

**INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
MESTRADO EM CIÊNCIAS MILITARES - SEGURANÇA E DEFESA**

2021/2022



DISSERTAÇÃO

**UMA ESTRATÉGIA DIGITAL PARA AS FORÇAS ARMADAS
PORTUGUESAS**

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

**Ernesto António de Jesus Alves
CAPITÃO-DE-FRAGATA FUZILEIRO**



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

**UMA ESTRATÉGIA DIGITAL PARA AS FORÇAS
ARMADAS PORTUGUESAS**

CAPITÃO-DE-FRAGATA FUZILEIRO, Ernesto António de Jesus Alves

alves.eaj@ium.pt

jesus.alves@marinha.pt

Dissertação do MCMDS

Pedrouços 2023



INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

UMA ESTRATÉGIA DIGITAL PARA AS FORÇAS
ARMADAS PORTUGUESAS

CAPITÃO-DE-FRAGATA FUZILEIRO, Ernesto António de Jesus Alves

Dissertação do MCMSD

Orientador: TENENTE-CORONEL, Mestre, Pedro Miguel da Silva Costa

Coorientador: CAPITÃO-DE-FRAGATA, Mestre, Filipe da Rocha Rei

Pedrouços 2023



Declaração de compromisso Antiplágio

Eu, Ernesto António de Jesus Alves, declaro por minha honra que o documento intitulado “Uma Estratégia Digital para as Forças Armadas portuguesas”, corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do MCMSD 2021/2022 no Instituto Universitário Militar e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

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

Pedrouços, 13 de dezembro de 2023.

Ernesto António de Jesus Alves



Agradecimentos

Embora a presente investigação tenha uma abrangência alargada de matérias inerentes à presente temática, permitiram-me na sequência da investigação desenvolvida durante a frequência do Curso de Estado-Maior Conjunto (CEMC), edição 2020/2021, aprofundar um tema que é transversal à sociedade, enriquecendo-me tanto a nível profissional como pessoal.

As minhas primeiras palavras, de agradecimento e apreço, dirigem-se ao Major-general Coelho Rebelo, quando foi apresentado o Trabalho de Investigação Individual do CEMC, pelo incentivo de prosseguir com esta temática para o presente Mestrado, onde poderiam ser realizados alguns melhoramentos. Da mesma forma, deixo um agradecimento aos demais pelos incentivos que me foram endereçados.

Ao meu Orientador, Tenente-coronel Silva Costa, uma palavra de estima e muita consideração pelo estimável apoio ao longo da presente investigação.

De igual forma, ao meu Coorientador, camarada e amigo Capitão-de-fragata Rocha Rei, uma palavra de agradecimento e apreço, por todo o apoio prestado e pela total disponibilidade.

Sem que seja menos importante, deixo uma palavra de agradecimento à minha família, pela disponibilidade e por todo o apoio prestado.



Índice

1.	Introdução	1
2.	Enquadramento e metodologia.....	3
2.1.	Enquadramento	3
2.2.	Metodologia.....	6
3.	Perceção digital das Forças Armadas portuguesas.....	8
3.1.	Análise de dados dos questionários	8
3.2.	Análise das entrevistas.....	9
3.2.1.	Estado-Maior-General das Forças Armadas.....	9
3.2.2.	Marinha	9
3.2.3.	Exército	10
3.2.4.	Força Aérea	11
3.3.	Síntese conclusiva.....	12
4.	Perspetiva internacional	13
4.1.	Ambiente estratégico	13
4.2.	Estados Unidos da América.....	14
4.3.	NATO	16
4.4.	União Europeia	17
4.5.	Síntese conclusiva.....	17
5.	Perspetiva operacional da estratégia digital	18
5.1.	Superioridade de informação	18
5.2.	Operações no, e através do, ciberespaço	20
5.3.	Comando e Controlo ágil.....	22
5.4.	Síntese conclusiva.....	25
6.	Perspetiva estrutural da Estratégia digital	26
6.1.	Liderança digital	26
6.2.	Competências digitais	27
6.3.	Otimização de processos.....	29
6.4.	Síntese conclusiva.....	32
7.	Perspetiva genética da Estratégia digital.....	33
7.1.	Capacidade de governação e gestão da arquitetura organizacional.....	33



7.2.	Capacidade de governação e gestão integrada dos dados e informação.....	36
7.3.	Capacidade de interação homem-máquina	39
7.4.	Síntese conclusiva.....	41
8.	Contributos para a formulação de uma Estratégia Digital nas Forças Armadas.....	42
8.1.	Caraterização do ambiente estratégico	42
8.2.	Mapa estratégico para a transição digital.....	43
8.3.	Linhas de ação estratégicas.....	44
8.4.	Alinhamento dos contributos para a formulação da estratégia.....	47
8.5.	Síntese conclusiva.....	48
9.	Conclusão.....	50
	Referências bibliográficas	53

Índice de Apêndices

Apêndice A -	Corpo de conceitos.....	Apd. A - 1
Apêndice B -	Resultados e avaliação do questionário sobre a maturidade digital e a indústria 4.0 nas Forças Armadas	Apd. B - 1
Apêndice C -	Guião e análise das entrevistas iniciais.....	Apd. C - 1
Apêndice D -	Guião e análise das entrevistas finais.....	Apd. D - 1
Apêndice E -	Caracterização da envolvente estratégica	Apd. E - 1
Apêndice F -	Alinhamento das LAE com os vetores capacidade.....	Apd. F - 1
Apêndice G -	Alinhamento das LAE com a estratégia e planos nacionais	Apd. G - 1

Índice de Figuras

Figura 1 -	Modelo de desenvolvimento	6
Figura 2 -	Perceção do domínio de digital.....	8
Figura 3 -	Avaliação da Maturidade Digital	9
Figura 4 -	Visão Estratégica da NATO	14
Figura 5 -	Modernização Digital	15
Figura 6 -	OODA Loop de Boyd.....	19
Figura 7 -	Uma visão do OODA loop apoiado por IA	20
Figura 8 -	Taxonomia das operações no ciberespaço	21
Figura 9 -	Modelo de Abordagem de C2.....	23
Figura 10 -	Visão geral do modelo conceptual de C2	24



Figura 11 - Modelo de um sistema de A3IC2	25
Figura 12 - Liderança digital	27
Figura 13 - Quadro de competências digitais	28
Figura 14 - Fatores de confiança dos processos	30
Figura 15 - RPA em sistemas inteligentes de processos organizacionais	31
Figura 16 - Relação de arquitetura	34
Figura 17 - Alinhamento da arquitetura organizacional.....	35
Figura 18 - Modelo de arquitetura Aplicacional e Técnica.....	35
Figura 19 - Estrutura da gestão de dados.....	36
Figura 20 - Relação entre IA, ML e DL	37
Figura 21 - Relação entre modelos e algoritmos	38
Figura 22 - Modelo de confiança Homem-Máquina	40
Figura 23 - Análise SWOT	43
Figura 24 - Mapa da estratégia para a transição digital.....	44

Índice de Quadros

Quadro 1 - Modelo de Análise	7
Quadro 2 - Guião de entrevistas	Apd. C - 1
Quadro 3 - Relação de Entrevistados	Apd. C - 2
Quadro 4 - Fatores do ambiente externo	Apd. E - 1
Quadro 5 - Fatores do ambiente interno	Apd. E - 2
Quadro 6 - Alinhamento das LAE com os vetores capacidade	Apd. F - 1
Quadro 7 - Alinhamento das LAE com a legislação nacional.....	Apd. G - 1

Índice de Tabelas

Tabela 1 - Linhas de Ação Estratégicas da Perspetiva Genética.....	45
Tabela 2 - Linhas de Ação Estratégicas da Perspetiva Estrutural	46
Tabela 3 - Linhas de Ação Estratégicas da Perspetiva Operacional.....	47
Tabela 4 - Análise síntese das entrevistas	Apd C - 3
Tabela 5 - Matriz de análise de conteúdo	Apd D - 4
Tabela 6 - Avaliação da probabilidade e impacto dos fatores	Apd E - 3
Tabela 7 - Matriz de Probabilidade/Impacto dos fatores.....	Apd E - 3



Resumo

A evolução tecnológica constitui-se como um catalisador de novas ameaças, oportunidades e desafios para a Segurança e Defesa, num ambiente multidomínio, tornando-o mais contestado e imprevisível. Paralelamente, as tecnologias disruptivas conexas à eficácia e eficiência, fazem da Transição Digital uma prioridade para a relevância das organizações na era digital.

A presente investigação visa desenvolver contributos para a formulação de uma estratégia digital para as Forças Armadas portuguesas que responda aos desafios deste novo ambiente estratégico.

Para tal, a investigação centrou-se num raciocínio indutivo, seguindo uma estratégia qualitativa e uma pesquisa interpretativa, assente na análise documental e em dados recolhidos de questionários e entrevistas nas Forças Armadas.

Os resultados obtidos permitiram concluir, que o produto operacional deve assentar em capacidades geradas, assentes na arquitetura, nos dados e na interação homem-máquina. Paralelamente, é essencial uma mudança de cultura assente no digital, a par da otimização de processos, permitindo melhorar o produto operacional, através de uma abordagem digital para que o processo de decisão seja mais rápido, ágil e mais bem informado num ambiente multidomínio. Resultante da análise ao ambiente estratégico foram deduzidos objetivos estratégicos e linhas de ação estratégicas, como medidas essenciais na formulação de uma estratégia digital nas Forças Armadas portuguesas.

Palavras-chave: Transformação digital, Transição Digital, Indústria 4.0, Inovação, Dados e Informação e Operações no ciberespaço.



Abstract

Technological evolution is a catalyst of new threats, opportunities and challenges for Defense and Security, in a multidomain environment, making it more contested and unpredictable. At the same time, disruptive technologies related to effectiveness and efficiency make the Digital Transition a priority for the relevance of organizations in the digital age.

The object of this research to develop contributions for the formulation of a digital strategy for the Portuguese Armed Forces to meet the challenges of this new strategic environment.

For this purpose, the research focused on inductive reasoning, following a qualitative strategy and interpretative research, based on documentary analysis and data collected from questionnaires and interviews in the Armed Forces.

The results obtained led to the conclusion that the operational product must be based on generated capabilities, based on architecture, data, and human-machine interaction. In parallel, a culture change based on digital is essential, along with process optimization, allowing for the improvement of the operational product through a digital approach so that the decision process is faster, more agile, and better informed in a multidomain environment. As a result of the analysis of the strategic environment, strategic objectives and strategic lines of action were deduced, as essentials measures in the formulation of a digital strategy in the Portuguese Armed Forces.

Keywords: *Digital transformation, Digital Transition, Industry 4.0, Innovation, Data and Information, and Cyberspace operations.*



Lista de abreviaturas, siglas e acrónimos

3

3D Impressão Tridimensional

5

5G 5.^a Geração

A

A Ameaças

A2AD *Anti-Access and Area Denial*

A3IC2 *Agile, Antifragile, Artificial-Intelligence-Enabled, Command and Control*

ABPM *Association of Business Process Management Professionals*

ADD Alocação dos Direitos de Decisão

AP Administração Pública

AUV *Autonomous underwater vehicle*

B

BGEN Brigadeiro-General

BI *Business Intelligence*

BTID Base Tecnológica e Industrial de Defesa

C

C2 Comando e Controlo

C3 Comando, Controlo e Comunicações

CALM Contra-Almirante

CMG Capitão-de-mar-e-guerra

CCEM Conselho de Chefes de Estado-Maior

CCOM Comando Operacional Conjunto para as Operações Militares

CE Comissão Europeia

CEM Conceito de Estratégia Militar

CEMC Curso de Estado-Maior Conjunto

CEMTEX Centro de Experimentação e Modernização Tecnológica do Exército

CEOM Centro de Experimentação Operacional da Marinha

CEU *Council of the European Union*



CFR	Capitão-de-fragata
CIAFA	Centro de Investigação da Academia da Força Aérea
CIE	Centro Informático do Exército
CINAMIL	Centro de Investigação da Academia Militar
CINAV	Centro de Investigação Naval
CIRT	<i>Computer Incident Response Capability</i>
COM	Comodoro
COR TIR	Coronel Tirocinado
COVID-19	<i>Coronavirus Disease 2019</i>
CPASIDN	Comissão de Políticas e Auditoria do Sistema de Informação da Defesa Nacional

D

DAMA	<i>Data Management</i>
DCSI	Direção de Comunicações e Sistemas de Informação
DEEMFA	Diretiva Estratégica do Estado-Maior da Força Aérea
DEEMGFA	Diretiva Estratégica do Estado-Maior-General das Forças Armadas
DL	<i>Deep Learning</i>
DN	Defesa Nacional
DND&CAF	<i>Department of National Defence and Canadian Armed Forces</i>
DoI	Distribuição de Informação.
DoD	<i>Department of Defense</i>
DODAF	<i>Department of Defense Architecture Framework</i>
DOTMLPII	Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade

E

EEAL	Equipa de Engenharia e Aplicações Legadas
EMA	Estado-Maior da Armada
EMGFA	Estado-Maior-General das Forças Armadas
EN	<i>European Standards</i>
ERP	<i>Enterprise Resource Planning</i>
EUA	Estados Unidos da América



F

FFAA Forças Armadas

I

i4.0 Indústria 4.0

i5.0 Indústria 5.0

i6.0 Indústria 6.0

IA Inteligência Artificial

IAPMEI Instituto de Apoio às Pequenas e Médias Empresas e à Inovação

ID&I Investigação, Desenvolvimento e Inovação

IoT *Internet of Things*

ISO *International Organization for Standardization*

ISQ Instituto de Soldadura e Qualidade

ISTAR *Intelligence, Surveillance, Target Acquisition, and Reconnaissance*

IUM Instituto Universitário Militar

L

LAE Linhas de Ação Estratégicas

LLAA Lições Aprendidas

LO Leis Orgânicas

LOEMGFA Lei Orgânica do Estado-Maior-General das Forças Armadas

LPM Lei de Programação Militar

M

MDN Ministério da Defesa Nacional

MDO *Multi-Domain Operations*

MIT *Massachusetts Institute of Technology*

ML *Machine Learning*

MoD *Ministry of Defence*

MS Microsoft

MUS *Maritime Unmanned Systems*

N

NAF *NATO Architecture Framework*



NATO	<i>North Atlantic Treaty Organization</i>
NEC	<i>Network Enabled Capability</i>
NEP/INV	Normas de Execução Permanente/Investigação

O

O	Oportunidades
OG	Objetivo Geral
OE	Objetivo Específico
OEst	Objetivo Estratégico
OECD	<i>Organisation for Economic Cooperation and Development</i>
OI	Organizações Internacionais
OODA	Observar, Orientar, Decidir e Agir

P

P	Potencialidades
PCM	Presidência do Conselho de Ministros
PdI	Padrões de Interação
PIDigi	Programa Intersectorial para a Transição Digital
PLN	Processamento de Linguagem Natural
PRR	Plano de Recuperação e Resiliência
PS3	<i>Portuguese Sky Sentinel System</i>
PTEX	Pólo Tecnológico do Exército

Q

QC	Questão Central
QD	Questão Derivada

R

RCA	Reuniões da Comissão de Acompanhamento
RCM	Resolução do Conselho de Ministros
REP	<i>Robotic Experimentation Prototyping</i>
RGPD	Regulamento Geral de Proteção de Dados
ROV	<i>Remotely Operated Vehicle</i>
RPA	<i>Robotic Process Automation</i>



S

SCTN	Sistema Científico e Tecnológico Nacional
SGMDN	Secretaria-Geral do Ministério da Defesa Nacional
SI	Sistemas de Informação
SIC	Sistemas de Informação e Comunicações
SIGDN	Sistema Integrado de Gestão da Defesa Nacional
SWOT	<i>Strengths, Weaknesses, Opportunities and Threats</i>

T

TCOR	Tenente-Coronel
TD	Transformação Digital
TDig	Transição Digital
TI	Tecnologias de Informação
TOGAF	<i>The Open Group Architecture Framework</i>

U

UE	União Europeia
UEO	Unidades, Estabelecimentos e Órgãos
UAV	<i>Unmanned Aerial Vehicles</i>
UGS	<i>Unmanned Ground Systems</i>

V

V	Vulnerabilidades
VICA	Volátil, Incerto, Complexo e Ambíguo

Z

ZLT	Zona Livre Tecnológica
-----	------------------------



1. Introdução

“Be not deceived. Revolutions do not go backward.”

Abraham Lincoln, 1856

A evolução tecnológica tem vindo a impulsionar a sociedade para a era digital, tendo sido a internet o catalisador da globalização, levando ao encurtamento das distâncias e ao aumento da interação entre as organizações, instituições e pessoas, tanto a nível social, como económico, político e militar. Todavia, a potencialização da internet ao nível da competitividade empresarial impulsionou o conceito de Transformação Digital (TD) nos mais diversos setores da sociedade, incluindo o da Segurança e Defesa.

O surgimento da quarta revolução industrial em 2013, conhecida pela “indústria 4.0” (i4.0), tem revolucionado a cadeia de valor das organizações, através da capacitação tecnológica assente em dados e na integração de processos digitais com processos físicos, facilitando o desenvolvimento de novos modelos. Como tal, surgiram novos conceitos tecnológicos, desde o gene à nanotecnologia ou das energias renováveis à computação quântica (Schwab, 2016), tecnologias disruptivas consubstanciadas na internet das coisas (*Internet of Things* [IoT]), na Inteligência Artificial (IA) e na robótica (Um, 2019).

A situação pandémica de *Coronavirus Disease* em 2019 (COVID-19), veio a acelerar a TD na sociedade, forçando a uma alteração significativa do modo de vida em torno do digital, como alternativa à interação física entre as organizações, instituições ou pessoas. Esta transformação tem vindo a ser potencializada pela i4.0, levando a uma mudança organizacional, assente na estrutura, na cultura e na liderança.

Desde então, a evolução tecnológica tem sido acelerada pela IA, tecnologia descoberta por Alan Turing em 1950 (*Organisation for Economic Cooperation and Development* [OECD], 2019). Porém, apenas com o i4.0 foram disponibilizadas as potencialidades desta tecnologia, no sentido de reforçar as capacidades humanas, havendo uma estreita colaboração entre humanos e máquinas, designada por indústria 5.0 (i5.0) (Demir & Cicibaş, 2019), visando humanizar a IA, através do desenvolvimento de uma abordagem centrada no ser humano, na sustentabilidade e na resiliência (Comissão Europeia [CE], 2021a).

Ainda, há questões éticas e de segurança relacionadas com i5.0, por se constituir uma tecnologia alarmante, caso haja uma perda de controle, estando na origem da indústria 6.0 (i6.0), direcionada para a segurança dos utilizadores e proteção de dados, ou seja, uma mistura entre a tecnologia e a ética (Zatta, 2020).

A evolução do digital integrando tecnologias disruptivas, abrangeu a sociedade com um forte impacto ao nível da Segurança e Defesa, dando origem a uma nova conflitualidade



para testar novos sistemas de armas ou para alcançar efeitos físicos através do ciberespaço, privilegiando as ameaças híbridas alargadas a todos os domínios (Morgan et al., 2020).

A pertinência desta dissertação subordinada ao tema “Uma Estratégia Digital nas Forças Armadas portuguesas”, é relevante no mundo atual, fustigado pelo surgimento de pandemias ou tecnologias emergentes que levam ao aumento de ameaças não convencionais, transnacionais e assimétricas, como os ataques informáticos ou híbridos. O aumento exponencial de cibernautas, tornou a cibercriminalidade e a utilização da internet para fins terroristas, na nova fronteira da guerra do século XXI (CE, 2017).

Assim, o objeto de estudo da presente investigação centra-se no desenvolvimento de contributos, que facilitem a formulação de uma Estratégia Digital para as Forças Armadas (FFAA) portuguesas e permita responder aos atuais desafios, tendo por base, o atual nível de compreensão das FFAA nesta temática e a evolução de tecnologias disruptivas.

O foco principal desta investigação visa o produto operacional das FFAA. Contudo, a transversalidade do assunto, não permite dissociar o ambiente operacional do administrativo.

Sem prejuízo da sua contextualização, a investigação foi delimitada (Santos & Lima, 2019, pp. 42-43) a nível temporal, orientado essencialmente para a atualidade, pese embora, abranja um horizonte prospetivo até 2030. A nível do espaço será centralizado nas FFAA portuguesas e a nível do conteúdo, a análise das perspetivas e da envolvente estratégica.

Assim sendo, formulou-se o Objetivo Geral (OG) “Propor contributos para uma Estratégia Digital nas Forças Armadas portuguesas”, seguido da Questão Central (QC): “Quais os contributos para uma Estratégia Digital nas Forças Armadas portuguesas?”.

O presente trabalho está estruturado em nove capítulos, sendo o primeiro, a introdução, onde trata uma abordagem inicial do tema, bem como aspetos relacionados com a escolha e estrutura do trabalho. O segundo apresenta uma revisão da literatura e metodologia aplicada. O terceiro centra-se na perceção da instituição militar sobre o tema, seguido de um quarto capítulo que aborda o ambiente estratégico internacional em torno das tecnologias digitais. Os três capítulos posteriores assentam na análise dos pilares das perspetivas da estratégia, seguido do oitavo que caracteriza o ambiente estratégico e deduz os objetivos e linhas de ação estratégicas, mantendo o alinhamento estratégico, permitindo responder à QC. O nono capítulo, designado por conclusões, sintetiza o percurso metodológico e os resultados obtidos, respondendo às questões que nortearam a investigação, contribuindo para o conhecimento no domínio da investigação, tecendo ainda, algumas recomendações para investigações que venham a ser desenvolvidos nesta área.



2. Enquadramento e metodologia

Nos termos da alínea c) do art.º 5º do Decreto-Lei n.º 249/2015, de 28 de outubro, a investigação em curso enquadra-se na área das “Técnicas e Tecnologias Militares” do domínio das Ciências Militares (Conselho de Ministros, 2015), decompondo-se nas subáreas de “Comando, Controlo, Comunicações, Computadores e Informação” e “Gestão Estratégica” (Academia das Ciências de Lisboa, 2011).

2.1. Enquadramento

O digital tem vindo a integrar tecnologias disruptivas em constante evolução, tendendo para uma maior interação entre humanos e máquinas, que levam a um aumento de competitividade e a mudanças no estilo de vida das sociedades modernas.

Ao nível da Segurança e Defesa, o digital veio potenciar a capacidade de atuação das FFAA, embora também tenha alargado as ameaças a todos os domínios. Segundo o Secretário-Geral da *North Atlantic Treaty Organization* (NATO), Jens Stoltenberg, “[...] a segurança do nosso futuro dependerá na nossa habilidade de compreender, adotar e implementar tecnologias, tais como, a IA, a autonomia e sistemas hipersónicos” (2020).

A Europa iniciou o seu percurso digital, em 2010, ao aprovar uma “Agenda Digital para a Europa”, como documento iniciador da transição digital na Europa (Parlamento Europeu, 2020), acelerado pela i4.0, designadamente na presidência de Juncker (2014) ao estabelecer como prioridade, a conexão de um mercado digital, e posteriormente reforçado como objetivo estratégico, pela presidente Von der Leyen (2019).

Na senda da Europa, Portugal iniciou a TD com o programa do XXI Governo Constitucional (Governo de Portugal, 2015), ao referir a necessidade de fortalecer, simplificar e digitalizar a Administração Pública, aprovando em 2017, uma estratégia para a *Transformação Digital na Administração Pública* (AP) (Presidência do Conselho de Ministros [PCM], 2017), documento que deu origem ao Plano Setorial para a Defesa Nacional (Governo de Portugal, 2018). O programa do XXII Governo Constitucional, contempla um desafio estratégico dedicado (Governo de Portugal, 2019), levando à aprovação de um *Plano de Ação para a Transição Digital* (PCM, 2020). Em 2021, o governo aprovou a Estratégia para a TD da AP entre 2021 e 2026, alinhando as reformas e objetivos do Plano de Recuperação e Resiliência (PRR) e contribuindo para a coerência global dos investimentos no quadro da transição digital da AP (Leitão, 2021). O programa do XXIII Governo Constitucional, mantém esta prioridade estratégica (Governo de Portugal, 2022), reforçada nos diversos *fora*, como exemplo: “*Portugal tem de encarar a transformação digital como um verdadeiro desafio estratégico*” (Governo de Portugal, 2020).



Na senda da prioridade nacional estabelecida, as FFAA têm vindo a estabelecer a inovação e o digital como prioridade, conforme a Diretiva Estratégica do Estado-Maior-General das Forças Armadas (DEEMGFA), para o período entre 2021 e 2023, através de um Objetivo Estratégico (OEst) dedicado: “Dinamizar a inovação e a transição digital nas Forças Armadas” (Estado-Maior-General das Forças Armadas [EMGFA], 2021). Os Ramos seguem esta orientação, vertendo nas respetivas diretivas conforme vão sendo renovadas: a Marinha, contempla como OEst dedicados, “Potenciar a inovação tecnológica”, “Acelerar a transição digital e a informatização” e “Promover a independência tecnológica” (2022); o Exército ambiciona por progredir na inovação, modernização tecnológica e transformação digital, transversais a todos os domínios do Exército, dispondo de um OEst dedicado: “Estimular a Inovação e a Modernização dos Sistemas e Tecnologias” (2022); a Força Aérea visa simplificar e agilizar a decisão, alavancada pela ligação entre sistemas físicos e virtuais, e pelas áreas que caracterizam as organizações 4.0, através de um processo de transição digital sustentado e apoiado por tecnologias disruptivas (2022).

Assim sendo, esta temática é relevante para as FFAA, conforme enquadrado nas respetivas diretivas supra, mas também, pela abordagem holística e sistémica das FFAA, enquanto instituição resiliente, que está alinhada com as demais instituições, enquanto produtoras de Segurança e Defesa.

A TD da Defesa consiste num processo complexo, multidimensional e interativo, de contínua modernização da capacidade de toda a organização e de integração empresarial, acompanhado por aceleradores de inovação, essenciais, como a IA, a robótica, o *data analytics* e o *blockchain*. Apesar de não ser um empreendimento puramente tecnológico, a cultura, a liderança e os processos adaptam-se para construírem uma organização, que seja fundamentalmente ágil e melhor preparada para identificar, desenvolver, testar, escalar, adquirir e integrar novas tecnologias, de forma contínua, e mais rapidamente do que os adversários (*Defence IQ*, 2021).

O termo transição digital (TDig) é usado como sinónimo de TD, embora haja distinções, pois a TD está mais focada na mudança assente na combinação de tecnologias digitais transformadoras, ferramentas, processos e, ainda, pessoas (cultura e mentalidade) que transformam a forma de fazer negócios, a TDig assenta essencialmente na atualização das tecnologias, ferramentas ou processos existentes, automatizando estes e melhorando o fluxo de trabalho de uma organização (Yerramsetty, 2017). Assim sendo, a transformação enquadra-se na transição, razão pela qual, o “*Plano de Ação para a Transição Digital*”



(Resolução do Conselho de Ministros [RCM] nº 30, 2020) considera a TD um dos três pilares que integram o plano.

Para além destas definições primordiais à perceção da temática, o presente trabalho incorpora um corpo de conceitos (*vide* Apêndice A), como enquadramento concetual da investigação, para facilitar a compreensão dos assuntos abordados.

A temática aborda a TDig na perspetiva da arte estratégica, definida por Ribeiro (2020), como a “...hábil formulação e operacionalização da modalidade de ação, onde se articulam fatores de decisão, segundo os princípios e regras estratégicas de aplicação, tendo em conta diversos modelos de ação estratégica validados pelas provas da estratégia...”.

Assim sendo, destaca-se Couto (1988, p. 230), pela necessidade de haver uma gestão entre a conceção e a execução, delineada entre o que se quer, o que deve e o que se pode fazer. Neste âmbito, a estratégia tem de ser focada no desenvolvimento da força, abrangendo os aspetos operacionais (emprego dos recursos), os estruturais (constituição, organização ou articulação dos recursos) e os genéticos (geração e edificação de recursos ou capacidades).

Na sequência do exposto, a necessidade do desenvolvimento da presente temática enquadra-se no OEst 3 da DEEMGFA (2021/2023) (2021). Mantendo o alinhamento ao OEst 3, define-se como visão estratégica para a potencialização do digital nas FFAA: *Processos de decisão mais ágeis e mais bem informados, capazes de responder aos desafios decorrentes dos avanços das tecnologias disruptivas*. É uma visão focada na superioridade de informação, na agilidade do comando e controlo (C2), de modo a ter uma decisão mais célere e competitiva, bem como, integrar as tecnologias emergentes.

A TD em termos militares deve ser enquadrada como um processo, catalisador de capacidades. Numa abordagem holística e sistémica, há uma correlação dos vetores que constituem uma capacidade militar (DOTMLPII¹), com os paradigmas ou perspetivas que enquadram uma estratégia (Figura 1).

¹ Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade.

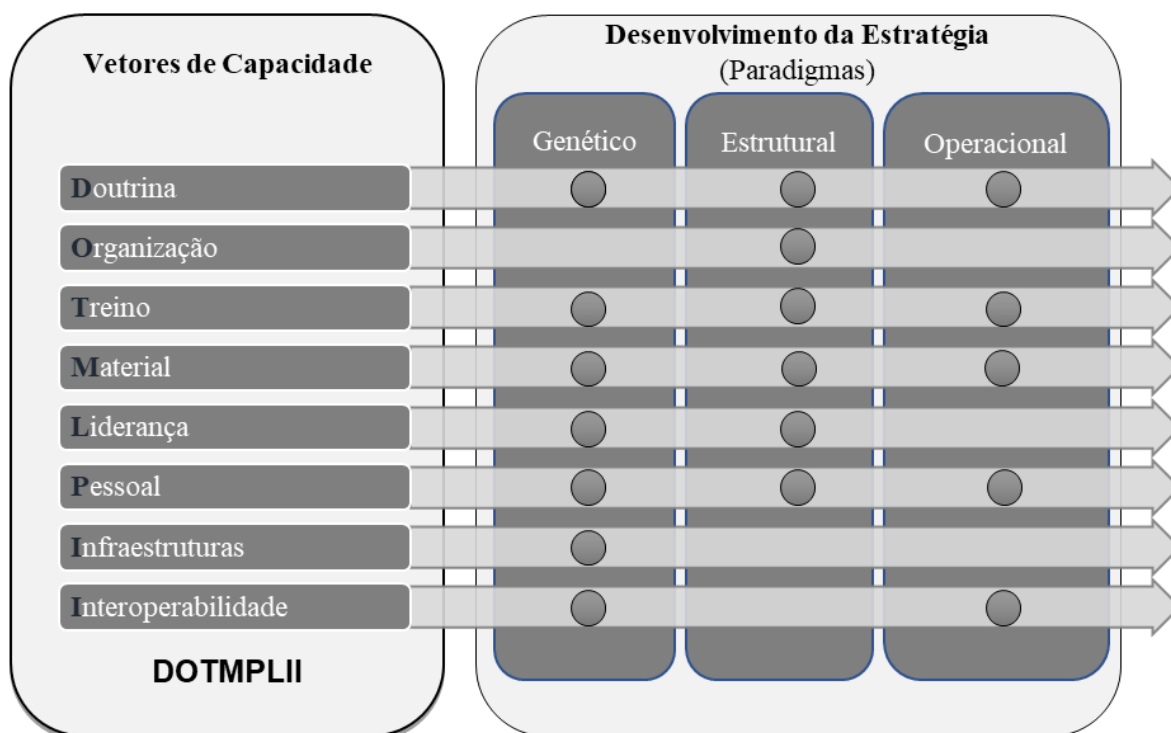


Figura 1 - Modelo de desenvolvimento

Fonte: Adaptado a partir de Nunes (2020, cit. por Alves, 2021).

2.2. Metodologia

A presente investigação assenta essencialmente nas normas do Instituto Universitário Militar (IUM) (Fachada et al., 2020; Norma de Execução Permanente/Investigação [NEP/INV] - 001 [A1], 2020; NEP/INV - 003 [A3], 2020; Santos & Lima, 2019).

Assim sendo, a abordagem reflete-se numa orientação ontológica de construtivista e epistemológico de interpretativista, enquadrada numa estratégia qualitativa, focada no raciocínio indutivo, centrando “...o ponto de partida na observação de factos particulares para, através da sua associação, estabelecer generalizações que permitam formular uma lei ou teoria” (Santos & Lima, 2019, p. 18). Como desenho de estudo, aplica-se o desenho de pesquisa interpretativa, complementado com o comparativo, de modo a analisar algumas Organizações Internacionais (OI) enquanto parceiros, bem como, FFAA congéneres. Como instrumentos metodológicos, assenta na recolha de dados baseada na análise documental, num questionário e em entrevistas semiestruturadas realizadas para o trabalho de investigação individual do Curso de Estado-Maior Conjunto (CEMC), edição 2020/2021, dados que face ao período temporal, ainda se mantêm atualizados. Em complemento serão realizadas algumas entrevistas semiestruturadas ao EMGFA e aos Ramos, de modo a manter o alinhamento sobre a temática em investigação.

A investigação desenvolveu-se segundo o modelo de análise apresentado no Quadro 1.



Quadro 1 - Modelo de Análise

Objetivo Geral	Propor contributos para uma Estratégia Digital nas FFAA portuguesas.				
Questão Central	Quais os contributos para uma Estratégia Digital nas FFAA portuguesas?				
Objetivos Específicos (OE):	Questões Derivadas (QD)	Conceito Estruturante	Dimensões	Indicadores	Recolha de dados
OE1: Identificar o nível de compreensão desta temática nas FFAA portuguesas.	QD1: Qual o nível de compreensão desta temática nas FFAA portuguesas?	Maturidade digital.	Estruturas das FFAA portuguesas.	Capacidades.	Questionários, Análise Documental e Entrevistas.
				Liderança.	
				Desafios.	
OE2: Descrever os elementos da transição digital que contribuem para a melhoria das capacidades decisórias das FFAA portuguesas.	QD2: Quais os elementos da transição digital que contribuem para a melhoria das capacidades decisórias das FFAA portuguesas?	Estratégia Operacional.	Capacidades decisórias.	Informação.	Análise Documental e Entrevistas.
				Ciberdefesa.	
				Agilidade.	
OE3: Estabelecer a composição, organização e articulação dos recursos, de modo a assegurar o melhor desempenho dos processos de decisão e das atuações dos meios.	QD3: Quais as orientações de ordem estrutural, que visam assegurar o melhor desempenho dos processos de decisão e das atuações dos meios?	Estratégia Estrutural.	Literacia e processos.	Liderança Digital.	Análise Documental e Entrevistas.
				Competências Digitais.	
				Processos.	
OE4: Analisar os recursos necessários à edificação harmoniosa e balanceada das capacidades, que possam contribuir para o nível digital das operações.	QD4: Quais as capacidades que melhor contribuem para o nível digital das operações?	Estratégia Genética.	Desenvolvimento de capacidades.	Arquitetura Organizacional.	Análise e Documental Entrevistas.
				Dados e informação.	
				Inovação.	

3. Perceção digital das Forças Armadas portuguesas

O presente capítulo visa compreender a perceção atual relativamente à TDig, assente em questionários, em entrevistas e na análise documental para responder à QD1.

3.1. Análise de dados dos questionários

Para uma compreensão da temática nas FFAA foram analisadas as perceções do domínio digital e dos desafios da i4.0 (vide Apêndice B), através de dois questionários realizados a militares em funções de Estados-Maiores. Ambos, são questionários certificados, o primeiro adaptado do modelo do *Massachusetts Institute of Technology* (MIT) e o segundo, do Instituto de Apoio às Pequenas e Médias Empresas e à Inovação (IAPMEI).

