais (RCM n.o 52/2023, de 5 de junho, 2023).

A rápida evolução tecnológica tem gerado profundas reflexões nos meios académico e industrial. Na feira de Hannover na Alemanha de 2011, foi mencionada pela primeira vez a Indústria 4.0 (i4.0), considerando-se que se estaria a transitar para a quarta revolução industrial (Barbier, 2020, p. 17).

Destarte, torna-se evidente que para atingir os objetivos estabelecidos na estratégia de desenvolvimento da BTID, é essencial um significativo investimento na modernização tecnológica. No entanto, a integração da i4.0 requer um estudo detalhado para compreender a situação atual da BTID, a fim de orientar a transformação digital nas organizações da indústria de defesa, em direção a uma indústria moderna e competitiva.

Este estudo permite contribuir para uma transição mais efetiva para a nova era industrial, marcada pela integração de tecnologias inovadoras e processos interligados e automatizados. A ausência de estudos detalhados sobre a BTID neste domínio pode constituir-se um obstáculo ao pleno desenvolvimento das potencialidades oferecidas pela i4.0, o que, por sua vez, pode influenciar o desenvolvimento e a competitividade da BTID.

O objeto de estudo deste trabalho centra-se na BTID, conforme definida na sua estratégia de desenvolvimento, aprovada a 5 de junho de 2023. É neste documento que se encontram delineados os objetivos estratégicos a alcançar com a BTID nacional, identificando, nomeadamente, as Áreas Tecnológicas de Interesse Prioritário (ATIP).

Objetivo Geral (OG) deste estudo consiste em propor contributos para a implementação e reforço da i4.0 na BTID, por forma a impulsionar o produto operacional das FFAA. Para alcançar o OG da investigação, foram estabelecidos os seguintes Objetivos Específicos (OE): OE1: Analisar a atual integração e adaptação da digitalização na BTID, identificando os principais desafios e sucessos alcançados;

OE2: Analisar o impacto dos fatores endógenos e exógenos da transformação digital na BTID e o impacto no produto operacional das FFAA; OE3: Analisar as capacidades e competências atuais da BTID nas ATIP.

Com o propósito de orientar a investigação, foi definida a seguinte Questão Central (QC): Como é que a BTID pode implementar ou reforçar os conceitos i4.0, de forma a maximizar o produto operacional das FFAA?

Esta investigação estrutura-se em cinco capítulos. Após a presente introdução, o segundo capítulo versa sobre o enquadramento teórico, abarcando a i4.0 e a maturidade digital, a que se segue uma análise ao estado da arte e ao quadro conceptual envolvente da BTID. O terceiro capítulo dedica-se à metodologia e ao método empregue, detalhando os participantes, procedimentos e os instrumentos utilizados na recolha e tratamento de dados. No quarto capítulo apresentam-se os dados e discutem-se os resultados, enfatizando a digitalização na BTID, a transformação digital e as capacidades e competências a desenvolver, culminando na apresentação dos contributos para a implementação e reforço dos conceitos i4.0 na BTID. O quinto e último capítulo sintetiza os resultados e apresenta as conclusões finais do estudo.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

2.1. Indústria de defesa

A indústria de defesa portuguesa, marcada por um passado histórico significativo, teve um papel preponderante durante as guerras nos territórios africanos entre 1961 e 1974, que na época se encontravam sob administração portuguesa. Empresas como as Indústrias Nacionais de Defesa (INDEP), as Oficinas Gerais de Material Aeronáutico (OGMA) e a Sociedade Portuguesa de Explosivos (SPEL), tiveram um papel determinante no apoio às necessidades militares de Portugal. Este período foi caracterizado por uma intensa atividade industrial e pela importância da produção bélica nacional (Pinto, 2009).

Após este período, especialmente no contexto do pós-Guerra Fria, a indústria de defesa em Portugal deparou-se com a necessidade imperativa de reestruturação. A diminuição dos gastos militares, um fenómeno global que também afetou Portugal, impôs uma revisão nas prioridades de defesa. Este cenário exigiu uma transformação da indústria, adaptando-se a um novo paradigma em que a eficiência e a inovação se tornaram essenciais (Barros, 2002). O conceito inicial de indústria de defesa, que se limitava às empresas que produziam apenas armas,

munições e equipamento militar, sofreu uma evolução, passando a abranger o conjunto de empresas que participam em alguma parte do ciclo de produção de equipamentos de defesa. Neste contexto de transformação, a Lei que regula as condições de acesso e exercício das atividades de comércio e indústria de bens e tecnologias militares, vem definir a indústria de defesa como o "complexo de actividades que tem por objecto a investigação, o planeamento, o ensaio, o fabrico, a montagem, a reparação, a transformação, a manutenção e a desmilitarização de bens ou tecnologias militares" (Lei n.º 49/2009, p. 5065).

2.2. Indústria 4.0

As denominadas revoluções industriais (Figura 1) surgiram quando inovações tecnológicas e novas perspetivas do mundo provocaram mudanças significativas na indústria.

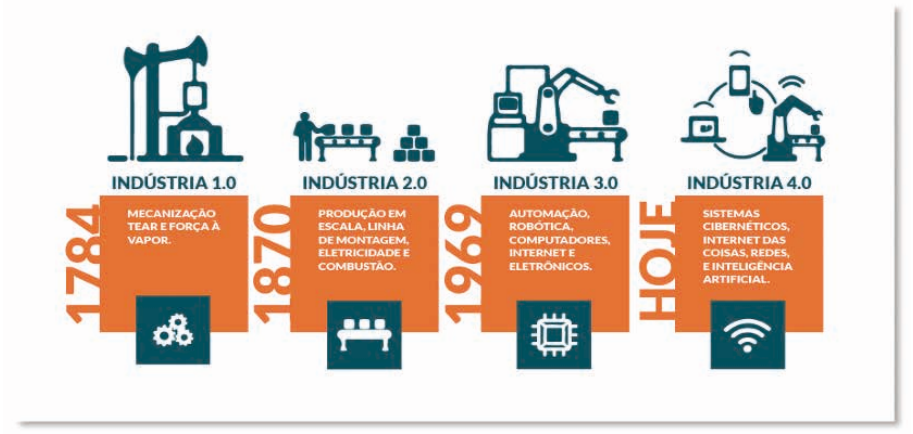

Figura 1 – Revolução industrial
Fonte: Silveira (2016)

Desde o início do século XXI d.C., a i4.0 introduziu uma nova dinâmica de produção, ancorada na digitalização e na automação dos processos produtivos assim como na construção de uma cadeia de valor digital interligada, que facilita a comunicação entre parceiros comerciais, produtos e o meio envolvente, integrando o universo físico ao digital (Soltovski et al., 2020).

A i4.0, ou a quarta revolução industrial, é um passo rumo ao futuro. Com sensores incorporados na quase totalidade dos materiais, bens e instalações

industriais, a i4.0 visa atingir a digitalização deste setor. Abrange desde o desenvolvimento de produtos e aquisições até à produção, distribuição e serviço, digitalizando e integrando processos verticalmente em toda a organização.

Os pilares desta revolução (Figura 2), incluem, entre outros, a internet das coisas, a Inteligência Artificial (IA), o *big data* e a análise de dados, a robótica avançada, e a realidade aumentada (Tabaković & Durakovic, 2021).

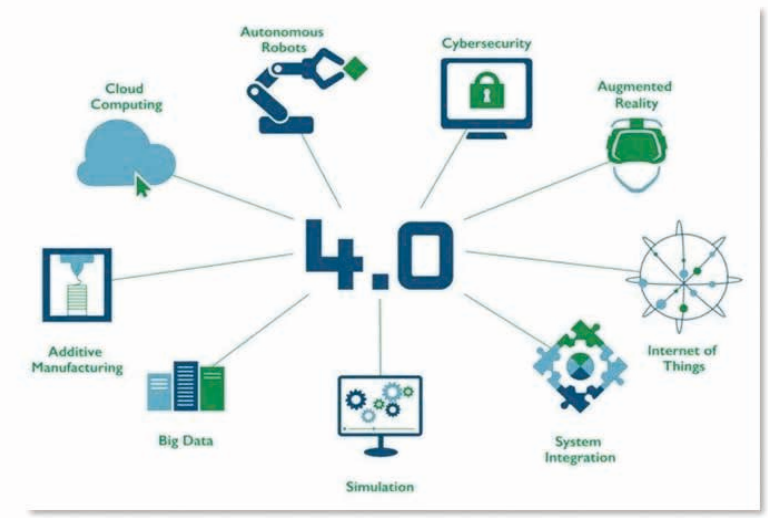

Figura 2 – Indústria 4.0
Fonte: Tabaković e Durakovic (2021).

Através da i4.0, a digitalização da indústria promete revolucionar o setor da defesa, apesar da realidade ainda se mostrar diferente do idealizado. Os obstáculos como a iliteracia digital e a escassez de fundos levam muitas empresas a interromper ou a reduzir suas ambições digitais, resultando em poucas transformações efetivas e muitas iniciativas fracassadas (Tabaković & Durakovic, 2021).

É notória a complexidade que as novas tecnologias apresentam. Conforme identificado por Tabaković e Durakovic (2021), apenas 3% das iniciativas de transformação digital alcançaram sucesso pleno, sendo que, a maioria das empresas acaba por se contentar com resultados modestos, longe do potencial da i4.0, isto devido à rápida evolução tecnológica que muitas vezes supera a capacidade de adaptação destas organizações.

