INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE PROMOÇÃO A OFICIAL GENERAL

2020/2021

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

O IMPACTO DAS REDES 5G NA SEGURANÇA E DEFESA NACIONAL

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

Jorge Manuel Guerreiro Gonçalves Pedro

CORONEL DE CAVALARIA

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O IMPACTO DAS REDES 5G NA SEGURANÇA E DEFESA NACIONAL

COR CAV Jorge Manuel Guerreiro Gonçalves Pedro

Trabalho de Investigação Individual do CPOG

Pedrouços 2021

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O IMPACTO DAS REDES 5G NA SEGURANÇA E DEFESA NACIONAL

COR CAV Jorge Manuel Guerreiro Gonçalves Pedro

Trabalho de Investigação Individual do CPOG

Orientador: COR TIR ART António José Pardal dos Santos

Pedrouços 2021

Declaração de compromisso Antiplágio

Eu, **Jorge Manuel Guerreiro Gonçalves Pedro**, declaro por minha honra que o documento intitulado "**O Impacto das Redes 5G na Segurança e Defesa Nacional**" corresponde ao resultado da investigação por mim desenvolvida enquanto auditor do **Curso de Promoção a Oficial General 2020/2021** 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, **5** de **maio** de **2021**

Assinado por : **Jorge Manuel Guerreiro Gonçalves Pedro**
Num. de Identificação: BI07650936
Data: 2021.05.05 10:11:05+01'00'

CHAVE MÓVEL

Jorge Manuel Guerreiro Gonçalves Pedro
Coronel de Cavalaria

Agradecimentos

Este trabalho de investigação é o resultado da colaboração de diversas entidades sem as quais não teria sido possível atingir os objetivos propostos. De todas importa destacar o meu orientador, Coronel Tirocinado António José Pardal dos Santos, pelo apoio e orientações que sempre me prestou, mostrando sempre total disponibilidade, camaradagem e elevado profissionalismo. Sem a sua dedicação e superior orientação este trabalho dificilmente teria chegado às suas conclusões, não só porque esteve sempre pronto a dar indicações sobre os caminhos mais adequados a seguir, como desde o início procurou motivar-me, encontrando sempre uma proposta de solução para as dificuldades encontradas. Ter a oportunidade do conhecer e de o ter como orientador foi uma honra e um privilégio que nunca irei esquecer.

Gostaria de agradecer a colaboração de todos os entrevistados que contribuíram com os seus conhecimentos, experiência e disponibilidade para este trabalho, não só na fase analítica como na fase exploratória. De todos não posso deixar de destacar o Contra-Almirante António José Gameiro Marques, pois foi a primeira pessoa a mostrar disponibilidade em apoiar e a fornecer todos os elementos enquadrantes do tema, indicando as diferentes possibilidades de abordagem do mesmo.

Por último, agradeço a todos os camaradas Auditores do Curso de Promoção a Oficial General 2020/2021 o excelente espírito de camaradagem proporcionado através da partilha de experiências e perspetivas, que permitiram a clarificação de conceitos e a revisão de textos, em especial o Coronel Lopes da Silva, bem como aos docentes do Instituto Universitário Militar que me apoiaram nos aspetos relativos à metodologia de investigação científica.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Índice de Tabelas

Resumo

As redes 5G irão proporcionar as condições necessárias à transformação digital da nossa sociedade, no sentido de aumentar a eficiência e a eficácia em diversos domínios como a energia, a saúde, os transportes e os sistemas de controlo industriais.

A implantação das redes 5G terá repercussões nas Forças Armadas ao nível do comando e controlo, da segurança, da logística, da manutenção, da formação e do treino, entre outros.

Neste contexto, este estudo foi realizado com o objetivo geral de formular as linhas de ação que as Forças Armadas Portuguesas devem ter em consideração aquando da implantação das redes 5G em Portugal.

Adotou-se um posicionamento odontológico construtivista e epistemológico interpretativista, baseado num raciocínio indutivo e numa estratégia qualitativa, com recurso a um desenho de pesquisa de estudo de caso, alicerçado na análise dos dados recolhidos em entrevistas semiestruturadas.

Através do levantamento das oportunidades, ameaças, pontos fortes e pontos fracos que caraterizam os ambientes externo e interno, foram formuladas oito linhas de ação que devem ser consideradas pelas Forças Armadas nos seus trabalhos relativos à implantação das redes 5G, de modo a potenciar o seu crescimento, otimização, dinamização e proteção.