O primeiro questionário visou avaliar a perceção da maturidade dos militares, com um bloco de questões direcionado para as capacidades digitais e outro, orientado para as capacidades de liderança. Pela perceção obtida, enquadram-se no quadrante de **Iniciantes** (Figura 2), embora haja uma perceção de evolução.

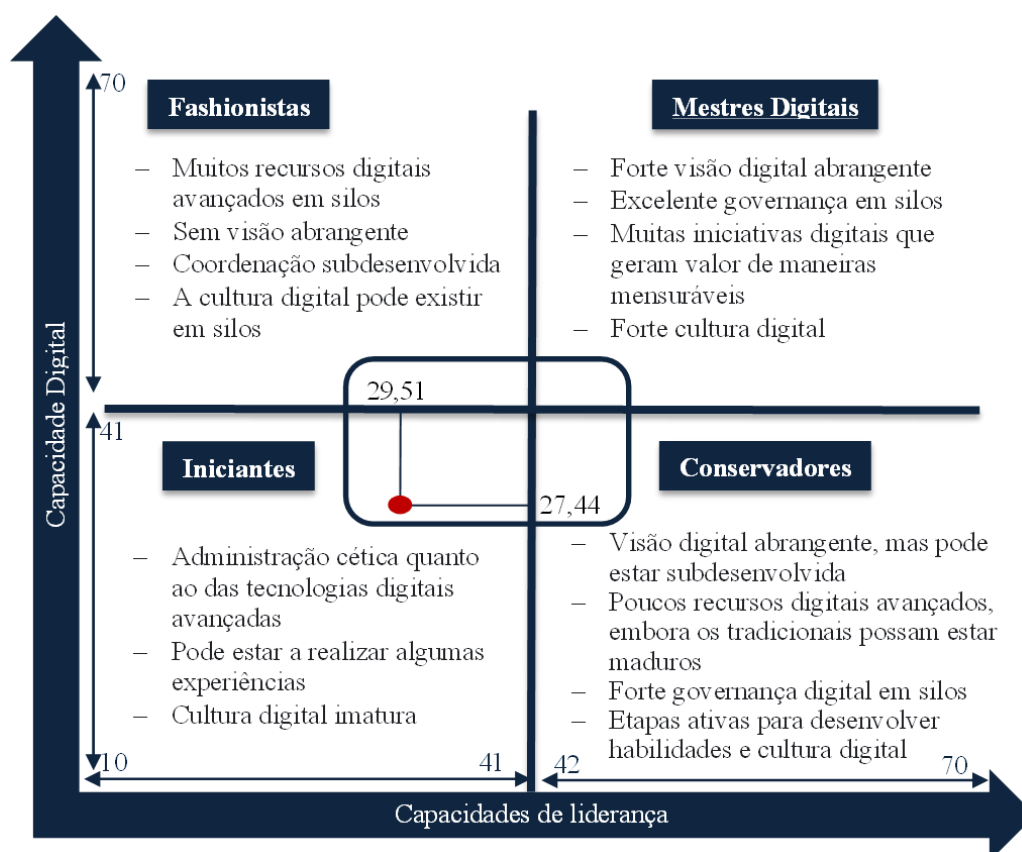


Figura 2 - Perceção do domínio de digital

Fonte: Adaptado a partir de Westerman, Bonnet e McAfee (2014, cit. por Alves, 2021).

O segundo questionário foi constituído por seis blocos de questões, de modo a facilitar a perceção para abraçar os desafios da i4.0. Resultante da ferramenta Shift 4.0 às 314 respostas, obteve-se uma avaliação global ponderada de 1,32, correspondendo ao nível 1 (Figura 3). Por blocos de respostas, apenas os blocos dos grupos de serviços baseados em

dados e dos recursos humanos, atingiram o nível 2, ficando os restantes no nível 1 (Estratégia e Organização; Infraestruturas Inteligentes; Operações Inteligentes; e Produtos Inteligentes).



Figura 3 - Avaliação da Maturidade Digital

Fonte: Adaptado a partir de IAPMEI (2021, cit. por Alves, 2021).

Face aos resultados, percebe-se que a compreensão do tema, ainda esteja num estado incipiente. Contudo, pode haver alguma falta de divulgação dos projetos em curso que contribuem para a TDig das FFAA, alinhados com a prioridade estratégica nacional.

3.2. Análise das entrevistas

3.2.1. Estado-Maior-General das Forças Armadas

Com a reforma do ensino superior militar, foram edificados Centros de Investigação, Desenvolvimento e Inovação (ID&I) (Decreto-Lei n.º 249/2015) que visam desenvolver conhecimento em áreas de especial interesse para a Segurança e Defesa Nacional.

A importância desta temática tem tido maior relevância desde 2015, com a edificação do Centro de Ciberdefesa e com projetos no âmbito da digitalização e simplificação de processos através de projetos inscritos no programa SIMPLEX².

A nível operacional, pretende-se agilizar a estrutura de C2 e o processo de decisão, através do projeto *Federation Mission Networking* (nível *instantiation*) (Rodrigues, 2021).

Em 2019 foi edificado o Departamento para a Inovação e Transformação (DIT), tendo em vista promover e coordenar soluções inovadoras (EMGFA, s.d.). A DEEMGFA (2021), já contempla um OEst dedicado à Inovação e TDig.

3.2.2. Marinha

A Diretiva Estratégica (2022) prevê uma Marinha tecnologicamente avançada, consubstanciada por três objetivos estratégicos: potenciar a inovação tecnológica; acelerar a digitalização e a informatização; e, promover a independência tecnológica. Paralelamente,

² Programa de modernização administrativa em Portugal que integra medidas de simplificação, modernização e inovação, consagrando o digital como regra de atuação.



dispõe de um Programa Intersectorial para a TDig, onde contém um conjunto alargado de iniciativas conducentes a uma TDig acelerada e concertada, que potenciam a utilização de tecnologias da i4.0, entre as quais, o *big data*, a IA e o *Machine Learning* (ML).

Segundo a entrevista (*vide* Apêndice D), a Marinha considera que a TDig poderá ser uma mais-valia na perspetiva operacional, nomeadamente ao nível do exercício do C2 e do processo de decisão. Ou seja, tornar estes processos mais céleres e automatizados, minimizando o erro humano. Respeitante à automatização, considera relevante para obter processos mais eficazes e eficientes, reduzindo a necessidade de recursos humanos em determinadas tarefas, realocando-os noutra tipologia de tarefas.

Quanto à arquitetura organizacional, considera essencial face à crescente e rápida evolução tecnológica, potencializando a otimização e a gestão de recursos das FFAA.

No que se prende com a interação homem-máquina assente na ID&I, considera essencial acompanhar a evolução, evitando cair na obsolescência de processos e de sistemas.

Por último, o entrevistado considerou que deve haver uma estratégia parcelar para a especificidade de cada Ramo e uma estratégia conjunta e coordenada para tudo aquilo que é transversal e de potencial utilização por todos os Ramos.

À semelhança dos outros Ramos, a Marinha dispõe do Centro de Investigação Naval (CINAV) (2010), orientado para o desenvolvimento de projetos de interesse, em parceria com academias e empresas (IdD Portugal Defence, s.d.). Na sequência destas parcerias foi edificado o exercício da série REP (MUS)³, orientado para testar sistemas não tripulados no domínio marítimo, tendo presentemente uma dimensão internacional. Em 2020 foi edificada a Divisão de Inovação e um Centro de Experimentação Operacional da Marinha (CEOM), dispondo de uma Zona Livre Tecnológica (ZLT), para promover a cooperação tecnológica focada no mar, particularmente em sistemas não tripulados, através de campanhas de experimentação nos ambientes subsuperfície, superfície e aéreo (Marinha, 2021b).

3.2.3. Exército

Segundo o entrevistado (*vide* Apêndice D), a TDig visa potenciar o produto operacional, direta ou indiretamente, pela simplificação e eficiência processual e de tomada de decisão, conforme plasmado na Diretiva Estratégica com o OEst 5 (Modernizar Sistemas e Infraestruturas) (2019), renovada na Diretiva em vigor, com a “...inovação, modernização tecnológica e transformação digital, transversais a todos os domínios do Exército” (2022). Para tal, as tecnologias disruptivas são essenciais para essa modernização, realçando-se a

³ Sigla que na língua inglesa designa a *Robotic Experimentation Prototyping augmented by Maritime Unmanned Systems*.



necessidade de maturar este processo, de modo a potencializar o proveito dessas ferramentas, através: das iniciativas do Centro de Investigação da Academia Militar (CINAMIL); da participação nos *fora* ou iniciativas deste âmbito; e, através do Pólo Tecnológico do Exército e do Centro de Experimentação e Modernização Tecnológica do Exército.

Na perspetiva operacional, a TDig deve ser o catalisador para modernizar o processo de decisão, assente na superioridade de informação, através da progressiva desmaterialização da informação, que permitirá o acesso mais célere à informação estruturada, permitindo decisões mais rápidas, oportunas e acertadas.

Relativamente à automatização, considera-se um pouco cético, realçando a necessidade de explorar este tipo de sistemas, de modo a alcançar um nível de maturidade antes da sua implementação, considerando ser vantajoso na otimização de recursos humanos, nomeadamente na sua realocação em áreas operacionais.

Respeitante à arquitetura organizacional, considera essencial para permitir uma criteriosa gestão de recursos e para potenciar a utilidade do produto operacional.

Quanto à interação homem-máquina, considera essencial, contudo importa ainda alcançar um nível de maturidade neste tipo de tecnologias através da ID&I.

Por último, considera que presentemente a implementação da TDig assenta em estratégias parcelares, considerando que os pontos de convergência e sincronia são de natureza administrativa e logística, centrada na Secretaria-Geral do Ministério da Defesa Nacional (MDN), orientado para os Sistemas de Informação. Decorrente das novas Leis Orgânicas é expectável que essa responsabilidade possa ser ao nível conjunto.

3.2.4. Força Aérea

A Diretiva Estratégica (2022) visa simplificar e agilizar a decisão, alavancada pela ligação entre sistemas físicos e virtuais e pelas áreas que caracterizam as organizações 4.0, através de um processo de TDig sustentado e apoiado por tecnologias disruptivas, materializado, com alguns OEst e Linhas de Ação Estratégicas (LAE) orientadas, para as operações multidomínio, para a ciência e tecnologia, e para o processo de decisão. Assim, tenciona expandir as áreas de investigação aos domínios do Espaço e Ciberespaço (LAE3.2); e otimizar a gestão da organização com processos simples e eficazes suportados em sistemas de informação atuais e resilientes (OEst 4).

Segundo o entrevistado (*vide* Apêndice D), estão em curso um conjunto de iniciativas integráveis ao nível da Defesa Nacional (DN) e, como contributo para o C2, a Força Aérea dispõe, o *Portuguese Sky Sentinel System* (PS3), com dois módulos que integram IA: o primeiro para apoio aos incêndios e um segundo para busca e salvamento. Presentemente



está em desenvolvimento um terceiro módulo de *Intelligence, Surveillance and Reconnaissance* (ISR) que irá integrar uma forte componente de IA, *Business Intelligence* (BI) e *Big Data*. Numa fase seguinte, tenciona desenvolver um quarto módulo de Lições Aprendidas (LLAA), alimentado pelos três módulos anteriores, armazenando e analisando a informação, através de uma forte componente de IA, BI e *Big Data*.

Na perspetiva operacional, a TDig poderá ser vantajosa na superioridade de informação, caso seja aprimorada com o BI e com o estabelecimento de objetivos e métricas.

Quanto à automatização, considera-a essencial na otimização de recursos humanos, realocando-os noutras tarefas, devendo a decisão assentar sempre no fator humano. Por outro lado, considera a necessidade de um estudo sobre custos-benefícios da automatização.

Quanto à implementação de uma arquitetura organizacional, considera essencial, para a definição de métricas e estabelecimento de métricas para a automatização.

Respeitante à interação homem-máquina assente na ID&I, considera ser fundamental para evitar a obsolescência dos sistemas tecnológicos e para acompanhar a evolução dos sistemas baseados em LLAA.

Por último, considera que deve haver uma estratégia conjunta para o que é transversal nas FFAA e uma estratégia parcelar para o que é específico de cada Ramo.

3.3. Síntese conclusiva

Face à análise dos questionários, há uma perceção que a instituição ainda está num nível incipiente. Por outro lado, as iniciativas integradas, os sistemas tecnológicos, os Centros de ID&I ou Polos Tecnológicos existentes no EMGFA e nos Ramos, aparentam que existe alguma falta de divulgação de informação relativamente ao que está em curso.

Segundo as Diretivas Estratégicas do EMGFA e dos Ramos, esta temática passou a constituir-se uma prioridade estratégica, vertida na visão, nos OEst e em LAE dedicadas.

Resultante das entrevistas recentes aos Ramos, os entrevistados consideram que esta temática deve ter uma abordagem conjunto para o que é transversal e parcelar para as especificidades de cada Ramo. Na generalidade, consideram essencial a arquitetura organizacional e a capacidade de interação homem-máquina assente na ID&I, e na implementação da TDig. Na perspetiva operacional, a TDig deverá constituir-se o elemento diferenciador para melhorar o processo de decisão.

Em resposta à QD1, considera-se que apesar da falta de divulgação das iniciativas em curso ou implementadas e a par da visão institucional refletida nas Diretivas Estratégicas, há um percurso incipiente, enquadrado num processo de transformação evolutivo, que requer um esforço concertado para acompanhar a sociedade e os parceiros.



4. Perspetiva internacional

A TDig é uma realidade com impacto nas culturas organizacionais, denotando uma nova era dos dados, em que o volume de informação, não sendo processável pela capacidade cognitiva, leva à adoção de práticas e processos de decisão centrados na tecnologia.

A omnipresença da informação permitida pela conectividade e capacidade de acesso, como a 5.^a Geração de Comunicações Móveis (5G), a evolução da engenharia de *software*, arquitetura de dados, o *big data*, a IoT, o surgimento da robótica, a IA e o ML vem alterar o rumo das operações militares, com novas oportunidades, desafios e ameaças, nomeadamente no espaço e ciberespaço, levadas a cabo por atores estatais e não estatais.

Atendendo que a doutrina americana, a da NATO e da União Europeia (UE) constituem-se uma referência (Pires, 2018, p. 3), este capítulo analisa o ambiente estratégico e a integração da TDig por esses parceiros.

4.1. Ambiente estratégico

O ambiente estratégico tem estado em constante mutação desde a Segunda Guerra Mundial até ao atual modelo de guerra híbrida, abrangendo todos os domínios.

A abordagem holística e integrada da conflitualidade tem levado a uma aproximação ao conceito das *Multi-Domain Operations* (MDO), operações onde a TDig tem sido relevante para o sucesso das mesmas, não só pela predominância de dados, mas pela necessidade de garantir a interoperabilidade entre aliados (NATO, 2022c). A invasão da Ucrânia, é um exemplo das MDO e de guerra híbrida, através do emprego de *Unmanned Aerial Vehicles* (UAV), armas hipersónicas, aeronaves diversas, forças terrestres, trabalhando todos em uníssono no contexto de sanções económicas e peso diplomático (Chaudhari, 2022).

Segundo Chaudhari⁴ (2022), a tendência dos conflitos será de natureza híbrida alargada a todos os domínios, desde o convencional ao não convencional, do cinético ao não cinético, do letal ao não letal, tudo sob uma saliência nuclear. As FFAA tendem a investir no desenvolvimento de tecnologias de nicho no campo dos recursos, baseados no espaço, *data linking* e IA integrada nos sistemas de apoio à decisão, para encurtar o sensor do ciclo do atirador e tornar o ciclo de *targeting* altamente responsivo.

A par desta expansão multidomínio dos campos de batalha à escala geográfica e a diversos tipos de atores, tem havido uma compressão dos ciclos de decisão e dos tempos de reação, além de uma maior congestão dos campos de batalha sob uma vigilância persistente.

⁴ Chefe da Força Aérea indiana.

Paralelamente, as operações cibernéticas e no espaço, a guerra eletrónica, a robótica e a IA contribuem para esta mudança (Kem & McConville, 2020). Porém, esta nova ordem enfrenta um desafio quanto à dimensão e natureza, sem precedência, tanto pela imprevisibilidade e mutação de novas formas de guerra híbrida, como pela necessidade de um processo de decisão atempada, para responder às diversificadas situações de instabilidade (*Italian Army*, 2019). Neste âmbito, a NATO considera que as forças modernas devem ser credíveis, ágeis, conscientes, capazes de operar em rede e resilientes.



Figura 4 - Visão Estratégica da NATO

Fonte: Exército italiano (2019).

Em suma, esta mudança assenta na IA, orientada para o campo da pesquisa e análise, logística, operações cibernéticas, C2, estando em curso uma disputa tecnológica pela liderança no contexto militar, entre a China, os Estados Unidos da América (EUA) e a Rússia. As forças americanas já integraram a IA em sistemas de combate para identificar alvos no conflito do Iraque e da Síria (Sayler, 2020).

4.2. Estados Unidos da América

A visão americana assenta na necessidade de preservar e expandir a vantagem militar neste novo ambiente operacional digital, através de FFAA adaptáveis, inovadoras e capazes de empregar as suas capacidades em múltiplas regiões e em todos os domínios. Para tal consideram vital, ter infraestruturas e serviços de Tecnologias de Informação (TI) ágeis, resilientes, transparentes, contínuos e seguros, capazes de transformar dados em informação, acessível e fiável ao cumprimento da missão, sem interferência acionável e que garantam uma execução fiável da missão, apesar da persistente ameaça cibernética (*Department of Defense [DoD]*, 2019).

Conforme a Figura 5, a TDig da Defesa assenta em quatro prioridades: cibersegurança, IA, *cloud* e, Comando, Controlo e Comunicações (C3).



Figura 5 - Modernização Digital

Fonte: DoD (2019).

O Exército americano aprovou uma estratégia de modernização (McCarthy et al., 2019), que ambiciona a condução de MDO. Assim, considera essencial desenvolver tecnologias de computação na *cloud*, melhorar o acesso aos dados e ambientes de partilha, e racionalizar as ferramentas e serviços de desenvolvimento de software, visando explorar a aprendizagem de máquinas emergentes através de IA, de modo a melhorar o processo de decisão. A arquitetura aberta da *cloud* permite acelerar o fluxo de informação, permitindo combater os adversários no ambiente informacional com a mesma eficácia que é feito nos domínios físicos, levando à vitória no espaço cognitivo⁵ (McCarthy et al., 2019).

O Corpo de Fuzileiros (*United States Marine Corps*) estabeleceu como prioridade, equipar a rede para integrar, partilhar e gerir dados, integrando a IA e o ML para se tornar mais rápido e eficiente. Segundo, o Brigadeiro-general Wortman (*GovDataDownload*, 2019), as experiências que integram a IA levam tempo, sendo uma abordagem integrada com a rede, a *cloud* e com uma estratégia de armazenamento de dados, simultaneamente eficaz.

A Força Aérea visa renovar a gestão de dados, a arquitetura de TI e as operações comerciais, para a aumentar a competitividade. A vantagem operacional depende da capacidade de fundir a vasta quantidade de dados para acelerar a decisão (Correl, 2019).

A visão da Marinha americana está orientada para a conceção, construção, experiências, implementação e sustentação dos sistemas de defesa, alterando o treino e moldando as formas de trabalho, usando práticas de engenharia digital, através de recursos digitais em desenvolvimento, integrando dados no processo de decisão operacional. Ainda, considera essencial compreender e implementar tecnologias emergentes e capacidades avançadas de análise para moldar o novo campo de batalha digital. O processo de decisão

⁵ É o espaço no qual é exercido o processo mental de aquisição e compreensão dos conhecimentos, situação que implica o consumo, a interpretação e a perceção da informação (Ottewell, 2020).



deve assentar em dados integrados em novas capacidades digitais, transformando as principais operações navais, acelerando os resultados e impulsionando a supremacia naval (Bussiere, 2022).

Em suma, as FFAA americanas estão numa fase de transformação, face à nova conflitualidade orientada para as MDO, enquadradas em tecnologias disruptivas, assentes no digital, sendo a IA o catalisador para sistemas semiautónomos e autónomos, que permitam encurtar o ciclo de decisão ou potencializar a eficácia de sistemas defensivos ou ofensivos.

4.3. NATO

A evolução do ambiente estratégico caracteriza-se por ser mais contestado e imprevisível (NATO, 2022d). Segundo o General Lavigne⁶ (NATO, 2022a), a NATO tem vindo a promover a interoperabilidade e iniciativas inovadoras desde 2003. Com o surgimento da i4.0, tem promovido o desenvolvimento de tecnologias emergentes e disruptivas, como a IA, as tecnologias quântica, autónoma e nano. A NATO está comprometida com a TD conforme vai moldando o espaço de batalha, numa abrangência multidomínio, contribuindo para o “Conceito de Capstone”⁷. Esta harmonia entre as MDO e a TD dita como a NATO deve pensar, organizar e agir de forma diferente, para ficar na vanguarda da complexidade dos conflitos, explorando a tecnologia emergente. Lavigne reforça: “...devemos iniciar a TD hoje se quisermos manter a nossa força amanhã.”

Ainda segundo Lavigne (*op. cit.*), é essencial acelerar e melhorar o processo de decisão, através de uma estratégia de dados e com processos ágeis, fomentando uma cultura de inovação, colaboração e cooperação, e valorizando o capital humano.

As operações assentam cada vez mais no (i) ciberespaço, áreas densamente populacionais e subterrâneas; (ii) tecnologias amplamente acessíveis; (iii) interação homem-máquina; (iv) sistemas automatizados e potencialmente autónomos; (v) sistemas de armas de destruição generalizada ou de amplo efeito; (vi) proliferação da IoT; e (vii) capacidade alargada de análise de dados para obter vantagem militar (NATO, 2018a, pp. 13-14). Contudo, as TI são o catalisador da superioridade de informação (2017).

Segundo Stoltenberg, “[...] a segurança do nosso futuro dependerá na nossa habilidade de compreender, adotar e implementar tecnologias, tais como, a IA, a autonomia e sistemas hipersónicos” (NATO, 2020, p. 2). Neste âmbito, a NATO aprovou a estratégia de IA que

⁶ Atual *Supreme Allied Commander Transformation* da NATO.

⁷ Segundo Fernandes (2016), é um “...conceito abrangente, com o objetivo de liderar o desenvolvimento e emprego de forças, fornecendo uma ampla descrição de como operar em parcelas significativas do espectro de operações e descrevendo o que é necessário para atingir os objetivos estratégicos.”



visa o ambiente global de defesa e segurança, sendo uma oportunidade para fortalecer a vantagem tecnológica, bem como, a escalada da velocidade das ameaças (2021a).

4.4. União Europeia

A abordagem assenta na superioridade de informação (*Council of the European Union* [CEU], 2020, p. 2), baseada numa perspetiva digital, coordenada e sincronizada.

O sucesso operacional está cada vez mais dependente da informação, do tempo, da interoperabilidade e da ação no ciberespaço (CEU, 2020, p. 4). Na perspetiva informacional é imperativo que haja maior ligação e integração entre todos os sistemas, desde o ser humano aos sistemas que incorporem IA, ou outras tecnologias disruptivas. A perspetiva temporal é essencial na abordagem digital das operações, nomeadamente para encurtar o processo de decisão, atendendo que o tratamento de dados e a produção de informação assentam em sistemas que integram IA. A interoperabilidade é imperativa entre as diversas forças e aliados pertencentes à UE, sendo essencial que haja um alinhamento de sinergias que contribuam para este desiderato. A liberdade de ação no ciberespaço é imperativo (CEU, 2020, p. 4), face à transversalidade deste domínio quanto aos demais.

Para que o digital seja um multiplicador de forças, é essencial que haja uma integração coordenada de capacidades, entre as quais, as de C2 num nó de rede única, que facilite a partilha de informação com segurança e credibilidade num ambiente multidomínio. Assim, é essencial uma interligação dos nós das TI, entre bases de dados, sensores e decisores, criando sinergias orientadas para os resultados, alinhados com os objetivos (CEU, 2020).

Embora a IA ainda esteja em evolução, deve assentar em dados com elevada qualidade para que sejam desenvolvidos algoritmos de IA corporizada e de confiança (CE, 2019).

4.5. Síntese conclusiva

Numa forma holística, conclui-se que as principais organizações parceiras e congéneres de referência no âmbito do sector da Defesa, estão a abraçar a TDig na perspetiva operacional, no sentido melhorar a capacidade de comando e controlo, alcançar uma decisão mais rápida e mais bem informada numa perspetiva de multidomínio, e tendencialmente com sistemas tecnológicos semiautónomos e em última instância totalmente autónomos. A nova ordem mundial, cada vez mais Volátil, Incerta, Complexa e Ambígua (VICA), está a alterar a natureza dos conflitos, exigindo forças militares credíveis, ágeis, conscientes, que operem em rede e resilientes, capazes de integrarem tecnologias emergentes, que permitam obter decisões mais céleres e mais bem informadas, bem como, sistemas de combate mais eficazes.

Os dados são o catalisador das tecnologias disruptivas e emergentes que contribuem para esta nova ordem mundial.

5. Perspetiva operacional da estratégia digital

A perspetiva operacional visa estabelecer as orientações adequadas ao emprego dos recursos, segundo capacidades expedicionárias, jurisdicionais e decisórias, visando a flexibilidade das operações. Segundo a Marinha (2015a), as capacidades expedicionárias projetam e sustentam a força; as jurisdicionais são aquelas requerem um empenhamento eficaz, mas também, aquelas que carecem de cooperação; e as decisórias são aquelas que são apoiadas pela superioridade de decisão e por uma arquitetura de informação em rede.

Face à dinâmica do ambiente estratégico, a par da evolução dos parceiros de referência, complementado pelas entrevistas realizadas e enquadrado no conceito, o presente capítulo integra a perspetiva operacional nas capacidades decisórias, abordando a superioridade de informação, o C2 ágil e o ciberespaço, para responder à QD2.

5.1. Superioridade de informação

Segundo Marques (2017), o termo informação define-se de forma generalizada, “...como tudo o que decorre da contextualização dos dados que lhe dão origem”, tornando-se um recurso intangível que contribui decisivamente para o processo de decisão.

Para a NATO (2015b), a superioridade de informação consiste na “...vantagem operacional derivada da capacidade de recolher, processar e disseminar um fluxo ininterrupto de informações, enquanto explora ou nega a capacidade de um adversário de fazer o mesmo”, logo é essencial para alimentar o processo de decisão.

A superioridade de informação já não é apenas um *enabler*, mas uma verdadeira arma estratégica, operacional e tática. Se utilizada de forma atempada e coerente, pode gerar vantagens sobre um adversário, produzindo tanto efeito como uma arma de precisão, para perturbar, confundir, agitar e radicalizar (*Ministry of Defence* [MoD], 2018b).

A vantagem competitiva resultante do conhecimento quanto ao emprego adequado da informação disponível, permite gerar os efeitos em tempo e no local certo (Ward & Peppard, 2002, pp. 503-507). Para gerar esses efeitos, a superioridade de informação deve ser permanente, de modo a permitir completar o ciclo de decisão, conhecido pelo “OODA Loop”⁸ (Figura 6), mais rapidamente que o adversário, interrompendo o seu ciclo de decisão antes de o completar (Coram, 2002, pp. 282-284).

⁸ Desenvolvido pelo Tenente-coronel Boyd da Força Aérea americano, fruto da experiência em combate, enquanto piloto de caça durante a 2ª Guerra Mundial e na guerra da Coreia. (Seolin & Edilson, 2017, p. 2).

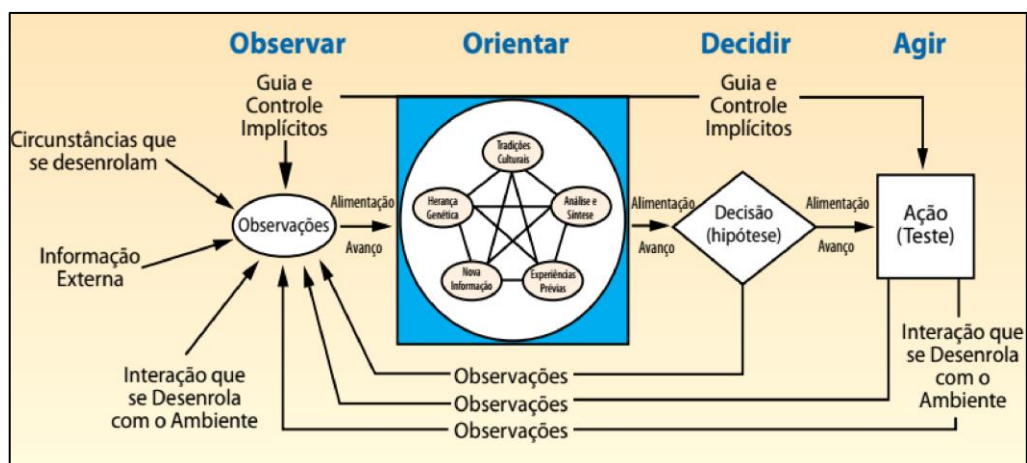


Figura 6 - OODA Loop de Boyd

Fonte: Martins (2017, cit. por Ashley, 2012).

O ciclo inicia com a observação do ambiente envolvente e as circunstâncias em que se desenrola, mas também, a partir de uma rede de dados ou mesmo de um serviço de informações, podendo orientar o esforço de pesquisa ou a criação do produto que permita apoiar a melhor decisão, antes de agir. Analisando na perspetiva da vantagem competitiva entre adversários, o ciclo de decisão entra num ciclo vicioso de ação-reação, sendo o fator tempo que permite a disputa pela vantagem competitiva (Martins, 2017).

Em boa verdade, os dados (factos não contextualizados) físicos ou informacionais constituem-se a base dos aceleradores tecnológicos que potencializam a superioridade de informação e o processo de decisão. Numa era expansionista de dados, há a necessidade de uma maior capacidade de armazenamento para posterior análise, sendo essencial uma gestão aprimorada, através da fusão e do apoio automatizado para analisar e visualizá-los, de modo a alcançar um processo de decisão mais eficaz e eficiente. Segundo Fawkes & Menzel (2018), a NATO desenvolveu um modelo de decisão (Figura 7), usando ferramentas de *big data*, IA, ML e *Deep Learning* (DL), adaptado a cada fase do ciclo de OODA.

Na fase da observação, face à vasta gama de sensores ou fontes de dados, devem ser fundidos numa visão unificada, através de uma infraestrutura de TI robusta, capaz de lidar com grandes quantidades de dados, de múltiplos níveis de segurança. Na fase da orientação, a utilização do *big data analytics* e algoritmos para processamento de dados, seguida da sua apresentação para filtrar e racionalizar, assente numa visão condensada e unificada, que permita ser digerida pelo ser humano. Na fase da decisão, a IA permite assegurar que os resultados são previsíveis e explicáveis, permitindo ao ser humano confiar devidamente no sistema. Na fase da ação, o ser humano pode aprovar a ação planeada ou então, a decisão poderá ser através de sistemas autónomos (Fawkes & Menzel, 2018).

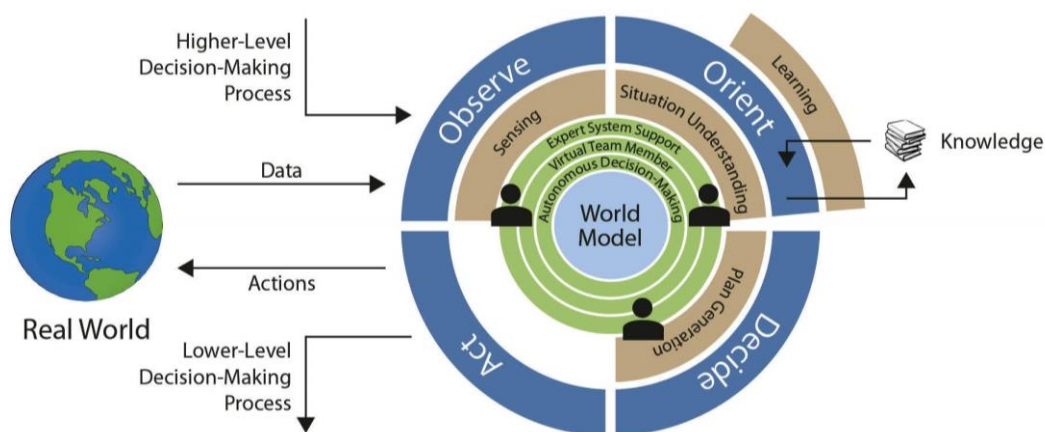


Figura 7 - Uma visão do OODA loop apoiado por IA

Fonte: Fawkes & Menzel (2018).

Na perspetiva de Sousa⁹ (entrevista presencial, 28 de dezembro de 2020), a globalização disponibilizou uma grande quantidade de dados e informação disponível nas fontes abertas, com relevância no processo de decisão. A superioridade de informação no processo de decisão é por via do nicho de países restritos que geram ou produzem conhecimento, ou através da competitividade dos que acedem aos 90 % dos dados e informação disponível em fontes abertas, perspetiva que requer uma abordagem digital.

5.2. Operações no, e através do, ciberespaço

O ciberespaço que foi reconhecido pela NATO (2016), na Cimeira de Varsóvia, como novo domínio operacional, é explorado por atores não estatais e estatais, como a intervenção da Rússia na Estónia, em 2007, ou presentemente na Ucrânia (Standard, 2022), levando à retaliação do grupo de hackers “Anonymous” (Tidy, 2022).

Na sequência da cimeira de Lisboa, onde a NATO elevou a segurança do ciberespaço a tarefas de Defesa Coletiva (2010), foi aprovada a Orientação Política para a Ciberdefesa (MDN, 2013), que valida a edificação desta capacidade, com três objetivos essenciais: (i) garantir a proteção, a resiliência, a segurança das redes e dos Sistemas de Informação e Comunicações (SIC) da DN contra ciberataques; (ii) assegurar a liberdade de ação do país no ciberespaço e, quando necessário e determinado, a exploração pró-ativa do ciberespaço para impedir ou dificultar o seu uso hostil contra o interesse Nacional; e (iii) contribuir de forma cooperativa para a Segurança Nacional. Nos termos da RCM n.º 92/2019, de 5 de junho, foi aprovada a Estratégia Nacional de Segurança do Ciberespaço, definindo a ciberdefesa como a atividade de assegurar a DN no, ou através do, ciberespaço (Conselho de Ministros, 2019).

⁹ À data da entrevista era Contra-almirante e desempenhava o cargo de Subchefe do Comando Operacional Conjunto para as Operações Militares (CCOM). Presentemente é Vice-almirante e é o Chefe do CCOM.

A NATO (2018b) classifica as operações no ciberespaço em operações de infraestrutura, defensivas, exploração (informações, vigilância e reconhecimento) e ofensivas, enquadradas como passivas ou ativas, conforme a sua tipologia (Figura 8). Contudo, apenas realiza operações na própria rede ou em redes abertas, reconhecendo a possibilidade das restantes operações serem realizadas pelas próprias nações.

Portugal, assumiu a possibilidade de realizar todo o espectro de operações no ciberespaço (defensivas, exploração e ofensivas) (MDN, 2013), podendo ser reforçado com todos os meios para responder a ciberataques, incluindo a capacidade ofensiva (Conselho de Ministros, 2019). As operações de infraestruturas estão descentralizadas nos núcleos de *Computer Incident Response Capability* (CIRT) (Marinha, 2018c, p. 53).