No entanto, o progresso tecnológico não se detém e a compreensão aprofundada sobre digitalização torna-se um requisito essencial para o mundo empresarial. Reconhece-se que as empresas que conseguirem integrar com êxito a digitalização nos seus modelos de negócios estarão a posicionar-se para colher benefícios significativos no futuro (Tabaković & Durakovic, 2021).

Face a este cenário, o setor de Investigação e Desenvolvimento (I&D) na indústria aeroespacial e de defesa dos Estados Unidos da América (EUA), reconhecido pela sua importância estratégica, está empenhado no desenvolvimento de novas tecnologias e métodos produtivos. Este considera que a i4.0 representa simultaneamente um desafio e uma oportunidade, catalisando a inovação e a digitalização no setor (Barbier, 2020, p. 23).

A implementação de tecnologias emergentes como *machine learning*, IA e a internet das coisas tem potencial para transformar radicalmente a I&D, promovendo um aumento de eficiência e uma redução significativa dos custos.

2.2.1. Transformação digital

De acordo com Matt et al. (2015), a transformação digital compreende a exploração e integração de novas tecnologias digitais por parte das empresas. Esta transformação implica mudanças significativas nas operações comerciais, influenciando tanto os produtos e processos como as estruturas organizacionais e os conceitos de gestão.

A transformação digital através da i4.0 adquire grande importância no contexto da indústria de defesa, visto que o desenvolvimento e a implementação de tecnologias de ponta são fundamentais para manter a competitividade e assegurar a segurança nacional. As empresas do setor de defesa enfrentam o desafio de se adaptarem a estas novas tecnologias para desenvolver armamentos modernos e sistemas de defesa mais eficazes (Voitko, et al., 2020).

Contudo, a transformação digital no setor de defesa enfrenta desafios significativos, incluindo a necessidade de padronização, desenvolvimento de competências digitais e adaptação das estratégias empresariais às novas realidades tecnológicas. Apesar destes obstáculos, o potencial para melhorias em eficiência, inovação e capacidade de resposta a ameaças é imenso, destacando-se que a adoção dessas tecnologias é um passo inevitável para as empresas e para os países que procuram manter e melhorar as suas capacidades de defesa (Voitko et al., 2020; Yaqub & Alsabban, 2023).

2.2.2. Maturidade digital

O conceito de maturidade digital encontra-se fortemente ligado ao processo de transformação digital, ou i4.0 no caso particular da indústria, podendo afirmar-se que a maturidade representa a etapa final da digitalização, sendo este o objetivo que as empresas pretendem alcançar. As organizações que atingiram tal nível de maturidade digital experienciaram avanços notáveis no seu funcionamento e, consequentemente, verificaram um aumento na satisfação dos seus clientes (Aslanova & Kulichkina, 2020, p. 443).

A maturidade digital compreende uma perspetiva de gestão, detalhando as realizações de uma empresa no âmbito dos seus esforços de transformação digital. Isto inclui alterações em produtos, serviços, processos, competências, cultura organizacional e a capacidade de gerir eficazmente processos de mudança (Teichert, 2019, p. 1675).

2.3. Quadro conceptual

Para a compreensão do tema, apresentam-se conceitos estruturantes para a investigação: a BTID e o Produto Operacional.

2.3.1. Base tecnológica e industrial de defesa

O conceito de BTID foi adotado em Portugal pela primeira vez em 2010, onde era entendido como "o conjunto das empresas e das entidades do sistema científico e tecnológico nacional, públicas (incluindo capacidades orgânicas das FFAA) e ou privadas, com capacidade para intervir numa ou mais das etapas do ciclo de vida logístico" dos sistemas e equipamentos das FFAA (RCM n.º 35/2010, de 06 de maio, 2010, p. 1600).

Este termo é abrangente e não engloba apenas a indústria de defesa propriamente dita, mas também as infraestruturas de ID&I, as instituições académicas, e outras entidades que contribuem para a inovação e o avanço tecnológico no âmbito da defesa.

No seguimento da revisão da estratégia de desenvolvimento, aprovada a 5 de junho de 2023, define a BTID nacional como o "conjunto das empresas e das entidades do Sistema Científico e Tecnológico Nacional (SCTN), públicas e/ou privadas, com capacidade para intervir numa ou mais das etapas do ciclo de vida logístico dos equipamentos" de defesa (RCM n.º 52/2023, de 5 de junho, 2023, p. 29).

Esta estratégia realça a importância da ID&I, incentiva a participação em projetos colaborativos internacionais e promove a integração de empresas portuguesas em consórcios de cooperação europeus ou internacionais de defesa.

O processo de desenvolvimento de produtos tecnologicamente inovadores, desde a fase de conceção até à produção, envolve a participação coordenada e cooperativa de três principais atores nacionais: a academia, a indústria e o governo. Sendo que, a interação entre estas três entidades é definida por Simões, Moreira e Dias (2020) como tripla-hélice essencial para a transferência de conhecimento.

Na atualidade, a BTID caracteriza-se pela diversidade e pela capacidade de gerar sinergias entre o uso civil e militar, englobando 40 setores de atividade diferentes com capacidade de desenvolver e fabricar produtos e serviços de duplo uso. É composta por 363 empresas e 61 entidades de I&D, conforme indicado pela idD Portugal Defence (2022).

Esta base tecnológica é maioritariamente (89%) formada por Pequenas e Médias Empresas (PME), o que sugere um tecido empresarial diversificado, mas que poderá enfrentar desafios na integração de tecnologias da i4.0, considerando que a maioria das empresas (57%) tem mais de 20 anos de atividade, o que demonstra a longa experiência com a capacidade instalada (Nunes et al., 2021).

2.3.2. Produto operacional

O produto operacional das FFAA compreende a eficácia com que se integram e coordenam as capacidades militares "nos domínios naval, terrestre, aéreo, espacial, cibernético e de informações", em resposta às complexas ameaças globais (Decreto-Lei n.º 19/2022, de 24 de janeiro, 2022, p. 3). Contudo, salienta-se que uma capacidade só está plenamente edificada quando todos os seus elementos estiverem garantidos, de modo a permitir produzir efeitos nos níveis estratégico, operacional e tático (Despacho n.º 11400/2014, de 11 de setembro, 2014, p. 23657).

Os elementos que formam a base para a edificação de capacidades militares são frequentemente designados como vetores de desenvolvimento. Estes incluem Doutrina, Organização, Treino, Material, Liderança, Pessoal, Instalações e Interoperabilidade, conforme elencado pela NATO (2016, p. 44). Estes vetores oferecem um quadro para a análise e desenvolvimento de capacidades no âmbito militar, assegurando que as FFAA se mantêm prontas e capazes de responder de forma coesa e integrada a qualquer desafio. Assim, o produto operacional não se define apenas pela disponibilidade de equipamento ou pela quantidade de efetivos,

mas pela capacidade de utilizar eficientemente todos estes recursos de modo harmonioso e adaptável a contextos de ameaça em constante evolução.

Neste contexto, a BTID está intrinsecamente ligada ao produto operacional, uma vez que os equipamentos desenvolvidos pela indústria de defesa têm um impacto significativo, especialmente nos vetores de desenvolvimento material e interoperabilidade. Esta influência permite a edificação de capacidades que, posteriormente, serão utilizadas pelas FFAA, culminando na geração do produto operacional.

3. METODOLOGIA E MÉTODO

Para a alcançar o OG do presente trabalho, adotou-se uma metodologia de raciocínio indutivo, partindo-se de factos de entidades particulares para a teorização (Santos & Lima, 2019, p. 18). Nesta investigação, foram analisadas algumas organizações da indústria de defesa, e foi feita uma generalização para a BTID como um todo, possibilitando obter contributos para implementar e fortalecer a digitalização na BTID, maximizando o produto operacional das FFAA.

O desenho da pesquisa assentou num estudo de caso, pois, seguindo o preconizado por Santos e Lima (2019, p. 36), o investigador "procura recolher informação detalhada sobre uma única unidade de estudo, podendo essa unidade ser o indivíduo, a comunidade ou até mesmo a nação", num horizonte temporal transversal, que se encontra delimitado à BTID portuguesa, num período compreendido desde junho de 2023, data de aprovação da estratégia de desenvolvimento da BTID, até março de 2024, data em que a análise documental sobre o tema se encontra consolidada, apelando-se à compreensão de um "fenómeno contemporâneo dentro do seu contexto da vida real, especialmente quando os limites entre o fenómeno e o contexto não estão claramente definidos" (Yin, 2005, p. 32).

Esta abordagem enquadrou-se no âmbito das estratégias de investigação mistas, pois combina "no mesmo projeto de investigação estratégias de investigação quantitativas e qualitativas" (Santos & Lima, 2019, p. 30), nomeadamente através da obtenção de respostas descritivas e respostas de classificação usando a escala de Likert.

A investigação baseou-se na análise documental, complementada pela recolha de dados e informações através de entrevistas semiestruturadas. O objetivo foi alcançar, de forma simultânea, a verificação e o aprofundamento dos dados,

conforme referido por Santos e Lima (2019, p. 102). Esta metodologia permitiu uma compreensão mais rica e detalhada do objeto de estudo, integrando diferentes fontes e perspetivas.

O estudo desenvolveu-se em duas fases distintas. Na primeira fase, exploratória, efetuou-se uma revisão bibliográfica extensiva, para fundamentar o estudo e estabelecer um entendimento inicial do estado da arte. Na segunda fase, de investigação, a atenção centrou- se na análise detalhada da documentação mais relevante e nas entrevistas realizadas, visando responder às QD e à QC do modelo análise.