Palavras-chave:

5G, Redes, Linhas de Ação, Forças Armadas, Defesa Nacional.

Abstract

5G networks will provide the necessary conditions for society's digital transformation that will increase efficiency and effectiveness in several areas such as energy, health, transport and industrial control systems.

5G networks will impact Portuguese Armed Forces in terms of command and control, security, logistics, maintenance, education and training, among others.

In this context, this study was carried out with the aim to formulate lines of action that Portuguese Armed Forces should take care when deploying 5G networks.

A constructivist ontologically and an interpretative epistemologically philosophies were adopted, based on inductive reasoning and qualitative strategy, using a case study research design, supported by the analysis of the data collected from semi-structured interviews.

Based on opportunities, threats, strengths and weaknesses that define the external and internal environments, eight lines of action were formulated in order to be considered by the Armed Forces in their tasks related with 5G networks deployment, in order to enlarge its growth, optimization, promotion and safety.

Keywords

5G, networks, Lines of action, Armed Forces, National Defence.

Lista de abreviaturas, siglas e acrónimos

1G – Primeira geração de comunicações móveis
2G – Segunda geração de comunicações móveis
3G – Terceira geração de comunicações móveis
4G – Quarta geração de comunicações móveis
5G – Quinta geração de comunicações móveis
ANACOM – Autoridade Nacional de Comunicações
Cat – Categoria
CEDN – Conceito Estratégico de Defesa Nacional
CPOG – Curso de Promoção a Oficial General
DCSI – Direção de Comunicações e Sistemas de Informação
DEstr – Diretiva Estratégica
DIRCSI – Direção de Comunicações e Sistemas de Informação do Estado-Maior-General das Forças Armadas
EMGFA – Estado-Maior-General das Forças Armadas
ENSC – Estratégia Nacional de Segurança no Ciberespaço
EPR – Entidade Primariamente Responsável
FFAA – Forças Armadas
GE1 – Guião de Entrevista n.º 1
GE2 – Guião de Entrevista n.º 2
GCSRI – Grupo de Cooperação Segurança das Redes e da Informação
GNS – Gabinete Nacional de Segurança
GSM – *Global System for Mobile*
ID&I – Investigação, Desenvolvimento e Inovação
IoT – Internet das Coisas (*Internet of Things*)
IUM – Instituto Universitário Militar
LA – Linhas de ação
LTE – *Long Term Evolution*
MDN – Ministério da Defesa Nacional
NATO – *North Atlantic Treaty Organization*
NCIA – *NATO Communications and Information Agency*
NEP – Norma de Execução Permanente
NIS – Segurança das Redes e da Informação (*Network and Information Security*)

O – Oportunidade (*Opportunitie*)
OE – Objetivo Específico
OEstr – Objetivo Estratégico
OG – Objetivo Geral
OOp – Objetivo Operacional
OTAN – Organização do Tratado do Atlântico Norte
Q – Questão
QC – Questão Central
QD – Questão Derivada
RA – Realidade aumentada
RCM – Resolução do Conselho de Ministros
RFID – Identificadores de Rádio Frequência (*Radio Frequency Identification*)
RV – Realidade virtual
S – Ponto Forte (*Strength*)
SWOT – *Strengths*, *Weaknesses*, *Opportunities* e *Threats*
T – Ameaça (*Threat*)
TII – Trabalho de Investigação Individual
UAV – Veículos Aéreos Não Tripulados (*Unmanned Aerial Vehicle*)
UnCont – Unidades de contexto
UE – União Europeia
UnEn – Unidades de enumeração
UnReg – Unidades de registo
W – Ponto Fraco (*Weakness*)

1. Introdução

A tecnologia das redes de comunicações móveis de quinta geração (5G) apresenta-se com um conjunto de características extremamente desafiantes, como sejam uma elevada velocidade de transmissão de dados (por exemplo um *download*[1] de um filme de duas horas que demora atualmente cerca seis minutos passará para três a quatro segundos), uma latência[2] quase nula e uma elevada capacidade em termos de largura de banda, ou seja de transmissão de dados (de MHz para GHz). As redes 5G irão criar as condições para se ter uma sociedade digital, constituindo-se como uma estrutura e uma plataforma crítica que permite finalmente concretizar o que até agora só era possível ver em filmes de ficção científica, como por exemplo a gestão inteligente de infraestruturas e a medicação inteligente (Damião, 2019).