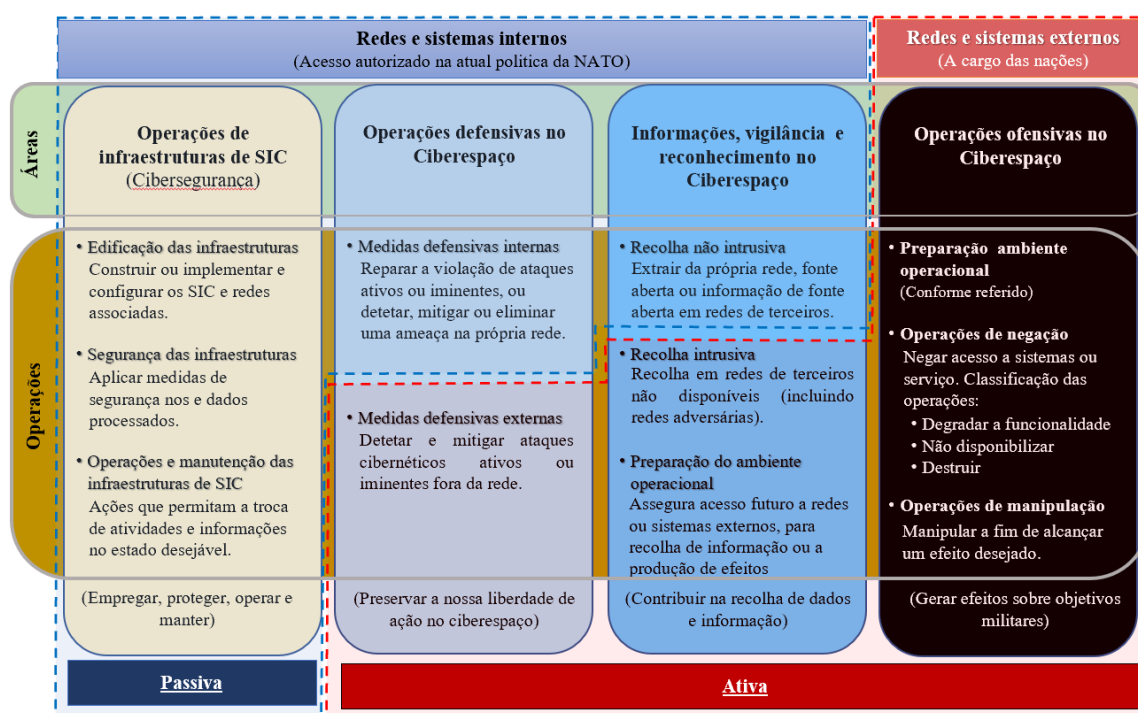


Figura 8 - Taxonomia das operações no ciberespaço

Fonte: Adaptado a partir de NATO (2018b) e Nunes (2020) (cit. por Alves, 2021) .

O ciberespaço pelo potencial disponível, constitui-se um elemento diferenciador nas FFAA, desde que seja amplamente explorado e disponha dos recursos humanos e tecnológicos adequados, pois além dos efeitos alcançados, também é o grande catalisador para se obter a superioridade de informação, pois é nele que circula a maioria dos dados e informação, contribuindo decisivamente para o processo de decisão.

A nova conflitualidade assenta em tecnologias disruptivas, tendendo a encurtar a duração dos conflitos de natureza assimétrica e de carácter híbrido, explorando a produção síncrona de efeitos em todos os domínios, através de meios cinéticos e não cinéticos, privilegiando o ciberespaço. Tem havido uma convergência das atividades de guerra



eletrónica com o ciberespaço¹⁰, para alcançar a vantagem operacional, como foi o caso na operação *Atlantic Resolve*, no flanco leste da Europa. Esta relação simbiótica está a ser aplicada em vários países para alcançarem a superioridade de informação e melhorar o processo de decisão (Willis & Stathopoulos, 2020).

Outra evolução neste domínio complexo é a utilização da IA, embora ainda não esteja tão desenvolvida quanto seria esperado, nomeadamente pela Rússia. Porém, é uma tecnologia que tem vindo a ser utilizada no atual conflito da Ucrânia, pelos ucranianos para reconhecimento facial dos agressores russos e identificação dos mortos, e pelos russos, nas campanhas de influência, com *deepfakes* e *bots* de desinformação (Tegler, 2022).

Embora a IA ainda esteja em desenvolvimento, é uma tecnologia essencial nas operações do ciberespaço, nomeadamente para melhorar a segurança e resiliência cibernética, identificação de *malwares* e de vulnerabilidades na rede, e nos sistemas adversários para eventual exploração através de um eventual ataque. Ainda, permite acelerar o processamento de grandes volumes de dados e o reconhecimento de padrões, na antecipação e combate de ameaças (Assis et al., 2020).

Em suma, a IA é um catalisador para explorar o ciberespaço, contribuindo para melhorar a superioridade da informação e o processo de decisão.

5.3. Comando e Controlo ágil

Face à evolução do espectro informacional assente maioritariamente no digital, dominado por um elevado volume de dados e informação no apoio à decisão, é requerido agilidade¹¹ na função de C2, para fazer face às mudanças de circunstâncias que exigem diferentes abordagens na decisão. Em resposta, a NATO (2014) desenvolveu o conceito “C2 Ágil”¹², definido pela capacidade de realizar, gerir e explorar com sucesso, as mudanças de circunstâncias, permitindo que entidades possam atempadamente empregar, com eficácia e eficiência, os recursos disponíveis. A abordagem ao C2 categoriza-se como os direitos de decisão são atribuídos (Alocação dos Direitos de Decisão [ADD]), como as entidades interagem (Padrões de Interação [PdI]) e como a informação é distribuída (Distribuição de Informação [DoI]), representados segundo um modelo de abordagem espacial (Figura 9).

Na prática estas dimensões são interdependentes, pois os direitos de decisão são alocados tendo em conta a influência sobre os padrões de interação e o fluxo informacional, na qual cada abordagem ao C2 ocupa uma região na abordagem espacial, que vão desde

¹⁰ Designadas na língua inglesa de *Cyber and Electromagnetic Activities* (CEMA).

¹¹ Capacidade de responder com sucesso à mudança.

¹² Na língua inglesa designado de “*Command and Control (C2) Agility*”.

posições centralizadas a descentralizadas. A NATO desenvolveu um modelo de maturidade de C2 da capacidade da rede, estabelecendo as seguintes abordagens:

- C2 em Conflito - Apenas há ligação dentro da respetiva equipa, sem que haja troca de informação ou interação entre si;
- C2 Descontrolado - Apenas os chefes comunicam entre si, permitindo uma partilha limitada de informação e interação entre si;
- C2 Coordenado - Interação para o coletivo das entidades participantes, visando aumentar a eficácia global ao procurar apoio mútuo para interação, desenvolvimento de relações e aumento de partilha de informação, de modo, a melhorar a qualidade da mesma;
- C2 Colaborativo - A comunicação é feita para fora do respetivo nível, com o objetivo de desenvolver sinergias;
- C2 Edge - Todos comunicam com todos (sistema de sistemas), exigindo uma compreensão partilhada em todo o processo de colaboração.

A representação gráfica destas abordagens de C2, segundo a NATO (*op. cit.*) enquadram-se numa diagonal, conforme os direitos de decisão atribuídos.

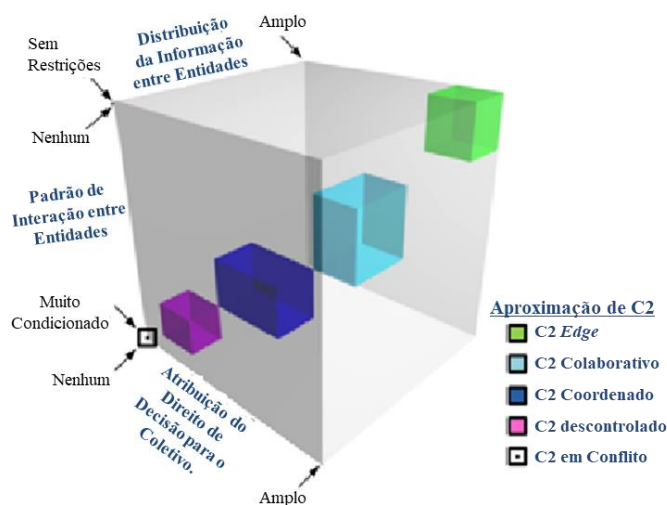


Figura 9 - Modelo de Abordagem de C2

Fonte: Adaptado a partir de NATO (2014, cit. por Alves, 2021).

A aproximação ao C2 estabelece a natureza do esforço, a relação entre os elementos e a instituição ou a força que os integra, bem como, a região informacional dos elementos, enquadrando-se no ciclo OODA conforme representado na Figura 10. Através do *sensemaking* é observado todo o meio envolvente, orientado o esforço face às alterações circunstanciais e tomadas decisões baseadas na melhor informação, ações que requerem a melhor abordagem de C2, conforme anteriormente referido. Segundo a NATO (*op. cit.*),

qualquer alteração pode influenciar a alteração de aproximação ao C2, influenciando o comportamento e moldando o conhecimento no processo de decisão.

O processo de *sensemaking* integra desde o individual ao coletivo (Figura 10), levando a que a decisão por um determinado tipo de abordagem de C2, determine a disponibilidade de informação e a natureza das interações, resultando a perceção, a compreensão e as decisões, como produtos do *sensemaking*. Sempre que sejam afetados os fluxos de informação, os direitos de decisão e o padrão de interação entre elementos, será afetada o tipo de aproximação de C2 e consequentemente, a natureza do conhecimento, da compreensão e das decisões adotadas, tanto a nível individual como coletivas. Qualquer ação afetada pela decisão de uma abordagem de C2, resulta em efeitos e com consequências diretas no mundo real, acabando por se constituir um processo dinâmico (NATO, 2007).

O C2 Ágil, é um conceito que contribui para o sucesso da missão, ao permitir que as entidades adotem abordagens mais apropriadas de C2 e ajustem as suas aproximações às alterações das circunstâncias e da missão.

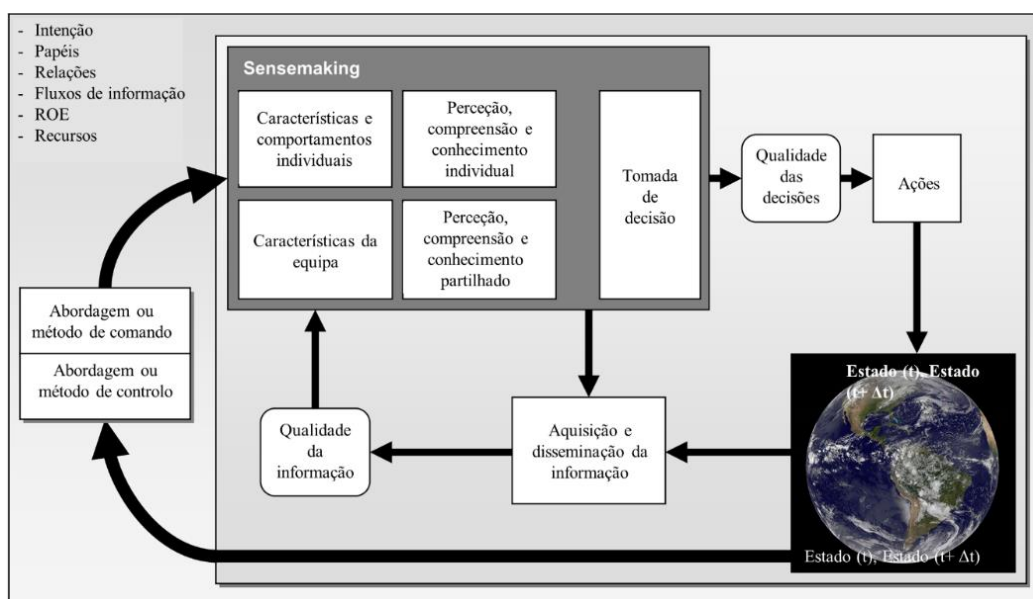


Figura 10 - Visão geral do modelo conceitual de C2

Fonte: Adaptado a partir de NATO (2014. cit. por Alves, 2021).

A integração da IA nos sistemas militares de C2 constitui-se uma estratégia das forças de defesa, embora ainda num processo em desenvolvimento. Contudo, já se vislumbra que traga um salto significativo na agilidade do C2 através da automatização. A par das oportunidades associadas, há desafios que poderão fragilizar o sistema de C2, resultando em falhas. Para as ultrapassar, a antifrágilidade¹³ com a agilidade, formam os princípios

¹³ A antifrágilidade é uma qualidade, ou característica, do sistema que permite não só ser robusto e resistente a ataques súbitos e fatores de stress, mas também aprender com estes fatores de stress para se aperfeiçoar da próxima vez que se deparar com eles (Simpson et al., 2021).

basilares da concepção dos sistemas de C2 que integram IA. Um estudo da Universidade de Cornell (Simpson et al., 2021), designa esta dualidade de *Agile, Antifragile, Artificial-Intelligence-Enabled, Command and Control* (A3IC2). Um sistema de A3IC2 (Figura 11) está sempre a melhorar o seu desempenho face a choques ou surpresas, através da sobrecompensação do *feedback* durante o ciclo de decisão, permitindo ao sistema sobreviver num ambiente operacional complexo, beneficiando com as dinâmicas da guerra.

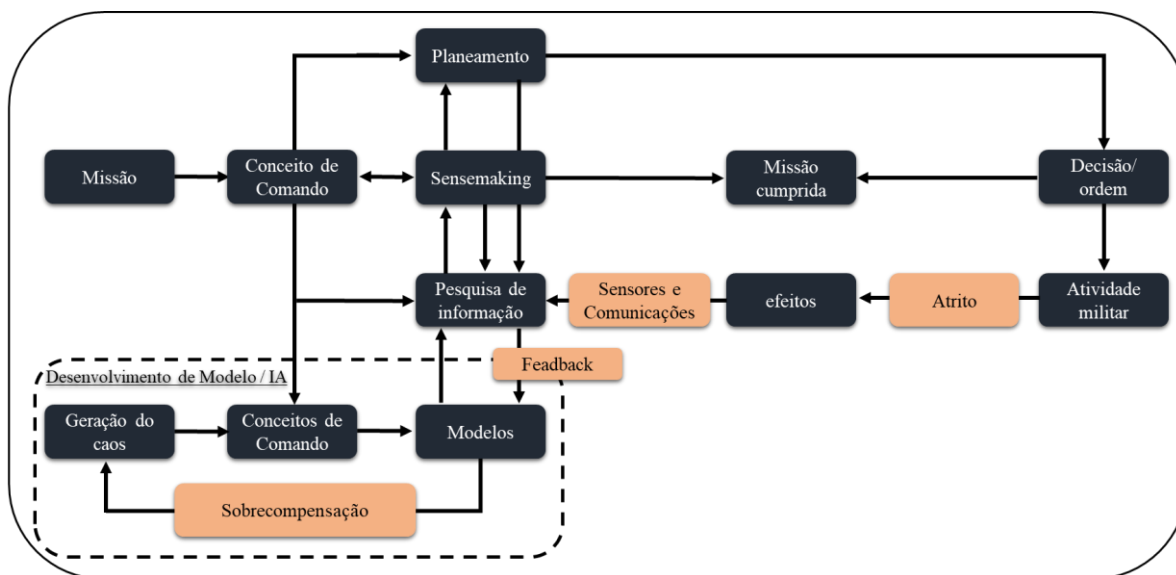


Figura 11 - Modelo de um sistema de A3IC2

Fonte: Adaptado a partir de Simpson et al. (2021).

5.4. Síntese conclusiva

A dinâmica do ambiente estratégico caracterizado pela abundância de dados e informação, requer uma abordagem mais tecnológica e digital, resiliente, capaz de integrar tecnologias emergentes no processo de decisão, de modo a conseguir obter a vantagem operacional. A par da necessidade da superioridade de informação é essencial alcançar a vantagem da informação, adaptando-se em tempo real às dinâmicas envolventes, mas também, uma abordagem agilizada de C2, descentralizando a decisão e a interação face a cada ambiente, contribuindo para um processo de decisão mais eficiente e eficaz.

Embora a IA seja uma tecnologia abrangente e ainda em desenvolvimento, está a ser promissora para alcançar a superioridade de informação e para acelerar, e agilizar a decisão nos diversos domínios, sendo o ciberespaço essencial na capacidade decisória.

Em resposta à QD2, conclui-se que a TDig na perspetiva operacional, assenta essencialmente numa decisão mais célere, ágil e eficaz, através da(s): (i) Superioridade de Informação; (ii) Operações no, e através do, Ciberespaço; e (iii) C2 Ágil.



6. Perspetiva estrutural da Estratégia digital

A perspetiva estrutural visa estabelecer a composição, organização e a articulação dos recursos materiais e humanos, que integram capacidades coerentes, interdependentes e colaborantes, através da inovação e sistemas de apoio à decisão, que facilitem a simplicidade, concentração, otimização, eficácia e eficiência, interoperabilidade e a racionalização de processos e recursos, assegurando o melhor desempenho dos processos de decisão e emprego dos meios (EMA, 2015b; A. Ribeiro et al., 2010).

As capacidades coerentes resultam de reajustes organizacionais e gestão de recursos humanos capazes, motivados e reconhecidos. As interdependentes resultam das qualificações e organização dos recursos humanos face à envolvimento. Por último, as colaborantes derivam dos processos informacionais no apoio à decisão e da cultura institucional desenvolvida (A. Ribeiro et al., 2010).

Face à contextualização desta perspetiva, que corresponde a uma organização capaz de maximizar e articular os recursos no emprego operacional, serão abordados no presente capítulo a liderança digital, enquadrada nas capacidades coerentes, as competências digitais, enquadradas nas capacidades interdependentes, e a otimização dos processos, enquadrados nas capacidades colaborantes, de modo a responder à QD3.

6.1. Liderança digital

A liderança define-se por um processo de influência do comportamento humano em determinado contexto, enquadrada numa realidade complexa e multivariada, devendo ser analisada de diferentes perspetivas e variáveis, nomeadamente a configuração organizacional, o ciclo de vida e a cultura das organizações (Rosinha, 2009). No contexto militar, a liderança difere pelas normas e valores que regem a instituição, e pela ação de comando conferida por lei a um indivíduo para dirigir, controlar e coordenar (Vieira, 2002).

A evolução do digital levou ao desenvolvimento do conceito de liderança digital assente na cultura, nas pessoas, nos processos e na tecnologia, paralelamente, norteadas pelo desenvolvimento e sustentação de uma cultura de inovação, assente na fruição de ideias, nas TI e numa arquitetura organizacional ágil (Tanniru, 2018).

A evolução tecnológica marcada por oportunidades e ameaças digitais provenientes da i4.0, levou a que determinados autores, passassem a designar por liderança 4.0, como uma liderança disruptiva com o modelo clássico, para uma liderança assente num sistema em rede, colaborativo, de gestão e de resposta rápida (Kelly, 2019). Segundo a Academia Militar (2019), assenta na incorporação de tecnologias de informação e comunicação de última geração, em novos modelos de negócio e desafios, em termos éticos e de segurança, bem

como em novos direitos e responsabilidades dos líderes, levando a modificações na liderança e ao surgimento de novas formas de liderar (Figura 12).



Figura 12 - Liderança digital

Fonte: Adaptado a partir de UOL EdTech (2020).

A nova ordem assenta em oportunidades e ameaças digitais, enquadradas num ecossistema em evolução e sobretudo por uma mentalidade e cultura digital, cada vez mais evidente na sociedade e concomitantemente no contexto militar. Por isso, é inevitável que este tipo de liderança não seja incluído no léxico militar em complementaridade ao modelo vigente, privilegiando o balanceamento dos diversos tipos de liderança no ambiente digital.

A par desta evolução do conceito de liderança, a implementação da TDig requer, segundo Marques (entrevista via *MicroSoft* [MS] Teams, 15 de março de 2021), um comprometimento ao mais alto nível, para garantir que haja uma mudança disruptiva, de modo a acompanhar a integração da tecnologia digital emergente.

Os resultados obtidos do questionário (*vide* Apêndice B), demonstraram pouca confiança na liderança e um conhecimento incipiente das iniciativas existentes, o que denota a falta de uma política de divulgação e de comunicação assertiva.

6.2. Competências digitais

Por definição, as competências digitais integram o conjunto de conhecimentos, capacidades, proficiências, estratégias e atitudes para utilizar as tecnologias e meios digitais (INCoDe.2030, 2019). As competências digitais são essenciais para a criação da cultura digital nas organizações, facilitando a liderança digital referida anteriormente, além de ser essencial para aproveitar as oportunidades e mitigar os riscos. Face à sua relevância neste

processo, constitui o primeiro pilar do *Plano de Ação para a Transição Digital*, designado de “Capacitação e Inclusão Digital das Pessoas”, articulado em: educação digital; formação profissional e requalificação; e inclusão e literacia digital (PCM, 2020).

A UE tem vindo a desenvolver quadros de referência para os cidadãos no espaço europeu. Contudo, a dinâmica da evolução das tecnologias digitais, tem levado a constantes atualizações, definindo-se um quadro de competências (Figura 13), articulado em: (i) literacia de dados e informação; (ii) comunicação e colaboração; (iii) criação de conteúdos digitais; (iv) segurança; e (v) resolução de problemas. Complementarmente, estabeleceu níveis de proficiência ligados às competências, subjacente à complexidade de cada tarefa, problema e nível de autonomia, permitindo a avaliação do nível para entrar num processo de qualificação ou requalificação, destacando-se nesta atualização, a confiança e a segurança com tecnologias digitais que integram a IA (CE, 2022).

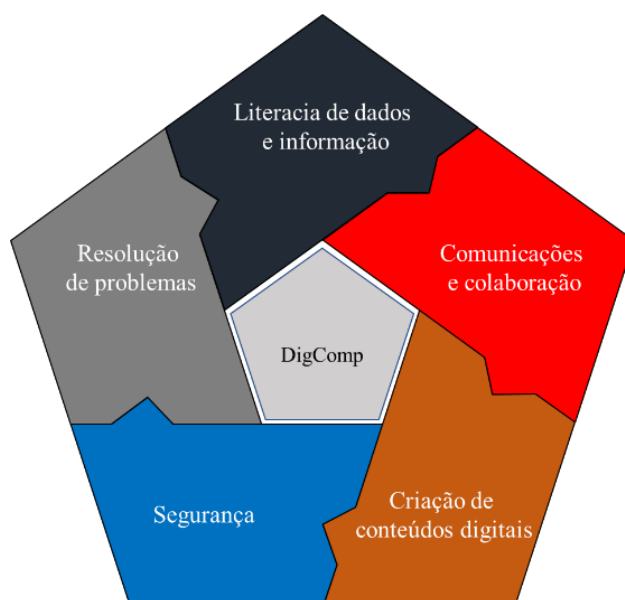


Figura 13 - Quadro de competências digitais

Fontes: Adaptado a partir de CE (2022).

Face à prioridade nacional, a “Iniciativa Nacional Competências Digitais e.2030” (INCoDe.2030) desenvolveu um quadro de competências, assente no quadro europeu, com a seguinte organização: (i) literacia de informação; (ii) comunicação e cidadania; (iii) criação de conteúdos; (iv) segurança e privacidade, e (v) desenvolvimento de soluções.

Segundo Marques (*op. cit.*), o desenvolvimento de competências digitais requer uma avaliação prévia do nível de conhecimentos de cada elemento da instituição, à semelhança



do Exército Americano (Mobley, 2011), para delinear programas de *upskillings*¹⁴, norteados pela visão da organização, tendo em conta a evolução tecnológica.

Naturalmente, a evolução da sociedade está a desenvolver as apetências dos cidadãos para o atual ecossistema verificando-se a tendência para acompanhar esta evolução.

6.3. Otimização de processos

Por definição, os processos são atividades interrelacionadas ou interatuantes que utilizam entradas para disponibilizar um resultado pretendido (NP EN ISO 9000, 2015), constituindo a base da organização da cadeia de valor organizacional e classificando-se em: (i) processos primários, são interfuncionais, ligados ao produto organizacional; (ii) processos de suporte, são aqueles que estão designados para apoiar os primários; e (iii) processos de gestão, designados para medir, monitorizar e controlar (Bilodeau et al., 2013, p. 60).

Presentemente, o défice de recursos humanos nas FFAA e a evolução tecnológica, assente no digital, leva a que haja uma necessidade de repensar os processos da instituição. Segundo Solis (2019, p. 16), cerca de 28% das organizações estão a financiar iniciativas de transformação, incidindo na modernização de processos.

A superioridade de informação requer cada vez mais uma abordagem holística e sistémica, assente na gestão por processos, como fator potenciador na disponibilidade da informação, condição imperativa para alcançar posições sustentadas de vantagem no processo de decisão. Para tal, torna-se necessário ter uma perceção do estado atual dos processos, de modo a conseguir-se definir quais os processos do futuro, e a forma de como os alcançar.

Para tal, numa primeira instância, os processos devem ser mapeados, identificando as atividades e os processos que podem ser operacionalizados recorrendo a tecnologia inovadora e apropriada. A modelação dos processos implementados e análise dos mesmos, permite igualmente, identificar quais os processos que necessitam de ser repensados, com foco no alinhamento do processo de ponta-a-ponta e na mudança das funções, dos processos, da organização, dos dados, das métricas e da tecnologia da organização, de acordo com os objetivos estratégicos e as necessidades da organização (Transformação dos Processos). Esta transformação de processos permite obter melhorias na eficácia e na eficiência, e principalmente no aumento significativo e mensurável do valor, assegurando igualmente, a conformidade com os diversos normativos (interno e externo) a que as organizações estão obrigados a cumprir (e.g. Regulamento Geral de Proteção de Dados) (Regulamento (UE)

¹⁴ Processo de elevar técnicas para outro nível, através de programas formativos para melhorar o nível de conhecimento numa determinada área do saber.

2016/679 do Parlamento Europeu e do Conselho de 27 de abril, 2016). Neste âmbito, foram realizados alguns projetos através do programa SIMPLEX, entre as quais, o Sistema Integrado de Gestão da Defesa Nacional (SIGDN), o Sistema de Informação de Avaliação do Mérito dos Militares das Forças Armadas, a Identificação Digital da Defesa e a Secretaria Virtual.

Esta transformação requer uma aproximação holística e sistémica, baseada numa abordagem estruturada, desde a conceção dos processos, orientados para o produto organizacional e alinhados com os objetivos estratégicos. Requer, igualmente, uma gestão disciplinada, que defina ações específicas, por objetivo estratégico e com métricas apropriadas de avaliação, e uma segmentação adequada de processos, para que haja uma abordagem diferenciada da conceção e da implementação. Qualquer modelo que seja desenvolvido durante a conceção deverá refletir os requisitos desses segmentos do processo, alinhados com os objetivos estratégicos respetivos da organização, mas também, o nível de ambição a alcançar. Os processos no final devem assentar na transparência, permitindo melhorar a qualidade, eficiência, agilidade, conformidade, integração externa e alinhamento interno, assim como, a inovação e a conservação (*Association of Business Process Management Professionals* [ABPM], 2019, p. 52).

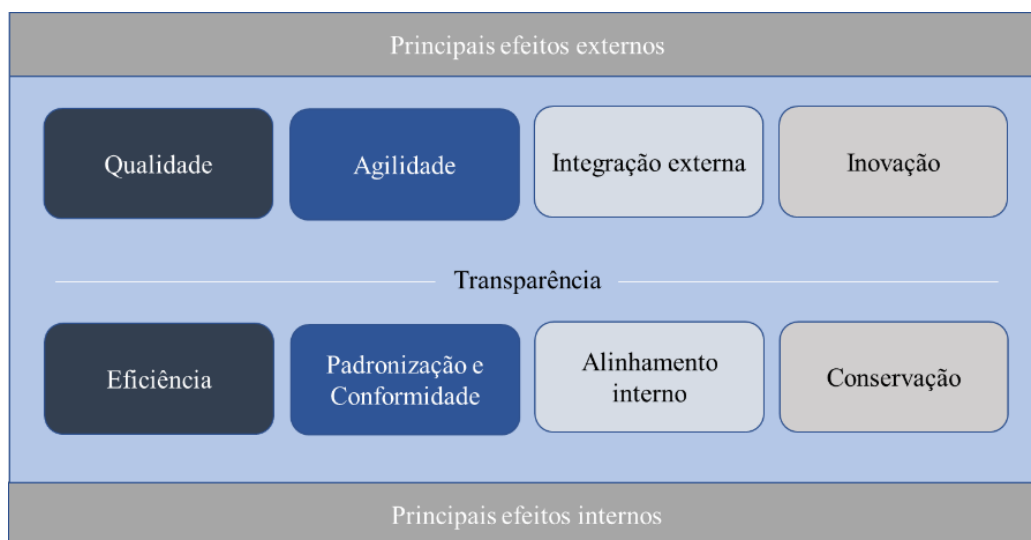


Figura 14 - Fatores de confiança dos processos

Fonte: Adaptado a partir de ABPMP (2019).

A evolução tecnológica no ecossistema digital atual e emergente, requer cada vez mais uma abordagem digital e automatizada, reduzindo os recursos humanos em atividades que podem ser robotizadas, redirecionando-os para atividades operacionais.

Na sequência da modelação e análise dos processos, serão identificados, entre outros parâmetros citados anteriormente, os requisitos da tecnologia necessária à otimização dos

mesmos. A evolução tecnológica tende cada vez mais, para a integração de sistemas semiautónomos e autónomos, para a gestão de tarefas repetitivas, reduzindo a intervenção humana e aumentando a eficiência.

Assim sendo, a evolução tende para sistemas, como o *Robotic Process Automation* (RPA) que integra tecnologias cognitivas, como o ML e o Processamento de Linguagem Natural (PLN), permitindo automatizar tarefas complexas que anteriormente requeriam a perceção e o julgamento humano (ABPMP, 2019). Estes robôs de software também realizam cálculos complexos e a tomada de decisões, assente em dados e em regras pré-definidas, permitindo reduzir os custos e riscos, bem como, melhorar a aprendizagem, contribuindo para a TDig (Deloitte Portugal, 2022; Madakam et al., 2019).

No caso do RPA são percecionados diversos benefícios, nomeadamente: maior qualidade e rigor, análises melhoradas, redução de custos, maior velocidade, versatilidade, simplicidade, escalabilidade, economia de tempo, não-invasivo, melhor gestão e serviço, e maior satisfação, além de maior disponibilidade (Madakam et al., 2019). Embora o RPA seja a primeira fase da robotização, ao juntar as capacidades de aprendizagem, obtém-se soluções capazes de simular a interação e a capacidade de decisão humana (Deloitte Portugal, 2022).

A gestão por processos numa organização é cada vez mais inteligente e avançada, prevendo-se que venha a apoiar todo o espectro da automatização do trabalho: estruturada, cognitiva, e apoiada pela IA, através de uma gestão dinâmica de casos para gerir o trabalho *ad hoc*, disponibilizando um modelo mais eficiente (Figura 15).

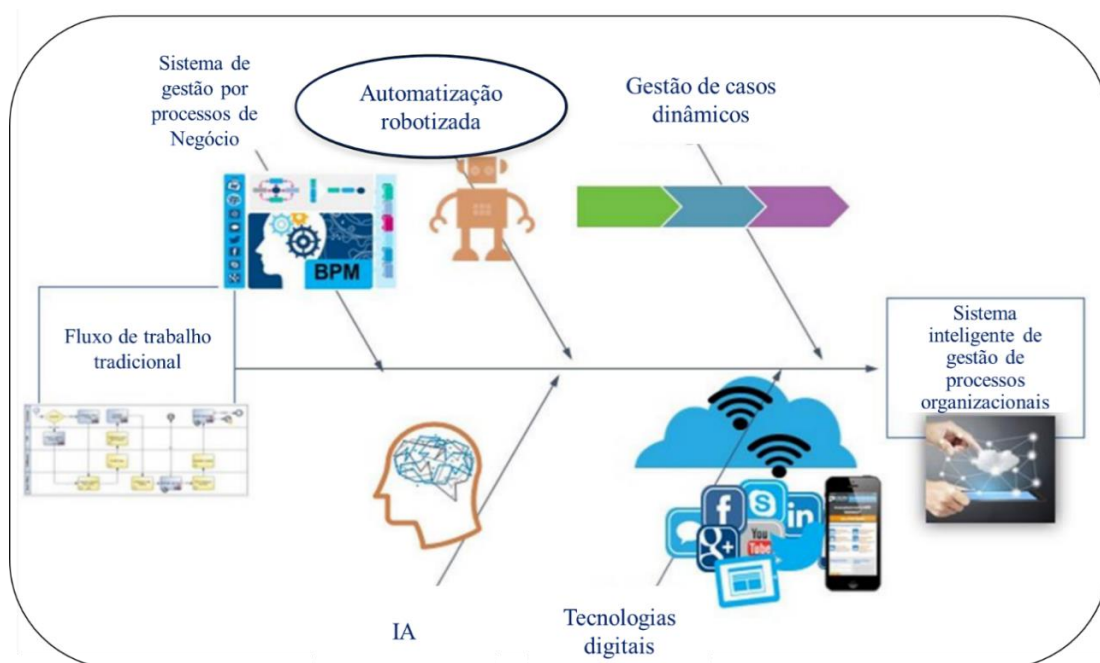


Figura 15 - RPA em sistemas inteligentes de processos organizacionais

Fonte: Adaptado a partir de ABPMP (2019).



Assim sendo, a evolução tecnológica assente no digital, requer cada vez mais uma gestão por processos, incorporando uma abordagem digital, através de tecnologias disruptivas, procurando cada vez mais a automatização dos processos possíveis, reduzindo os recursos humanos em tarefas que podem ser robotizadas e contribuindo para a decisão mais célere e mais bem informada.

6.4. Síntese conclusiva

A articulação entre uma liderança digital e a aquisição de competências digitais sólidas, são essenciais para desenvolver a literacia e a cultura digital assente em tecnologias inovadoras na instituição militar, de modo a facilitar uma abordagem mais digital, mais automatizada e menos burocrática nos processos, apoiando as decisões com disponibilidade de informação oportuna.

Esta abordagem permite reduzir os recursos humanos neste tipo tarefas e potencializá-los para tarefas operacionais, otimizando os recursos através de uma abordagem assente na eficiência.

Em resposta à QD3, consideram-se as seguintes orientações estruturais para um melhor desempenho dos processos de decisão e atuação dos meios: a liderança digital (contribui para a maneira de pensar e agir do pessoal); as competências digitais (aumento de literacia digital do pessoal através da formação); e a otimização de processos (promovendo a automatização e a simplificação dos processos através de uma abordagem com uma grande componente digital).



7. Perspetiva genética da Estratégia digital

A perspetiva genética estipula o planeamento e a edificação de capacidades conjuntas e interoperáveis, necessárias ao planeamento, direção e controlo do emprego das FFAA (EMGFA, 2021), devendo ser integráveis para melhorar o nível digital nas operações.

As capacidades conjuntas resultam da junção dos meios de cada Ramo, em vez de resultarem do seu planeamento e desenvolvimento de raiz. Contudo, é essencial estabelecer relações em rede que permitam uma maior articulação, cooperação e colaboração entre os Ramos (Moreno, 2021). As capacidades interoperáveis resultam da capacidade de atuar em conjunto ou combinado, com coerência, eficácia e eficiência, para alcançar os objetivos táticos, operacionais e estratégicos (NATO, 2019a). As capacidades integráveis decorrem da incorporação tecnológica e da adoção de uma atitude experimental e inovadora, face à escolha, de soluções técnicas sofisticadas nos aspetos relacionados com a investigação, o desenvolvimento de conceitos, a experimentação, a formação e o treino (Ribeiro, 2008).

Face ao exposto, neste capítulo serão analisadas as seguintes capacidades: a de governação e gestão da arquitetura organizacional, contribuindo para a perceção das capacidades interoperáveis e integráveis; a de governação e gestão integrada de dados e informação, enquadrada nas capacidades conjuntas; e a interação homem-máquina, enquadrada nas capacidades integráveis e interoperáveis, nomeadamente no desenvolvimento de conceitos e experimentação, contribuindo para responder à QD4.