Quadro 1 – Modelo de Análise

<table>
<tr><td>Objeto da Investigação (OI):</td><td colspan="5">Base Tecnológica e Industrial de Defesa (BTID)</td></tr>
<tr><td>Objetivo Geral (OG):</td><td colspan="5">Propor contributos para a implementação e reforço da i4.0 na BTID, por forma a impulsionar o produto operacional das FFAA.</td></tr>
<tr><td rowspan="2">Objetivos Específicos (OE)</td><td>Questão Central (QC):</td><td colspan="4">Como é que a BTID pode implementar ou reforçar os conceitos i4.0, de forma a maximizar o produto operacional das FFAA?</td></tr>
<tr><td>Questões Derivadas</td><td>Conceitos</td><td>Dimensões</td><td>Indicadores</td><td>Recolha de Dados</td></tr>
<tr><td>OE1: Analisar a atual integração e adaptação da digitalização na BTID, identificando os principais desafios e sucessos alcançados.</td><td>QD 1: De que forma se posiciona atualmente a BTID na transformação digital, e quais os principais desafios e sucessos alcançados?</td><td rowspan="3">BTID</td><td rowspan="2">Indústria 4.0</td><td>Nível de integração da Indústria 4.0
Desafios na implementação da Indústria 4.0
Sucessos alcançados com Indústria 4.0</td><td rowspan="3">Análise documental

Entrevistas</td></tr>
<tr><td>OE2: Analisar o impacto dos fatores endógenos e exógenos da transformação digital na BTID e o impacto no produto operacional das FFAA.</td><td>QD 2: De que forma a transformação digital da BTID é influenciada por fatores endógenos e exógenos, e qual o impacto no produto operacional das FFAA?</td><td>Influência da cultura interna
Impacto das Políticas Governamentais
Efeito das tendências de mercado
Potenciar o produto operacional</td></tr>
<tr><td>OE 3: Analisar as capacidades e competências atuais da BTID nas ATIP.</td><td>QD 3: De que forma as capacidades e competências da BTID se alinham com as ATIP?</td><td>Áreas tecnológicas de interesse prioritário</td><td>Competências nas áreas de interesse prioritário
Prioridade no desenvolvimento de novas competências
Planos de melhoria de capacidades</td></tr>
</table>

Considerando a natureza do estudo, foram realizadas 17 entrevistas às entidades apresentadas da Tabela 1, oferecendo uma perspetiva abrangente da BTID e proporcionando uma visão holística do objeto de investigação.

Tabela 1 – Identificação dos entrevistados

Nome	Entidade
Carla Costa e Silva	Diretora da qualidade da Milicia - Bens de Segurança e Tecnologia Militares
Ana Santos	Diretora de Produção da Trotinete, Lda
Philippe Carvalho Atgé	Gerente da Europa Victrix
Luís Félix	Diretor do CIAFA
Delfim Rego	Project Management da Thales Edisoft Portugal
José Neves	Administrador da GMV
Ana Martins	Gestão de Inovação da Connect Robotics
Carlos Batalha	Chefe da DIVITO da Força Aérea Portuguesa
Dário Pedro	CEO da Beyond VIsion
EB10*	CINAMIL
EB11*	ARDITI
EB12*	EID S.A.
Rodrigo Pascoal	Business Development Director da Critical Software S.A.
Gilda Santos	Gestor de área: Proteção e Defesa da CITEVE
João Gaspar	Gerente da Swatter Company
Pedro Miguel do Vale Cruz	Chefe da Divisão de Inovação e Doutrina do Exército
Raul Lourenço	Defence & Security Manager da AED Cluster Portugal

Recorreu-se a uma amostragem não-probabilística intencional para obter as múltiplas perspetivas relevantes para o estudo (Santos & Lima, 2019, p. 69). Esta abordagem permitiu maximizar a recolha das visões representativas, assim como aprofundar tanto a perspetiva interna quanto externa da BTID. Os entrevistados responderam a um guião previamente elaborado, tendo as respostas sido obtidas entre 16 de fevereiro e 27 de março de 2024, por via eletrónica (através de e-mail) e presencialmente.

Relativamente à recolha de dados para este estudo, os instrumentos principais incluíram a análise documental e a realização de entrevistas semiestruturadas. A análise documental incidiu em três áreas-chave: normativos nacionais relacionados com a indústria de defesa, artigos científicos relativos ao tema e estudos de caso nacionais e internacionais considerados relevantes para esta investigação.

As entrevistas tiveram o objetivo de verificar e aprofundar o conhecimento adquirido, direcionando-se à chefia de uma amostra de organizações da indústria de defesa e a entidades-chave no âmbito da BTID, nomeadamente a AED Cluster Portugal, aos responsáveis pela inovação no Exército e na Força Aérea Portuguesa, e aos Centros e Investigação dos ramos das Forças Armadas.

Para o tratamento das entrevistas, recorreu-se à análise de conteúdo, tendo-se seguido as três fases de análise propostas por Bardin (2016, p. 125), nomeadamente: i) a pré-análise, onde se efetuou a leitura flutuante dos resultados das entrevistas, para a posterior codificação; ii) a exploração do material, onde se estabeleceu a frequência de aparição, como regra para a enumeração (regras de contagem) das Unidades de Registo (UR); iii) o tratamento dos resultados, foi nesta fase que se elaboraram os quadros com as Unidades de Contexto (UC) das respostas dos entrevistados, às quais se atribuíram as UR respetivas.

Para obter estatísticas descritivas das classificações alcançadas nas respostas quantitativas, recorreu-se ao *software* de análise estatística "SPSS", versão 29.0.0.0. No que concerne às respostas qualitativas, o tratamento dos dados foi efetuado utilizando o *software* de análise qualitativa "MAXDQA Analytics Pro", versão 24.2.0, do qual se extraiu a informação necessária para a análise efetuada no capítulo seguinte. Conforme Rädiker (2023) salienta, a pertinência do MAXQDA manifesta-se especialmente pela sua capacidade de proporcionar um acesso rápido a todos os dados relevantes, bem como pela transparência e rastreabilidade que confere ao processo analítico.

4. APRESENTAÇÃO DOS DADOS E DISCUSSÃO DOS RESULTADOS

Neste capítulo, são apresentados os dados e discutidos os resultados do presente estudo. Esta análise consolida a revisão da literatura com os conhecimentos adquiridos a partir das entrevistas realizadas, com o objetivo de responder às três QD e, posteriormente, à QC de investigação.

4.1. Digitalização na BTID

A BTID constitui um pilar fundamental para o desenvolvimento e a inovação no âmbito da defesa nacional, integrando um vasto leque de competências e capacidades tecnológicas. De seguida, procede-se à análise da perceção da

integração da transformação digital pela BTID, identificando-se os principais desafios e sucessos alcançados.

4.1.1. Maturidade da BTID

Os dados obtidos, conforme ilustrados no Quadro 1, referentes ao grau de incorporação das tecnologias i4.0 nos processos da BTID, destacam as estatísticas da perceção global. Com uma média de 3,56, constata-se uma avaliação positiva em relação à adoção das tecnologias i4.0 na BTID.

No entanto, a análise revela uma heterogeneidade nas opiniões dos entrevistados, com as classificações a variar entre 0 e 5 e um desvio padrão de 1,153. Isso indica que alguns setores de atividade da BTID ainda não beneficiam plenamente da integração i4.0, enquanto outros estão mais avançados.

Em termos comparativos, a BTID situa-se numa posição favorável em relação ao panorama empresarial nacional. De acordo com o relatório de Castro, Nieto-Carrillo e Associação Portuguesa de Sistemas de Informação (2023), o nível de maturidade digital das empresas portuguesas foi classificado na categoria de "Iniciado" (Figura 3), com uma classificação mediana de 1,18. Em contrapartida, com base nos dados recolhidos junto da BTID, esta poderia ser incluída na categoria de "Experiente", demonstrando uma maturidade mais avançada na integração das tecnologias i4.0.

Figura 3 – Níveis de maturidade i4.0
Fonte: Castro, Nieto-Carrillo e Associação Portuguesa de Sistemas de Informação (2023, p. 10).

A disparidade observada entre a BTID e o cenário global das empresas em Portugal realça o êxito da BTID na integração das tecnologias i4.0. Consequentemente, o setor da defesa apresenta-se como um modelo de excelência em práticas inovadoras a nível nacional.

4.1.2. Integração das tecnologias i4.0 na BTID

A transformação digital tem sido acompanhada por diversos desafios e sucessos. Da análise de conteúdo realizada, retiram-se contributos importantes sobre as principais preocupações e avanços conseguidos pelas organizações da BTID.

Em relação aos desafios, a necessidade de integrar "Tecnologias Emergentes" e efetivar os "Sistemas e Integração" evidenciam-se como as preocupações mais mencionadas pelos participantes. A adaptação às novas tecnologias e a sua integração harmoniosa nos sistemas existentes são vistas como etapas críticas para alcançar o sucesso na era i4.0. Especificamente, a integração de IA e a utilização da realidade aumentada, com o objetivo de aperfeiçoar os processos de produção, sobressaem como áreas de interesse. Estas preocupações realçam a importância da inovação tecnológica contínua e da capacidade de integração sistémica como fatores-chave para acompanhar a competitividade industrial.