A União Europeia (UE) reconhece que a implantação das redes 5G se traduz em novas oportunidades que devem elevar as preocupações de segurança relacionadas com a integridade e a disponibilidade dessas redes, implicando que os Estados-Membros tenham em especial consideração a salvaguarda da cibersegurança e de todos os serviços a elas associadas (Conselho da União Europeia, 2019). Apesar do processo de implementação das redes 5G ter evoluído na UE, no final de dezembro de 2020, apenas Chipre, Lituânia, Malta e Portugal ainda não tinham lançado serviços 5G (Pujol, Manero, Carle, & Remis, 2021, p. 21).

A Organização do Tratado do Atlântico Norte (OTAN)[3] também reconhece a importância e o impacto das redes 5G no âmbito militar, como foi constatado no conjunto de *workshops* realizados, desde dezembro de 2020, para debater a temática que envolve a implantação das redes 5G (NATO Communications and Information Agency [NCIA], 2021).

Face ainda à Resolução de Conselho de Ministros (RCM) n.º 7-A/2020, 7 fevereiro, que reconhece as caraterísticas das redes 5G como uma importante ferramenta para a transição digital, considera-se de elevada importância o desenvolvimento da presente

[1] Transferência de ficheiros de um computador remoto para um computador local através da internet (Yasmin, 2019).
[2] "Período de tempo decorrido entre o momento em que é dado um comando e a efetiva execução da respetiva operação" (Infopédia - Dicionários Porto Editora, s.d.).
[3] Frequentemente utiliza-se o acrónimo em inglês: NATO - North Atlantic Threaty Organization.

investigação, tendo em vista produzir conhecimento que contribua para as Forças Armadas (FFAA) prepararem a operação em ambiente de redes 5G.

Este trabalho enquadra-se no âmbito das Ciências Militares, na área das Técnicas e Tecnologias Militares (Decreto-Lei n.º 249/2015, de 28 de outubro, 2015, p. 9300), subárea de Comando, Controlo, Comunicações, Computadores e Informação (Academia das Ciências de Lisboa, s.d.), seguindo-se as orientações metodológicas em vigor no Instituto Universitário Militar (IUM) (Fachada, et al., 2020; Santos & Lima, 2019; IUM, 2020a; IUM, 2020b).

O objeto de estudo da presente investigação são as redes 5G, procurando-se saber o seu impacto nas FFAA portuguesas, no contexto das orientações recebidas da UE e OTAN e tendo em consideração as caraterísticas e os campos de aplicação da 5G.

Tendo em consideração a abrangência do tema e o período estabelecido para a realização da investigação, este trabalho foi limitado no conteúdo, espaço e tempo (Santos & Lima, 2019, p. 41). No conteúdo: (i) às caraterísticas da 5G e campos de aplicação militar; (ii) às orientações estabelecidas pela UE e OTAN, designadamente as recomendações e as resoluções da Comissão Europeia, bem como os cenários desenvolvidos pelo Grupo de Cooperação Segurança das Redes e da Informação (GCSRI) e pela NCIA; (iii) às linhas de ação (LA) estabelecidas na Estratégia Nacional de Segurança no Ciberespaço (ENSC); (iv) aos Objetivos Estratégicos (OEstr) estabelecidos nas Diretivas Estratégicas (DEstr) do Estado-Maior-General das Forças Armadas (EMGFA) e Ramos; (v) ao impacto das redes 5G na capacidade militar. No espaço, a investigação foi conduzida a nível nacional, no âmbito da Segurança Nacional, na componente de Segurança no Ciberespaço, e no âmbito da Defesa Nacional, na componente militar. No tempo, procurou-se analisar a situação atual para perspetivar o futuro próximo.

O Objetivo Geral (OG), os Objetivos Específicos (OE), a Questão Central (QC) e as quatro Questões Derivadas (QD) decorrentes dos objetivos estabelecidos, bem como as respetivas relações entre eles, são apresentados na Figura 1.