7.1. Capacidade de governação e gestão da arquitetura organizacional

A arquitetura organizacional assenta na análise, na conceção, no planeamento e na organização, através de uma abordagem de engenharia holística na implementação de estratégias, de modo a apoiar no desenvolvimento de soluções orientadas para a satisfação das necessidades em alinhamento com as orientações estratégicas (NATO, 2018c).

A gestão da arquitetura visa estabelecer e manter orientações coerentes, princípios e regimes de governação, que norteiam e apoiam no desenvolvimento da conceção e da estrutura, orientada para alcançar a visão e os objetivos estratégicos (Ahlemann et al., 2012).

Este modelo permite melhorar o desempenho organizacional, planeando a transição de uma determinada capacidade ao longo do seu ciclo de vida; garantir a flexibilidade, a adaptabilidade e a capacidade de adquirir sistemas multinacionais de apoio às operações; melhorar a compreensão e mitigação dos riscos; garantir o alinhamento de processos e tecnologia, articulada com as prioridades; e melhorar a comunicação dentro dos domínios técnicos e entre os utilizadores (NATO, 2018c).

Numa perspetiva holística, a arquitetura assenta no *blueprint*¹⁵ para responder aos processos de negócio¹⁶; nos dados recolhidos, gerados e analisados; nas aplicações necessárias no apoio do processo e a necessidade de dados; e nas tecnologias necessárias.

Para facilitar a compreensão, o modelo original de Zachman (Figura 16) e de referência, assenta em quatro domínios interdependentes: arquitetura de Negócio (capacidades que refletem a visão das funções e processos), arquitetura de Dados e Informação (normas que orientam e definem a recolha e gestão de dados), arquitetura Aplicacional (define aplicações e métodos de distribuição da informação) e arquitetura Técnica (define o hardware e software necessário e adequado) (Pereira & Sousa, 2004).



Figura 16 - Relação de arquitetura

Fonte: Adaptado a partir de Pereira & Sousa (2004).

Embora existam diferentes quadros conceptuais de arquiteturas organizacionais, designados por *frameworks*, para relacionar os processos organizacionais, todas começam com uma estratégia e têm objetivos organizacionais, seguidas da sequência de negócio, dados, aplicações e tecnologia, estando cada um destes, alinhado com o precedente na sequência, de modo a responder às seguintes questões: Porquê? (propósito); Quando? (período); Como? (processo); O quê? (*output*); Quem? (pessoa ou regra); e onde? (local ou facilidade). Assim sendo, a Figura 17 ilustra o fluxo dos princípios básicos partilhados, que integram qualquer *framework*. Existem diversos *frameworks*, destacando-se o de Zackman, o NATO *Architecture Framework* (NAF), o DoD *Architecture Framework* (DoDAF) e *The Open Group Architecture Framework* (TOGAF).

¹⁵ Plano que define a estrutura e o funcionamento para alcançar os objetivos atuais e futuros com eficácia.

¹⁶ Atividades organizacionais, parcialmente ordenadas, a realizar para alcançar um resultado desejado na prossecução de um determinado objetivo de uma organização (ISO/IEC/IEEE 24765:2017(en), 2017).

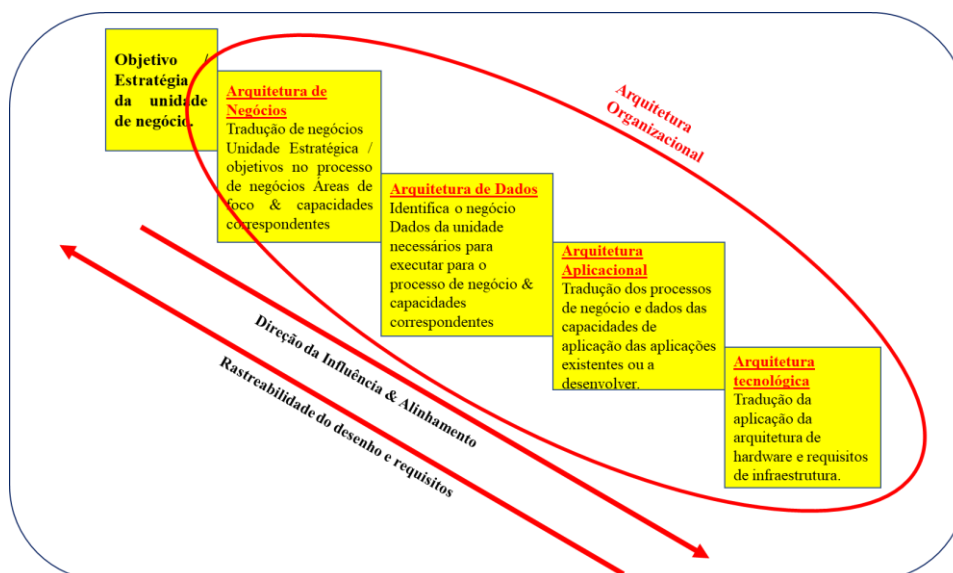


Figura 17 - Alinhamento da arquitetura organizacional

Fonte: Adaptado a partir de ABPMP (2019).

Esta capacidade é fundamental para garantir o mapeamento, alinhamento e manutenção, face à visão, avaliando necessidades, estabelecendo prioridades e mitigando riscos, contribuindo para a interoperabilidade e integração da tecnologia como um todo.

No caso específico das FFAA, denota-se que a arquitetura Aplicacional e a arquitetura Técnica têm componentes que são transversais ao EMGFA e aos Ramos, que poderiam ser integradas numa gestão comum, e tem outras componentes que, face à especificidade, devem ter uma gestão específica, contribuindo para uma melhor eficiência (Figura 18).

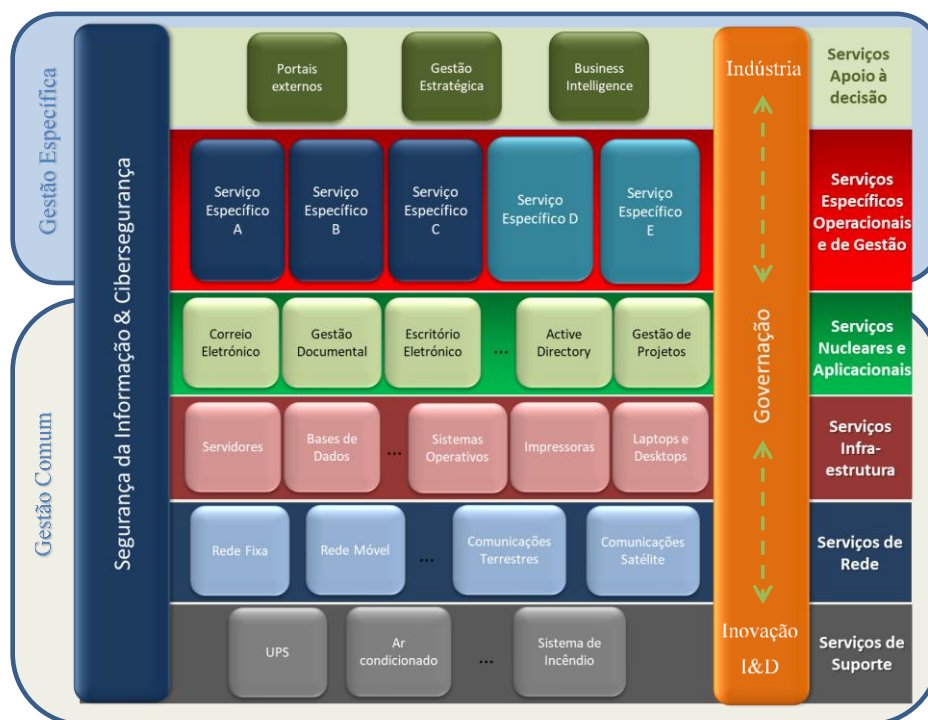


Figura 18 - Modelo de arquitetura Aplicacional e Técnica

Fonte: Adaptado a partir de Marques (2021, cit. por Alves, 2021).

Em suma, a arquitetura organizacional permite garantir um alinhamento de necessidades orientadas para a visão e objetivos organizacionais, articulando-se em quatro arquiteturas, a de Negócio que abrange os processos, desenvolvido no capítulo anterior, a de dados ainda a desenvolver, e a Aplicacional e a Técnica conforme foi apresentado.

7.2. Capacidade de governação e gestão integrada dos dados e informação

Os dados são factos não contextualizados, com um valor estratégico incalculável, constituindo-se a base da pirâmide do conhecimento¹⁷. Assim, as tecnologias dependem da qualidade¹⁸ dos dados, que permite sustentar uma decisão mais rápida e mais bem informada.

A gestão dos dados traduz-se no desenvolvimento, execução, supervisão de planos, políticas e programas que entregam, controlam, protegem e potenciam o seu valor ao longo do ciclo de vida, enquanto que a governação consiste em processos, políticas, organização e tecnologias para gerir e assegurar a disponibilidade, usabilidade, integridade, consistência, auditoria e segurança dos dados (*Data Management [DAMA] International*, 2017).

Contudo é essencial dispor de uma estratégia ou normativo que estabeleça orientações de armazenamento e gestão de dados, devendo integrar áreas do conhecimento para desenvolver, realizar e supervisionar planos, políticas, programas e práticas que forneçam, controlem, protejam e aumentem o valor ao longo do seu ciclo de vida (Figura 19).



Figura 19 - Estrutura da gestão de dados

Fonte: Adaptado a partir de *Data Management International* (2017).

¹⁷ É a hierarquia que modela os conceitos usados na gestão da informação e do conhecimento, organizados em dados, informação, conhecimento e sabedoria, relacionando-os entre si.

¹⁸ É uma medida de desvio de um resultado esperado, ou seja, quanto menor for a diferença, melhor os dados satisfazem as expectativas, logo melhor é a qualidade dos dados (DAMA, 2017, p. 531).

Presentemente, existem vários fatores que forçam a edificação desta capacidade (*Department of National Defence and Canadian Armed Forces [DND&CAF], 2019*):

- Abrangência dos conflitos integrados num ambiente multidomínio;
- Volume e a diversidade de dados veiculados por meios militares;
- Tecnologias disruptivas dependentes de dados com elevada qualidade;
- Análise quantitativa e qualitativa na medição de resultados;
- A competitividade requer melhor otimização da despesa, através de tecnologias que promovam a vantagem com maior eficiência.

Segundo Boris Johnson (MoD, 2021), “os vencedores do futuro serão aqueles que forem capazes de dominar os dados e as novas tecnologias”, situação compreendida na nova ordem.

O Departamento de Defesa dos EUA considera os dados um bem estratégico e valioso que permite alcançar a vantagem sobre qualquer adversário, através de decisões céleres e melhores informadas, estando na base da i4.0, nomeadamente na IA (2020).

A IA não passa de algoritmos desenvolvidos com base em dados de qualidade, que se divide em dois tipos: inteligência artificial geral, para fazer referência ao pensamento da máquina como pessoa e para fazer coisas semelhantes aos humanos; e a inteligência artificial estreita para fazer referência à utilização da máquina para tarefas muito específicas, tais como, automatização de processos ou atividades específicas nesse processo. No sentido lato, a IA decompõe-se em ML e esta em DL (Figura 20).

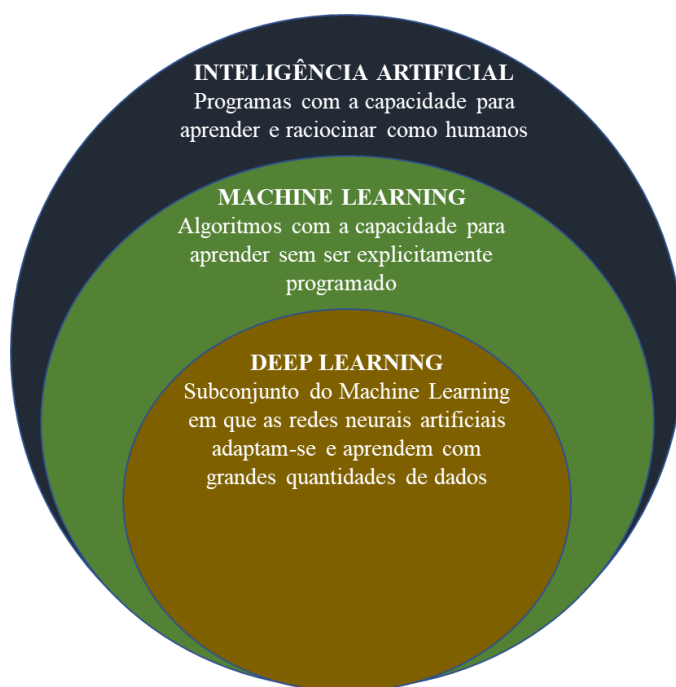


Figura 20 - Relação entre IA, ML e DL

Fonte: Adaptado a partir de ABPMP (2019).

Embora a IA assenta no desenvolvimento de algoritmos treinados, baseados na qualidade dos dados disponibilizados, pode evoluir para um processo de autoaprendizagem e de constante evolução, através de processos, procedimentos, regras e técnicas que assegurem a qualidade, a gestão e a exploração dos dados (Figura 21).

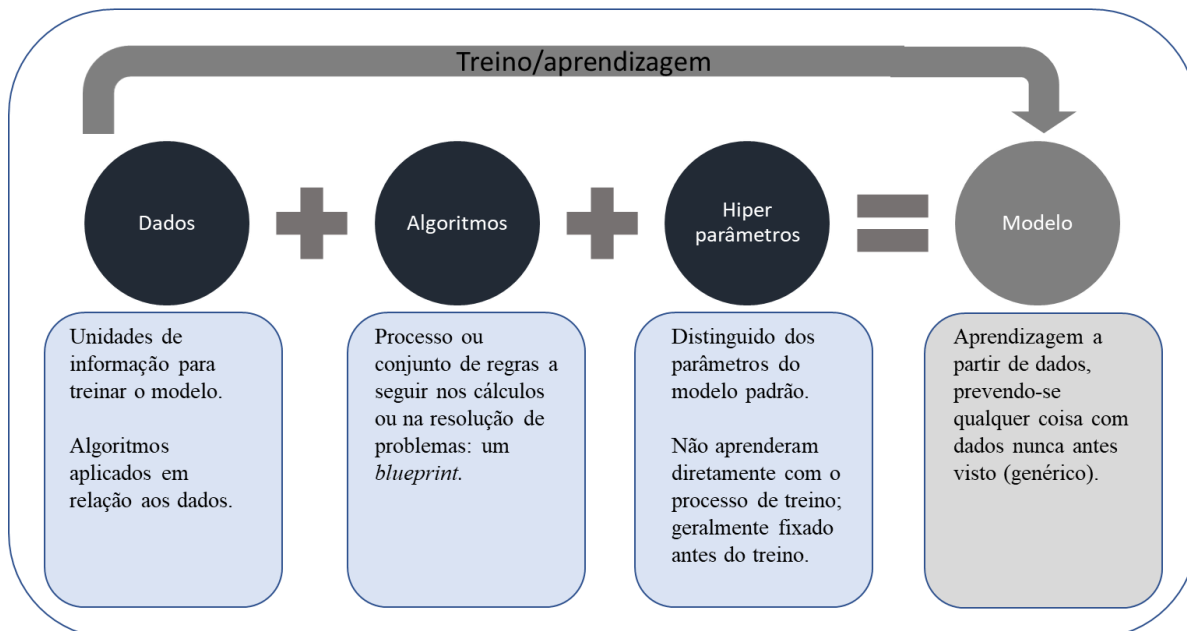


Figura 21 - Relação entre modelos e algoritmos

Fonte: Adaptado a partir de ABPMP (2019).

No contexto da defesa, a qualidade dos dados permite potencializar o emprego de tecnologias no contexto operacional, destacando-se alguns exemplos (DND&CAF, 2019):

- *Business intelligence* e *analytics* em apoio ao planeamento e à decisão;
- Análise avançada no apoio à área logística e na elaboração de doutrina;
- *Digital Twin* e realidade virtual no apoio da formação e do treino;
- A IA na automatização de tarefas repetitivas;
- Realidade aumentada, como exemplo, para a navegação durante as operações;
- Veículos autónomos (e.g. *drones*) e robótica, como exemplo, para a vigilância;
- Manufatura de produtos aditivos, ou seja, Impressão Tridimensional (3D);
- Biometria para identificar pessoas (e.g. impressões digitais, pela retina ou voz);
- *Intelligence Mission Data* permite aumentar o espectro de capacidades de combate das plataformas;
- IoT na aquisição, troca e trabalho com base de dados;
- *Blockchain* na segurança do armazenamento ou gestão de abastecimentos.

A evolução tecnológica tende a substituir a computação convencional pela quântica, baseada em energia quântica, permitindo ultrapassar limitações da computação clássica,

como, a capacidade de processamento e armazenamento, que condiciona o uso de IA avançada.

A evolução demonstra algumas tendências de substituição gradual de humanos por máquinas, primeiro nas tarefas repetitivas e conforme a tecnologia vai sendo aprimorada, vai substituindo, gradualmente, os humanos nos processos de decisão. Porém, ainda há algum ceticismo quanto a questões legais e éticas no uso indiscriminado da IA para sistemas semiautónomos ou autónomos. Embora a China e a Rússia sejam menos sensíveis a este tipo de questões, a NATO assumiu que a IA deve obedecer a seis princípios: legalidade; responsabilidade e responsabilização, explicação e rastreabilidade, confiabilidade, governabilidade; e mitigação de enviesamentos (2021b). A UE considera que a IA de confiança deve ser legal, ética e sólida, do ponto de vista técnico e social. Em termos éticos deve obedecer a quatro princípios: respeito pela autonomia humana, prevenção, equidade e explicabilidade (transparência) (CE, 2019).

7.3. Capacidade de interação homem-máquina

Os EUA consideram o conceito de julgamento humano o que melhor compreende a relação homem-máquina ao longo do desenvolvimento e emprego de um sistema, sem que seja limitado ao momento da decisão do seu emprego contra um alvo, situação que ainda consideram um conceito ambíguo que requer alguns ajustes. O Ex-Secretário da Defesa, Ashton Carter, reiterou, a par da IA, a importância da interação homem-máquina, como forma de manter a superioridade contra as nações mais poderosas (Morgan et al., 2020).

Neste âmbito, os EUA têm implementado este conceito no sentido de explorar os avanços tecnológicos para superar os dos potenciais adversários, nomeadamente os sistemas de *Anti-Access and Area Denial* (A2AD), contribuindo para manter a superioridade enquanto potência militar. Esta interação aplica-se a sistemas que vão desde a utilização de exoesqueletos, apoiando no desempenho físico e provendo de proteção balística até à colaboração e resolução coletiva de problemas complexos (Winkler et al., 2019).

No campo da investigação, o termo “máquina” está associado a dispositivos de controlo para situações dinâmicas e complexas, enquanto que as atividades humanas estão orientadas para as decisões, monitorização, deteção, antecipação e recuperação de falhas (Boy, 2011).

Os programadores tendem a classificar a interação homem-máquina sob três categorias distintas: (1) “*Human-in-the-loop*” quando o operador tem de tomar uma decisão positiva para eventual emprego contra um alvo, ou seja, neste caso o sistema de arma consegue observar e orientar de forma autónoma, logo que encontre e identifique alvos opositores,

colocando-os em espera e aguardando a decisão humana (sistema semiautónomo); (2) “*Human-on-the-loop*” quando o operador monitoriza a situação, mantendo a capacidade de prevenir ou interromper o ataque, ou seja, um sistema de armas pode encontrar, identificar e ser empregue contra alvos sem interação humana (sistema autónomo sob supervisão); (3) “*Human-out-of-the-loop*” quando o operador não tem qualquer capacidade de intervenção no emprego do sistema de arma (sistema totalmente autónomo) (Morgan et al., 2020).

Porém, há implicações legais e morais significativas que condicionam o emprego de sistemas autónomos, preferindo os que são controlados pelos humanos. Em termos tecnológicos é uma questão de configuração dos sistemas, sem que haja diferenças entre os sistemas tecnológicos. Contudo, importa realçar que a tendência da evolução tende para sistemas totalmente autónomos, nomeadamente em casos que o *OODA loop* é demasiado rápido para que um ser humano consiga intervir em tempo oportuno (Morgan et al., 2020).

No entanto, o problema centra-se na confiança do processo de interação (Figura 22), caracterizada pela interdependência entre um administrador e um utilizador, como se dependessem reciprocamente das características de cada indivíduo e da interação entre eles, tendo o administrador qualidades e o utilizador apetência para confiar nelas, gerando uma relação de confiança, enquadrado no princípio da confiança (Celaya & Yeung, 2019).

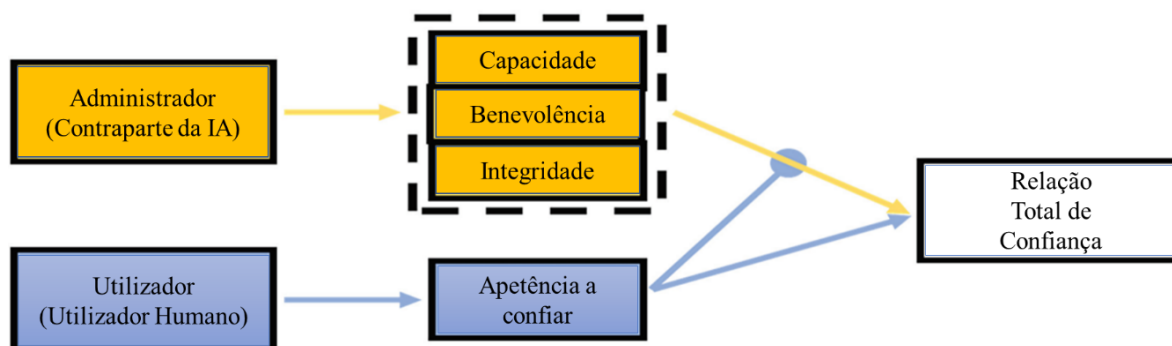


Figura 22 - Modelo de confiança Homem-Máquina

Fonte: Adaptado a partir de Celaya & Yeung (2019, cit. por Alves, 2021).

A vantagem militar tende para uma integração eficaz de humanos, IA e robótica nos sistemas de combate, designado por interação homem-máquina, explorando as capacidades das pessoas e das tecnologias para conseguir alcançar a superioridade (MoD, 2018a).

O desenvolvimento da IA e da robótica requer um investimento numa estratégia agressiva de experimentação interativa, prototipagem, desenvolvimento de conceitos e tecnologias, e aperfeiçoamento na organização, que permita a compreensão dos pontos fortes e fracos, bem como, limitações críticas de tais sistemas, de modo a aperfeiçoar uma melhor compreensão destas tecnologias e das necessidades futuras das FFAA (MoD, 2018a).



Segundo Moreira (2021), a Defesa deverá salientar-se na “...procura e implementação de abordagens holísticas, de novas medidas e iniciativas, o que constitui uma oportunidade para promover a renovação, evolução e modernização das FFAA, ajustadas às ameaças e aos desafios...”. Segundo Tendeiro (entrevista via e-mail, 17 de novembro de 2020), a inovação não é apenas liderada pelas nações maiores, pois esta deve ter uma abordagem coletiva. Assim sendo, esta é uma área em que as FFAA podem ser diferenciadoras, permitindo explorar e desenvolver a capacidade de interação homem-máquina através da ID&I.

7.4. Síntese conclusiva

Na perspetiva genética, a estratégia digital deve assentar em capacidades conjuntas, interoperáveis e integráveis, essenciais para melhorar o nível digital nas operações. Na lógica deste corolário, articulou-se o capítulo na capacidade de governação e gestão da arquitetura organizacional, na capacidade de governação e gestão integrada de dados e informação, e na capacidade de interação homem-máquina, de modo a contribuir na resposta de um ambiente operacional cada vez mais volátil, incerto, complexo e ambíguo, através de uma abordagem assente na tecnologia digital.

Assim sendo, a capacidade de governação e gestão da arquitetura organizacional, permite integrar a organização de diversas perspetivas, identificando as necessidades tecnológicas, os benefícios e os riscos dessas necessidades na organização, ou seja, contribui para uma gestão integrada, face à visão e aos objetivos da organização.

A governação e a gestão integrada de dados e informação contribuem para a racionalização de dados de qualidade para o desenvolvimento de algoritmos de IA no desempenho de tarefas repetitivas, contribuindo para a superioridade de informação e para um processo de decisão mais célere e eficaz. Porém, os algoritmos de IA são essenciais na automatização do conflito face à evolução do ambiente operacional.

Por último, a interação homem-máquina, é uma das capacidades emergentes na nova conflitualidade, dependente essencialmente da IA. Embora, este conceito não seja particularmente novo, apenas agora está em desenvolvimento, mas muito dependente da ID&I, num ambiente cada vez mais colaborativo entre os diversos setores da sociedade. Contudo, conclui-se que é uma capacidade essencial para as FFAA serem úteis, significativas e relevantes, face à evolução da conflitualidade robotizada.

Em resposta à QD4, considera-se como necessidades genéticas as seguintes capacidades: (i) governação e gestão da arquitetura; (ii) governação e gestão de dados e informação; e (iii) Interação homem-máquina assente na ID&I colaborativa.



8. Contributos para a formulação de uma Estratégia Digital nas Forças Armadas

Na sequência dos capítulos precedentes, onde foi analisada a compreensão do tema e os respetivos indicadores, o presente capítulo visa caracterizar o ambiente estratégico, de modo a identificar os diversos fatores, que permitam a dedução dos OEst e LAE, contribuindo para a formulação de uma estratégia credível, de modo a responder à QC.

8.1. Caraterização do ambiente estratégico

Resultante da análise documental, entrevistas e questionários, foram identificadas Oportunidades (O) e Ameaças (A) do ambiente externo, que permitem influenciar a atividade e o desempenho. De igual modo, foram identificadas Potencialidades (P) e Vulnerabilidades (V) do ambiente interno, que permitem identificar recursos e capacidades que possam gerar vantagens competitivas (EMA, 2015). Os fatores (*vide* Apêndice E) foram alinhados com os vetores da capacidade militar, garantindo um fator por vetor, num total de oito fatores, tendo sido priorizados quanto ao impacto.

Na lógica da estratégia bem-sucedida, resultante do ajustamento das Oportunidades com os recursos e capacidades (Potencialidades) da organização, minimizando o efeito das Vulnerabilidades e evitando ser afetado pelas Ameaças, aplicou-se a análise de *Strengths, Weaknesses, Opportunities and Threats* (SWOT), assegurando o alinhamento com o meio envolvente, de modo maximizar as Potencialidades organizacionais para aproveitar ao máximo as Oportunidades detetadas (estratégia maxi-maxi); minimizar o efeito negativo das Vulnerabilidades e simultaneamente, aproveitar as Oportunidades emergentes (estratégia mini-maxi); maximizar as Potencialidades para minimizar o efeito das Ameaças detetadas (estratégia maxi-mini); minimizar as Vulnerabilidades, fazendo face às Ameaças (estratégia mini-mini) (Marinha, 2015b), resultando nove objetivos estratégicos (Figura 23):

- OEst1 - Estabelecer a capacidade de gestão integrada de dados e informação;
- OEst2 - Incrementar uma arquitetura organizacional conjunta;
- OEst3 - Fortalecer a capacidade de ID&I;
- OEst4 - Incentivar o desenvolvimento de competências digitais;
- OEst5 - Desenvolver a liderança digital;
- OEst6 - Consolidar a otimização de processos;
- OEst7 - Potenciar a superioridade de informação e do conhecimento;
- OEst8 - Implementar um processo de decisão, de coordenação e de C2 mais ágil;
- OEst9 - Consolidar a capacidade de ciberdefesa.



		Ambiente Interno	
		S Potencialidades	W Vulnerabilidades
		P1 - Normativos que integram a inovação e a transição digital. P2 - Implementados projetos digitais e ciberdefesa. P3 - Qualidade de formação e com competências digitais. P4 - Existência de TIC e capacidade de gestão da informação. P5 - Liderança e vontade de integrar a evolução tecnológica. P6 - Elevado sentido de missão na concretização dos objetivos. P7 - Existência de infraestruturas dedicadas. P8 - Edificação de capacidades conjuntas interoperáveis entre si e com os aliados.	V1 - Falta de uma estratégia única e doutrina conjunta. V2 - Processo decisório, de coordenação e de C2 com fragilidades e burocratizados. V3 - Competências digitais escassas para integração da i4.0. V4 - Tecnologias em quantidade e qualidade em algumas áreas. V5 - Fragilidades de liderança digital orientada na transição digital. V6 - Recrutamento e retenção de talentos de digitais para a i4.0. V7 - Arquitetura focada na tecnologia e na segurança digital. V8 - Fragilidades na partilha de informação.
Ambiente Externo	O Oportunidades	CRESCIMENTO	FOCALIZAÇÃO
	O1 - Perspetiva internacional, nomeadamente da NATO e da EU.	FORTALECER a capacidade de ID&I. (P1, P5, P7, P8) x (O1, O4, O5, O6, O8) POTENCIAR a superioridade de informação e do conhecimento. (P1, P3, P4, P5, P6, P7, P8) x (O1, O2, O4, O6, O7, O8) CONSOLIDAR a otimização de processos. (P1, P2, P5, P8) x (O1, O2, O4, O5, O6, O8)	IMPLEMENTAR um processo de decisão, de coordenação e de C2 mais ágil. (V2, V7, V8) x (O1, O2, O4, O5, O6, O8) INCENTIVAR o desenvolvimento de competências digitais. (V3; V6; V7, V8) x (O1, O3, O5, O6)
	O2 - Processos decisórios ágeis assente na superioridade informação.		
	O3 - Desenvolvimento de competências digitais.		
	O4 - Potencialidade da i4.0 no domínio informacional e na automatização dos processos e sistemas.		
	O5 - Empenhamento do sistema político na ID&I e transição digital.		
	O6 - Maior necessidade de otimização dos recursos humanos.		
	O7 - Maior racionalização de estruturas.		
	O8 - Maior investimento em tecnologia interoperável.		
	T Ameaças	DIVERSIFICAÇÃO	DEFESA
	A1 - Algumas diferenças de abordagem à Transição Digital.	ESTABELECER a capacidade de gestão integrada de dados e informação. (P1, P3, P4, P5, P7) x (A4, A6, A7, A8) CONSOLIDAR a capacidade de ciberdefesa. (P2, P3, P4, P7, P8) x (A2, A4, A5, A6, A7)	INCREMENTAR uma arquitetura organizacional conjunta. (V4, V5, V7, V8) X (A2, A5, A6, A7) DESENVOLVER a liderança digital. (V1, V5, V6, V7) x (A1, A2, A3, A4, A6, A7, A8)
	A2 - Aumento da instabilidade geopolítica que pode levar a um ataque a membros da NATO/EU, com maior incidência no ciberespaço.		
	A3 - Manutenção das competências digitais face a evolução tecnológica.		
	A4 - Volume de dados e informação não tratada que leva à desinformação.		
	A5 - Ameaças cibernéticas que comprometem a salvaguarda da informação.		
	A6 - Alargamento exponencial do mercado aos talentos digitais.		
	A7 - Maior exploração da dimensão informacional para fins maliciosos.		
	A8 - A velocidade da evolução tecnológica dificulta a interoperabilidade.		

Figura 23 - Análise SWOT

Fonte: Adaptado a partir de EMGFA (2021) e EMA (2015b).

8.2. Mapa estratégico para a transição digital

Seguindo a metodologia utilizada na DEEMGFA, foi desenvolvido o mapa estratégico para a TDig, mantendo o alinhamento com o quadro de valores, com os temas e com as orientações estratégicas estabelecidas na referida Diretiva (Figura 24), adaptando-o à integração da TDig nas FFAA.

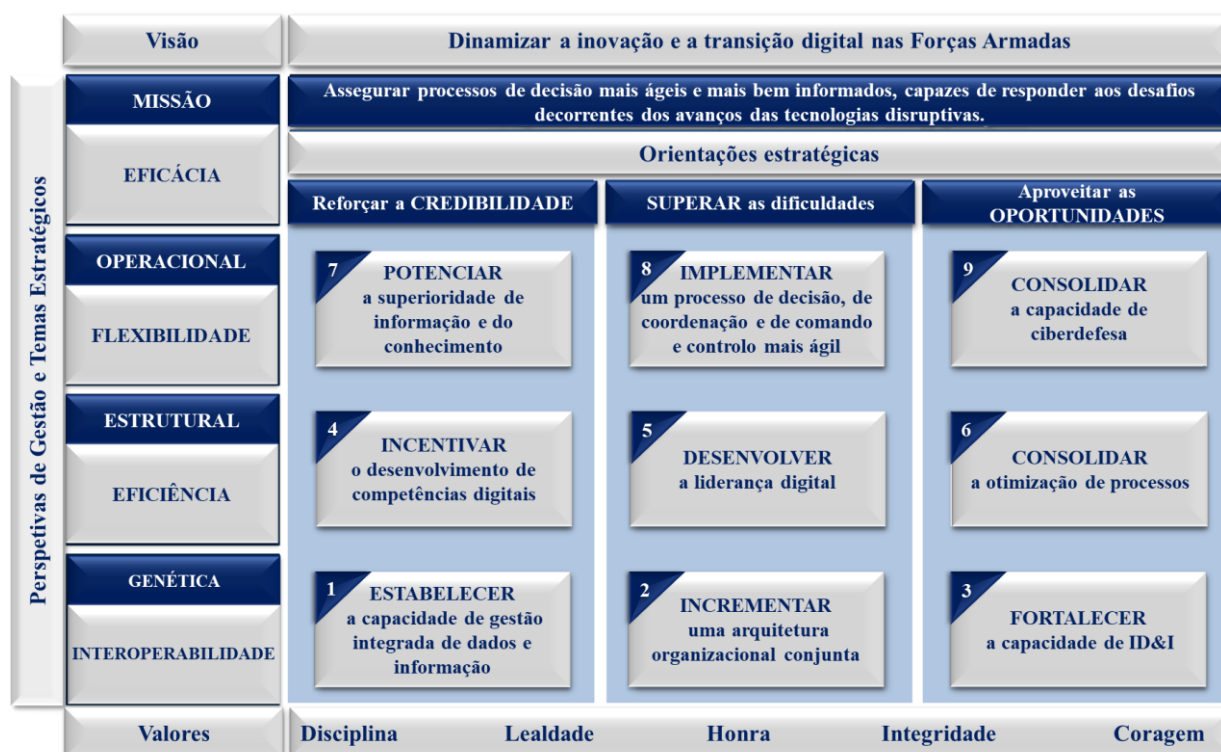


Figura 24 - Mapa da estratégia para a transição digital

Fonte: Adaptado a partir de EMGFA (2021).

8.3. Linhas de ação estratégicas

Decorrente da observação analítica da matriz SWOT (Figura 23), da análise documental e das entrevistas, resulta a dedução de LAE que facilitam a gestão das Oportunidades e Ameaças, decorrentes dos fatores externos, à luz das Potencialidades e Vulnerabilidades organizacionais (Marinha, 2015b). Embora pudessem ter sido deduzidas mais, considerou-se apenas três LAE por cada OEst, evitando uma lista exaustiva.

Sendo a genética a base da estratégia, responsável pela geração de recursos e capacidades empregues para alcançar o produto operacional, foram deduzidas três LAE para cada OEst, num total de nove para a perspetiva genética (Tabela 1), constituindo-se os pilares basilares da estratégia. Estas medidas contribuem para a inclusão das tecnologias da i4.0, viabilizando a integração com tecnologias emergentes, levando a que as FFAA sejam mais digitais desde o processo de decisão ao seu emprego no campo de batalha, contribuindo para sua eficácia e eficiência.