O segmento "Recursos Humanos" emerge igualmente como um desafio amplamente citado. A transformação digital impõe a necessidade de qualificar e adaptar os trabalhadores, tanto nas competências técnicas como na transição para uma cultura de inovação. A resistência à mudança, a necessidade de formação contínua e a atração de talentos qualificados, são alguns dos pontos identificados pelos entrevistados, refletindo a complexidade do processo de adaptação dos recursos humanos à i4.0. Este desafio identificado é corroborado pelo artigo de Tabaković e Durakovic (2021, p. 66), tendo identificado que "70% dos programas empresariais de transformação digital falham devido à falta de literacia ou sensibilização digital".

Por outro lado, nos sucessos identificados, o segmento "Gestão de Dados e Segurança" destaca-se como um aspeto central, evidenciando progressos notáveis na capacidade das empresas para proteger e otimizar o tratamento dos dados. A implementação de soluções avançadas de cibersegurança, a integração de sistemas de gestão de qualidade e o emprego de IA na ciberdefesa, são considerados desenvolvimentos prioritários para a eficiência e segurança da atividade industrial.

Adicionalmente, realça-se o segmento "Tecnologias e Sistemas", onde os sucessos alcançados ressaltam o impacto positivo da adoção de novas tecnologias na eficácia e na inovação empresarial. A implementação de plataformas online para a gestão de stocks, a utilização de sistemas de aterragem automática para drones, e o desenvolvimento de soluções integradas de comunicação, evidenciam o esforço empregue para potenciar a autonomia, a flexibilidade e a capacidade de inovação das empresas face aos desafios contemporâneos.

Perante o nível de integração das tecnologias i4.0 analisado e aos sucessos e desafios elencados, considera-se respondida a QD1.

4.2. A transformação digital da BTID

A transformação digital constitui um desafio considerável para a BTID, exigindo uma análise minuciosa dos fatores que influenciam este processo. Este subcapítulo tem como objetivo avaliar o impacto desses fatores na implementação dos conceitos i4.0 e o seu efeito no produto operacional das FFAA.

4.2.1. Fatores endógenos

A influência da cultura organizacional no processo de transformação digital, apresenta-se como uma relevante área de estudo, evidenciando tanto forças como fragilidades na implementação de novas tecnologias. A análise das respostas, permite identificar os segmentos mais relevantes e as implicações no processo de integração das tecnologias i4.0.

A "Dinâmica Interna" das organizações emerge como um fator determinante, atuando tanto para potenciar como para limitar a integração das tecnologias i4.0. Por um lado, as entidades detentoras de uma cultura organizacional vocacionada para a inovação, apoiada pela gestão de topo, como é o caso da Thales Edisoft Portugal, encontram-se numa posição mais vantajosa para adotar as mudanças impostas pela transformação digital. Por outro lado, organizações com tradições profundamente enraizadas, como as identificadas na Europa Victrix, podem enfrentar barreiras significativas à implementação de novas tecnologias. Neste contexto, Alves (2020, p. 20) corrobora esta análise, afirmando que "o grande desafio da i4.0 para as organizações não está centrado na implementação das tecnologias digitais, mas sim nas transformações ao nível da cultura", realçando a importância da dinâmica interna e da cultura organizacional como fatores relevantes na digitalização.

Paralelamente, o segmento "Tecnologia e Inovação" destaca o papel de uma postura aberta à inovação e à experimentação para o sucesso transformação digital. As organizações que se destacam neste segmento promovem a incorporação de IA e das tecnologias emergentes nos seus processos, demonstrando maior facilidade para se adaptar às tecnologias i4.0, obtendo vantagens competitivas neste novo paradigma. Esta abordagem enfatiza a relevância de se criar um ecossistema de inovação interno para a exploração eficaz das oportunidades oferecidas pelas novas tecnologias.

Além disso, é mencionado no segmento de "Recursos Humanos", que a mentalidade dos colaboradores pode ser tanto um entrave como um impulsionador na introdução de novas tecnologias. A falta de recursos humanos é apontada como um desafio, enquanto a experiência e o conhecimento acumulado pelos colaboradores são vistos como ativos valiosos. Iniciativas como formações, conferências e webinars são citadas como meios eficazes para manter os colaboradores atualizados com as temáticas inovadoras.

Por fim, a análise aponta a "Qualidade e Eficiência" e os "Recursos e Capacidades" como elementos integrantes da cultura organizacional que, apesar de menos referenciados, desempenham um papel essencial na digitalização. A aposta na qualidade e na eficiência, embora mencionada apenas por dois entrevistados, sugere uma orientação para a melhoria contínua, fundamental para a integração i4.0 bem-sucedida. Ao mesmo tempo, a gestão dos recursos e capacidades evidenciam a necessidade de um equilíbrio entre a inovação e a compatibilidade com sistemas e processos existentes, destacando-se a importância da valorização do conhecimento e da ID&I para a sustentabilidade da transformação digital.

4.2.2. Fatores exógenos

A adoção das tecnologias i4.0 é igualmente influenciada por fatores externos, destacando-se, neste contexto, o impacto das políticas governamentais e das tendências de mercado.

Relativamente às políticas governamentais, os dados estatísticos indicam uma influência moderada no processo de transformação digital da BTID, registando uma média de 2,56, numa escala de 1 a 5. Esta avaliação sugere uma influência percetível, porém não dominante, das iniciativas governamentais no desenvolvimento tecnológico da BTID. Por outro lado, o desvio padrão de 1,153

revela uma disparidade considerável nas perceções dos inquiridos, evidenciando uma diversidade de experiências nas organizações da BTID.

A nível nacional, "a implementação da i4.0 está a ser dinamizada pelo governo através de programas coordenados pela Comissão Europeia inseridos na Estratégia de Digitalização da Indústria lançada em abril de 2016" (Pereira, 2021, p. 18). Porém, a heterogeneidade das respostas obtidas sugere que, enquanto algumas empresas podem beneficiar diretamente das políticas de incentivo, outras podem receber menos apoio, realçando a necessidade de uma abordagem mais especifica das políticas governamentais, capaz de promover de forma eficiente a inovação e a transformação digital no setor da defesa.

No que diz respeito às tendências de mercado, o "Aumento da Competitividade" e a "Tecnologia e Inovação", emergem como os segmentos mais relevantes, refletindo as dinâmicas e a pressão competitiva que caracterizam o ambiente de mercado atual.

O "Aumento da Competitividade" surge como um dos segmentos mais mencionados, evidenciando a pressão do mercado como um fator que incentiva as empresas a manterem- se na vanguarda da inovação e eficiência. A necessidade de acompanhar as exigências do mercado, a procura de rapidez e eficácia na resposta, e a implementação de práticas que promovam a produtividade, são apontadas como as principais razões para adotar as tecnologias i4.0. Em resposta às incertezas geopolíticas, tem-se observado um aumento na adoção de tecnologias de defesa fora da base industrial de defesa tradicional. Este fenômeno é ilustrado pela Figura 4, e destaca três ondas distintas de *startups* de tecnologia de defesa nos EUA, salientando a importância de inovar para enfrentar os desafios de mercado (Klempner et al., 2024).

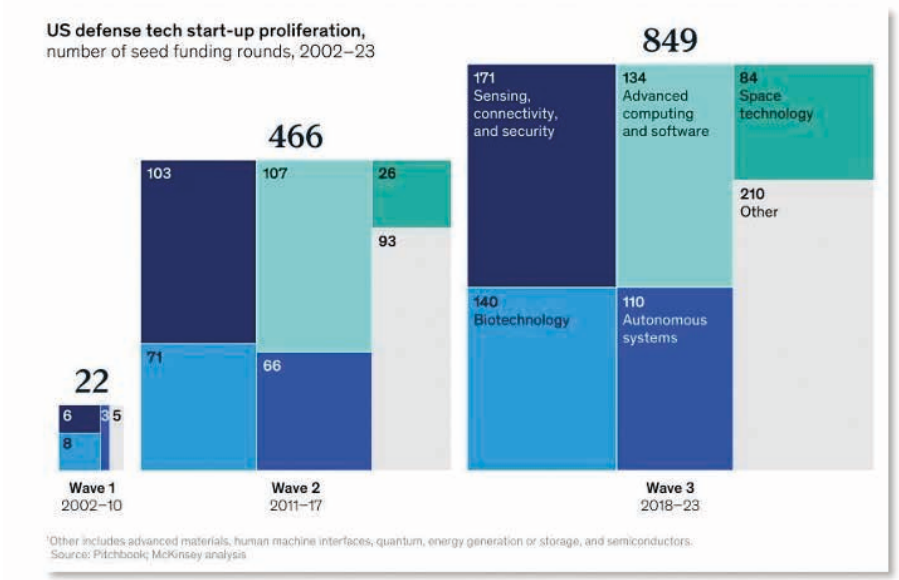

Figura 4 – Ondas de *stratups* nos EUA
Fonte: Klempner et al. (2024, p. 2).

Por outro lado, acompanhar a "Tecnologia e Inovação" em rápida evolução, determina o posicionamento no mercado, refletindo a importância de adotar novas tecnologias para responder eficazmente aos desafios atuais e futuros. A implementação de tecnologias avançadas, como autómatos e IA, são vistas como fundamentais para o desenvolvimento e adaptação às novas dinâmicas do mercado.

Também os "Processos e Operações" e a "Gestão Organizacional" são reconhecidos como influentes. Estes aspetos refletem a necessidade de ajustar a estrutura organizacional e os processos internos às novas realidades impostas pelo mercado, nomeadamente à integração i4.0. Tal indica que, além das tecnologias em si, a transformação digital exige uma revisão profunda da forma como as organizações operam e se organizam internamente.