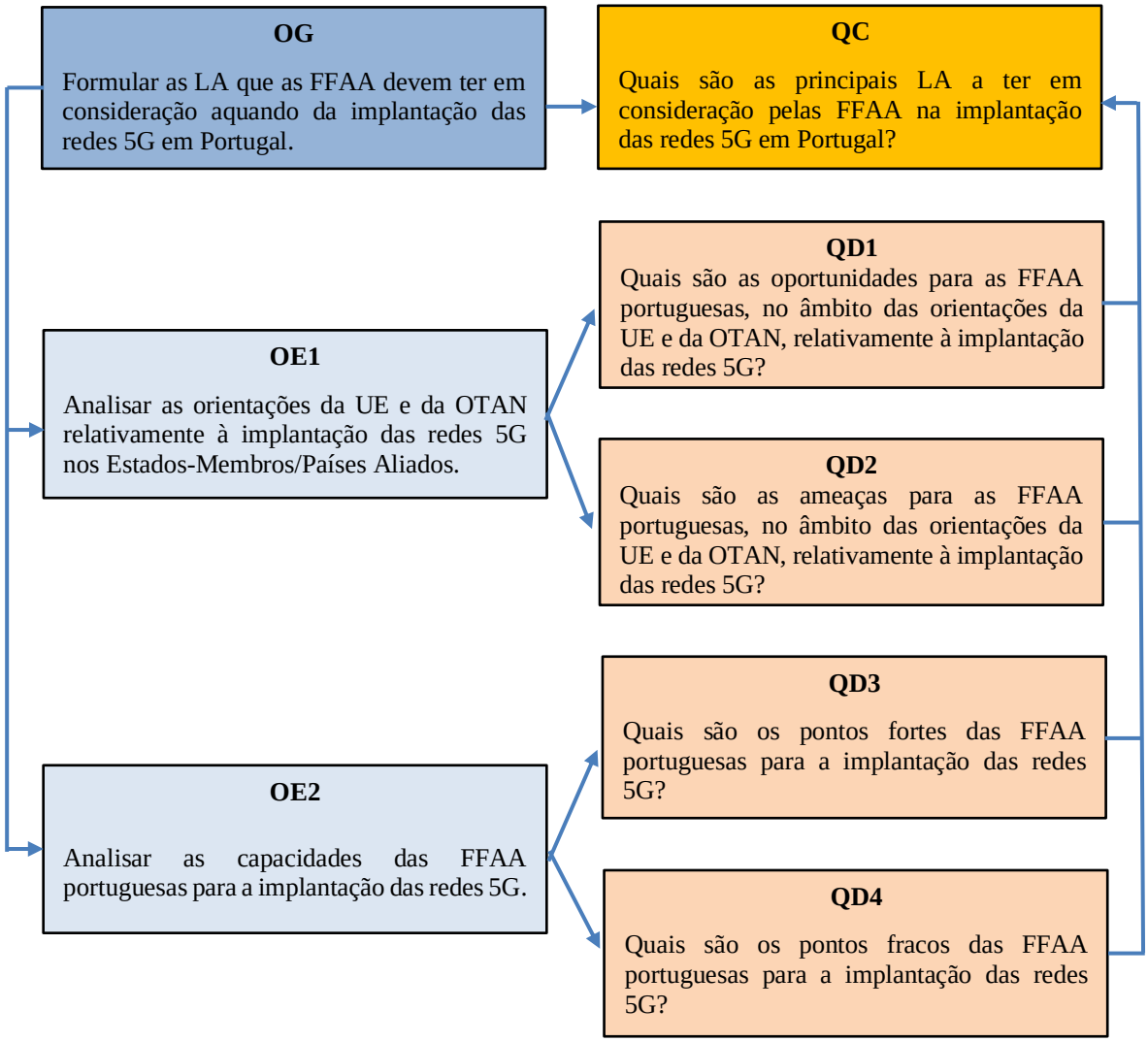


Figura 1 – Objetivos e questões de investigação

A estrutura do presente trabalho de investigação segue o formato de artigo científico (IUM, 2020b, pp. 2-4), estando organizado na presente introdução e nos seguintes capítulos:

- Segundo capítulo, com o enquadramento teórico e conceptual, onde se apresenta o estado da arte no que diz respeito à evolução das redes de comunicações móveis, caraterísticas e possibilidades das redes 5G, as orientações estabelecidas pela UE e OTAN relativas à implantação das redes 5G e o modelo de análise utilizado na investigação;