Tabela 1 - Linhas de Ação Estratégicas da Perspetiva Genética

OEst1 - ESTABELEECER a capacidade de gestão integrada de dados e informação	
LAE1.1	Edificar uma visão, princípios orientadores, valências básicas e objetivos da gestão integrada de dados e informação. <u>Racional</u> - Criar uma Diretiva Estratégica de dados e informação orientada para alcançar a vantagem da informação.
LAE1.2	Estabelecer uma estrutura conjunta de gestão de dados e informação. <u>Racional</u> - Criar um grupo de trabalho para operacionalizar a estratégia.
LAE1.3	Garantir a partilha de dados com qualidade e segurança. <u>Racional</u> - Disponibilizar para apoio à decisão.
OEst2 - INCREMENTAR uma arquitetura organizacional conjunta	
LAE2.1	Edificar o modelo de governação e gestão da arquitetura organizacional. <u>Racional</u> - Estabelecer orientações, princípios de arquitetura e regimes de governação para avaliação de necessidades, riscos e medidas de mitigação, face à visão e aos objetivos estabelecidos.
LAE2.2	Erguer a arquitetura organizacional da defesa. <u>Racional</u> - Operacionalizar a análise, o planeamento e a implementação através de uma abordagem de engenharia holística.
LAE2.3	Produzir doutrina conjunta. <u>Racional</u> - Estabelecer conceitos e procedimentos harmoniosos na instituição.
OEst3 - FORTALECER a capacidade de ID&I	
LAE3.1	Edificar uma estrutura conjunta com ligação à indústria, universidades e polos ou centros de investigação e desenvolvimento. <u>Racional</u> - Estabelecer um ecossistema aberto à angariação de investigadores, técnicos ou outros, para desenvolver tecnologias que possam ser inovadoras para a instituição.
LAE3.2	Estimular a interação homem-máquina e outras tecnologias disruptivas. <u>Racional</u> - Potencializar a ID&I em sistemas que viabilizem a competitividade tecnológica.
LAE3.3	Garantir a interoperabilidade. <u>Racional</u> - Fundamental para garantir a capacidade de operar junto dos parceiros.

A dedução das LAE dos OEst que contribuem para a edificação da perspetiva estrutural seguiu a mesma lógica aplicada à perspetiva genética. Foram cruzados os fatores resultantes da caracterização do ambiente estratégico, deduzindo as LAE contempladas na Tabela 2. De modo a manter o princípio do equilíbrio, foram deduzidos de igual modo, nove LAE, ou seja, três por cada OEst. Estas medidas contribuem para o desenvolvimento da cultura e da literacia digital, a par de uma melhor articulação dos recursos e otimização de processos, que facilitam a integração de capacidades orientadas para o produto operacional.



Tabela 2 - Linhas de Ação Estratégicas da Perspetiva Estrutural

OEst4 - INCENTIVAR o desenvolvimento de competências digitais	
LAE4.1	Estabelecer um plano de conhecimento por níveis, face à categoria e à função. <u>Racional</u> - Identificar necessidades tendo em conta os cargos e os recursos humanos existentes.
LAE4.2	Estimular a avaliação digital. <u>Racional</u> - Reconhecer de forma credível e acionável, o atual conhecimento digital dos recursos humanos.
LAE4.3	Promover programas de formação adaptados às necessidades e ao atual nível de conhecimento. <u>Racional</u> - Potencializar e alargar a cultura e literacia digital por níveis de necessidade definidos no plano anterior.
OEst5 - DESENVOLVER a liderança digital	
LAE5.1	Potencializar o processo de decisão mais descentralizado e ágil. <u>Racional</u> - Descentralizar mais a decisão, desde o topo da liderança ao individual, fortalecendo as responsabilidades nas decisões.
LAE5.2	Incentivar uma cultura centrada nas pessoas e nos processos, recorrendo à tecnologia. <u>Racional</u> - Desenvolver a cultura digital orientada para o bem-estar das pessoas, assente nos processos desburocratizados e ágeis, conectada pelas tecnologias.
LAE5.3	Estimular uma cultura de inovação assente na fruição de ideias e em processos ágeis e interativos. <u>Racional</u> - Desenvolver um ecossistema orientado para novas ideias tecnológicas (e.g. academias, empresas, investigadores, núcleos tecnológicos, entre outros).
OEst6 - CONSOLIDAR a otimização de processos	
LAE6.1	Centralizar componentes transversais numa gestão comum. <u>Racional</u> - Racionalizar ou concentrar serviços, sistemas ou capacidades, evitando redundâncias transversais, otimizando recursos e obtendo ganhos na eficiência.
LAE6.2	Reforçar a desmaterialização, integrando IA e o PLN nos processos de gestão, tendendo para a automatização. <u>Racional</u> - Finalizar o processo de desmaterialização em curso assente numa orientação estratégica, abrangendo as FFAA como um todo. A IA e o PLN deve contribuir para reduzir custos e mitigar riscos. A automatização deverá enquadrar-se como uma tendência natural.
LAE6.3	Agilizar os fluxos de trabalho entre Unidades ou Serviços (<i>smart working</i>). <u>Racional</u> - Deixar de utilizar papel, agilizar a tramitação de processos e os despachos entre unidades e serviços, reduzindo a pegada carbónica e contribuindo para a sustentabilidade ambiental.

Por último e de igual forma, foram deduzidas as LAE dos OEst que integram a perspetiva operacional, resultantes da dedução do cruzamento de fatores da caracterização do ambiente estratégico (Tabela 3). Mantendo o princípio, foram deduzidas três LAE por cada OEst, ou seja, nove LAE para a perspetiva operacional. Estas medidas integram a tecnologia da i4.0, de modo a agilizar a coordenação e o C2, bem como a obtenção de um processo de decisão assente na superioridade de informação.

Tabela 3 - Linhas de Ação Estratégicas da Perspetiva Operacional

OEst7 - POTENCIAR a superioridade de informação e do conhecimento	
LAE7.1	Modernizar a infraestrutura de rede, integrando e promovendo as boas práticas empresariais. <u>Racional</u> - Otimizar a infraestrutura de rede baseado nos conhecimentos e nas boas práticas residentes na indústria, evoluindo para uma infraestrutura de rede moderna, unificada e lógica.
LAE7.2	Edificar uma organização de inovação capacitada para acompanhar e integrar tecnologias emergentes. <u>Racional</u> - Identificar projetos ID&I essenciais, incluindo tecnologias emergentes e integrar no ciclo da inovação as que são utilizáveis. A inovação e a rapidez da sua relevância possibilitarão que uma nova capacidade operacional seja desenvolvida, integrada, acreditada e implementada com maior celeridade.
LAE7.3	Proteger a informação. <u>Racional</u> - Incorporar medidas defensivas nos processos, nos sistemas tecnológicos e nas pessoas.
OEst8 - IMPLEMENTAR um processo de decisão, de coordenação e de C2 mais ágil	
LAE8.1	Edificar um modelo de C2 Ágil. <u>Racional</u> - Empregar com maior eficácia e eficiência os recursos disponíveis em tempo útil numa diversidade de missões e circunstâncias.
LAE8.2	Integrar IA em sistemas de C2. <u>Racional</u> - Gestão e análise do fluxo de dados e informação, que permita uma decisão atempada, eficiente e eficaz, face à rapidez dos conflitos modernos.
LAE8.3	Desenvolver treino do exercício de C2 Ágil. <u>Racional</u> - Treino de cenários que obriguem a adoção de novas posturas de C2 incluindo a incorporação de processos de tomada de decisão colaborativos.
OEst9 - CONSOLIDAR a capacidade de ciberdefesa	
LAE9.1	Contribuir para a superioridade e partilha de informação. <u>Racional</u> - Melhorar a partilha da informação, contribuindo para a superioridade de informação no apoio à decisão.
LAE9.2	Promover as capacidades de computer network. <u>Racional</u> - Aumentar o espetro de operação da defesa ao ataque, permitindo alcançar a vantagem competitiva da informação.
LAE9.3	Contribuir para a segurança da informação. <u>Racional</u> - Assegurar a segurança dos dados e da informação.

8.4. Alinhamento dos contributos para a formulação da estratégia

A credibilidade da estratégia depende da aceitabilidade (ação política), da adequabilidade (ação militar) e da exequibilidade (ação financeira) (EMGFA, 2020).

No que concerne à aceitabilidade, os contributos formulados estão alinhados com a Estratégia para a TD na AP (PCM, 2017), com o Plano de Ação para a TDig (Conselho de



Ministros, 2020) e com a Estratégia para a TD da AP 2021-2026 (PCM, 2021) (*vide* Apêndice G).

Quanto à adequabilidade, os contributos formulados enquadram-se nos vetores integrantes de uma capacidade militar (DOTMLPII) (*vide* Apêndice F), preservando o alinhamento à DEEMGFA (EMGFA, 2021).

Respeitante à exequibilidade, os contributos enunciados enquadram-se no quarto desafio estratégico (Sociedade Digital, da Criatividade e da Inovação) do programa do XXIII Governo Constitucional, apoiado pelo Quadro Financeiro Plurianual para o período compreendido entre 2021 e 2027 (Conselho da União Europeia, 2020). Ao nível da Lei de Programação Militar (LPM), enquanto instrumento plurianual que define os investimentos a realizar nas FFAA, encontra-se presentemente no processo regular de revisão para o horizonte até 2034. Com esta revisão pretende-se desenvolver uma estratégia de edificação de capacidades militares assentes na inovação e com valor acrescentado para a economia nacional, onde o MDN estabelece a edificação de capacidades no domínio das tecnologias disruptivas e de duplo uso através da ID&I (XXIII Governo da República Portuguesa, 2022). Outra fonte de financiamento a explorar, é através do PRR, prevista a sua execução até 2026, enquadrando-se no alinhamento com os seis pilares da estratégia europeia 2030, onde um dos pilares mais relevantes é a TDig (XXIII Governo da República Portuguesa, 2021).

Assim sendo, ficou demonstrado que é uma estratégia credível pela sua aceitabilidade (ação política), adequabilidade (ação militar) e exequibilidade (ação financeira).

8.5. Síntese conclusiva

Na sequência dos capítulos anteriores, foi realizada a caracterização do ambiente estratégico, seguida da edificação de uma matriz e posterior análise SWOT, tendo sido deduzidos nove OEst, facilitando a elaboração da proposta de um mapa estratégico.

Seguidamente foram deduzidas três LAE por cada OEst a partir da caracterização do ambiente estratégico, justificando a importância de cada LAE na formulação da estratégia.

Por último, os contributos foram submetidos à prova da estratégia no que respeita à credibilidade dos mesmos, demonstrando cumprir com os critérios da aceitabilidade, adequabilidade e exequibilidade. Os contributos formulados, além de estarem alinhados com as políticas nacionais, também estão com as políticas usadas pelos parceiros de referência, no quadro internacional.

Em suma, os contributos propostos, permitem que as FFAA possam edificar uma estratégia dedicada à implementação da transição digital, orientados para as tecnologias



disruptivas e para fazer face às tecnologias emergentes, na ótica da otimização e da eficiência, ficando assim respondida à QC da presente investigação.

9. Conclusão

Portugal estabelece a TDig como prioridade estratégica, enquanto nação Atlântica e porta de entrada na Europa, com relevância pela sua posição geoestratégica, constituindo-se como a mais importante rota comercial entre os continentes americano, africano e europeu, abrangendo a terceira maior zona económica exclusiva da UE. A TDig passou a ser essencial na relevância da competitividade de uma sociedade globalizada.

As FFAA não estão indiferentes a esta evolução, pois a iniciativa e resiliência nesta vertente, iniciou com a edificação de centros de ID&I nas respetivas Academias, desde a década transata, na exploração de projetos relevantes. Desde então, esta área tem evoluído com a edificação de Departamentos orientados para TDig e Inovação, Centros de Experimentação, investimentos na robotização (e.g. UAV, *Unmanned Ground Systems* [UGS], *Remotely Operated Vehicle* [ROV], *Autonomous underwater vehicle* [AUV], entre outros), bem como, na simplificação de alguns processos administrativos e logísticos, através, como por exemplo, do programa SIMPLEX. Esta prioridade tem vindo a ser plasmada na renovação das Diretivas, constituindo-se a TDig e a Inovação uma das prioridades estratégicas.

Naturalmente, a relevância das FFAA no quadro dos parceiros de referência, vem estabelecer requisitos de evolução tecnológica, assente no digital e na i4.0, além do ambiente estratégico estar cada vez mais contestado e imprevisível, abrangendo todos os domínios, o que exige das FFAA um renascer para as tecnologias disruptivas emergentes.

Atendendo à pertinência e prioridade que está a ser dada a esta temática, foi estabelecido como OG desta investigação: “Propor contributos para uma Estratégia Digital nas Forças Armadas portuguesas”, para o qual foi levantada a QC: “Quais os contributos para uma Estratégia Digital nas Forças Armadas portuguesas?”, tendo sido estabelecidos quatro OE e quatro QD, alinhados respetivamente, com o OG e com a QC.

Respeitante à metodologia, a investigação assentou numa orientação ontológica de construtivismo e epistemológico de interpretativismo, seguindo uma estratégia qualitativa, baseada no raciocínio indutivo, aplicando-se o desenho de pesquisa interpretativa. A recolha de dados assentou em questionários, entrevistas e análise documental.

O trabalho foi estruturado em nove capítulos: introdução; enquadramento e metodologia; perceção digital das FFAA portuguesas; perspetiva internacional; perspetivas operacional, estrutural e genética; contributos para a formulação de uma Estratégia Digital nas FFAA; e conclusões.



Mantendo o alinhamento com o OEst3 da DEEMGFA, foi estabelecido como visão estratégica: *“Processos de decisão mais ágeis e mais bem informados, capazes de responder aos desafios decorrentes dos avanços das tecnologias disruptivas”* e foram preservados os valores, os temas e as orientações estratégicas contemplados na respetiva diretiva.

Para responder à QD1 e cumprir com o OE1: *“Identificar o nível de compreensão desta temática nas FFAA portuguesas”*, foi realizada uma análise quantitativa e qualitativa aos questionários, concluindo-se que o conhecimento ainda é incipiente relativamente a esta temática nas FFAA. Contudo, após a análise das Diretivas Estratégicas e das entrevistas realizadas aos Ramos, há a perceção que as FFAA passaram a encarar a TDig como uma prioridade estratégica, com projetos implementados e iniciativas que contribuem para a integração e evolução da TDig, incorporando tecnologias disruptivas no apoio à decisão.

Para a resposta à QD2, de modo a cumprir com o OE2: *“Descrever os elementos da transição digital que contribuem para a melhoria das capacidades decisórias das FFAA portuguesas”*, deve haver uma abordagem essencialmente digital, orientada para a superioridade de informação, de modo melhorar o processo de decisão; a realização de operações no, e através do, ciberespaço, abrangendo todo o espectro de operações; e por último, um C2 Ágil, que permita descentralizar o processo de decisão, contribuindo para que seja mais célere, ágil e eficaz.

Para responder à QD3 e cumprir com o OE3: *“Estabelecer a composição, organização e articulação dos recursos, de modo a assegurar o melhor desempenho dos processos de decisão e das atuações dos meios”*, é essencial desenvolver uma cultura digital descentralizada e transversal, orientada para a otimização dos processos, assente na liderança digital a todos os níveis (contribui para a maneira de pensar e agir do pessoal); no desenvolvimento de competências digitais (aumento de literacia digital do pessoal através da formação); e na otimização de processos (promovendo a automatização e a simplificação dos processos através de uma abordagem digital).

Para a resposta à QD4 e cumprir com o OE4: *“Analisar os recursos necessários à edificação harmoniosa e balanceada das capacidades, que possam contribuir para o nível digital das operações”*, é fundamental gerar capacidades orientadas para um produto operacional mais eficaz e eficiente, baseado na governação e gestão da arquitetura organizacional, contribuindo para a perceção de capacidades integráveis, incorporando tecnologia; na governação e gestão de dados e informação, estabelecendo medidas para edificação dos recursos; e a interação homem-máquina, enquadrado nas capacidades integráveis, que assentam na ID&I, constituindo-se a base das tecnologias emergentes.



Para responder à QC e cumprir com o OG, formularam-se nove OEst, resultantes da análise SWOT e a dedução de 27 LAE, que sustentam a credibilidade dos contributos formulados, pela satisfação dos critérios da aceitabilidade, da adequabilidade e da exequibilidade. Os contributos formulados, além de estarem alinhados com as políticas nacionais, estão alinhados com o ambiente estratégico internacional e com os parceiros de referência.

Resultante do trabalho, embora seja uma área em evolução que integra matérias incipientes, nomeadamente, indicadores para cada perspetiva elencada, realça-se como **contributos para o conhecimento**, a otimização de processos, a arquitetura organizacional, a gestão integrada de dados e informação e a interação homem-máquina, seguido dos OEst e das LAE formuladas. Contudo, apresentam-se algumas **limitações**, que se prendem pela falta de trabalhos académicos e um referencial de bibliografia.

Na sequência da investigação, destaco como temas de **trabalho futuro**, “Aspetos legais e éticos da integração da Inteligência Artificial nas Forças Armadas” e o “Desenvolvimento da interação homem-máquina nas Forças Armadas”. Como **recomendação prática**, considera-se a operacionalização dos presentes contributos.

Assim sendo, as tecnologias disruptivas e as emergentes estão a mudar a natureza da conflitualidade, contribuindo para que esta seja mais contestada e imprevisível. A relevância das FFAA nesta nova conflitualidade requer uma abordagem mais digital, que permita reduzir o ciclo de decisão e potencializar a capacidade de sistemas de armas autónomos e semiautónomos, constituindo-se um elemento diferenciador.

“O sucesso depende tanto do esforço como da atitude certa para fazer acontecer”.

Clarice Lispector



Referências bibliográficas

- Academia das Ciências de Lisboa. (2011). *Definição/Conceito de Ciências Militares*. (Informação). Lisboa: Autor.
- Academia Militar. (2019). *Liderança 4.0 - As suas implicações no comando e liderança*. [Página online] Retirado de <https://academiamilitar.pt/4-iscl.html>.
- Ahlemann, F., Stettiner, E., Messerschmidt, M., & Legner, C. (2012). *Strategic Enterprise - Architecture Management*. London: Springer.
- Alves, E. (2021). *Transformação digital nas Forças Armadas: perspetiva estratégica*. (Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto, edição 2020/2021). Instituto Universitário Militar [IUM], Lisboa.
- Armada Española. (2019). *Plan de Transformación Digital de la Armada*. Madrid: Autor.
- Assis, A., Bittencourt, N., & Tavares, S. (2020). Armas inteligentes no ciberespaço: oportunidades inovadoras e desafios prementes. *Revista Brasileira de Estudos de Defesa*, 7(2), pp. 133–157. doi.org/10.26792/RBED.v7n2.2020.75211
- Association of Business Process Management Professionals. (2013). *Best Practice Management CBOK - Version 3.0 (1st edition)*. [versão PDF] Retirado de <https://pt.3lib.net/book/5225726/2ec7e1>.
- Association of Business Process Management Professionals. (2019). *Guide to the Business Process Management Common Body of Knowledge (BPM CBOK) - version 4.0*. [versão PDF] Retirado de www.abpmp.org.
- Bilodeau, N., Vitkus, P., & Powell, E. (2013). *Business Process Panagement CBOK (Version 3.0)*. [versão PDF]. Retirado de <https://pt.3lib.net/book/5225726/2ec7e1>.
- Boy, G. A. (2011). *The Handbook of Human-Machine Interaction*. Burlington: Ashgate.
- Braz, C. (2008). *A Liderança nas Forças Armadas e o Processo de Formação de Líderes Militares*. (Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto, edição 2007/2008). Instituto de Estudos Superiores Militares [IESM], Lisboa.
- Bussiere, M. (2022). *Estratégia de Transformação Digital da Marinha*. [Página online] Retirado de <https://www.senedia.org/senedia-tech-talk-navy-digital-transformation-strategy/>.
- Cambridge dictionary. (n.d.). *Networking noun (Computers)*. [Página online]. Retirado de <https://dictionary.cambridge.org/pt/dicionario/ingles/networking>.
- Celaya, A., & Yeung, N. (2019). Human psychology and intelligent machines. Em A. Gili (Ed.), *The Brain and the Processor: Unpacking the Challenges of Human-Machine Interaction* (pp. 17-26). Roma: NATO Defense College, Reseach Division.



- Chaudhari, V. (2022). *Reflexão da guerra da Ucrânia sobre operações completas de vários domínios*. [Página online] Retirado de https://www.business-standard.com/article/current-affairs/ukraine-war-reflection-of-complete-multi-domain-operations-iaf-chief-122041200504_1.html.
- Comissão Europeia. (2004). *European Guide to good Practice in Knowledge Management - Part 5: Knowledge Management Terminology*. Bruxelas: Autor.
- Comissão Europeia. (2017). *Documento de reflexão sobre o futuro da defesa europeia*. Bruxelas: Autor.
- Comissão Europeia. (2018). *Risk Management Plan - Template (P2M Wiki)*. [Página online]. Retirado de <https://webgate.ec.europa.eu>.
- Comissão Europeia. (2019). *Orientações Éticas para uma Inteligência Artificial de Confiança*. Bruxelas: Autor.
- Conselho da União Europeia. (2020). *Adotado o quadro financeiro plurianual para 2021-2027*. [Página online] Retirado de <https://www.consilium.europa.eu>
- Coram, R. (2002). *Boyd: The Fighter Pilot Who Changed the Art of War*. [versão PDF]. Retirado de <https://www.pdfdrive.com>.
- Correl, D. (2019). *Air Force unveils Digital Air Force initiative*. [Página online] Retirado de <https://www.airforcetimes.com/news/your-air-force/2019/07/10/air-force-unveils-digital-air-forc>.
- Council of the European Union. (2020). *Strategic Implementation Plan for the Digitalisation of European Union Forces*. Bruxelas: Autor.
- Couto, A. C. (1988). *Elementos de Estratégia - Apontamentos para um Curso*. Lisboa: Instituto Universitário Militar.
- Data Management International. (2017). *Data Management Body of Knowledge (2nd edition)*. Lindsley: Technics Publications.
- Decreto-Lei n.º 249/2015, de 28 de outubro. (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar*. Diário da República, 1.ª Série, 211, 9298-9311. Lisboa: Conselho de Ministros.
- Defence iQ. (2021). *Digital Transformation in Defence - webinar series*. [versão PDF]. Retirado de <https://www.defenceiq.com/events-webinarseries/agenda-mc>.
- Defesa Nacional. (2021). *Centro de Ciberdefesa*. [Página online]. Retirado de <https://www.defesa.gov.pt/pt/pdefesa/ciberdefesa/centro>.
- Deloitte Portugal. (2022). *Robotic Process Automation (RPA)*. [Página online] Retirado de



- <https://www2.deloitte.com/pt/pt/pages/strategy-operations/articles/robotic-process-automation.html>.
- Department of Defense. (2019). *Digital Modernization Strategy*. [versão PDF]. Retirado de <https://media.defense.gov/2019/Jul/>.
- Department of Defense. (2020). *Department of Defense Data Strategy*. Washington: Office of Prepublication and Security review.
- Department of National Defence and Canadian Armed Forces. (2019). *Data Strategy*. Canada: Autores.
- Despacho n.º 13692/2013, de 28 de outubro. (2013). *Orientação Política para a Ciberdefesa*. Diário da República, 2.ª série, 208, 31976-31979. Lisboa: Ministério da Defesa Nacional.
- ELO Group. (2011). *Coletânea ELO Group de ideias e tendências em Best Practices Management em 2010/2011*. [versão PDF] Retirado de Evolução do Tema Best Practices Management nas Organizações. <http://ep.ifsp.edu.br>
- Estado-Maior-General das Forças Armadas. (n.d.). *Departamento para a Inovação e Transformação*. [Página online] Retirado de <https://www.emgfa.pt/Paginas/Departamento-para-a-Inovacao-e-Transformacao.aspx>
- Estado-Maior-General das Forças Armadas. (2020). *Planeamento Estratégico Militar*. Lisboa: Chefe do Estado-Maior General das Forças Armadas.
- Estado-Maior-General das Forças Armadas. (2021). *Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2021/2023 (versão draft)*. Lisboa: Gabinete do Chefe do Estado-Maior-General das Forças Armadas.
- European Commission. (2022). *DigComp 2.2: The Digital Competence Framework for Citizens*. <https://doi.org/10.2760/115376>
- Exército. (2019). *Diretiva estratégica do Exército 2019-2021*. Lisboa: Gabinete do Chefe do Estado-Maior do Exército.
- Exército. (2022). *Diretiva Estratégica do Exército 2022 - 2023*. [versão PDF] Retirado de <https://assets.exercito.pt/SiteAssets/GabCEME/Comunica%C3%A7%C3%A3o/Diretivas%20Estrat%C3%A9gicas/2022-02%20DEE%2022-23.pdf>.
- Fachada, C. P. A., Ranhola, N. M. B., Marreiros, J. P. R., & Santos, L. A. B. (2020). *Normas de Autor no IUM*. (3.ª Ed., revista e atualizada). IUM Atualidade, 7. Lisboa: Instituto Universitário Militar.
- Fawkes, A., & Menzek, M. (2018). The Future Role of Artificial Intelligence: Military Opportunities and Challenges. Em *Transforming Joint Air Power: The Journal of the*



- JAPCC, 27, pp. 70–77. [Página online] Retirado de <https://www.japcc.org/the-future-role-of-artificial-intelligence/>.
- Fernandes, H. (2016). *As Novas Guerras: O Desafio da Guerra Híbrida*, 4(2), pp. 13–40. Retirado de <http://www.iesm.pt/cisdi/index.php/publicacoes/revista-de-ciencias-militares/edicoes>.
- Força Aérea. (2022). *Diretiva Nº 09/CEMFA/2022 - Diretiva Estratégica da Força Aérea: 2022-2025*. Lisboa: Gabinete do Chefe do Estado-Maior da Força Aérea.
- Frankenfield, J. (2020). *Quantum Computing*. [Página online]. Retirado de <https://www.investopedia.com/terms/q/quantum-computing.asp>.
- Furlan, J. (2009). *Business Process Management - Common Body of Knowledge - BPM CBOOK (Version 2.0)*. [Versão PDF]. Retirado de <https://www.academia.edu>.
- Gil, S. (2015). *As perspetivas civis do contrato de trabalho - o teletrabalho subordinado: seu estudo nos ordenamentos jurídicos português e espanhol*. (Tese de Doutoramento em Ordenamentos Jurídicos português e espanhol). Universidade da Corunha, Corunha.
- GovDataDownload. (2019). *The U.S. Marine Corps Embarks on its Digital Transformation Journey with AI and Data Management*. [Página online] Retirado de <https://govdatadownload.netapp.com/2019/05/us-marine-corps-digital-transformation-journey-ai-data-management/#.YmRHee3MLb0>.
- Governo de Portugal. (2019). *Programa do XXII Governo Constitucional 2019-2023*. [Versão PDF]. Retirado de <https://www.portugal.gov.pt>.
- Governo de Portugal. (s.d.). *Programa SIMPLEX 20-21*. [Versão PDF]. Retirado de <https://www.simplex.gov.pt>.
- Governo de Portugal. (2018). *Plano Setorial TIC da Área da Governamental da Defesa Nacional*. [versão PDF]. Retirado de <https://tic.gov.pt>.
- Governo de Portugal. (2019). *INCoDe.2030 - AI Portugal 2030 - Portuguese National Initiative on Digital Skills – An Innovation and growth strategy to foster Artificial Intelligence in Portugal in the European context*. Lisboa: Fundação para a Ciência e Tecnologia.
- Governo de Portugal. (2020). *Plano de Ação para a Transição Digital de Portugal*. [Versão PDF]. Retirado de <https://www.portugal.gov.pt/gc22/portugal-digital/plano-de-acao-para-a-transicao-digital-pdf.aspx>.
- Governo de Portugal. (2022). *Programa do XXIII Governo Constitucional (2022-2026)*. [versão PDF] Retirado de <https://www.portugal.gov.pt/pt/gc23/governo/programa-do-governo>.



- IdD Portugal Defence. (s.d.). *Centro de Investigação Naval*. [Página online] Retirado de. Retrieved April 3, 2022, from <https://btid.iddportugal.pt/listing/cinav/>
- INCoDe.2030. (2019). *Quadro Dinâmico de Referência de Competência Digital para Portugal*. [versão PDF] Retirado de <https://www.incode2030.gov.pt>
- Instituto Brasileiro de Engenharia de Custos. (2017). *Influência da tecnologia: como o mercado de trabalho está mudando*. [Página online]. Retirado de <https://ibecensino.org.br/blog/influencia-da-tecnologia-como-o-mercado-de-trabalho-esta-mudando/>.
- Instituto de Apoio às Pequenas e Médias Empresas e à Inovação. (2021). *Resultado da avaliação do inquérito à maturidade i4.0*. Lisboa: Autor.
- ISO/IEC/IEEE 24765:2017(en). (2017). *Systems and software engineering — Vocabulary*. [Página online] Retirado de <https://www.iso.org/obp/ui/#iso:std:iso-iec-ieee:24765:ed-2:v1:en:term:3.445>.
- ISO/IEC 38500:2015 (en). (2015). *Information technology - Governance of IT for the organization*. [Página online]. Retirado de <https://www.iso.org/obp/ui/#iso:std:iso-iec:38500:ed-2:v1:en>.
- ISO/IEC TR 29119-11:2020 (en). (2020). *Software and systems engineering - Software testing - Part 11: Guidelines on the testing of AI-based systems*. [Página online]. Retirado de <https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:29119:-11:ed-1:v1:en>.
- Italian Army. (2019). *Future Operating Environment post 2035 - Implications for Land Forces*. Rome: Italian Army Headquarters.
- Kelly, R. (2019). *Constructing Leadership 4.0 - Swarm Leadership and the Fourth Industrial Revolution*. Gewerbestrasse: Palgrave Macmillan.
- Kem, J., & McConville, J. (2020). *Key Strategic Issues List*. Pennsylvania: United States Army War College.
- Leitão, A. (2021). *Governo aprova Estratégia para a Transformação Digital da Administração Pública 2021-2026 - XXII Governo - República Portuguesa*. [Página online] Retirado de <https://www.portugal.gov.pt>
- Lima, R. (2020). *Deepfake: o que é e como funciona?* - *TecMundo*. [Página online] Retirado de <https://www.tecmundo.com.br/internet/206706-deepfake-funciona.htm>.
- Madakam, S., Holmukhe, M., & Kumar, D. (2019). The Future Digital Work Force: Robotic Process Automation (RPA). *Journal of Information Systems and Technology Management*, 16, 1–17. <https://doi.org/10.4301/s1807-1775201916001>
- Magno, S. (2020). *Exame Informática: Blockchain - o que é e como funciona*. [Página



- online] Retirado de <https://visao.sapo.pt/exameinformatica/tutoriais/2020-12-10-blockchain-o-que-e-e-como-funciona/>.
- Marinha. (2010). *Despacho do Almirante Chefe do Estado-Maior da Armada, n.º 13/10, de 03 de Fevereiro - Centro de Investigação Naval*. [versão PDF] Retirado de https://escolanaval.marinha.pt/pt/investigacao_web/organizacao_web/PublishingImages/Paginas/Regulamentos/OA1_N%C2%BA09_10FEV2010.pdf.
- Marinha. (2015a). *PAA 1003: A Gestão Estratégica na Marinha*. Lisboa: Estado-Maior da Armada.
- Marinha. (2015b). *PAA 1003 - A Gestão Estratégica na Marinha*. Lisboa: Estado-Maior da Armada.
- Marinha. (2018a). *Diretiva Setorial das Tecnologias da Informação 2018*. Marinha: Superintendência das Tecnologias da Informação.
- Marinha. (2018b). *Núcleo Computer Incident Response Capability*. Lisboa: Superintendência das Tecnologias da Informação.
- Marinha. (2020a). *Paradigma Estrutural da Marinha*. Lisboa: Gabinete do Chefe do Estado-Maior da Armada.
- Marinha. (2020b). *Programas Intersectorias - Anexos à Diretiva Estratégica da Marinha 2018*. Lisboa: Gabinete do Chefe do Estado-Maior da Armada.
- Marinha. (2021a). *Estratégia Operacional da Marinha*. Lisboa: Gabinete do Chefe do Estado-Maior da Armada.
- Marinha. (2021b). *Marinha apresenta Zona Livre Tecnológica*. [Página online] Retirado de <https://www.marinha.pt/pt/media-center/Noticias/Paginas/Marinha-apresenta-Zona-Livre-Tecnologica.aspx>.
- Marinha. (2022). *Diretiva Estratégica da Marinha*. Lisboa: Gabinete do Chefe do Estado-Maior da Armada.
- Marques, A. G. (2017). O Poder da Informação no Poder Militar. *Revista Militar* N.º 2589, pp. 771–780. [Página online] Retirado de <https://www.revistamilitar.pt/artigopdf/1271>
- Martins, J. (2017). *O Contributo das Operações de Informação para a Superioridade de Informação*. (Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto, edição 2016/2017). Instituto Universitário Militar [IUM], Lisboa.
- McCarthy, R., McConville, J., & Grinston, M. (2019). *Army Modernization Strategy*. [versão PDF] Retirado de <https://www.army.mil/e2/downloads/>
- Ministère des Armées. (2019). *Artificial Intelligence in Support of Defence*. Paris: Ministère des Armées.



- Ministério da Defesa Nacional. (2015). *Defesa 2020*. Lisboa: Autor.
- Ministério da Defesa Nacional. (2020). *Estratégia de Defesa Nacional para o Espaço 2020|2030..* [versão PDF] Retirado de <https://www.defesa.gov.pt>
- Ministério da Defesa Nacional - Conselho de Chefes de Estado-Maior. (2014). *Conceito de Estratégia Militar - CEM 2014*. Aprovado pelo Ministro da Defesa Nacional em 22 de julho de 2014. Confirmado em Conselho Superior de Defesa Nacional de 30 de julho de 2014. Lisboa: Autores.
- Ministro da Defesa Nacional. (2020). *Informação Defesa Nacional de 01 de abril de 2020 - Lei de Programação Militar: taxa de execução cresce em 2019*. [versão PDF]. Retirado de <https://www.defesa.gov.pt>.
- Ministry of Defence. (2018a). *Joint Concept Note 1/18 - Human-Machine teaming*. Swindon: UK Ministry of Defence.
- Ministry of Defence. (2018b). *Joint Concept Note 2/18 - Information Advantage*. [versão PDF] Retirado de <https://www.gov.uk/government/publications/information-advantage-jcn-218>.
- Mobley, J. (2011). *Study to Establish Levels of Digital Literacy for Soldiers and Leaders in the U . S . Army*. Kansas city: Jane Mobley Associates.
- Monteiro, L. (2020). *Gestão Estratégica: Contributos para o Paradigma Estrutural da Marinha Portuguesa*. Cadernos do IUM, 44. Lisboa: Instituto Universitário Militar.
- Moreira, A. (2021). *A Inovação nas Forças Armadas: Contributos para uma Estratégia*. (Trabalho de Investigação Individual do Curso de Promoção a Oficial General, edição 2020/2021). Instituto Universitário Militar [IUM], Lisboa.
- Moreno, D. (2021). A governance das forças armadas no planeamento estratégico militar. *Revista Científica Academia da Força Aérea*, 11, pp. 124–145. [versão PDF] Retirado de <https://www.academiafa.edu.pt>
- Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). *Military applications of artificial intelligence - Ethical Concerns in an Uncertain World*. [versão PDF] Retirado de <https://www.rand.org>
- NEP/INV - 001 (A1). (2020). *Procedimentos relativos à elaboração de trabalhos de investigação realizados no âmbito de cursos não atribuem grau académico*. Lisboa: Instituto Universitário Militar.
- NEP/INV - 003 (A3). (2020). *Estrutura e regras de citação e referência de trabalhos escritos a realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.