4.2.3. A digitalização no produto operacional das Forças Armadas

A incorporação dos conceitos i4.0 pela BTID é reconhecido como um elemento essencial para a melhoria do produto operacional das FFAA. A partir da análise das respostas recolhidas, destaca-se a "Tecnologia Avançada" como o segmento de maior relevância.

A "Tecnologia Avançada" assume um papel preponderante na otimização das operações militares. Desde a gestão de informação e otimização logística até à antecipação de falhas em equipamentos críticos, a adoção de tecnologias como *digital twins, Unmanned Aerial Vehicle* (UAV) avançados com sistemas de IA, e ferramentas de realidade aumentada, são vistos como essenciais para garantir uma maior eficiência e eficácia operacional. As respostas obtidas evidenciam que a digitalização da BTID, não só potencia as capacidades de vigilância e reconhecimento em ambientes complexos, mas também facilita a manutenção de equipamentos e a gestão de ativos, salientando-se a necessidade de "estimular o alinhamento dos interesses das FFAA com os da Indústria e Academias, por forma a dinamizar a BTID e o SCTN no desenvolvimento de capacidades militares futuras" (Estado-Maior-General das Forças Armadas [EMGFA], 2022, p. 27).

Por outro lado, o segmento "Eficiência e Otimização" indica que a tecnologia i4.0 contribui para a melhoria dos processos e para a maximização de recursos. A otimização da cadeia de abastecimento, a automação e a gestão de ativos em nuvem são mencionadas como práticas que conduzem a elevados ganhos de eficiência operacional, com menos recursos e menor custo. Tais práticas permitem uma distribuição mais eficiente de materiais, reduzindo custos logísticos e tempos de inatividade, o que se traduz numa vantagem significativa para as FFAA.

Por fim, a análise dos segmentos "Gestão e Decisão" e "Desafios e Adaptação", enfatizam a importância da análise de dados em tempo real para a tomada de decisões estratégicas e salientam os desafios associados à cibersegurança e à modernização dos processos. Estes aspetos realçam a importância transformação digital da BTID, destacando a necessidade de "criação de ecossistemas de inovação que potenciem a participação da indústria de defesa na modernização e transformação das FFAA" (EMGFA, 2022, p. 21).

Tendo em conta a análise efetuada aos fatores que influenciam a transformação digital na BTID, considera-se respondida a QD2.

4.3. Capacidades e Competências da BTID

Este subcapítulo explora detalhadamente as capacidades, competências e planos de investimento da indústria de defesa.

4.3.1. Capacidades e competências

A análise das capacidades e competências da BTID, conforme sintetizado no

Quadro 7, revela uma indústria de defesa em pleno processo de transição face aos desafios tecnológicos contemporâneos.

No que respeita às competências, os dados destacam a importância da formação contínua dos colaboradores e a valorização de uma cultura forte em I&D. Verifica-se um relevante investimento na qualificação dos colaboradores, com ênfase em formações que acompanham a introdução de novas ferramentas e tecnologias. Salienta-se a necessidade de reforçar as competências em gestão de projetos, dada a crescente complexidade dos projetos i4. A cultura de I&D facilita uma resposta ágil à evolução tecnológica constante. Esta base de competências revela-se fundamental para a sustentabilidade e o crescimento da BTID.

A Comissão Europeia reconheceu a necessidade de se desenvolver uma indústria de defesa capaz de produzir equipamentos essenciais, nomeadamente "munições, drones, mísseis e sistemas de defesa aérea, capacidades de ataque em profundidade e de informações, vigilância e reconhecimento, bem como a capacidade de garantir a sua disponibilidade de forma rápida e suficiente" (European Comission, 2024, p. 3). Esta afirmação realça a importância de se desenvolver e manter uma base industrial robusta e diversificada, para garantir a prontidão e a capacidade de resposta adequadas em situações de conflito ou crises de segurança.

A análise das respostas identifica a necessidade de se fortalecerem várias áreas tecnológicas, tais como antidrone, biotecnologia e capacitação humana, ciberdefesa e cibersegurança, comunicações seguras, dados e sua análise, hipersónico, interoperabilidade de sistemas e quântica. No entanto, áreas como a produção de munições, mísseis e sistemas de defesa aérea, mencionadas pela Comissão Europeia, não foram identificadas pelos entrevistados como áreas que necessitem de desenvolvimento.

Por outro lado, os entrevistados enumeraram capacidades existentes na BTID em áreas como o desenvolvimento de software, comunicações, produção têxtil, IA, sistemas de navegação, sistemas autónomos e integração de sistemas. A inovação em áreas como a economia circular coloca a indústria de defesa numa posição estratégica frente aos desafios emergentes, sendo fundamental promover o desenvolvimento em áreas críticas para reforçar a resiliência e a prontidão operacional das FFAA.

4.3.2. Planos de investimento tecnológico

Observando o Quadro 8 verifica-se uma tendência clara por parte da BTID em direção ao desenvolvimento de novas capacidades tecnológicas. A atribuição de uma média de 4,00 numa escala de 1 a 5, indica uma forte intenção para desenvolver novas capacidades, realçando a proatividade da BTID para se adaptar e inovar face às exigências tecnológicas em constante evolução.

A análise das respostas obtidas nas entrevistas, sistematizadas no Quadro 9, permite identificar as áreas específicas nas quais os planos de investimento tecnológico da BTID preveem implementar melhorias. A IA surge como uma das áreas com maior destaque, refletindo a importância crescente desta tecnologia em várias aplicações, desde o desenvolvimento de UAVs mais avançados, até à análise de grandes volumes de dados. A ênfase dada à IA, evidencia uma BTID consciente sobre o papel desta tecnologia na obtenção de vantagens competitivas e operacionais.

A cibersegurança é também destacada como uma área de investimento prioritário, sublinhando a crescente preocupação com a segurança de sistemas e dados, num contexto de ameaças digitais em constante evolução. Os investimentos planeados em cibersegurança visam proteger infraestruturas críticas, assim como reforçar a inovação, para permitir o aumento da competitividade.

Além disso, a automação e a robótica destacam-se pela sua importância na otimização da eficiência e na redução de custos. Paralelamente, emergem novas tecnologias, como a realidade aumentada e a impressão 3D, reconhecidas como catalisadores de inovação e permitem a implementação de processos mais flexíveis e personalizados.

Ao comparar os planos de investimento da BTID com as tendências tecnológicas do relatório NATO Science & Technology Organization (2023), verifica-se um alinhamento nas áreas de IA, cibersegurança, automação e robótica, o que evidencia uma estratégia coerente com prioridades de defesa e segurança internacionais. No entanto, outros domínios críticos como energia, biotecnologia, hipersónicos e materiais avançados, não foram identificados nos planos de investimento da BTID. Tal sugere a necessidade de um ajuste no planeamento estratégico, com o intuito de assegurar uma cobertura das tecnologias emergentes, reforçando a resiliência e a prontidão operacional das FFAA, face aos desafios de segurança contemporâneos e futuros.

Considerando a análise efetuada sobre as capacidades e competências da BTID, considera-se respondida a QD3.

4.4. Contributos para a implementação das tecnologias i4.0

Neste subcapítulo, é apresentada a matriz SWOT referente à BTID, seguida da análise cruzada que proporciona contributos para a implementação e reforço das tecnologias i4.0.

4.4.1. Matriz SWOT

A Matriz SWOT, apresentada no Quadro 2, sintetiza as principais características da BTID, com base na revisão de literatura e na análise das QD das secções anteriores. Esta matriz identifica Forças e Fraquezas internas da BTID, assim como as Oportunidades e Ameaças externas.

Quadro 2 – Matriz SWOT

Fatores internos			
Forças (S)		**Fraquezas (W)**	
Secção	Segmento	Secção	Segmento
4.1.1 4.1.2	S1 - Adoção das tecnologias i4.0 na BTID superior à média das empresas portuguesas	4.1.1 4.2.1	W1 - Heterogeneidade na integração da i4.0 entre setores da BTID
4.1.2 4.2.1 4.3.1	S2 - Competências reconhecidas em áreas como *software*, comunicações, têxteis, IA e sistemas autónomos	4.3.1 4.3.2	W2 - Lacunas em capacidades críticas como produção de armamentos, munições e sistemas de defesa aérea
4.2.1 4.3.1	S3 - Investimento contínuo em formação de colaboradores e cultura de I&D	4.1.2 4.2.1	W3 - Necessidade de reforçar a interoperabilidade e integração de sistemas novos com existentes
4.2.3 4.3.2	S4 - Planos de investimento (IA, cibersegurança, automação) alinhados com tendências tecnológicas da NATO	2.1.2 4.1.2	W4 - Dificuldades em atrair e reter pessoal qualificado em áreas tecnológicas emergentes
Fatores externos			
Oportunidades (O)		**Ameaças (T)**	
Secção	Segmento	Secção	Segmento
2.1.3 4.2.2 4.2.3 4.3.1	O1 - Desenvolvimento de novas tecnologias, incluindo de duplo uso (civil e militar)	4.2.2	T1 - Concorrência no mercado global de defesa e segurança
4.2.2	O2 - Acesso a incentivos e políticas governamentais para implementar i4.0 e inovação	2.1.1 2.1.2	T2 - Orçamentos limitados de defesa podem restringir transformação digital da BTID

[Cont.]