- Terceiro capítulo, com o percurso metodológico utlizado, participantes e procedimento, instrumentos de recolha e técnicas de tratamento de dados;

- Quarto capítulo, com a apresentação dos dados e discussão dos resultados, através da sua estruturação em quadros e tabelas, respondendo a todas as QD levantadas e atingindo os OE estabelecidos, respondendo à QC e cumprindo o OG, ou seja, apresentando as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal;

- Quinto e último capítulo, com as conclusões, constituídas por um breve enquadramento do tema e do procedimento metodológico utilizado, os resultados obtidos e os contributos que trazem para o objeto de investigação. Ainda neste capítulo, são indicadas as limitações da investigação, os possíveis estudos futuros e as recomendações a ter em consideração no futuro próximo.

2. Enquadramento teórico e conceptual

Neste capítulo apresenta-se o estado da arte com as teorias e os conceitos estruturantes e descreve-se o modelo de análise.

2.1. Estado da arte

As redes de comunicações móveis tiveram o seu início em 1979, com a primeira geração (1G) constituída por dispositivos analógicos, sem opções de personalização, e que só conseguiam comunicar com equipamentos iguais (Hernández, 2020). Na década seguinte surgiu a segunda geração, o 2G, com equipamentos que permitiam enviar mensagens de texto e com capacidade de *roaming*[4], operando no sistema global para as comunicações móveis, vulgarmente conhecido pela sigla GSM (*Global System for Mobile*).

Em 1998, são lançados os primeiros equipamentos de terceira geração (3G) com possibilidade de receber/enviar dados de multimédia, texto e internet (Hernández, 2020).

Por fim, a quarta geração de telecomunicações móveis (4G) e *Long Term Evolution* (LTE), surge em 2008 e materializa os verdadeiros dados com acesso a informação dinâmica, melhorando substancialmente as velocidades de banda larga sem fios, de modo a satisfazer a crescente procura (Gilli & Bechis, 2020). Em 2018 surgem as primeiras redes 5G cujas principais caraterísticas são apresentadas na Figura 2.

Em resumo verifica-se que as diferentes gerações de comunicações móveis estão separadas por períodos aproximados de dez anos, conforme esquematizado na Figura 3.

[4] "Valência proporcionada por certos operadores de telecomunicações, que permite ao utilizador usufruir dos serviços contratados para um dispositivo móvel em áreas que não aquela em que está registado (habitualmente no estrangeiro), através da utilização de redes locais" (Infopédia - Dicionários Porto Editora, s.d.).