- North Atlantic Treaty Organization. (2017). *NATO Enterprise C&I Vision*. Bruxelas: Autor.
- North Atlantic Treaty Organization. (2019a). *AAP-6 - NATO Glossary of terms and definitions (English and French) (Edition 2019)*. Bruxelas: NATO Standardization Office.
- North Atlantic Treaty Organization. (2019b). *Empowering the Alliance's technological edge*. NATO: Science and Technology Organization.
- North Atlantic Treaty Organization. (2006). *Nato NEC C2 Maturity Model (SAS-065)*. Bruxelas: NATO Standardization Office.
- North Atlantic Treaty Organization. (2007). *TR-SAS-050 - Exploring New Command and Control Concepts and Capabilities*. Brussels: Research and Technology Organisation.
- North Atlantic Treaty Organization. (2010). *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization*. Belgium: NATO Public Diplomacy Division.
- North Atlantic Treaty Organization. (2014). *C2 Agility*. (Task Group SAS-085 Final Report). Bruxelas: Science and Technology Organization.
- North Atlantic Treaty Organization. (2015a). *NATO Network Enabled Capability (archived)*. [Página online]. Retirado de https://www.nato.int/cps/en/natohq/topics_54644.htm.
- North Atlantic Treaty Organization. (2015b). *NATO Network Enabler Capability*. [Página online] Retirado de https://www.nato.int/cps/en/natohq/topics_54644.htm.
- North Atlantic Treaty Organization. (2016). *Warsaw Summit Communiqué (at NATO Portal)*. [Página online]. Retirado de <https://www.nato.int>
- North Atlantic Treaty Organization. (2018a). *Framework for Future Alliance Operation - 2018 Report*. Bruxelas: Autor.
- North Atlantic Treaty Organization. (2018b). *High level taxonomy of Ciberspace Operations*. Brussels: International Military Staff.
- North Atlantic Treaty Organization. (2018c). *NATO Architecture Framework*. Brussels: Consultation, Command & Control Board.
- North Atlantic Treaty Organization. (2020). *Science and Technology Trends 2020-2040*. Bruxelas: Autor.
- North Atlantic Treaty Organization. (2021a). *NATO Artificial Intelligence Strategy*. [Página online] Retirado de https://www.nato.int/cps/en/natohq/official_texts_187617.htm.
- North Atlantic Treaty Organization. (2021b). *Resumo da Estratégia de Inteligência Artificial da NATO*. [Página online] Retirado de <https://www.nato.int>
- North Atlantic Treaty Organization. (2022a). *Ecossistema de inovação crescente da NATO*.



- [Página online]. Retirado de <https://www.act.nato.int/articles/nato-growing-innovation-ecosystem>.
- North Atlantic Treaty Organization. (2022b). *General Lavigne aborda o Conselho do Atlântico Norte em sua visão de três anos*. [Página online] Retirado de <https://www.act.nato.int/articles/sact-vision-nac>.
- North Atlantic Treaty Organization. (2022c). *Multi-Domains Operations Conference – What we are learning*. [Página online] Retirado de <https://www.act.nato.int/articles/multi-domains-operations-lessons-learned>.
- North Atlantic Treaty Organization. (2022d). *NATO 2022 - Strategic Concept*. [versão PDF] Retirado de www.nato.int/strategic-concept.
- NP EN ISO 9000. (2015). *Sistemas de gestão da qualidade. Fundamentos e vocabulário*. Lisboa: Instituto Português da Qualidade.
- Nunes, P. (2020). *A Edificação da Capacidade de Ciberdefesa Nacional*. (Trabalho de Investigação Individual do Curso de Promoção a Oficial General, edição 2019/2020). Instituto Universitário Militar [IUM], Lisboa.
- OECD. (2019). *Artificial Intelligence in Society*, OECD Publishing, Paris,. OECD Publishing, Paris,. <https://doi.org/10.1787/eedfee77-en>
- Ottewell, P. (2020). *Defining the Cognitive Domain*. [Página online] Retirado de <https://othjournal.com/2020/12/07/defining-the-cognitive-domain/>.
- Pereira, C., & Sousa, P. (2004). A method to define an enterprise architecture using the zachman framework. *Proceedings of the ACM Symposium on Applied Computing*, 2, 1366–1371. <https://doi.org/10.1145/967900.968175>
- Pires, N. (2018). *O Conceito Multi-Domínio e as Possíveis Aplicações às Forças Armadas Portuguesas*. Coleção “ARES”, 24. Lisboa: Instituto Universitário Militar.
- Porter, M. E. (1996). What is strategy? *Harvard Business Review*. 1, pp. 1–22. [Versão PDF]. Retirado de <https://d1wqtxts1xzle7.cloudfront.net/>.
- PwC Portugal. (2021). *Digital Upskilling*. [Página online]. Retirado de <https://www.pwc.pt/pt/formacao/digital-upskilling.html>.
- Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril. (2016). *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial da União Europeia, 4.5.2016, L119/1-L119/88. Bruxelas: Parlamento Europeu e Conselho.
- Rei, F. (2013). *A relevância da superioridade de informação competitiva no quadro da*



- gestão do conhecimento e da tomada de decisão informada nas Forças Armadas.* (Trabalho de Investigação Individual do Curso de Promoção a Oficial Superior, ed. 2012/2013). Instituto de Estudos Superiores Militares [IESM], Lisboa.
- Resolução do Conselho de Ministros n.º 108/2017, de 2 de março. (2017). *Estratégia TIC 2020: Estratégia para a Transformação Digital na Administração Pública*. Diário da República, 1.ª Série, 143, 3938-4201. Lisboa: Presidência do Conselho de Ministros.
- Resolução do Conselho de Ministros n.º 30/2020, de 21 de abril. (2020). *Plano de Ação para a Transição Digital*. Diário da República, 1.ª série, 78, 6-32. Lisboa: Presidência do Conselho de Ministros.
- Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. (2019). *Estratégia Nacional de Segurança do Ciberespaço*. Diário da República, 1.ª Série, 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.
- Ribeiro, A. (2020). *Intervenção do Almirante Chefe do Estado-Maior-General das Forças Armadas*. Em: Instituto de Defesa Nacional, As Forças Armadas na resposta de emergência a crises complexas, Seminário de Defesa Nacional organizado pelo Instituto de Defesa Nacional, Lisboa.
- Ribeiro, A. S. (2008). Formulação da Estratégia Naval Portuguesa - Modelo e Processo. *Cadernos Navais*, 1 (27), pp. 1-80. Lisboa: Edições Culturais da Marinha.
- Ribeiro, A. S. (2020). *O Essencial ao Processo Estratégico: Teoria Geral da Estratégia*. Coimbra: Almedina.
- Ribeiro, A., Silva, F., Palma, J., & Monteiro, N. (2010). Estratégia Naval Portuguesa - o processo, o contexto e o conteúdo. *Cadernos Navais*, 1 (34), pp. 1-145. Lisboa: Edições Culturais da Marinha.
- Rodrigues, S. (2021). Federated Mission Networking. Em: *Curso Estado-Maior Conjunto, Enquadramento Doutrinário das Operações*. Palestra organizada pelo Instituto Universitário Militar, Lisboa.
- 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.
- Sayler, K. (2020). *Artificial Intelligence and National Security (Congressional Research Service)*. Retirado de <https://sgp.fas.org/crs/natsec/R45178.pdf>.
- Schwab, K. (2016). *The Fourth Industrial Revolution*. [versão PDF]. Retirado de <https://www.pdfdrive.com/>.
- Seolin, L., & Edilson, G. (2017). *O Ciclo OODA Loop e sua aplicabilidade no*



- Gerenciamento de Projetos*. Em: Associação Paranaense de Engenharia de Produção, Engenharia de produção. Congresso brasileiro organizado pela Associação Paranaense de Engenharia de Produção, Ponta Grossa.
- Simpson, J., Oosthuizen, R., Sawah, S., & Abbass, H. (2021). *Agile, Antifragile, Artificial-Intelligence-Enabled, Command and Control*. [versão PDF] Retirado de <http://arxiv.org/abs/2109.06874>.
- Solis, B. (2019). *The State of Digital Transformation -2018-2019 Edition*. San Francisco: Altimeter.
- Standard, B. (2022). *Ataques cibernéticos russos com o objetivo de coletar dados da Ucrânia*. [Página online] Retirado de https://www.business-standard.com/article/international/russian-cyber-attacks-aims-data-collection-from-ukraine-digital-dossiers-122042800476_1.html.
- Tanniru, M. R. (2018). Digital Leadership. Em *Management of Information Systems* (pp. 93–109). <https://doi.org/10.5772/intechopen.76045>
- Tegler, E. (2022). *The Vulnerability of AI Systems May Explain Why Russia Isn't Using Them Extensively in Ukraine*. [Página online] Retirado de <https://www.forbes.com/sites/annakaplan/2022/04/28/nato-could-provide-arrangements-for-sweden-and-finland-during-membership-process-secretary-general-says/?sh=6a8405a07e11>.
- Tidy, J. (2022). *Anonymous: como hackers estão tentando minar Putin*. [Página online] Retirado de <https://www.bbc.com/portuguese/internacional-60813283>.
- UK Ministry of Defence. (2021). *Data Strategy for Defence*. [versão PDF] Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020553/Data_Strategy_for_Defence.pdf.
- Um, J.-S. (2019). *Drones as Cyber-Physical Systems – Concepts and Applications for the Fourth Industrial Revolution*. Singapura: Springer.
- UOL EdTech. (2020). *Você exerce uma liderança digital?* [Página online] Retirado de <http://uolledtech.com.br/blog/voce-exerce-uma-lideranca-digital-2>.
- Vieira, B. (2002). *Manual de Liderança Militar*. Lisboa: Edições Atena, lda.
- Ward, J., & Peppard, J. (2002). *Strategic planning for an information system (third edition)*. Cranfield: John Wiley & Sons Ltd. [https://doi.org/10.1016/0024-6301\(90\)90122-k](https://doi.org/10.1016/0024-6301(90)90122-k)
- Westerman, G., & Soule, D. (2016). *Fostering a Digital Organization: Building Sustainable Digital Advantage in Traditional Companies*. Paper apresentado no âmbito da iniciativa sobre a economia digital do Instituto de Tecnologia de Massachusetts, Cambridge.



- Westerman, George, Bonnet, D., & McAfee, A. (2014). *Leading Digital: Turning Technology into business transformation*. Boston, Massachusetts: Harvard Business Review Press.
- Willis, M., & Stathopoulos, P. (2020). Cyber-Electromagnetic Domain. Em *Transforming Joint Air Power: The Journal of the JAPCC*, 30, pp. 72–77. [versão PDF] Retirado de <https://www.japcc.org/cyber-electromagnetic-domain/>.
- Winkler, J., Marler, T., Posard, M., Cohen, R., & Smith, M. (2019). *Reflections on the Future of Warfare and Implications for Personnel Policies of the U.S. Department of Defense*. [versão PDF] Retirado de <https://www.rand.org/pubs/perspectives/PE324.html>. <https://doi.org/10.7249/pe324>
- XXIII Governo da República Portuguesa. (2021). *Plano de Recuperação e Resiliência*. [versão PDF] Retirado de <https://www.portugal2020.pt>
- XXIII Governo da República Portuguesa. (2022). *Revisão da Lei de Programação Militar*. [Página online] Retirado de <https://www.portugal.gov.pt>
- Yerramsetty, S. (2017). *When is it Digital Transition and not Digital Transformation?* | *LinkedIn*. [Publicação no LinkedIn]. Retirado de <https://www.linkedin.com/pulse/when-digital-transition-transformation-sai-yerramsetty/>. <https://www.linkedin.com/pulse/when-digital-transition-transformation-sai-yerramsetty/>



Apêndice A — Corpo de conceitos

Big data - Conjunto de técnicas normalmente baseadas na utilização de IA, que permite a análise e exploração de grandes volumes de dados que não podem ser processados utilizando *software* convencional (Armada Española, 2019, cit. por Alves, 2021).

Blockchain - É uma base de dados que regista ativos e transações replicadas nos computadores de uma rede ponto a ponto. É um género de registo público de quem tem o quê e de quem transaciona o quê (os dados estão encriptados para manter a confidencialidade). As transações são certificadas através de hashes (função matemática que gera um código em função de uma entrada) e, ao longo do tempo, o histórico das transações fica bloqueado em blocos de dados, sendo criptograficamente ligados uns a outros para garantir a segurança (Magno, 2020).

Capacidade militar - É o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para a realização de um conjunto de tarefas operacionais, ou efeito que é necessário atingir, englobando componentes de Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLP II) (EMGFA, 2020, p. 2.4, cit. por Alves, 2021).

Computação quântica - É a tecnologia computacional baseada nos princípios da teoria quântica, distinguindo-se dos computadores tradicionais porque passam a ter uma unidade de informação, que aumenta a sua capacidade de processamento, de forma exponencial e com menor consumo de energia (Frankenfield, 2020, , cit. por Alves, 2021).

Conhecimento - É o resultado de um processo humano dinâmico, que justifica a produção de informação pessoal ou que sustenta crenças como parte da aspiração à “verdade”, e que pode ser retratada, como sendo, a combinação da informação com a experiência, contexto, interpretação e reflexão (Ward & Peppard, 2002, pp. 504-505, cit. por Alves, 2021).

Dado - São factos discretos e objetivos (números, símbolos, figuras) sem estarem contextualizados e interpretados (Comissão Europeia, 2004, p. 9, cit. por Alves, 2021).

Deepfake - Técnica que utiliza recursos de IA para substituir rostos em vídeos e imagens com o propósito de chegar o mais próximo possível da realidade. O termo é uma mistura das expressões *deep learning* e *fake* e significa o emprego da IA para criar uma situação falsa (Lima, 2020).

Deep learning - Abordagem à criação de representações hierárquicas valiosas através da formação de redes neurais com uma ou mais camadas ocultas. Uma aprendizagem profunda, utilizando redes multicamadas de unidades informáticas simples (ou "neurónios"). Nestas redes neurais, cada unidade combina um conjunto de valores de entrada para produzir um valor de saída, que por sua vez, é passado para outros neurónios a jusante (ISO/IEC TR 29119-11:2020 (en), 2020, cit. por Alves, 2021).

Estratégia - É a ciência e arte de edificar, dispor e empregar meios de coação num dado meio e tempo, para se materializarem objetivos fixados pela política, superando problemas e explorando eventualidades em ambiente de desacordo (Ribeiro, 2020, p. 22, cit. por Alves, 2021).

Estratégia genética - Estratégia que visa a invenção, a construção ou a obtenção de novos meios a colocar à disposição da estratégia operacional, no momento adequado, devendo ter em conta a evolução da previsível conjuntura (Couto, 1988, p. 231, cit. por Alves, 2021).

Estratégia estrutural - Estratégia que visa detetar e analisar as vulnerabilidades e potencialidades das estruturas existentes, com vista à definição das medidas mais adequadas, incluindo a criação de novas estruturas, que conduzem à eliminação ou atenuação das vulnerabilidades, a um reforço das potencialidades e, em última análise, a um melhor rendimento dos meios ou recursos (Ribeiro, 2020, p. 33, cit. por Alves, 2021).

Estratégia operacional - Estratégia que concilia os objetivos a atingir com as possibilidades proporcionadas pelas estratégias, genética e estrutural, mas também, orienta a evolução destas, de forma a adaptá-las às necessidades operacionais (Ribeiro, 2020, p. 33, cit. por Alves, 2021).

Fluxo de processos - É a agregação de subprocessos numa relação sequencial que mostra a ordem em que são realizados (Association of Business Process Management Professionals, 2013, p. 436, cit. por Alves, 2021).



Gestão - É a arte de ser diferente, através da criação de uma proposta de valor única (Porter, 1996, p. 1, cit. por Alves, 2021).

Gestão de processos - É a abordagem sistémica para mapeamento, análise, redesenho, melhoria e gestão de um processo (ELO Group, 2011, cit. por Alves, 2021).

Gestão por processos - É a metodologia que pressupõe estruturar, organizar, mensurar e gerenciar uma organização, a partir dos seus processos de negócio (ELO Group, 2011, cit. por Alves, 2021).

Governança - Consiste num sistema de direção e controlo, sendo o órgão de governança uma pessoa ou um grupo de pessoas, que são responsáveis pelo desempenho e pela conformidade da organização (ISO/IEC 38500 (EN), 2015, cit. por Alves, 2021).

Governança corporativa - Sistema pelo qual as organizações são geridas e controladas (ISO/IEC 38500 (EN), 2015, cit. por Alves, 2021).

Impressão tridimensional - Consiste em criar um objeto físico através da impressão de camada sobre camada, a partir de um desenho ou modelo digital 3D (Schwab, 2016, p. 20, cit. por Alves, 2021).

Informação - Baseia-se em dados e acrescenta valor à compreensão de um assunto, e de forma contextualizada, constituindo a base do conhecimento (Comissão Europeia, 2004, p. 10, cit. por Alves, 2021).

Inteligência artificial - É o campo interdisciplinar do estudo teórico e prático que procura compreender os mecanismos da cognição e pensamento, e utiliza uma combinação de *hardware* e *software* para imitá-los, de modo a ajudar, ou substituir as atividades humanas (*Ministère des Armées*, 2019, p. 3, cit. por Alves, 2021).

Internet das coisas - É uma relação entre as coisas (produtos, serviços, lugares, etc.) e as pessoas que se torna possível através de tecnologias ligadas e várias plataformas (Schwab, 2016, p. 22, cit. por Alves, 2021).

Maturidade digital - É um Processo gradual de integração e implementação de processos organizacionais, pessoas e outros recursos em processos digitais e vice-versa (Aslanova and Kulichkina, 2020).

Machine learning - Processo que utiliza técnicas computacionais para permitir que os sistemas aprendam com os dados, ou com a experiência (ISO/IEC TR 29119-11:2020 (en), 2020, cit. por Alves, 2021).

Negócio - Atividades organizacionais, parcialmente ordenadas, a realizar para alcançar um resultado desejado na prossecução de um determinado objetivo de uma organização (ISO/IEC/IEEE 24765:2017(en), 2017).

Networking - É o processo de ligação de computadores, para que possa partilhar informação entre utilizadores (*Cambridge dictionary*, s.d. , cit. por Alves, 2021).

Processo - É um conjunto definido de atividades ou comportamentos executados por humanos ou máquinas, para alcançar uma ou mais metas (Furlan, 2009, p. 30, cit. por Alves, 2021).

Transformação - É um processo de adaptação contínuo e pró-ativo, do desenvolvimento e integração de conceitos, doutrina e capacidades inovadores, para melhorar a eficiência e a interoperabilidade das forças militares (NATO, 2019a, p. 130, cit. por Alves, 2021).

Robótica - São máquinas com deteção e controlo melhorados que são utilizadas para automatizar ou aumentar as atividades (DND&CAF, 2019, p. 32).

Sensemaking - Um processo cognitivo que envolve a construção e posterior desenvolvimento de modelos mentais, consciência situacional e compreensão, e que em última análise, conduz à tomada de decisões. Este processo é frequentemente informado pela interação social, bem como, permite a evolução da consciência e compreensão situacional partilhada (NATO, 2006, p. 165, cit. por Alves, 2021).

Smart working - A expressão é considerada uma designação mais abrangente do que o teletrabalho, embora parte integrante do conceito. Aliada às TI, junta-se a flexibilidade, elemento nevrálgico, em que o local de trabalho é irrelevante (Gil, 2015, p. 79).

Superioridade de informação - É a vantagem operacional derivada da capacidade de recolher, processar e disseminar um fluxo ininterrupto de informações, enquanto explora ou nega a capacidade de um adversário de fazer o mesmo (NATO, 2015a, cit. por Alves, 2021).

Upskillings - Reflete a velocidade e imprevisibilidade da evolução tecnológica e a aposta numa formação que possa potenciar novas competências nas empresas (PwC Portugal, 2021).



Apêndice B — Resultados e avaliação do questionário sobre a maturidade digital e a indústria 4.0 nas Forças Armadas

O presente questionário teve como público-alvo, os militares que prestam serviço nos Estados-Maiores ou equivalentes, do EMGFA e dos Ramos. O questionário apresenta-se organizado com uma parte introdutória, seguido de um primeiro bloco destinado, essencialmente, a avaliar a perceção da maturidade digital desses militares e um segundo bloco destinado a avaliar a maturidade da organização para os desafios da indústria 4.0. O primeiro bloco assenta na adaptação do modelo certificado pelo MIT e o segundo bloco no modelo da IAPMEI, certificado pelo Instituto de Soldadura e Qualidade (ISQ).

1. Indique o Ramo/EMGFA a que pertence?



2. Qual a sua Função?



3. Qual o seu posto atual?



4. Indique a sua idade?
Foram dadas 310 respostas a esta questão, sendo que o militar mais novo tem 22 anos e o mais velho tem 66 anos. A média de idades é de 43 anos.
5. Indique o seu sexo:
A esta questão responderam 312 militares, sendo que, 37 militares são do sexo feminino e 275 do sexo Masculino.

Conclusão nº 1:

Relativamente a esta parte introdutória, constata-se que das 314 entradas, verifica-se que houve uma taxa de desistência de 1% relativamente às entradas em resposta ao presente questionário.



Bloco 1 - Avaliação da maturidade digital

1. Capacidades Digitais:

Destina-se a avaliar o estado digital, de modo, a criar iniciativas para melhorar os processos da instituição. Considera que na sua Unidade/Departamento/Serviço.

Responda às seguintes questões classificando de 1 a 5, sendo 1 discordo totalmente e 5 concordo totalmente

Os processos organizacionais estão automatizados?

Está instituída a digitalização de processos, com a implementação de tecnologia e sistemas de informação (e.g. aplicações, programas de análise, redes sociais ou outros, comunicações moveis e dispositivos incorporados)?

Existe uma integração entre sistemas e/ou equipamentos com recurso à IoT (Internet das coisas)?

Estão implementados sistemas que permitam o controlo eficiente dos processos, produtos e serviços, com modelos analíticos ou de análise no apoio à tomada de decisão?

Existe uma visão digital integrada dos processos organizacionais e operacionais com os trabalhadores.

São utilizadas tecnologias digitais para aumentar o desempenho ou o valor acrescentado de produtos e serviços existentes?

São incrementados novos processos organizacionais baseados em tecnologias digitais?

São utilizados canais digitais (tais como websites, redes sociais, e-mails ou outros) para divulgação de informação a públicos-alvo?

São disponibilizados os produtos informacionais e operacionais através de canais digitais?

São usados canais digitais para fornecer um melhor atendimento do público-alvo?

[1]	[2]	[3]	[4]	[5]	Resp	Média
20	54	86	49	4	213	2,83
15	49	74	71	4	213	3,00
59	47	68	33	5	212	2,42
39	66	66	36	4	211	2,53
44	63	57	40	6	210	2,53
21	36	73	70	11	211	3,07
18	45	66	71	11	211	3,06
7	22	46	96	40	211	3,66
8	33	70	82	18	211	3,33
15	48	66	67	15	211	3,09

Total 29,51

2. Capacidades de Liderança

Destina-se a avaliar a dinâmica de integração de novas iniciativas. Responda às seguintes questões classificando de 1 a 5, sendo 1 discordo totalmente e 5 concordo totalmente

Existe uma visão transformadora do futuro digital da instituição e está alinhada com a estratégia e os objetivos operacionais da instituição militar onde está inserido?

As chefias superiores e intermédias partilham uma visão comum da transformação digital?

Existem oportunidades para que todos participem ativamente na mudança em torno da transformação digital?

Estão a ser promovidas as mudanças culturais necessárias para materializar a transformação digital?

Estão a investir nas competências necessárias da organização?

As iniciativas digitais são alinhadas e coordenadas entre os diversos setores, unidades, departamentos e serviços?

Estão definidas claramente as funções e responsabilidades da gestão das iniciativas digitais?

As iniciativas digitais são avaliadas através de um conjunto comum de indicadores e níveis de desempenho?

Existe um clima de cooperação e de parceria entre os responsáveis pelas TIC e pelos processos/estratégias?

Os desempenhos dos serviços de informática respondem às necessidades?

[1]	[2]	[3]	[4]	[5]	Resp	Média
13	39	66	62	7	187	3,06
22	44	57	55	9	187	2,92
25	61	53	42	6	187	2,70
21	51	56	53	6	187	2,85
33	53	59	36	6	187	2,62
30	57	59	37	4	187	2,61
25	59	68	28	7	187	2,64
38	52	75	21	1	187	2,44
22	47	71	42	6	188	2,80
23	51	60	49	5	188	2,80

Total 27,44



Conclusão nº 2:

Relativamente a este bloco verifica-se que apenas 67% das entradas responderam ao grupo de questões sobre as capacidades digitais e 60% das entradas responderam ao grupo de questões sobre a capacidade de liderança.

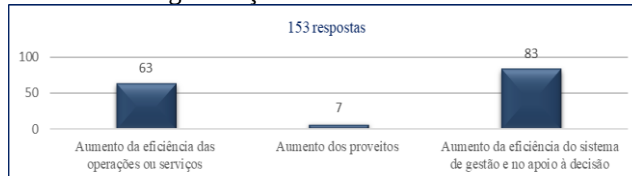
Bloco 2 - Avaliação da maturidade para os desafios da indústria 4.0

Grupo A - Diagnóstico da instituição face aos desafios da indústria 4.0 (i4.0)

1. Conhece os conceitos de digitalização e i4.0?



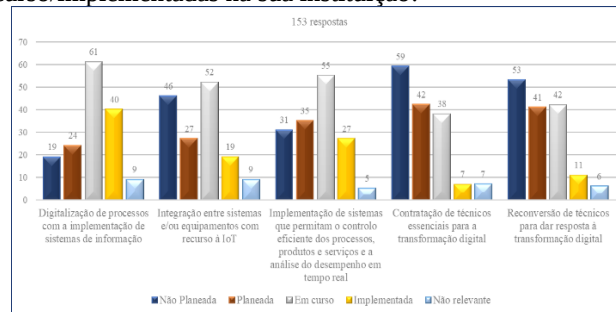
3. Que objetivos pretende atingir com a adoção dos conceitos da digitalização e i4.0? *



2. O que motiva a sua instituição a abraçar os desafios da digitalização e i4.0?



4. Tipifique atividades i4.0 planeadas/em curso/implementadas na sua instituição:



Conclusão nº 3:

No que respeita às questões do Grupo A deste bloco, constata-se que apenas 50% das entradas respondeu à questão nº 1 e 49% das entradas responderam às restantes questões, o que dá a perceção de alguma falta de literacia sobre esta temática na instituição ou alguma falta de divulgação dos projetos em curso ou planeados. A questão nº 1 deste grupo demonstra bem isso, pois 41% dos 156 militares que responderam a esta questão, nunca ouviram falar, 50% ouviram falar superficialmente, mas consideram um assunto a explorar e cerca de 9% já tem conhecimento, e até consideram que a organização já tem alguns projetos pilotos em curso. Quanto à motivação da instituição, o grande foco é o espírito inovador da instituição. Respeitante aos objetivos da organização com estes conceitos, de uma forma ou de outra tende para a eficiência. No que concerne à última questão sobre projetos da i4.0 na instituição, conclui-se 49,6% dos 153 militares que responderam, consideram que há projetos em curso, o que revelam alguma incoerência relativamente à primeira questão, embora haja 28% de respostas que consideram que não há projetos planeados e 22% considera que está planeada.

Grupo B - Estratégia e Organização

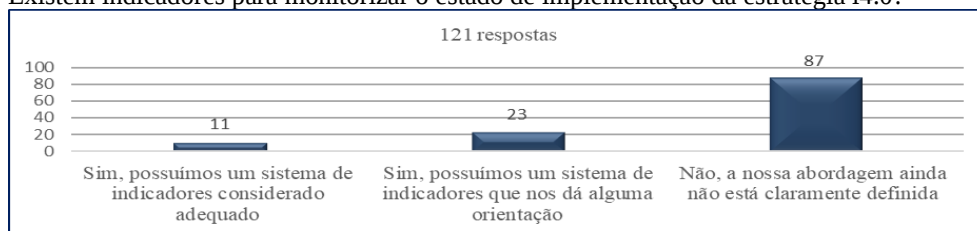
O conceito i4.0 vai muito além da melhoria de produtos, bens, serviços e processos por via da transformação digital. Na realidade, oferece a oportunidade de se desenvolverem novos modelos de negócio, razão pela qual, a sua implementação tem uma importância estratégica.

1. Como descreve o nível de implementação da estratégia i4.0 na sua instituição?

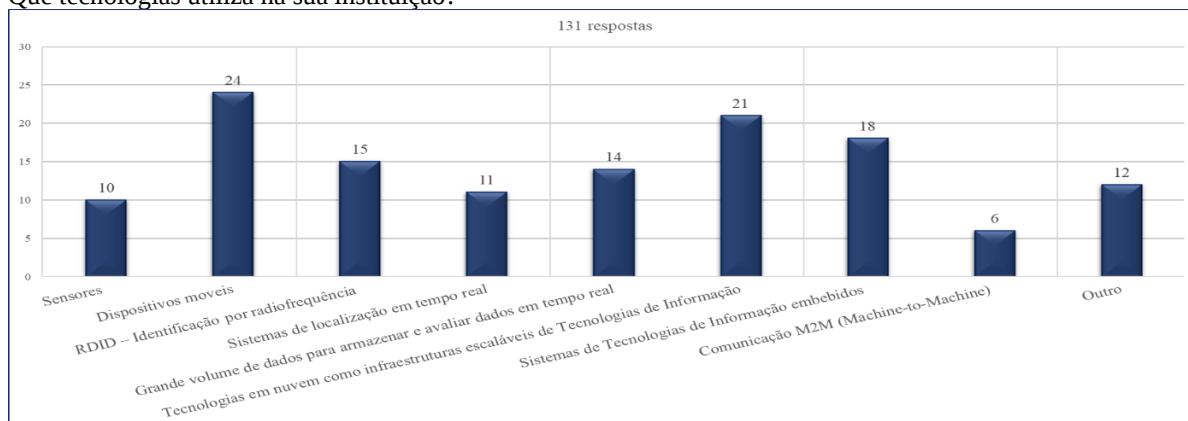




2. Existem indicadores para monitorizar o estado de implementação da estratégia i4.0?

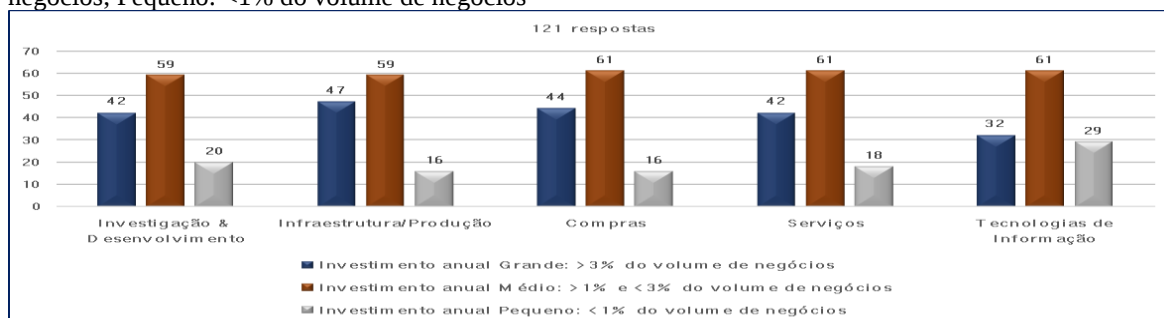


3. Que tecnologias utiliza na sua instituição?



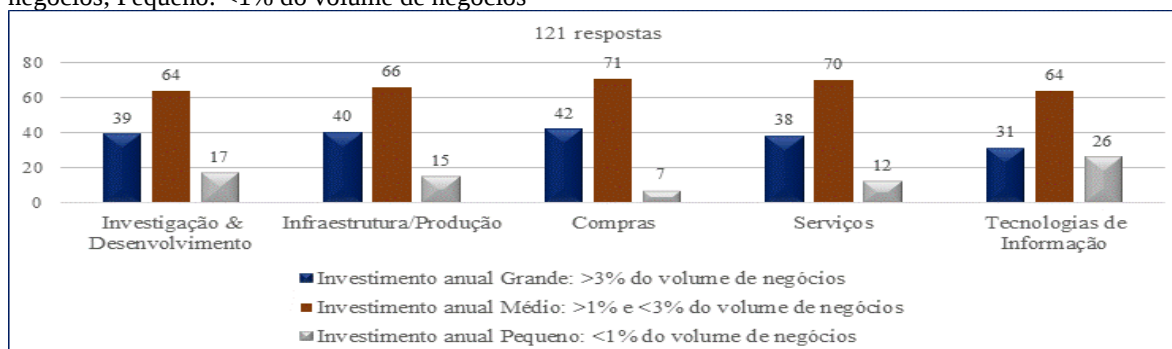
4. Em que áreas da instituição, existiu investimento em i4.0 nos últimos 2 anos?

Indicadores: Investimento anual Grande: >3% do volume de negócios; Médio: >1 e <3% do volume de negócios; Pequeno: <1% do volume de negócios

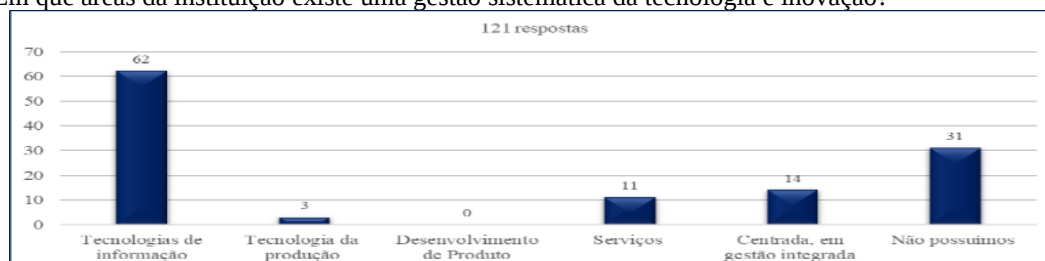


5. Em que áreas da instituição, existiu investimento em i4.0 nos últimos 5 anos?

Indicadores: Investimento anual Grande: >3% do volume de negócios; Médio: >1 e <3% do volume de negócios; Pequeno: <1% do volume de negócios



6. Em que áreas da instituição existe uma gestão sistemática da tecnologia e inovação?





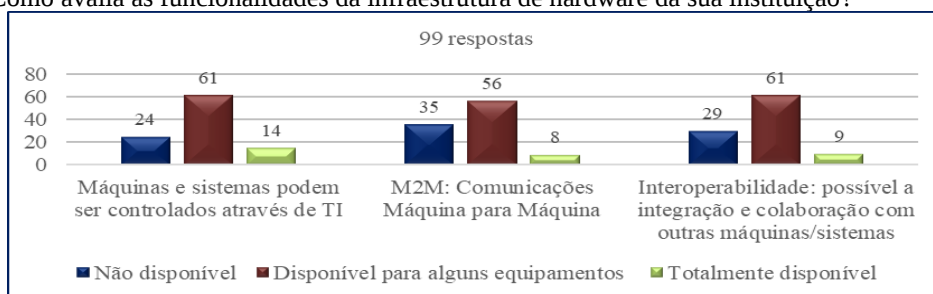
Conclusão nº 4:

No que se prende com este grupo, constituído por seis questões, responderam 39% das entradas, com exceção da questão nº 3, que responderam 42% das entradas. Como verificamos, as respostas são diversas, tendo sido considerado por 36% dos 122 militares que responderam à questão nº 1, que não há uma estratégia de implementação de uma estratégia para a i4.0, embora 29% consideram que já há alguns projetos, 24% consideram que está em desenvolvimento e 10% dos que responderam consideram que está a ser implementada. Logo de seguida verifica-se que não há uma abordagem clara na instituição quanto a esta matéria. Contudo, foi unânime que a organização utiliza tecnologias digitais, embora o foco sejam os dispositivos móveis. Por último, todos confirmam um investimento nos últimos cinco anos. Quanto à existência de uma gestão sistemática da tecnologia e inovação, 51% dos 121 militares que responderam à última questão, consideram as TI. Em suma, verifica-se que 26% dos que responderam a esta questão, tem um conhecimento muito incipiente.