4.2.3 4.3.2	O3 - Procura crescente por soluções de cibersegurança, robótica e	4.2.3	T3 - Ciberataques e riscos de segurança associados à digitalização
2.2.1 4.2.2 4.3.1	O4 - Participar em cooperações internacionais de projetos de defesa e acesso a mercados externos	2.1.2 4.3.2	T4 - Rápida evolução tecnológica e emergência constante de novas tecnologias disruptivas

4.4.2. Análise cruzada

Analisou-se como as forças poderiam ser utilizadas para explorar as oportunidades e mitigar as ameaças, além de identificar estratégias para superar as fraquezas. Esta abordagem permitiu obter os principais contributos para implementar e reforçar a i4.0 na BTID, de forma a maximizar o produto operacional das FFAA. Os contributos de seguida apresentados visam responder à QC e, consequentemente, atingir o OG da investigação.

Contributo 1 – Aumentar o apoio governamental e incentivos financeiros – para fortalecer a BTID, deve ser reforçado o apoio governamental através de incentivos fiscais, subsídios e programas de financiamento específicos para a inovação tecnológica, especialmente nas ATIP. A Estratégia para a Indústria de Defesa Europeia (EIDE), de 4 de março de 2024, só será alcançada com o comprometimento e incentivos financeiros dos Estados-membros, pois, conforme indicado por Besch (2024), "mesmo que os países consigam chegar a acordo sobre a forma da política industrial proposta pela Comissão Europeia, sem financiamento seguro a longo prazo, a estratégia está destinada ao fracasso".

Contributo 2 – Desenvolver uma estratégia de especialização para a BTID – Dada a composição da BTID, que inclui mais de 420 entidades, das quais 89% são PME atuando em 40 setores diferentes, é essencial formular uma estratégia de especialização. Segundo a teoria da "vantagem absoluta" de Adam Smith, "os países teriam de se especializar de acordo com as suas vantagens absolutas, produzindo e exportando os produtos em que tivessem maior produtividade e eficiência e importando aqueles em que os outros seriam melhores" (Coelho et al., 2017, p. 88). Esta abordagem continua pertinente e é reforçada pelo objetivo europeu de criar uma BTIDE robusta e coesa, minimizando redundâncias entre os Estados-membros. Assim, é essencial desenvolver uma estratégia que permita à BTID nacional focar-se em domínios onde já possui um conhecimento aprofundado e vantagens competitivas claras, alinhando-se com as necessidades estratégicas das FFAA, especialmente em bens essencialmente militares como armamento e munições.

Contributo 3 – Alinhar a estratégia da BTID com as necessidades das FFAA – A interação entre a BTID e as FFAA é essencial para garantir que o desenvolvimento industrial esteja em consonância com as necessidades militares. A França exemplifica uma prática eficiente nesta área, com uma coordenação bem estabelecida entre o governo e a indústria de defesa. De acordo com a *Instruction Ministérielle N° 5871/ARM/CAB*, a França mantém um serviço específico dentro da *Direction Générale de l'Armement* (DGA) responsável por garantir a visibilidade da base industrial e coordenar iniciativas estratégicas (Ministère des Armées, 2022). Em Portugal, a idD – Portugal Defense assume uma função semelhante, estabelecendo a ponte entre as indústrias de defesa e as FFAA e fomentando a inovação e o desenvolvimento tecnológico que atendam aos requisitos militares. O reforço desta colaboração, poderia incluir um envolvimento mais intensivo no planeamento estratégico e na precisão dos requisitos técnicos das FFAA, potencializando assim a eficácia do desenvolvimento de soluções para a defesa nacional.

Contributo 4 – Reforçar as infraestruturas de tecnologia da informação e cibersegurança contra ameaças digitais – O aumento da utilização de dispositivos integrados à i4.0 eleva substancialmente a vulnerabilidade a ataques digitais, tornando as infraestruturas mais expostas a riscos cibernéticos. Como indicado por Pedreira, Barros e Pinto (2021), o crescimento no número de dispositivos ligados às redes i4.0 amplia a área suscetível a ataques, facilitando a exploração de falhas por indivíduos mal-intencionados que podem causar danos significativos, desde a paralisação de processos produtivos até o acesso não autorizado a informações confidenciais e segredos industriais. Assim, torna-se essencial "monitorizar continuamente os riscos de cibersegurança" (Pedreira et al., 2021, p. 2) e implementar estratégias eficazes de prevenção para assegurar a proteção das implementações i4.0 e dos sistemas de Tecnologia da Informação (TI). Fortalecer estas infraestruturas é fundamental para defender as organizações da BTID contra ameaças digitais e garantir a continuidade das suas operações.

Contributo 5 – Criar uma cultura de adaptação proativa às mudanças tecnológicas – A evolução tecnológica avança rapidamente, requerendo das organizações uma adaptação constante para se manterem alinhadas com as novas tendências. Neste contexto, é imperativo que as empresas do setor de defesa se mantenham atentas em relação às pesquisas e evoluções tecnológicas, identificando precocemente as tendências emergentes para capitalizar as oportunidades que as novas tecnologias oferecem. Tarcin (2023) sublinha a importância de participar em

estudos e estar sempre informado sobre os avanços do mercado, o que permite à indústria de defesa antecipar mudanças, ajustando seus processos e produtos de forma a melhor responder aos requisitos do setor de defesa. Assim, fomentar uma cultura de adaptação proativa é vital para que as organizações possam responder eficazmente às exigências de um ambiente tecnológico em constante transformação.

Contributo 6 – Reforçar parcerias com empresas estabelecidas – No contexto atual, em que a BTID se depara com desafios tecnológicos cada vez mais complexos, a cooperação com empresas de renome no setor pode ser decisiva. Conforme indicado por Klempner et al. (2024), estabelecer parcerias com empresas da indústria de defesa já estabelecidas pode facilitar a entrada no mercado. Estas colaborações permitem às entidades da BTID adotar mais rapidamente novas tecnologias e processos, aproveitando a experiência e o conhecimento acumulado desses parceiros estabelecidos. Além disso, tais parcerias estratégicas oferecem acesso a infraestruturas e redes de contatos que ampliam a eficiência e o alcance das soluções desenvolvidas, impulsionando significativamente a inovação no contexto da defesa.

Contributo 7 – Qualificar os recursos humanos para a era digital – A formação adequada dos recursos humanos para a digitalização é fundamental para enfrentar os desafios de atrair e reter talentos nas áreas de tecnologias emergentes. Tarcin (2023) destaca a importância de reforçar a qualificação dos recursos humanos, assegurando que estes estejam treinados e especializados para atender às necessidades do ecossistema de defesa e segurança, sendo esta uma responsabilidade de âmbito nacional. Tal desenvolvimento pode ser fomentado por meio de parcerias entre universidades e centros de investigação, beneficiando de apoios governamentais destinados à inovação i4.0 e ampliando a integração em projetos de defesa internacionais. Esta estratégia é vital para garantir que a força de trabalho esteja preparada para contribuir eficazmente para os avanços no setor de defesa.

Contributo 8 – Elaborar um plano de ação para a transformação digital – É imperativo que as organizações da BTID desenvolvam planos detalhados e realistas para a transformação digital, facilitando uma transição eficiente para a i4.0. Esta necessidade é corroborada pela análise de Marín (2020) sobre a indústria de defesa espanhola, que aponta a consciência das empresas sobre a relevância da transformação digital. No entanto, muitas vezes, essa consciência não se

concretiza em planos de ação efetivos, o que pode ser atribuído à insuficiência de financiamento para a sua implementação.

Contributo 9 – Desenvolver capacidades na BTID para colmatar as lacunas nas áreas críticas – A EIDE destaca a urgente necessidade de desenvolvimento de capacidades críticas nas áreas de armamento e munições, em resposta ao crescente número de ameaças à segurança. Esta abordagem estratégica reconhece que, "em tempos de guerra de alta intensidade, é necessário ter a capacidade de produzir em massa um vasto conjunto de equipamentos de defesa, como munições, drones, mísseis e sistemas de defesa aérea" (European Comission, 2024, p. 3). Além disso, a análise de Kosaretsky et al., (2021) sublinha a relevância das munições como um dos principais componentes da capacidade de destruição pelo fogo, apontando que "a quantidade de munição não pode ser ilimitada, mas deve ser suficiente". Esta visão destaca a necessidade de um planeamento cuidadoso e meticuloso da produção e do armazenamento de munições, tanto em tempos de paz quanto em situações de conflito, sublinhando a urgência em reforçar as capacidades da BTID para preencher lacunas críticas em áreas fundamentais como armamento e munições.

Contributo 10 – Reforçar a integração e cooperação entre organizações da BTID – É essencial promover um ambiente que estimule a inovação e a partilha de conhecimento nas organizações, fomentando a criatividade e a experimentação. Essa abordagem é suportada pela Diretiva Estratégica para a Inovação nas Forças Armadas (2022-2032) e pela Diretiva para a Investigação, Desenvolvimento e Inovação no Exército, de 22 de fevereiro de 2024. Esta última inclui referência ao *ARmy Technological EXperimentation* (ARTEX), que, segundo o Chefe do Estado-Maior do Exército (2024), permite gerar "valor tangível para o Exército, envolvendo a Defesa, a Indústria, a Academia e eventuais parceiros internacionais". Nestas circunstâncias, é fundamental reforçar as iniciativas já existentes e desenvolver novas, com o objetivo de envolver ativamente todas as entidades da tripla-hélice, interligando os clusters da indústria de defesa aos ecossistemas de inovação das FFAA.