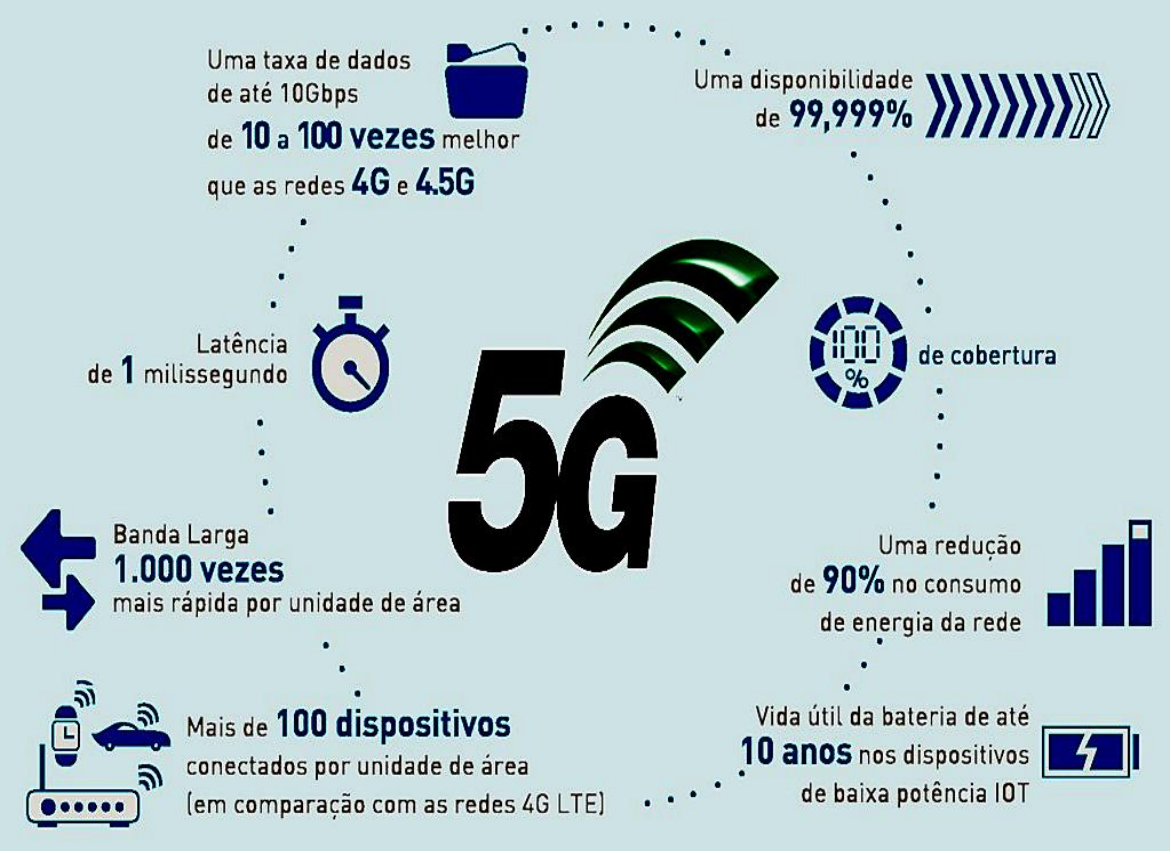


Figura 2 – Principais características das redes 5G

Fonte: Adaptado a partir de Thales Group (2019).

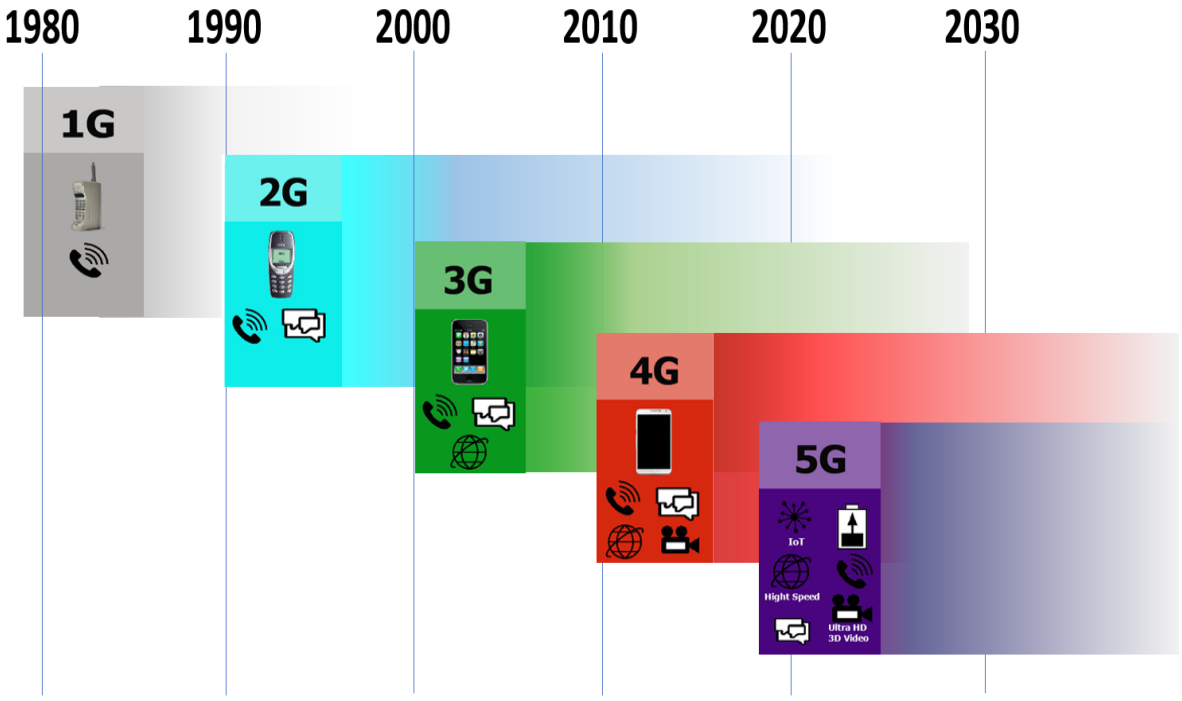


Figura 3 – Evolução das redes de comunicações móveis

Fonte: Adaptado a partir de *What You Need to Know about 5G* (s.d.).