Grupo C - Infraestruturas inteligentes

A existência de uma infraestrutura inteligente constitui um dos fundamentos da i4.0. A recolha de todos os dados relevantes aos processos ou às transações (em tempo real), o seu processamento, fornecimento de informação e utilização de recursos pode ser obtido através da ligação entre os sistemas e pessoas.

1. Como avalia as funcionalidades da infraestrutura de hardware da sua instituição?



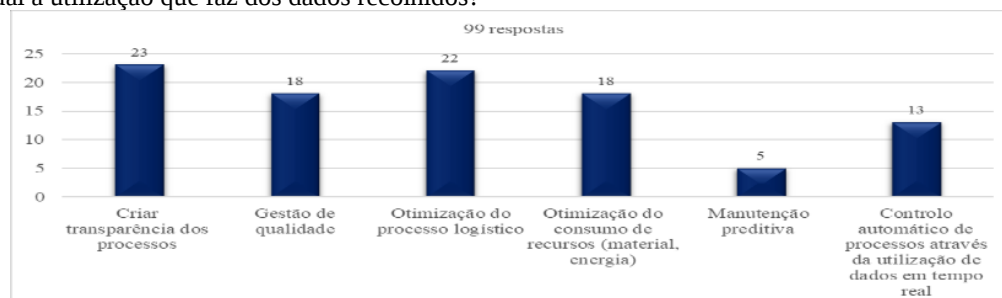
2. A digitalização de equipamentos/processos torna possível criar um modelo digital da infraestrutura. A sua instituição já recolhe dados dos equipamentos e dos processos? (Em relação às máquinas considere apenas as que possuem a capacidade de comunicação).



3. De que forma realiza a recolha de dados?

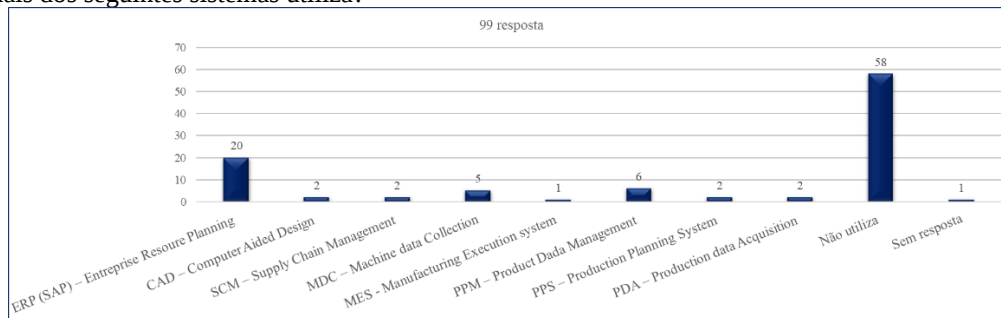


4. Qual a utilização que faz dos dados recolhidos?

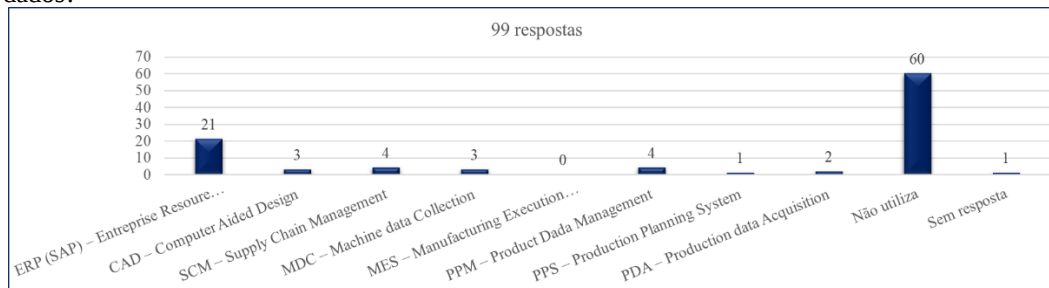




5. Quais dos seguintes sistemas utiliza?



6. Dos sistemas que utiliza, quais possuem alguma interface com o sistema central de armazenamento e tratamento de dados?



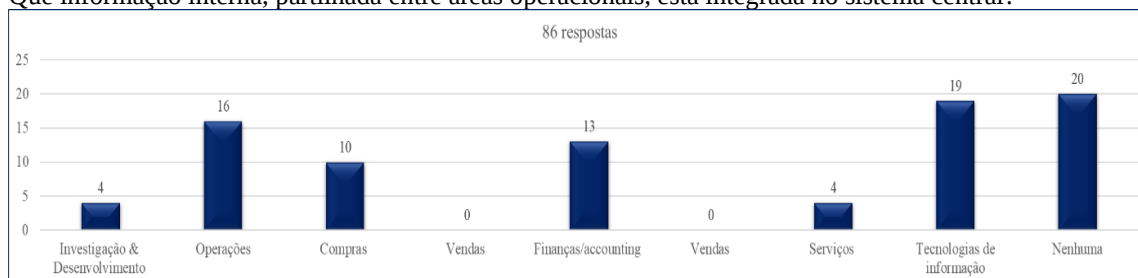
Conclusão nº 5:

Respeitante a este grupo de questões apenas obteve-se 32% de respostas. Quanto à avaliação das funcionalidades da infraestrutura de hardware, as respostas foram de forma generalizada para a disponibilidade em alguns equipamentos, embora não permita retirar conclusão pela uniformização de respostas nos três sistemas. Quanto à recolha de dados de equipamento e processos, cerca de 71% dos 99 militares que responderam à questão nº 3 consideram que a organização já realiza estas tarefas, confirmando-se na questão seguinte, embora haja respostas dispares quanto à forma como é realizada e quanto à utilidade dos mesmos. As duas últimas questões seguintes revelam algum desconhecimento, pois em 99 respostas 61% refere a não utilização, e apenas 21% consideram o *Enterprise Resource Planning* (ERP), quando este está agregado ao SIGDN e já está a ser usado pelas FFAA.

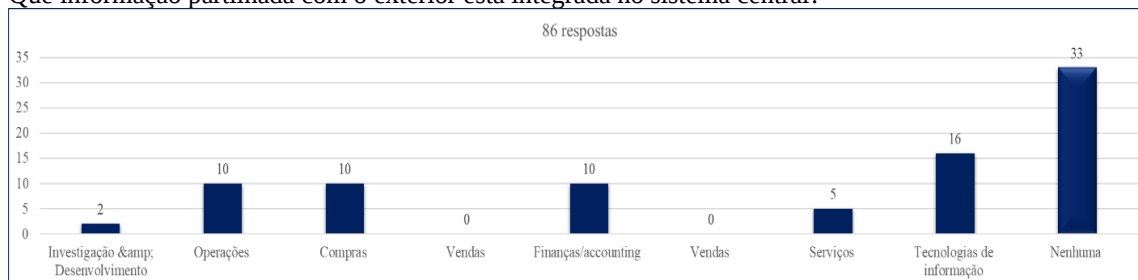
Grupo D - Operações inteligentes

A i4.0 possibilita a integração de todos os componentes e sistemas dentro da instituição e destes com o exterior. Esta é a base da integração horizontal e vertical ao longo da Cadeia de Valor. A recolha, processamento e partilha de dados tornam possível estas novas abordagens, aportando eficiência e conhecimento às operações. Nestas inclui-se a capacidade de as operações serem controladas de forma mais autónoma, com menor intervenção humana, e com a capacidade de se adaptarem a alterações das condições operacionais.

1. Que informação interna, partilhada entre áreas operacionais, está integrada no sistema central?



2. Que informação partilhada com o exterior está integrada no sistema central?





3. Na sua instituição já se observam casos de controlo autónomo?



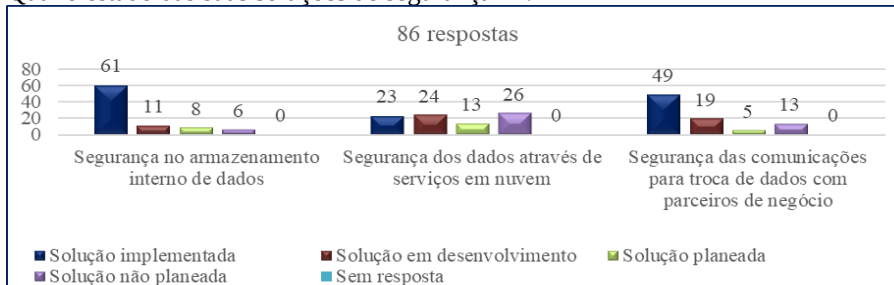
4. Na sua instituição existem processos que sejam reativos e reajustáveis, em tempo útil, a alterações nas condições operacionais?



5. Como está organizada a área das TI na sua instituição?



6. Qual o estado das suas soluções de segurança TI?



7. Já utiliza serviços em nuvem?



Conclusão nº 6:

Relativo a este grupo de questões, apenas, 27% das entradas responderam às questões supra. Quanto à informação se está integrada ou partilhada com o sistema central, cerca de 23% dos 86 militares que responderam à questão nº1 consideram nenhuma das áreas expostas, quando em boa verdade temos áreas que já se encontram, como algumas das respostas mencionadas, nomeadamente as TI, I&D, finanças e compras. Quanto ao controlo autónomo, 66% dos 86 militares que responderam à questão nº3, desconhecem que haja casos na instituição. Quanto à existência de processos reativos e reajustáveis, 56% consideram não existir, quando na realidade existem como a gestão estratégica da organização. Respeitante às TI, 65% dos que responderam à questão nº 5 consideram que estão centralizados em serviços de informática. Quanto à segurança das TI, 52% dos que responderam à questão nº6 consideram que as soluções estão implementadas, embora

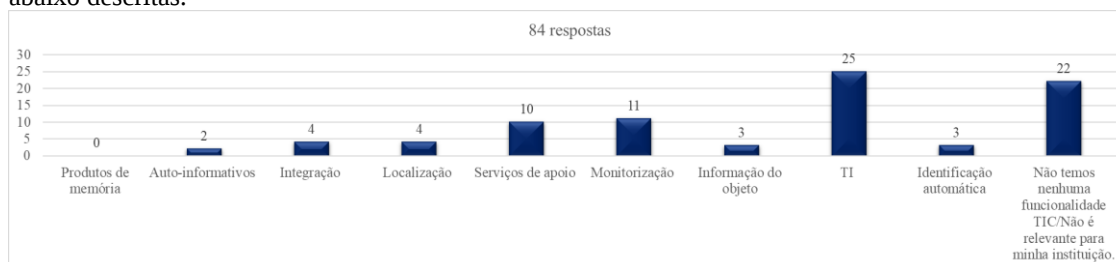


quanto a dados através de serviços em nuvem as respostas divergem de forma equitativa entre o estar implementado e o não planeado. Quanto à utilização de serviços em nuvem as respostas divergem, pois, no software baseado em nuvem as respostas repartem-se equitativamente entre o sim (49%) e o não (47%), quando em boa verdade, por exemplo, já se utiliza o office 365. No entanto, poderão existir Ramos ou Unidades que não utilizem.

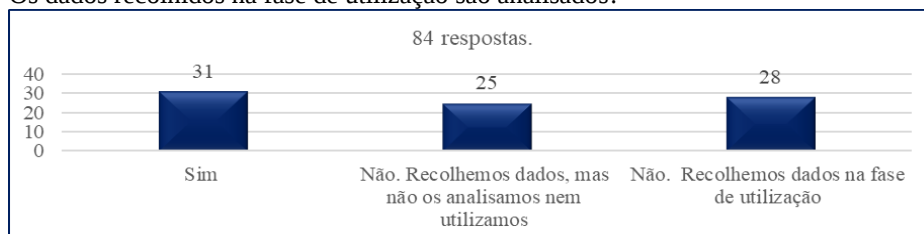
Grupo E - Produtos inteligentes

Os produtos físicos que estão equipados com funcionalidades de TIC, permitem a recolha de dados, assim como, a eficiência das operações. Por sua vez, os produtos digitais, terão de ser suportados por produtos físicos com funcionalidades de TIC que permitam a recolha de dados na fase de utilização.

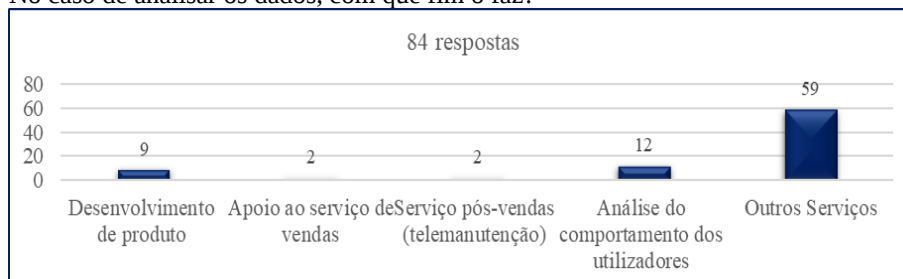
1. Indique os produtos físicos da sua instituição que já vêm equipados com funcionalidades baseadas em TIC, abaixo descritas.



2. Os dados recolhidos na fase de utilização são analisados?



3. No caso de analisar os dados, com que fim o faz?



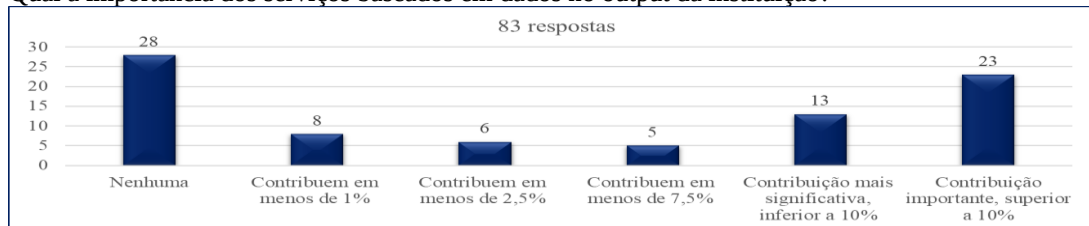
Conclusão nº 7:

No que que respeita a este grupo de questões, apenas 27% das entradas responderam às questões apresentadas. Quanto a produtos físicos da sua instituição equipados com funcionalidades baseadas em TIC, 30% dos 84 militares que responderam à questão nº 1 referem as TI e 26% dizem que não têm, quando a identificação automática é um dos mais usados no acesso a diversas áreas das unidades militares. Quanto à análise dos dados há 30% que referem que recolhem dados, mas não são analisados nem utilizados e 33%, consideram que são recolhidos dados na fase da utilização.

Grupo F - Serviços baseados em dados

O objetivo dos serviços baseados em dados é o de alinhar os futuros processos organizacionais e melhorar os benefícios do público-alvo, mas também proporcionar informações credíveis na tomada de decisão aos diversos níveis. Os produtos ou serviços devem ser suportados por sistemas TI, de forma a poderem enviar, receber ou processar a informação necessária aos processos operacionais.

1. Qual a importância dos serviços baseados em dados no output da instituição?





2. Qual o nível de utilização dos dados recolhidos?



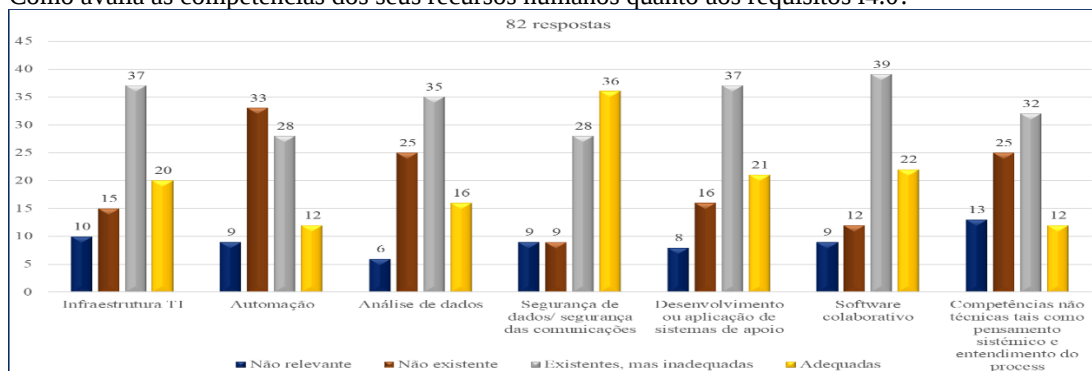
Conclusão nº 8:

Quanto às questões deste grupo, apenas 26% das entradas responderam às questões. Respeitante à importância dos dados no output da instituição, 34% dos 83 militares que responderam à questão nº 1, consideram que não tem utilidade, mas 28% referem que tem uma contribuição significativa. Respeitante ao nível de utilização, cerca de 36% consideram que não são utilizados.

Grupo H - Recursos humanos

As pessoas são a força motriz da transformação digital e são os mais afetados por este processo de mudança. O seu ambiente de trabalho direto é alterado, obrigando-as a adquirir novas competências e qualificações. Por isso, é cada vez mais crítico que as instituições preparem as pessoas para estas mudanças através de programas adequados de formação.

1. Como avalia as competências dos seus recursos humanos quanto aos requisitos i4.0?



2. Está a desenvolver esforços na aquisição das competências em falta? (Através de ações de formação, seminários, transferência de conhecimento, coaching, etc.)



Conclusão nº 9:

Relativamente às questões deste grupo, apenas 26% das entradas responderam às questões. Quanto à competência dos recursos humanos aos requisitos da i4.0, 76% dos 82 militares que responderam, consideram que há competência, embora apenas 24% consideram que são adequadas. Quanto ao desenvolvimento de esforços para aquisição de competência em falta, cerca de 40% responderam que não, 54% responderam que desenvolvem alguns esforços, nomeadamente em algumas competências e apenas 6% é que responderam que desenvolvem esforços em todas as competências, o que revela alguma falta de cultura digital.



Apêndice C — Guião e análise das entrevistas exploratórias

O presente guião foi elaborado com base na revisão da literatura, permitindo elencar os segmentos de resposta contemplados no Quadro 2, como respostas esperadas dos entrevistados, sem condicionar outras respostas.

Quadro 2 - Guião de entrevistas

Objetivo Específico	Questão	Segmentos de Respostas
OE1 - Identificar o nível de compreensão desta temática nas FFAA portuguesas.	1. Qual o entendimento ou visão das Forças Armadas portuguesas relativamente à “Transformação Digital”?	A.1.1 - Implicitamente a TD está nas FAA. A.1.2 - Está previsto uma estratégia da TD. A.1.3 - Tema deve integrar a Diretiva Estratégica. A.1.4 - Não é relevante a TD.
	2. Quais as Potencialidades e Vulnerabilidades da Transformação Digital para as FFAA?	B.1.1 - Potencialidades - Implementação implícita da TD nas FFAA. B.1.2 - Vulnerabilidades - Cultura digital, conhecimento, pessoas com falta de talento. B.1.3 - Segurança.
	3. Quais as Oportunidades e Ameaças da Transformação Digital para as FFAA?	C.1.1 - Oportunidades - Prioridade da atual governação. C.1.2 - Oportunidades - Alinhamento com NATO e UE. C.1.3 - Ameaças - Segurança da informação. C.1.4 - Ameaças - Talentos digitais.
OE2 - Descrever os elementos da transição digital que contribuem para a melhoria das capacidades decisórias das FFAA portuguesas	4. A que nível considera que a TD deve ser implementada nas FFAA: conjunta, nos Ramos ou de forma híbrida, garantindo eficiência e interoperabilidade?	D.1.1 - Perspetiva Conjunta. D.1.2 - Ao nível do Ramos. D.1.3 - Num modelo híbrido. D.1.4 - Interoperabilidade é essencial. D.1.5 - Fundamental a eficiência.
	5. Numa perspetiva operacional quais os indicadores que devem ser explorados para a visão conjunta, que abranja todo o output das Forças Armadas?	E.1.1 - Superioridade informação/conhecimento. E.1.2 - Otimizar Processos Administrativos. E.1.3 - Otimizar Processos Logísticos. E.1.4 - Melhorar serviço publico alvo. E.1.5 - Defesa e ações no ciberespaço.
OE3 - Estabelecer a composição, organização e articulação dos recursos, de modo a assegurar o melhor desempenho dos processos de decisão e das atuações dos meios.	6. Na perspetiva estrutural quais os indicadores que devem ser explorados para a visão conjunta?	F.1.1 - Reestruturação baseada no digital. F.1.2 - Desmaterialização de Processos. F.1.3 - Centralização da gestão informação.
	7. Quais as soluções que acha adequadas ao nível da segurança da informação, para que a transformação digital não se torne numa ameaça para as FFAA?	H.1.1 - Cloud da defesa. H.1.2 - Cloud MS com protocolos de segurança. H.1.3 - Rede segregada. H.1.4 - Sistema de segurança blockchain. H.1.5 - Sistema que confirmam: Confidencialidade, Integridade, Disponibilidade e Autenticidade.
OE4 - Analisar os recursos necessários à edificação harmoniosa e balanceada de capacidades, que possam contribuir para o nível digital das operações.	8. Numa perspetiva genética, talvez a mais difícil, quais os indicadores que considera que devem ser explorados para a visão conjunta, de modo a concorrer para as restantes perspetivas?	G.1.1 - Talentos digitais. G.1.2 - Tecnologias disruptivas. G.1.3 - Doutrina. G.1.4 - Investimento. G.1.5 - Liderança digital. G.1.6 - Cultura digital. G.1.7 - Formação e treino digital.
OE2 - Descrever os elementos da transição digital que contribuem para a melhoria das capacidades decisórias das FFAA portuguesas	9. Considera que deve haver alinhamento na implementação da TD com FFAA congéneres, com a UE ou a NATO (interoperabilidade)?	I.1.1 - Desconheço alinhamentos a nível digital. I.1.2 - Desconheço o que está a ser feito fora. I.1.3 - Não considero relevante. I.1.4 - Devemos estar alinhados ao nível digital. I.1.5 - Interoperabilidade - chave do alinhamento.
	10. Considera que todas as operações realizadas nas FFAA devem centralizar-se nas operações centradas em rede?	J.1.1 - Irrelevante face núm. de op. Conjuntas. J.1.2 - Relevante para o EMGFA e os Ramos. J.1.3 - Relevante desde que as operações sejam todas planeadas e conduzidas a partir do EMGFA, o que requer uma reestruturação das FFAA.
OE4 - Analisar os recursos necessários à edificação harmoniosa e balanceada de capacidades, que possam contribuir para o nível digital das operações.	11. Considera que a TD nas FFAA, deve integrar a Indústria 4.0”? Como deve ser incorporada esta tecnologia nas FFAA?	K.1.1 - Irrelevante. K.1.2 - Importante e deve integrar de forma transversal para conseguir um alinhamento no panorama internacional.

No âmbito da presente investigação foram entrevistados militares especialistas na área digital e militares que pelo exercício de funções têm de tomar decisões operacionais (Quadro 3).



Quadro 3 - Relação de Entrevistados

Entidade	Nome
Divisão de Planeamento do Estado-Maior da Armada.	Capitão-de-mar-e-guerra (CMG) Sardinha Monteiro e Capitão-de-fragata (CFR) Andrade Gonçalves.
Direção de Análise e Gestão de Informação de Marinha.	CFR Oliveira Vieira.
Secretaria-Geral do MDN.	Comodoro (COM) Alves Francisco.
Academia Militar.	Coronel Tirolado (COR TIR) Viegas Nunes.
Comando Conjunto para as Operações Militares.	Contra-Almirante (CALM) N. Sousa.
Departamento para Inovação e Transformação do EMGFA.	Brigadeiro-General (BGEN) Rui Tendeiro.
Divisão de Sistemas de Comunicações, C2 do Estado-Maior da Força Aérea.	Tenente-Coronel (TCOR) Bruno Cabaço.
Centro de Ciberdefesa.	CFR Caldeira Carvalho.
Gabinete Nacional de Segurança.	CALM Gameiro Marques.

Os entrevistados abordaram de forma generalizada os segmentos de resposta resultantes da análise documental, obtendo-se seguintes respostas:

1. Qual o entendimento ou visão das FFAA portuguesas relativamente à TD? O COM Francisco considera que deve assentar na modernização. O CFR Carvalho considera essencial, mas deve ser de forma segura e consciente. O BGEN Tendeiro considera que as FFAA devem ser pioneiras, gerando um efeito mobilizador na modernização. O CALM Marques considera que a visão deve assentar nas potencialidades e vulnerabilidades, e nas oportunidades e ameaças. O CALM Sousa considera inevitável não acompanhar com pragmatismo. O COR TIR Nunes considera que deriva da dependência e evolução tecnológica dos meios e dos processos, logo requer uma capacidade de inovação.

2. Quais as Potencialidades e Vulnerabilidades da TD para as FFAA? O COM Francisco considera como potencialidades, o conhecimento organizacional e como vulnerabilidades, a falta de competência digital, sendo crítica a segurança. O CFR Carvalho considera que a maior vulnerabilidade é a segurança. O BGEN R. Tendeiro e o COR TIR V. Nunes consideram como potencialidades a investigação e o desenvolvimento, contudo a vulnerabilidade passa pela falta de uma inovação colaborativa. O CALM G. Marques considera como potencialidades, o bom edifício formativo que tem e como vulnerabilidade a diferença de visão entre os Ramos. O CALM N. Sousa considera que a maior vulnerabilidade passa pela resistência.

3. Quais as Oportunidades e Ameaças da TD, para as FFAA? O COM Francisco considera como oportunidade, o facto de ser uma das prioridades nacionais e como ameaças a falta de talentos digitais. O CFR Carvalho considera como oportunidade o alinhamento com FFAA congéneres e como ameaças, a segurança da informação e o recrutamento de talentos digitais. O BGEN R. Tendeiro considera como ameaça a segurança da informação. O CALM N. Sousa considera como ameaça a quantidade de dados que circula.

4. A que nível considera que a TD deve ser implementada nas FFAA: conjunta, nos Ramos ou híbrida, garantindo eficiência e interoperabilidade? O COM Francisco e o CALM Marques consideram que deve ser implementado um modelo híbrido. O BGEN R. Tendeiro e o CFR C. Carvalho consideram que deve ser implementado um modelo conjunto. O CALM N. Sousa considera que deve ser ao nível dos Ramos, garantindo a eficiência. O COR TIR V. Nunes considera que deve imperar a eficiência e a eficácia.

5. Numa perspetiva operacional quais os indicadores a explorar, para a visão conjunta, que abranja todo o output das FFAA? O COM Francisco e o CFR Carvalho consideram com indicadores a superioridade de informação, a otimização de processos e o ciberespaço. O BGEN Tendeiro considera como indicadores a eficácia, a eficiência, a interoperabilidade e a paridade. O CALM Marques considera como indicadores o processo de decisão e a governação. O CALM Sousa considera como indicadores a superioridade de informação e a otimização de processos. O COR TIR Nunes considera a eficiência e a eficácia.

6. Na perspetiva estrutural quais os indicadores que considera que devem ser explorados, para a visão conjunta? O COM Francisco e o CFR Carvalho consideram como indicadores a reestruturação, a desmaterialização e a gestão da informação. O BGEN Tendeiro considera como indicadores a reestruturação, os recursos e o treino. O CALM G. Marques considera como indicadores a desmaterialização e a gestão da informação. O COR TIR V. Nunes considera que deve imperar a reestruturação na perspetiva da inovação.

7. Numa perspetiva genética, talvez a mais difícil, quais os indicadores que considera que devem ser explorados para a visão conjunta, de modo a concorrer para as restantes perspetivas? O COM Francisco e o CFR Carvalho consideram todos os segmentos. O CALM Marques concorda com os segmentos apresentados, contudo reforça a integridade e a ID&I. O BGEN Tendeiro considera a tecnologia, a doutrina e ID&I. O CALM N. Sousa considera a tecnologia, a formação e o treino. O COR TIR V. Nunes considera que os indicadores genéticos devem ter uma base de capacidades, sendo abrangentes aos vetores DOTMLPII.

8. Quais as soluções que acha adequadas ao nível da segurança da informação, para que a TD não se torne numa ameaça para as FFAA? O COM Francisco refere que todos os segmentos de resposta estão adequados, exceto o *blockchain*. O CALM Marques e o CFR Carvalho consideram todos adequados, com



exceção da *cloud* da MS. O BGEN Tendeiro considera apenas adequado a *cloud* da Defesa, a rede segregada e sistemas seguros. E o COR Nunes considera que deve assentar em sistema seguros.

9. Considera que deve haver alinhamento na implementação da TD com FFAA congéneres, com a EU ou a NATO (interoperabilidade)? Na generalidade consideram que devemos estar alinhados com os aliados e que deve privilegiar a interoperabilidade de sistemas.

10. Considera que as operações realizadas nas FFAA devem centralizar-se nas operações centradas em rede? Apenas o COR TIR V. Nunes, BGEN R. Tendeiro e o CFR C. Carvalho consideram ser relevante. O CALM N. de Sousa considera irrelevante para as operações conjuntas que são realizadas.

11. Considera que a TD nas FFAA, deve integrar a Indústria 4.0”? Como deve ser incorporada? Na generalidade os entrevistados consideram relevantes. O CALM Marques e o COR TIR Nunes acrescentaram que deve basear-se numa capacidade interna de ID&I.

Tabela 4 - Análise síntese das entrevistas

Questão	Segmentos de Respostas	COM A. Francisco	COR V. Nunes	CALM N. de Sousa	BGEN R. Tendeiro	CFR C. Carvalho	CALM G. Marques
1. Visão	A.1.1 - Implícita nas FFAA	X					
	A.1.2 - Prevista Estratégia	X (necess.)				X	
	A.1.3 - Diretiva EMGFA		X	X	X	X	X
	A.1.4 - Irrelevante						
2. Potencialidade Vulnerabilidades	B.1.1 - Pot. Implícita FFAA	X	X (I&D)		X (I&D)		Formação
	B.1.2 - Vul. - Educação digital	X	X(inova.)	Resistência	X(inova.)		Dif. visões
	B.1.3 - Vul. - Segurança	X			X	X	Competências
3. Oportunidades e Ameaças	C.1.1 - Op. - Prior, governo	X					
	C.1.2 - Op. - Alinh. Externo	X	X			X	
	C.1.3 - Am. - Segurança			X dados	X	X	
	C.1.4 - Am. - Talentos digitais	X				X	
4.Implementação	D.1.1 - Perspetiva Conjunta				X (Comb)	X	
	D.1.2 - Nível dos Ramos			X			
	D.1.3 - Modelo híbrido	X					X
	D.1.4 - Interoperabilidade						
	D.1.5 - Eficiência			X			
5.Indicadores operacionais	E.1.1 - Sup. Informação	X	Eficácia	X	Eficácia	X	X
	E.1.2 - Otimizar Processos adm	X	Eficiência	X	Eficiência	X	T. Decisão
	E.1.3 - Otimizar Processos Log	X		X	Interop.	X	Governance
	E.1.4 - Serviço público-alvo				Paridade		
	E.1.5 - Ciberespaço	X				X	
6.Indicadores estruturais	F.1.1 - Reestruturação	X	X		X	X	
	F.1.2 - Desmaterialização	X			Recursos	X	X (definida)
	F.1.3 - Gestão informação	X			Treino	X	X
7.Indicadores genéticos	G.1.1 - Talentos digitais	X	X			X	X
	G.1.2 - Tecnologias	X	X	X	X	X	X (Integridade)
	G.1.3 - Doutrina		X		X	X	X
	G.1.4 - Investimento	X	X		X (ID&I)	X	ID&I
	G.1.5 - Liderança digital	X	X			X	X
	G.1.6 - Cultura digital	X	X			X	X
	G.1.7 - Formação e treino	X	X	X		X	X
8.Segurança da informação	H.1.1 - <i>Cloud</i> da defesa.	X			X	X	X
	H.1.2 - <i>Cloud</i> MS	X					
	H.1.3 - Rede segregada	X			X	X	X
	H.1.4 - Blockchain					X	X
	H.1.5 - Sistemas seguros	X	X		X	X	X
9.Alinhamento internacional	I.1.1 -Desconheço			X			
	I.1.2 - Não sei o que fazem.			X			
	I.1.3 - Irrelevante						
	I.1.4 - Devemos estar	X	X	X	X	X	X
	I.1.5-Interoperabilidade	X	X		X	X	X
10.Operações centradas em rede	J.1.1 - Irrelevante			X			
	J.1.2 - Relevante		X		X	X	
	J.1.3 - Reestruturação						
11.Indústria 4.0	K.1.1 - Irrelevante						
	K.1.2 - Relevante	X	X		X	X	X(ID&I)



Apêndice D — Guião e análise das entrevistas finais

No sentido de se obter uma posição do EMGFA e dos Ramos sobre a temática em estudo, foi realizada uma entrevista assente nas seguintes questões:

1. Qual o estado atual e a ambição/visão do EMGFA/Marinha/Exército/FAP, relativamente à implementação da transição digital? Está prevista alguma Estratégia ou Diretiva Estratégica?
2. Qual a ambição da implementação de tecnologias da indústria 4.0, nomeadamente o *big data*, a Internet das coisas (IoT), a Inteligência Artificial, *Machine Learning* ou *Deep Learning*?
3. Como vê que a transição digital poderá ser uma mais-valia na perspetiva operacional? Poderá melhorar o comando e controlo, bem como, o processo de decisão?
4. Na perspetiva estrutural como considera que a transição digital poderá agilizar os processos, contribuindo para a redução de recursos humanos nas FFAA? (Será o *Robotic Process Automation* [RPA] uma solução?)
5. Na perspetiva genética, considera que a edificação das capacidades de uma arquitetura organizacional que permita otimizar a gestão de recursos da organização, seja uma oportunidade para a implementação do processo da transição digital?
6. Considera essencial que a evolução das FFAA acompanhem o desenvolvimento tecnológico, promovendo a interação homem-máquina, através da investigação, desenvolvimento e inovação?
7. Considera que a transição digital deverá ser uma estratégia parcelar de cada Ramo ou uma estratégia conjunta?

Apenas responderam ao presente questionário os Ramos, tendo respondido da Marinha em 24 de junho de 2022, o CFR M Véstia Cagarrinho, da Divisão de Planeamento, demonstrando a posição formal do Ramo respeitante às questões supra. Do Exército respondeu o TCOR TM Paulo Soares, da Direção de Comunicações e Sistemas de Informação (DCSI) em 01 de agosto de 2022, realçando que as respostas respeitantes ao Ramo, são da sua exclusiva responsabilidade. Da Força Aérea respondeu às questões o Coronel Bruno Cabaço da DIRCSI em 29 de julho de 2022.

Respostas às questões:

1. Marinha:

Respeitante à questão 1, a Diretiva Estratégica do ALM CEMA de 2022 prevê a finalidade de uma Marinha tecnologicamente avançada, consubstanciada por três objetivos estratégicos: potenciar a inovação tecnológica; acelerar a digitalização e a informatização; e, promover a independência tecnológica.

Adicionalmente a Marinha edificou o Programa Intersectorial para a Transição Digital (PIDigi), o qual contém um conjunto alargado de iniciativas conducentes a uma transição digital acelerada e concertada.