Contributo 11 – Criação de padrões de interoperabilidade – Estabelecer normas de interoperabilidade é essencial para enfrentar os desafios apresentados pelo rápido desenvolvimento tecnológico e pela necessidade de integração entre sistemas novos e preexistentes. Burns et al., (2019) indicam que a ausência de padronização constitui um dos principais entraves à interoperabilidade

eficiente na i4.0, ressaltando a importância de criar normas globais que permitam uma comunicação e operação coordenadas entre diversos dispositivos e plataformas. De modo semelhante, Salierno et al., (2021) destacam que as inovações nas fábricas do futuro dependem significativamente da capacidade de sistemas diferentes trabalharem juntos de forma eficaz, o que apenas pode ser alcançado por meio de uma estrutura de interoperabilidade bem definida. Assim, o desenvolvimento de normas de interoperabilidade é fundamental para ampliar o potencial das novas tecnologias, facilitando que a indústria se adapte e responda prontamente às necessidades em constante mudança.

Contributo 12 – Melhorar o recrutamento e a qualificação dos recursos humanos – Na estratégia de desenvolvimento da BTID, é importante incluir planos de recrutamento e formação. Inspirado no modelo israelita, onde a integração de ex-militares na indústria de defesa resulta num capital humano altamente qualificado e ajustado às necessidades do setor (Frühling et al., 2023), Portugal poderia tirar proveito da implementação de programas de transição e integração para ex-militares. Tais programas seriam uma forma de valorizar as competências e experiências únicas adquiridas durante o serviço militar, colmatando as lacunas de qualificação existentes na indústria de defesa nacional. Além disso, o estabelecimento de programas que permitam a integração de militares da reserva ativa na BTID, incluindo a participação destes em exercícios militares, reforçaria a colaboração e a sinergia entre o aspeto operacional e as inovações industriais, contribuindo para uma BTID mais sólida e alinhada com os objetivos de defesa e segurança do país.

5. CONCLUSÕES

Este estudo incidiu sobre a transformação digital na BTID, num período em que as FFAA se deparam com novos desafios em matéria de defesa e segurança. Durante uma fase caracterizada por investimentos limitados na defesa e por uma crescente dependência de tecnologia externa, a recente escalada das tensões geopolíticas e o aumento da adoção de políticas de defesa comuns na UE sublinharam a urgência de modernizar e inovar no setor da defesa.

Para atingir o OG deste estudo, adotou-se uma abordagem metodológica baseada no raciocínio indutivo, analisando diversas organizações do setor de defesa para, em seguida, extrapolar essas observações para a BTID como um todo. O desenho da pesquisa fundamentou-se num estudo de caso, integrado em estratégias

de investigação mistas, que englobam métodos quantitativos e qualitativos. A metodologia incluiu análise documental e entrevistas semiestruturadas, permitindo uma compreensão profunda dos fenómenos estudados. O estudo desdobrou-se em duas fases: uma exploratória, com entrevistas exploratórias e revisão da literatura, e outra de investigação, centrada na análise minuciosa de documentos e entrevistas semiestruturadas.

Os resultados obtidos oferecem uma visão ampla sobre o estado atual da transformação digital na BTID, evidenciando que este setor está numa fase avançada de adoção das tecnologias i4.0, com um nível de maturidade superior ao do panorama empresarial em Portugal. No entanto, notou-se uma disparidade significativa entre diferentes setores, ressaltando a necessidade de políticas governamentais que promova a inovação de maneira equilibrada.

A investigação realizada destaca que a integração de tecnologias emergentes, como a automação e a realidade aumentada, representam desafios relevantes, assim como a gestão de recursos humanos. Os resultados indicam que a adoção destas tecnologias pode aumentar significativamente a eficiência e eficácia operacional das FFAA, mas também revelam a necessidade de fortalecer o desenvolvimento de capacidades em áreas críticas, como a produção de armamento e munições, para assegurar a resiliência e prontidão operacional.

Através de uma análise SWOT cruzada, alcançou-se o OG de investigação, identificando-se 12 contributos que orientam a estratégia de implementação da indústria 4.0 na BTID, garantindo o alinhamento com as necessidades operacionais das FFAA.

Entre os principais contributos, destaca-se o reforço do apoio governamental e incentivos financeiros, que deveriam ser ampliados por meio de incentivos fiscais e subsídios focados na inovação tecnológica, em consonância com a EIDE. Este apoio é visto como essencial para o sucesso da estratégia de desenvolvimento da BTID. Adicionalmente, salienta-se a importância de desenvolver uma estratégia de especialização para a BTID, que aproveite as vantagens competitivas nacionais, sugerindo um alinhamento com as teorias de vantagem absoluta de Adam Smith, favorecendo uma BTID mais integrada e menos redundante nos esforços entre os Estados-membros.

O exercício ARTEX ilustra uma abordagem inovadora de como a integração e cooperação entre as organizações da BTID podem ser fortalecidas, criando valor tangível ao envolver não só a Defesa e a Indústria, mas também a Academia e

parceiros internacionais, fomentando uma sinergia eficaz dentro do ecossistema de inovação das FFAA. Esta abordagem é complementada pela criação de padrões de interoperabilidade, essenciais perante a rápida evolução tecnológica e a necessidade de integração eficaz entre sistemas novos e existentes. As normas de interoperabilidade são sublinhadas como fundamentais para uma operação coordenada e eficiente, essencial para responder às constantes mudanças e maximizar o potencial das inovações tecnológicas da i4.0.

Este trabalho contribui para o conhecimento ao identificar os principais aspetos a considerar para uma implementação bem-sucedida da i4.0 na BTID, ressaltando a necessidade de um alinhamento estratégico mais robusto entre as capacidades tecnológicas da indústria de defesa e as exigências operacionais das FFAA, bem como a importância da inovação contínua e da adaptação às novas tecnologias.

As limitações desta investigação relacionam-se com a diversidade e o elevado número de organizações que compõem a BTID. Devido a essa complexidade, o estudo não conseguiu analisar a realidade específica de cada entidade, o que pode influenciar a generalização dos resultados.

Para estudos futuros, recomenda-se o desenvolvimento de uma estratégia de especialização para a BTID, de modo a tornar a BTID nacional uma referência a nível internacional. Esta estratégia deverá considerar as particularidades das entidades que compõem a BTID e alinhar-se com as diretrizes europeias e internacionais.

As recomendações de ordem prática incluem a aplicação dos contributos elencados nesta investigação e a avaliação do seu impacto na digitalização da BTID. Este passo é decisivo para garantir que a BTID acompanhe a evolução tecnológica e se posicione na vanguarda da inovação no setor de defesa.

REFERÊNCIAS BIBLIOGRÁFICAS

Alves, M. G. P. (2020). *Impacto das tecnologias digitais da Indústria 4.0 na Cultura Organizacional das Empresas* (Dissertação de Mestrado em Economia e Administração de Empresas). Faculdade de Economia da Universidade do Porto [FEUP], Porto.

Antunes, A. J. L. (2013). *Indústria de defesa pública ou privada? O caso da OGMA* (Trabalho final de mestrado em Economia e Políticas Públicas). Instituto Superior de Economia e Gestão [ISEG], Lisboa.

Aslanova, I. V., & Kulichkina, A. I. (2020). *Digital Maturity: Definition and Model. Apresentado na Modern Management Trends and the Digital Economy: from*

Regional Development to Global Economic Growth da Faculty of Business, Novosibirsk State Technical University, Novosibirsk, Russia.

Barbier, L. (2020). *Industry 4.0 Adoption for US Aerospace and Defense Industry*. (Bachelor's Thesis em International Business). Aalto University, Mikkeli Campus.

Bardin, L. (2016). *Análise de conteúdo*. Edições 70.

Barros, C. P. (2002). Small countries and the consolidation of the European defence industry: Portugal as a case study. *Defence and Peace Economics, 13*(4), 311–319. https://doi.org/10.1080/10242690212359

Besch, S. (2024). Understanding the EU's New Defense Industrial Strategy. Retirado de Carnegie Endowment for International Peace website: https://carnegieendowment.org/2024/03/08/understanding-eu-s-new-defense-industrial-strategy-pub-91937

Briani, V., Marrone, A., Mölling, C., & Valasek, T. (2013). *The development of a European defence technological and industrial base* (EDTIB). https://data.europa.eu/doi/10.2861/15836

Burns, T., Cosgrove, J., & Doyle, F. (2019). A Review of Interoperability Standards for Industry 4.0. *Procedia Manufacturing, 38,* 646–653. https://doi.org/10.1016/j.promfg.2020.01.083.

Castro, H., Nieto-Carrillo, E., & Associação Portuguesa de Sistemas de Informação. (2023). *Relatório de avaliação de resultados e mapeamento*. SHIFT2FUTURE. https://www.shift2future.pt/resultados

Chefe do Estado-Maior do Exército. (2024). *Diretiva para a Investigação Desenvolvimento e Inovação no Exército (Diretiva n.o 42/CEME/2024)*. Lisboa: Estado-Maior do Exército.

Chin, W. (2019). Technology, war and the state: Past, present and future. *International Affairs, 95*(4), 765–783. https://doi.org/10.1093/ia/iiz106

Coelho, R. A., Espírito Santo, M., Coelho, R. R., & Frade, R. (2017). Revisão Bibliográfica sobre Comércio Internacional. *III Encontro Científico da I2ES do ISLA Santarém*, 85–93.