No que concerne à questão 2, os OEst, assim como o PIDigi, atrás referidos são operacionalizados por um conjunto de iniciativas estratégicas em que parte delas potenciam a utilização do *big data*, da IA e do ML, pelo que está presente a ambição da sua implementação a curto/médio prazo. No entanto é necessário ter a consciência que o IoT, por exemplo, apresenta imensas potencialidades, mas acarreta riscos que devem ser acautelados ou pelo menos identificados. Por exemplo os vírus, *malware*, *spyware*, etc... que antigamente podiam comprometer as *pen drives*, ou outros dispositivos móveis (*smartphones*, portáteis) poderão prejudicar ou atacar/danificar sistemas complexos de C2, ou outros, com impactos muito significativos.

Quanto à questão 3, a utilização de ferramentas que facilitem o C2 e a decisão poderá ter um impacto significativo na perspetiva operacional uma vez que tornará a utilização destes processos mais célere e automatizada procurando minimizar ao máximo o erro humano, facilitando o decisor nas suas funções.

Relativo à questão 4, a digitalização dos processos por si só poderá não contribuir para a redução da necessidade de intervenção por recursos humanos. É importante acompanhar a digitalização com automatização, recorrendo a ferramentas que efetivamente garantam essa redução, ou melhor, uma realocação ou alteração de tarefas. No entanto, neste contexto de transição digital, julgo que o foco não deverá ser o de reduzir recursos humanos nas FFAA, mas sim, o de libertar esses recursos para tarefas mais importantes que não poderão ser substituídas por processos digitalizados. As pessoas são uma parte fundamental do sucesso ou do fracasso desta transformação. O RPA poderá, por exemplo, ser utilizado para automatizar a troca de dados entre sistemas, mas existem outras técnicas que poderão ser adotadas, tal como o PLN, com o objetivo de reduzir a necessidade de intervenção de recursos humanos e contribuir dessa forma para a sua otimização. De referir que a adoção destas duas técnicas consta no PIDigi.

Respeitante à questão 5, respondeu sim, havendo várias formas de otimizar recursos, no entanto, face à crescente e rápida evolução tecnológica com que atualmente nos deparamos a adoção de uma arquitetura da organização baseada numa transição digital poderá potenciar a otimização e a gestão de recursos das FFAA:

No que se prende com a questão 6, considera importante acompanhar os desenvolvimentos tecnológicos como forma de não cairmos na obsolescência de processos e de sistemas.



Adicionalmente, sem investigação e desenvolvimento, qualquer evolução é mais lenta, senão mesmo inexistente, pelo que é importante investir na inovação, na investigação, na experimentação e no desenvolvimento para aumentar a independência tecnológica necessária para que as FFAA consigam cumprir com a sua missão sem depender de terceiros.

Relativo à questão 7, deverá ser um processo do Ramo para aquilo que é mais específico, em paralelo com um processo conjunto e coordenado para tudo aquilo que é transversal e de potencial utilização por todos os Ramos.

2. Exército:

Relativo à questão 1, respondeu que todos os *stakeholders* do ecossistema da DN e em particular os constituintes das FFAA estão empenhados na TD (forma como o Exército designa a TDig), como forma de potenciar o seu produto operacional, direta ou indiretamente, pela simplificação e eficiência processual e de tomada de decisão. No caso do Exército, a visão que materializa esta ambição está incorporada nas Diretivas Estratégicas do Exército, desde 2019, como um OEst a alcançar, sendo que, desde a criação do Centro Informático do Exército (CIE), este tem sido um objetivo presente no Exército, exceto talvez no momento da criação na Secretaria-Geral do MDN (SGMDN) da Equipa de Engenharia e Aplicações Legadas (EEAL), e extinção do CIE até 2013, quando ocorreu a transferência da EEAL para a DCSI.

Respeitante à questão 2, respondeu que estas tecnologias são o futuro e as potencialidades que prometem têm de ser utilizadas em proveito das FFAA, quando forem maduras, mas para isso as instituições que as vão utilizar têm de evoluir no seu conhecimento das mesmas e internamente para as poderem absorver de forma útil e proveitosa e adaptando-se para que a implementação ocorra sem impactos negativos. O Exército está ativamente nesse caminho e tem participado e promovido várias iniciativas e estruturas para aprender estas e outras tecnologias, nomeadamente:

- a. Nas iniciativas do CINAMIL, à semelhança do CINAV e CIAFA na Marinha e Força Aérea, respetivamente;
- b. A participação e proposta de iniciativas estratégicas nestes domínios;
- c. A edificação, no contexto do Pólo Tecnológico do Exército (PTEx), para uma colaboração próxima e profícua com o Sistema Científico e Tecnológico Nacional (SCTN) e com a Base Tecnológica e Industrial de Defesa (BTID), como entidade responsável pelos pilares da Inovação e Desenvolvimento Tecnológico do Exército do Centro de Experimentação e Modernização Tecnológica do Exército (CEMTEX), que se encontra em edificação decorrente da publicação da alteração da Lei Orgânica do Exército em 24 de janeiro de 2022.

Quanto à questão 3, respondeu que o Exército, tem como um dos objetivos máximos, a exploração das oportunidades da TD para modernizar o processo de decisão. De facto, esse compromisso está vertido na Diretiva Sectorial 22/23 da DCSI, sendo uma das principais responsabilidades desta Direção. A DCSI pretende assegurar a superioridade de informação e de decisão no Exército, proporcionando pela progressiva desmaterialização da informação, o acesso mais célere à informação estruturada, permitindo decisões cada vez mais rápidas, oportunas e acertadas. Na perspetiva operacional consideramos que o processo de decisão tem como corolário, a utilização operacional da informação necessária, no momento certo e de forma segura, a todos os níveis e escalões hierárquicos, sendo que no atual contexto legislativo (LOEMGFA e alterações das Leis Orgânicas [LO] dos Ramos) tem de ser o EMGFA a liderar os esforços de integração no nível operacional.

Relativamente à questão 4, respondeu que a intenção do Exército subjacente à promoção da TD nunca foi de redução de recursos humanos, mas de, por esta via, reafectar os recursos humanos existentes a outras áreas de ação, nomeadamente a tática e operacional. A TD por via da promoção da desmaterialização e agilização de processos, favorece a forma como os militares e civis do Exército trabalham e se relacionam. Por um lado, contribui para um incremento da eficiência e, por outro, permite antecipar necessidades, estabelecer meios mais eficazes de comunicação e melhorar continuamente os serviços a disponibilizar. O principal desafio da TD do Exército é proporcionar aos seus utilizadores, serviços seguros, acessíveis e sem esforço, facilitando e reduzindo interações, disponibilizando e reutilizando dados e promovendo a eficiência, sustentabilidade e simplificação dos processos de funcionamento do Exército. O RPA é uma solução, sendo um domínio, que tal como as tecnologias mencionadas na questão 2 tem de ser estudada para poder ser assimilada de forma útil e proveitosa, e sem impactos negativos, nomeadamente a drástica redução de recursos humanos.

Relativo à questão 5, respondeu que sim. A TD deve estar presente na edificação de capacidades, para permitir a criteriosa gestão de recursos e para potenciar a utilidade do produto operacional das capacidades edificadas.

Relativo à questão 6, respondeu que sim. Remetemos para a resposta à questão 2. O Exército está empenhado na sua evolução, a par do desenvolvimento tecnológico e tem várias iniciativas em curso.

Relativo à questão 7, respondeu que a TD é atualmente uma estratégia parcelar, sendo escassos os pontos de contacto e de sincronia conjuntos e todos eles essencialmente centrados na SGMDN, com as Reuniões da Comissão de Acompanhamento (RCA) para os Sistemas de Informação (SI), no âmbito da Comissão de Políticas e Auditoria do Sistema de Informação da Defesa Nacional (CPASIDN). O facto é que o EMGFA não dispõe de capacidade instalada para planear, normalizar e sincronizar a TD nas FFAA, mas decorrente das novas LO publicadas em 24 de janeiro é expectável que essa responsabilidade seja assumida pelo EMGFA.



3. Força Aérea:

Relativamente à questão 1, respondeu que a Força Aérea dispõe de um conjunto de metas/iniciativas assentes na TDig, enquadradas no âmbito das iniciativas integráveis das FFAA, que assentam muitas delas no SIGDN e outras enquadram-se no SIMPLEX, e ainda, tem outras orientadas para o produto operacional, nomeadamente no que respeita ao C2 (pese embora haja sempre o *caveat* da segurança da informação). A DEEMFA, aprovada a 07 de julho de 2022, realça a TDig como prioridade estratégica, pretendendo simplificar e agilizar a decisão, alavancada pela ligação entre sistemas físicos e virtuais e pelas áreas que caracterizam as organizações 4.0, através de um processo de TDig sustentado e apoiado por tecnologias disruptivas.

Respeitante à questão 2, respondeu que é uma ambição refletida na Diretiva Estratégica do Estado-Maior da Força Aérea (DEEMFA), embora seja uma tecnologia que está parcialmente implementada, nomeadamente na evolução dos sistemas de C2, através da edificação do *Portuguese Sky Sentinel System* (PS3) (semelhante ao *oversees* da Marinha, mas orientado para o vetor aéreo). Embora o PS3 ainda esteja em desenvolvimento, já dispõe de dois módulos a operar que integram IA:

1º Módulo para apoio no combate aos incêndios – A Força Aérea fornece produtos e serviços ao CCOM, assente em informação não classificada;

2º Módulo de busca e salvamento (informação classificada);

Além destes, está em desenvolvimento um 3º Módulo de ISR (informação não classificada) que integra uma componente forte de IA, BI e *big data*.

Contudo, a Força Aérea ambiciona ainda, desenvolver um 4º módulo de Lições Aprendidas que recebe informação dos três módulos anteriores, armazenando e analisando os dados e informação para apoio operacional. Este módulo integrará uma forte componente de IA e BI e *big data*.

Quanto à questão 3, respondeu que a TDig poderá ser uma mais-valia nesta perspetiva, se for edificada de forma transversal, ou seja tem de ser um planeamento delineado e integrado pelos três Ramos e pelo EMGFA, de modo a conseguir obter-se a vantagem da informação, contribuindo para o conjunto, bem como, para a especificidade de cada Ramo.

A TDig poderá ser vantajosa na superioridade informacional, caso seja aprimorada com o processo de BI, filtrando a informação e com o estabelecimento de objetivos e métricas. A TDig permite fazer esse filtro a toda a informação e com o BI, podemos ter métricas bem definidas, contribuindo para a visão e orientação estratégica, melhorando a decisão.

Relativo à questão 4, respondeu que importa realçar três perspetivas:

1. A decisão assenta no fator humano;
2. A decisão assenta no fator máquina;
3. A decisão repartida entre ambos, ou seja, para tarefas repetitivas, pode recair na máquina, mas as de maior responsabilidade ficarem exclusivas ao fator humano.

Na perspetiva da Força Aérea em particular, e das FFAA em geral, o fator humano deverá estar sempre presente no processo de decisão, sendo a terceira perspetiva a que melhor se enquadra.

Porém o foco, deverá recair no percurso da automatização e digitalização de processos. Todavia, importa realçar que a automatização requer investimentos, logo é um processo que poderá trazer vantagem operacional, mas com grande desvantagem orçamental, o que requer uma clarificação entre ganhos e perdas. A confiança na gestão dos processos é outro problema conexo a sistemas automatizados que dificulta a sua implementação.

Respeitante à questão 5, respondeu que sim, porque vai obrigar à definição de indicadores e métricas para automatização. Presentemente está em curso o mapeamento da estrutura, dos cargos, sendo que ao nível tecnológico (arquitetura de base) está numa fase de evolução, com diversas ferramentas tecnológicas nas variadas áreas da estrutura, que permite garantir produtos e serviços para os Ramos e EMGFA (CCOM).

A nível administrativo o SIGDN é o parceiro de excelência porque associado ao SIMPLEX permite desenvolver projetos na arquitetura organizacional. Constitui-se uma oportunidade que não devemos perder, contudo dificilmente conseguiremos implementar com a celeridade desejada, face ao peso orçamental.

Quanto à questão 6, respondeu que sim, pois o poder aéreo de 5ª geração, é um bom exemplo desta capacidade e necessidade de interação homem-máquina. Sendo a Força Aérea um Ramo altamente tecnológico, é fundamental ter uma capacidade de ID&I para alimentar a capacidade de interação homem-máquina e de toda a componente tecnológica, tanto pela obsolescência (descontinuidade que limita a interoperabilidade com sistemas mais modernos, ou descontinuidade na manutenção ou sustentação logística), a par da necessidade de acompanhar a evolução no espectro combinado. Logo, é importante sempre aprender, evoluir e automatizar com base nas Lições Aprendidas.

Relativamente à questão 7, respondeu que poderá haver uma estratégia conjunta, orientada para o que é transversal às FFAA, sendo que a gestão do que é específico a cargo do Ramo. Por exemplo, na estratégia conjunto poder-se-ia enquadrar a Gestão documental e a Gestão de Pessoal, entre outras áreas.

De modo a simplificar a leitura do conteúdo das entrevistas, apresenta-se uma matriz de análise de conteúdo das mesmas, conforme Tabela 5.



Tabela 5 - Matriz de análise de conteúdo

Questão	Marinha	Exército	Força Aérea
1. Qual o estado atual e a ambição/visão do EMGFA/Marinha/Exército/FAP, relativamente à implementação da transição digital? Está prevista alguma Estratégia ou Diretiva Estratégica?	Potenciar a inovação tecnológica; acelerar a digitalização e a informatização; e, promover a independência tecnológica	Potenciar o seu produto operacional, direta ou indiretamente, pela simplificação e eficiência processual e de tomada de decisão	<u>Simplificar e agilizar a decisão</u>
2. Qual a ambição da implementação de tecnologias da indústria 4.0, nomeadamente o <i>big data</i> , a Internet das coisas (IoT), a Inteligência Artificial, <i>Machine Learning</i> ou <i>Deep Learning</i> ?	Iniciativas estratégicas que potenciam a implementação destas tecnologias e curto/médio prazo.	Iniciativas estratégicas que requerem ainda experimentação e maior maturidade antes da sua implementação.	Ambição prevista e em desenvolvimento, vertida em sistemas complexos.
3. Como vê que a transição digital poderá ser uma mais-valia na perspetiva operacional? Poderá melhorar o comando e controlo, bem como, o processo de decisão?	Através de ferramentas que possam tornar o processo mais célere e automatizado, reduzindo o erro humano.	Através da superioridade de informação e decisão, através do acesso mais célere à informação estruturada, permitindo decisões mais rápidas, oportunas e acertadas.	Permite obter vantagem da informação se for aprimorada com o processo de BI e com métricas, alinhadas com a visão e orientação estratégica.
4. Na perspetiva estrutural como considera que a transição digital poderá agilizar os processos, contribuindo para a redução de recursos humanos nas FFAA? (Será o RPA uma solução?)	Considera essencial haver a digitalização acompanhada pela automatização, permitindo libertar RH para outro tipo de tarefas. O RPA é uma solução entre outras.	Considera essencial por via da desmaterialização e agilização de processos, sendo o RPA uma solução, contribuindo para uma redução de RH.	Considera essencial a agilização de processos e que a tendência é a automatização, contudo as decisões mais relevantes devem estar nos humanos.
5. Na perspetiva genética, considera que a edificação das capacidades de uma arquitetura organizacional que permita otimizar a gestão de recursos da organização, seja uma oportunidade para a implementação do processo da transição digital?	É essencial para potenciar a otimização e a gestão de recursos nas FFAA.	É essencial para permitir a criteriosa gestão de recursos e para potenciar a utilidade do produto operacional.	É essencial obrigando a definição de indicadores e métricas para a automatização. Neste momento está em curso o mapeamento da estrutura.
6. Considera essencial que a evolução das FFAA acompanhem o desenvolvimento tecnológico, promovendo a interação homem-máquina, através da investigação, desenvolvimento e inovação?	É essencial para não se cair na obsolescência de processos e de sistemas.	É essencial, tendo em curso diversas iniciativas desenvolvidas pelos centros tecnológicos.	É essencial, pois esta é a base para aprender, evoluir e automatizar com base nas lições aprendidas.
7. Considera que a transição digital deverá ser uma estratégia parcelar de cada Ramo ou uma estratégia conjunta?	Deve ser conjunto para tudo que é transversal e do Ramos apenas para o que é específico.	Embora seja parcelar, a tendência é ser conjunta.	Deve ser conjunta para o que é transversal e parcelar para o que é específico.



Apêndice E — Caracterização da envolvente estratégica

O ambiente estratégico abrange uma análise do ambiente externo (Oportunidades e Ameaças) e do ambiente interno (Potencialidades e Vulnerabilidades), integrados nos vetores que edificam uma capacidade militar (DOTMLPII).

Os fatores foram elencados baseados na análise dos questionários (Capítulo 3 e Apêndice B) e entrevistas (Apêndice D), a par da análise documental, assente nos documentos doutrinários das organizações internacionais que Portugal é parceiro, nomeadamente a NATO e a UE, bem como as FFAA dos EUA, enquanto parceiro de referência, conforme vertido no capítulo 4 desta investigação, onde analisa o ambiente estratégica na perspetiva internacional. A nível nacional, a identificação dos fatores do ambiente externo deve assentar na legislação e documentos de referência do Estado, e para identificação dos fatores do ambiente interno em documentos enquadrantes das FFAA portuguesas.

Quadro 4 - Fatores do ambiente externo

Vetor de Capacidade	Oportunidades		Fonte	Ameaças		Fonte
Doutrina	O1	Perspetiva internacional, nomeadamente da NATO e da EU.	(CEU, 2020); Conselho de Ministros (2017); e NATO (2019b).	A1	Algumas diferenças de abordagem à Transição Digital.	Acordo capítulo II do Corpo de Trabalho; G. Westerman & Soul (2016).
Organização	O2	Processos decisórios ágeis assente na superioridade de informação.	Conselho de Ministros (2017); Nunes (<i>op. cit.</i>); Tendeiro (<i>op. cit.</i>); CEU (2020); MDN-CCEM (2014) Carvalho (<i>op. cit.</i>); e Sousa (<i>op. cit.</i>).	A2	Aumento da instabilidade geopolítica que pode levar a um ataque a membros da NATO/EU, com maior incidência no ciberespaço.	Comissão Europeia (2017) e EMGFA (2021).
Treino	O3	Desenvolvimento de competências digitais.	Conselho de Ministros (2020).	A3	Manutenção das competências digitais face a evolução tecnológica.	(IBEC, 2017) e Corpo do trabalho.
Material	O4	Potencialidade da i4.0 no domínio informacional e na automatização dos processos e sistemas.	(Governo de Portugal, 2019).	A4	Volume de dados e informação não tratada que leva à desinformação.	(Marinha, 2018a, p. E-6) e Sousa (<i>op. cit.</i>).
Liderança	O5	Empenhamento do sistema político na ID&I, e na transição digital.	Gov. de Portugal. (2019); (Conselho de Ministros, 2020); (Governo de Portugal, 2019); (MDN, 2020); Marques (<i>op. cit.</i>); e (Moreira, 2021).	A5	Ameaças cibernéticas que comprometem a salvaguarda da informação.	Carvalho (<i>op. cit.</i>).
Pessoal	O6	Maior necessidade de otimização dos recursos humanos.	(MDN, 2015).	A6	Alargamento exponencial do mercado aos talentos digitais.	Carvalho (<i>op. cit.</i>) e (Monteiro, 2020).
Infraestruturas	O7	Maior racionalização de estruturas.	(MDN, 2020).	A7	Maior exploração da dimensão informacional para fins maliciosos.	Ribeiro (2020) e Sousa (<i>op. cit.</i>).
Interoperabilidade	O8	Maior investimento em tecnologia interoperável.	MDN (2020); Ribeiro (2020).	A8	A velocidade da evolução tecnológica dificulta a interoperabilidade.	Conselho de Ministros (2017).



Quadro 5 - Fatores do ambiente interno

Vetor de Capacidade	Potencialidades		Fonte	Vulnerabilidades		Fonte
Doutrina	P1	Normativos que integram a inovação e a transição digital.	EMGFA (2021); Marinha (2020a); Marinha (2021a); MDN (2020); e Despacho n.º 13692/2013, de 28 de outubro.	V1	Falta de uma estratégia única e doutrina conjunta.	Todos os entrevistados de forma geral fizeram referência; Carvalho (<i>op. cit.</i>); e Tendeiro (<i>op. cit.</i>).
Organização	P2	Implementados projetos digitais e ciberdefesa.	Governo de Portugal (2018); Governo de Portugal (s.d.); Conselho de Ministros (2019) e Carvalho (<i>op. cit.</i>).	V2	Processo decisório, de coordenação e de C2 com fragilidades e burocratizados.	EMGFA (2021); Tendeiro (<i>op. cit.</i>).
Treino	P3	Qualidade de formação e com competências digitais.	Marques (<i>op. cit.</i>); Marinha (2021a, p. 10) e Acordo apêndice B do presente trabalho.	V3	Competências digitais escassas para integração da i4.0.	Francisco (2020); Marques (<i>op. cit.</i>); Apêndice B do presente trabalho e todos os entrevistados fizeram referência.
Material	P4	Existência de TIC e capacidade de gestão da informação.	(Monteiro, 2020); Tendeiro (<i>op. cit.</i>); e Marques (<i>op. cit.</i>).	V4	Tecnologias em quantidade e qualidade em algumas áreas.	Acordo Apêndice B do presente trabalho.
Liderança	P5	Liderança e vontade de integrar a evolução tecnológica.	(Braz, 2008); Tendeiro (<i>op. cit.</i>); (Governo de Portugal, 2018); (EMGFA, 2021); (Marinha, 2020b); e Tendeiro (<i>op. cit.</i>).	V5	Fragilidades de liderança digital orientada para a transição digital.	Francisco (<i>op. cit.</i>) e S Carvalho (<i>op. cit.</i>).
Pessoal	P6	Elevado sentido de missão na concretização dos objetivos.	Marques (<i>op. cit.</i>); e Apêndice B do presente trabalho.	V6	Recrutamento e retenção de talentos de digitais para os desafios da i4.0.	Marques (<i>op. cit.</i>); Francisco (<i>op. cit.</i>); e Carvalho (<i>op. cit.</i>).
Infraestruturas	P7	Existência de infraestruturas dedicadas.	Leis Orgânicas do EMGFA e Ramos; e Lei de Defesa Nacional (2021).	V7	Arquitetura focada na tecnologia e na segurança digital.	Carvalho (<i>op. cit.</i>); e Tendeiro (<i>op. cit.</i>).
Interoperabilidade	P8	Edificação de capacidades conjuntas interoperáveis entre si e com os aliados.	Ribeiro (2020) e (EMGFA, 2021).	V8	Fragilidades na partilha de informação.	Sousa (<i>op. cit.</i>); (EMGFA, 2021); e Marques (<i>op. cit.</i>).

1. Priorização dos fatores

Na sequência da caracterização do ambiente estratégico, importa priorizar os fatores face à gestão to risco tendo em conta a probabilidade e o impacto, ou seja, potencializando a probabilidade de ocorrer e minimizando o impacto, procurando obter-se o nível de risco associado (Probabilidade X Impacto) (Comissão Europeia, 2018). No sentido de agilizar o processo de priorização, foram definidas as seguintes escalas:

- Probabilidade: Muito alto = 5 / Alto = 4 / Médio = 3 / Baixo = 2 / Muito Baixo = 1.
- Impacto: Muito alto = 5 / Alto = 4 / Médio = 3 / Baixo = 2 / Muito Baixo = 1.

Tabela 6 - Avaliação da probabilidade e impacto dos fatores

Fatores de Oportunidades	Probabilidade	Impacto	Nível de risco associado	Fatores de Ameaças	Probabilidade	Impacto	Nível de risco associado	Fatores de Potencialidades	Probabilidade	Impacto	Nível de risco associado	Fatores de Vulnerabilidades	Probabilidade	Impacto	Nível de risco associado
O1	4	4	16	A1	3	2	6	P1	5	3	15	V1	3	3	9
O2	2	5	10	A2	4	3	12	P2	4	3	12	V2	2	5	10
O3	3	5	15	A3	2	4	8	P3	5	2	10	V3	4	5	20
O4	5	3	15	A4	4	4	16	P4	2	4	8	V4	3	2	6
O5	3	3	9	A5	2	5	10	P5	3	3	9	V5	2	4	8
O6	2	5	10	A6	3	4	12	P6	4	4	16	V6	4	4	16
O7	1	5	5	A7	4	5	20	P7	4	2	8	V7	3	5	15
O8	3	4	12	A8	5	3	15	P8	3	5	15	V8	4	3	12

Tabela 7 - Matriz de Probabilidade/Impacto dos fatores

		Impacto				
		1=Muito baixo	2=Baixo	3=Médio	4=Alto	5=Muito Alto
Probabilidade	5=Muito Alto		P3	O4 / A8 / P1		
	4=Alto		P7	O8 / A2 / P2 / V8	O1 / A4 / P6 / V6	A7 / V3
	3=Médio		A1 / V4	O5 / P5 / V1	A6	O3 / P8 / V7
	2=Baixo				O6 / A3 / P4 / V5	O2 / A5 / V2
	1=Muito baixo					O7

Legenda:

	Risco muito baixo.
	Risco médio.
	Risco elevado.
- - -	Propensão ao risco.

Fonte: Adaptado a partir de P2M da Comissão Europeia (2018).

Da matriz supra, pode-se concluir que apenas a ameaça A7 (Maior exploração da dimensão informacional para fins maliciosos) e a vulnerabilidade V3 (Fragilidades ao nível das competências digitais para integração das tecnologias da i4.0) apresentam um risco muito elevado, atendendo que A7 apresenta cada vez maior probabilidade e maior risco nas sociedades modernas. A V3 também apresenta grande probabilidade face às competências digitais necessárias para incrementar tecnologias da i4.0, a par do impacto que estas podem trazer para a organização pela não integração destas tecnologias perante o aumento de ameaças híbridas e com tecnologias avançadas.



Apêndice F — Alinhamento das LAE com os vetores capacidade

Quadro 6 - Alinhamento das LAE com os vetores capacidade

			D	O	T	M	P	L	I	I
Perspetiva Genética	OEst1 - ESTABELECER a capacidade de gestão integrada de dados e informação.	LAE1.1	Edificar uma visão, princípios orientadores, valências básicas e objetivos da gestão integrada de dados e informação.	X						
		LAE1.2	Estabelecer uma estrutura conjunta de gestão de dados e informação.		X			X		
		LAE1.3	Garantir a partilha de dados com qualidade e segurança.		X				X	X
	OEst2 - INCREMENTAR uma arquitetura organizacional conjunta.	LAE2.1	Edificar o modelo de governação e gestão da arquitetura organizacional.		X					
		LAE2.2	Erguer a arquitetura organizacional da defesa.	X	X			X	X	X
		LAE2.3	Produzir doutrina conjunta.	X						
	OEst3 - FORTALECER a capacidade de ID&I.	LAE3.1	Edificar uma estrutura conjunta com ligação à indústria, universidades e polos ou centros de investigação e desenvolvimento.		X			X	X	X
		LAE3.2	Estimular a interação homem-máquina e outras tecnologias disruptivas.					X	X	
		LAE3.3	Garantir a interoperabilidade.							X
Perspetiva Estrutural	OEst4 - INCENTIVAR o desenvolvimento de competências digitais.	LAE4.1	Estabelecer um plano de conhecimentos por níveis, face à categoria e à função.		X			X		
		LAE4.2	Estimular a avaliação digital.		X	X			X	
		LAE4.3	Promover programas de formação adaptados às necessidades e ao atual nível de conhecimento.			X				
	OEst5 - DESENVOLVER a liderança digital.	LAE5.1	Potencializar o processo de decisão mais descentralizado e ágil.			X			X	
		LAE5.2	Incentivar uma cultura centrada nas pessoas e nos processos, recorrendo à tecnologia.			X		X		
		LAE5.3	Estimular uma cultura de inovação assente na fruição de ideias e em processos ágeis e interativos.						X	
	OEst6 - CONSOLIDAR a otimização de processos.	LAE6.1	Centralizar componentes transversais numa gestão comum.		X		X	X		X
		LAE6.2	Reforçar a desmaterialização, integrando IA e o PLN nos processos de gestão, tendendo para a automatização.		X		X	X		X
		LAE6.3	Agilizar os fluxos de trabalho entre Unidades ou Serviços (<i>smart working</i>).		X	X		X		
Perspetiva Operacional	OEst7 - POTENCIAR a superioridade de informação e do conhecimento.	LAE7.1	Modernizar a infraestrutura de rede, integrando e promovendo as boas práticas empresariais.				X			X
		LAE7.2	Edificar uma organização de inovação capacitada para acompanhar e integrar tecnologias emergentes.		X			X	X	
		LAE7.3	Proteger a informação.			X	X	X		X
	OEst8 - IMPLEMENTAR um processo de decisão, de coordenação e de C2 ágil.	LAE8.1	Edificar um modelo de C2 Ágil.	X	X	X				
		LAE8.2	Integrar IA em sistemas de C2.				X			
		LAE8.3	Desenvolver treino do exercício de C2 Ágil.			X				
	OEst9 - CONSOLIDAR a capacidade de ciberdefesa.	LAE9.1	Contribuir para a superioridade e partilha de informação.		X	X		X		
		LAE9.2	Promover as capacidades de <i>computer network</i> .		X	X				
		LAE9.3	Contribuir para a segurança da informação.	X	X	X	X			X



Apêndice G — Alinhamento das LAE com a estratégia e planos nacionais

Quadro 7 - Alinhamento das LAE com a legislação nacional

			Estratégia para a TD na AP (RCM n.º 108/2017, 2 de março)	Plano de Ação para Transição Digital (RCM n.º 30/2020, 21 de abril)	Estratégia para a TD na AP 2021-26 (RCM n.º 131/2021, 10 de setembro)
Perspetiva Genética	OEst1	LAE1.1	Eixo (E) I - Integração e Interoperabilidade (Medida (M) 1: Governação TIC).	Catalisador (C) 2 - Economia circular dos dados.	LAE II - Valorização dos dados (OEst 2.5)
		LAE1.2	E I - Integração e Interoperabilidade (M4: Arquitetura ref. TIC).	C2; C3 - Conectividade e infraestrutura; e C4 - Tecnologias disruptivas.	LAE II - Valorização dos dados (OEst 2.4)
		LAE1.3	EIII - Partilha recursos (M10: Centros de dados nuvem).	C2 - Economia circular dos dados.	LAE II - Valorização dos dados (OEst 2.2)
	OEst2	LAE2.1	E I - (M1) / (M4).	D - Modelo de governação (p.27); C3.	LAE III – Arquiteturas de referência (OEst 3.1)
		LAE2.2	E I - (M4: Arquitetura de ref. TIC).	C3 - Conectividade e infraestrutura.	LAE III – Arquiteturas de referência (OEst 3.1)
		LAE2.3	Objetivo principal: “Potenciar a adesão aos serviços digitais por parte dos cidadãos e das empresas”.	C5 - Alinhamento com a estratégia digital europeia; C6 - Comunicação e promoção.	LAE III – Arquiteturas de referência (OEst 3.8)
	OEst3	LAE3.1	E II - Inovação e competitividade (M8: Inovação setorial).	Subpilar (Su) II.2 - Tecido empresarial; C4; M8 - <i>Digital Innovation Hubs</i>	LAE IV - Competências das TIC (OEst 4.5)
		LAE3.2	E II - Inovação e competitividade (M8).	C4; C5 - Alinhamento com a estratégia digital europeia.	LAE II - Valorização dos dados (OEst 2.5)
		LAE3.3	E I - (M3: Interoperabilidade).	C3 - Conectividade e infraestrutura.	LAE III – Arquiteturas de referência (OEst 3.8)
Perspetiva Estrutural	OEst4	LAE4.1	Princípio Orientador: “O reforço das competências digitais dos colaboradores da AP...”	Su I.1 - Educação digital.	LAE IV - Competências das TIC (OEst 4.2)
		LAE4.2		Su I.3 - Inclusão e literacia digital; (C6).	LAE IV - Competências das TIC (OEst 4.3)
		LAE4.3		Su I.2 - Formação profissional e requalificação; M2 - Programa de formação intensiva e especializada.	LAE IV - Competências das TIC (OEst 4.4)
	OEst5	LAE5.1	Projeto Estratégico da DN: “Apoio à tomada de decisão”. Ainda refere: “...AP mais ágil...”	Su III.2 - Administração central ágil e aberta;	LAE II - Valorização dos dados (OEst 2.1)
		LAE5.2	“Tornar serviços digitais simples, acessíveis e inclusivos”.	Su I.3 - Inclusão e literacia digital.	LAE IV - Competências das TIC (OEst 4.4)
		LAE5.3	E II - Inovação e competitividade (M8).	Su II.1 - Empreendedorismo e investimento; (C6)	LAE IV - Competências das TIC (OEst 4.4)
	OEst6	LAE6.1	E I - (M4). EIII - (M9). (M12: Aplicações comuns...).	Su III.2 - Administração central ágil e aberta; (C3)	LAE I -Serviços Públicos Digitais (OEst 1.3)
		LAE6.2	E I - (M3); E II - (M7 - Serviços eletrónicos; M8).	Su III.1 - Serviços públicos digitais; Su III.2 (C2, C4).	LAE II - Valorização dos dados (OEst 2.4)
		LAE6.3	E II - Inovação e competitividade (M8)	Su III.2 - Administração Central ágil e aberta.	LAE VI - Segurança e Confiança (OEst 6.3)
Perspetiva Operacional	OEst7	LAE7.1	E II - Inovação e competitividade (M8); EIII - Partilha de recursos. (M10: Centros de dados na nuvem).	C2 - Economia circular dos dados; C3 - Conectividade e infraestrutura; C4 - Tecnologias disruptivas.	LAE V - Infraestrutura e Serviços TIC (OEst5.2)
		LAE7.2	E II - (M 8); E I - Integração e Interoperabilidade. (M4).	C2; C4 - Tecnologias disruptivas.	LAE IV - Competências das TIC (OEst 4.5)
		LAE7.3	“A segurança, resiliência e privacidade dos dados, por forma a assegurar a salvaguarda da informação”	C1 - Regulação, privacidade, cibersegurança e ciberdefesa.	LAE VI - Segurança e Confiança (OEst 6.4)
	OEst8	LAE8.1	Projeto Estratégico da DN: “Apoio à tomada de decisão”. Ainda refere: “...AP mais ágil...”	Su III.2 - Administração central ágil e aberta.	LAE IV - Competências das TIC (OEst 4.1)
		LAE8.2	E II - Inovação e competitividade (M8).	C4 - Tecnologias disruptivas.	LAE II - Valorização dos dados (OEst 2.5)
		LAE8.3	EIII - Partilha de recursos. (M9).	Su I.2 - Formação profissional e requalificação.	LAE IV - Competências das TIC (OEst 4.4)
	OEst9	LAE9.1	E II - (M6: Transparência e participação).	C2; C3; C4 - Tecnologias disruptivas.	LAE V - Infraest. e Serviços TIC (OEst5.3)
		LAE9.2	E II - Inovação e competitividade (M 8).	C2; C3; C4 - Tecnologias disruptivas.	LAE VI - Segurança e Confiança (OEst 6.2)
		LAE9.3	Princípio Orientador: “...assegurar a salvaguarda da informação...” E I- (M4: Arquitetura de ref. TIC).	C1 - Regulação, privacidade, cibersegurança e ciberdefesa.	LAE VI - Segurança e Confiança (OEst 6.4)

Fonte: Adaptado a partir de Estratégia para a TD na AP (2017), do Plano de Ação para a Transição Digital (2020) e Estratégia para a Transformação Digital na AP (2021).