Comissão Europeia. (2007). *Uma estratégia para uma Base Tecnológica e Industrial de Defesa europeia mais forte*. https://eur-lex.europa.eu/legal- content/PT/TXT/PDF/?uri=CELEX:52007DC0764

Conselho da União Europeia. (2009). *Estratégia Europeia em matéria de segurança: Uma Europa segura num mundo melhor*. Publications Office. https://data.europa.eu/doi/10.2860/16255

Decreto-Lei n.o 19/2022, de 24 de janeiro. (2022). *Estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas*. Diário da República 1a Série, 16. 3-97. https://files.diariodarepublica.pt/1s/2022/01/01600/0000300097.pdf

Despacho n.o 11400/2014, de 11 de setembro. (2014). *Diretiva Ministerial de Planeamento de Defesa Militar*. Diário da República, 2.a série, 175, 23656 - 23657. https://files.diariodarepublica.pt/2s/2014/09/175000000/2365623657.pdf

Estado-Maior-General das Forças Armadas [EMGFA]. (2022). *Diretiva Estratégica para a Inovação nas Forças Armadas (2022-2032)*. Lisboa: Estado-Maior das Forças Armadas.

European Comission. (2024). *A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry*. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2024:10:FIN

European Defence Agency. (2007). *Strategy for the european defence technological and industrial base*. https://eda.europa.eu/docs/documents/strategy_for_the_european_defence_technological_and_industrial_base.pdf

European Union. (2022). *A Strategic Compass for Security and Defence*. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_w eb.pdf

Frühling, S., Louis, K., Wilson, J., & Dunk, G. (2023). *Defence Industry in National Defence: Rethinking the future of Australian defence industry policy. (Australian Industry Group and Strategic and Defence Studies Centre, Australian National University)*. https://www.aigroup.com.au/globalassets/news/reports/2023/ai-group-sdsc-dind- report.pdf

Hurzhyi, N., Kravchenko, A., Kulinich, T., Saienko, V., Chopko, N., & Skomorovskyi, A. (2022). Enterprise Development Strategies in a Post-Industrial Society. *Postmodern Openings, 13*(1 Sup1), 173–183. https://doi.org/10.18662/po/13.1Sup1/420

idD Portugal Defence. (2022). *Factsheet Economia de Defesa em Portugal*. https://www.iddportugal.pt/wp-content/uploads/2022/10/Factsheet-Economia-de- Defesa-em-Portugal-2022-PT.pdf

Klempner, J., Rodriguez, C., & Swartz, D. (2024). A rising wave of tech disruptors: The future of defense innovation? *McKinsey & Company*. Obtido de https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/a-rising- wave-of-tech-disruptors-the-future-of-defense-innovation#/

Kosaretsky, Y. I., Kutovoi, O. P., Bondarenko, O. O., Lavruk, M. P., & Syniavskyi, V. V. (2021). Methodical approach to assessing the effectiveness of the result of mobilization planning for the ammunition industry. *Political Science and Security Studies Journal, 2*(1), 33–39. https://doi.org/10.5281/zenodo.4651584

Lei n.o 49/2009, de 5 de agosto. (2009). *Regula as condições de acesso e exercício das actividades de comércio e indústria de bens e tecnologias militares*. Diário da República, 1.a série, 150. 5065 a 5072. Lisboa: Assembleia da República.

Lezana, R. (2020). *Análise Cruzada da Matriz SWOT*. Retirado de Academia Perspectiva. https://blog.academiaperspectiva.com/analise-cruzada-da-matriz-swot/

Marín, M. A. F.-V. (2020). The Transformation of the Defense and Security Sector to the New Logistics 4.0: Public–Private Cooperation as a Necessary Catalyst Strategy. Em Á. Rocha & R. P. Pereira (Eds.), *Developments and Advances in Defense and Security* (pp. 293–303). Singapore: Springer Singapore. https://doi.org/10.1007/978-981-13- 9155-2_24

Matt, C., Hess, T., & Benlian, A. (2015). Digital Transformation Strategies. *Business & Information Systems Engineering, 57*(5), 339–343. http://doi.org/10.1007/s12599-015-0401-5

Ministère des Armées. (2022). *INSTRUCTION MINISTÉRIELLE N° 5871/ARM/CAB relative au Plan ACTION PME rénové du ministère des armées en appui des petites et moyennes entreprises et des entreprises de taille intermédiaire*. Bulletin officiel des armées, Chronological Edition No. 35 du 6 mai 2022. https://www.defense.gouv.fr/sites/default/files/sga/1%20INSTRUCTION%20MINIST%C3%89RIELLE%20N%C2%B0%205871ARMCAB.pdf

NATO. (2016). *Joint Analysis Handbook* (4th Edition). Monsanto, Lisbon, Portugal. https://www.jallc.nato.int/application/files/9416/0261/6056/Joint_Analysis_Handb ook_4th_edition.pdf

NATO Science & Technology Organization. (2023). *Science & Technology Trends 2023-2043* (VOLUME 1: Overview). https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf

Nunes, C., Alves, R. P., Santos, S., Merenda, R., Sebastian, M., & Fernandes, J. M. (2021). *Economia de Defesa em Portugal – A Caminhar em Direção ao Futuro*. https://www.iddportugal.pt/wp-content/uploads/2021/12/Economia -de-Defesa-em- Portugal-A-Caminhar-em-Direcao-ao-Futuro.pdf

Pedreira, V., Barros, D., & Pinto, P. (2021). A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead. *Sensors, 21*(15), 5189. https://doi.org/10.3390/s21155189

Pereira, A. A. M. M. (2021). *A Indústria 4.0 em Portugal – O estado da arte* (Dissertação de Mestrado em Gestão de Empresas). Instituto Universitário de Lisboa [ISCTE], Lisboa.

Pinto, R. F. M. (2009). *As Indústrias Militares e As Armas de Fogo Portáteis no Exército Português*. Revista Militar. https://www.revistamilitar.pt/artigo/528

Rädiker, S. (2023). *Doing grounded theory with MAXQDA. Guidance und tips for your practice*. Berlin: MAXQDA Press. https://doi.org/10.36192/978-3- 948768164

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

Resolução do Conselho de Ministros n.o 35/2010, de 06 de maio. (2010). *Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa*. Diário da República 1a Série, 88. 1599 a 1609. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.o 52/2023, de 5 de junho. (2023). *Estratégia de Desenvolvimento da Base Tecnológica e Industrial de Defesa*. Diário da República 1a Série, 108. 26 a 39. Lisboa: Presidência do Conselho de Ministros.

Salierno, G., Leonardi, L., & Cabri, G. (2021). The Future of Factories: Different Trends. *Applied Sciences, 11*(21), 9980 https://doi.org/10.3390/app11219980

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

Silveira, C. B. (2016). Indústria 4.0: O que é, e como ela vai impactar o mundo. https://www.citisystems.com.br/industria-4-0/

Simões, P. C., Moreira, A. C., & Mendes Dias, C. (2020). Portugal's Changing Defense Industry: Is the Triple Helix Model of Knowledge Society Replacing State Leadership Model? *Journal of Open Innovation: Technology, Market, and Complexity, 6*(4), 183. https://doi.org/10.3390/joitmc6040183

Soltovski, R., Resende, L. M. M., Pontes, J., Yoshino, R. T., & Silva, L. B. P. (2020). Um estudo quantitativo sobre os riscos da indústria 4.0 no contexto industrial: Uma revisão sistemática da literatura. *Revista Gestão e Desenvolvimento, 17*(3), 165–191. https://doi.org/10.25112/rgd.v17i3.2245

Tabaković, N., & Durakovic, B. (2021). Impact of Industry 4.0 on Aerospace and Defense Systems. *Defense and Security Studies, 2*, 63–78. https://doi.org/10.37868/dss.v2.id170

Tarcin, U. (2023). Strategic Analysis in The Defense Industry: A Comprehensive Approach to Increase Situational Awareness in National and NATO Processes. *Journal of Global Strategic Management, 17*. https://doi.org/10.20460/JGSM.2023.326

Teichert, R. (2019). Digital Transformation Maturity: A Systematic Review of Literature. *Acta Universitatis Agriculturae et Silviculturae Mendelianae Brunensis, 67*(6), 1673–1687. https://doi.org/10.11118/actaun201967061673

Voitko, S., Polishchuk, A., & Tkachenko, O. (2020). *Development of the defense and industrial complex on the basis of Industry 4.0*. doi: 10.5281/ZENODO.4310124

Yaqub, M. Z., & Alsabban, A. (2023). Industry-4.0-Enabled Digital Transformation: Prospects, Instruments, Challenges, and Implications for Business Strategies. *Sustainability, 15*(11), 8553. https://doi.org/10.3390/su15118553

Yin, R. K. (2005). Estudo de caso: Planejamento e métodos (3a Edição; D. Grassi, Trad.). Porto Alegre: Bookman.

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

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

N.os Publicados:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

57 – Ameaças Híbridas - Desafios para Portugal
Coordenador: Tenente-coronel de Artilharia Diogo Lourenço Serrão

58 – Cadernos de Saúde Militar e Medicina Operacional – Vol. I
Coordenadores: Coronel (REF) António Correia
Primeiro-tenente Nicole Esteves Fernandes

59 – *Military Operations in Cyberspace*
Coordinator: Lieutenant-colonel João Paulo Ferreira Lourenço

60 – Inteligência Artificial: Estudos Pioneiros em Contexto Militar
Coordenadora: Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

61 – Direito Internacional e Conflitos Armados: Desafios Éticos e Legais na Guerra Contemporânea
Coordenador: Tenente-coronel Pedro da Silva Monteiro

62 – Inovação e Eficiência na Administração Militar
Coordenadora: Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

Editorial: cidium@ium.pt
Telefone: (+351) 213 002 100; Fax: (+351) 213 002 162
Morada: Rua de Pedrouços - 1449-027 Lisboa