De modo a garantir uma melhor compreensão do trabalho deve ser considerado o seguinte conceito de redes 5G:

> Conjunto de todos os elementos relevantes da infraestrutura das redes para tecnologias de comunicações móveis e sem fios utilizadas para fins de conectividade e em serviços de valor acrescentado, com características de desempenho avançadas, tais como velocidades de débito e capacidade de dados muito elevadas, comunicações de baixa latência, fiabilidade ultraelevada ou que suportem um grande número de dispositivos conectados. Podem incluir elementos das redes históricas baseados em gerações de tecnologias de comunicações móveis e sem fios anteriores, tais como as tecnologias 4G ou 3G. As redes 5G devem ser entendidas como incluindo todas as partes relevantes da rede. (Comissão Europeia, 2019d)

Os restantes conceitos utilizados neste trabalho encontram-se vertidos no Apêndice A.

Segundo a Comissão Europeia (2020a, p. 1) as redes 5G na Europa irão trazer os seguintes benefícios:

- Saúde *online* – com acompanhamento e diagnóstico do estado de saúde de forma remota e automatizada. Realização de intervenções cirúrgicas robotizadas;
- Redes energéticas inteligentes – com gestão mais eficiente e eficaz da energia elétrica, baixos níveis de quebra energética e impacto ambiental;
- Fábricas inteligentes – com redução de custos e tempos de fabricação através do controlo remoto de dispositivos;
- Meios audiovisuais e entretenimento – com utilização alargada da realidade aumentada (RA), da realidade virtual (RV) e de aplicações de banda larga ultrarrápida (e.g. vídeo em modo contínuo);
- Mobilidade – com uma redução significativa do número de acidentes (tendencialmente para zero) através da condução autónoma e conectividade de todos os meios de transporte.

Já Hernández (2020, pp. 16-18) acrescenta as seguintes possibilidades:

- Territórios inteligentes – com uma melhoria significativa na prestação de serviços públicos de apoio à terceira idade, gestão de tráfego, gestão de serviços (água, eletricidade e gás), turismo e eventos de massa;

- Agricultura e pecuária inteligentes – com uma gestão mais eficiente e eficaz da maquinaria agrícola, das produções agrícolas e agropecuárias e do controlo das pragas;
- Domótica[5] – melhorando a gestão energética dos edifícios;
- Teletrabalho – com o uso da RV e RA para se aceder em qualquer local às informações da empresa, possibilitando a deslocalização de equipas de trabalho;
- Trabalhos especializados – com operação remota de maquinaria pesada;
- Satélites – com aumento do número de equipamentos em órbita responsáveis pelas comunicações móveis terrestres;
- Veículos Aéreos Não Tripulados (UAV) – empregues em operações de socorro e resgate, vigilância e controlo, que poderão operar dentro de um sistema centralizado de gestão de tráfego integrado no sistema de gestão de espaço aéreo;
- Crises – com a gestão de recursos remotos em tempo real, de forma coordenada e centralizada melhorando a gestão dos acidentes e reduzindo os custos;
- Segurança e vigilância – com uma melhor gestão dos serviços e dos dados pessoais;
- Turismo – com recurso à RV e RA para possibilitar experiências personalizadas e imersivas, à medida do cliente;
- Meios de comunicação social – com melhor qualidade de áudio e de vídeo, podendo fazer uso da RV, RA e do vídeo imersivo, para ampliar a qualidade de experiência do seu público.

No âmbito militar, segundo a Booz Allen Hamilton Holding Corporation (s.d., p. 8) existem duas áreas de aplicação:

- Bases inteligentes
  - Segurança do Perímetro: com alertas automáticos gerados através do sistema de vigilância periférico local que avalia o tipo de ameaça e executa o reconhecimento facial, podendo ser instalado em dispositivos móveis ao mais baixo escalão;

[5] "A domótica é a integração de todos esses sistemas independentes, em prol da segurança, comodidade e da poupança de energia" (Machado, 2018).

  - Formação e treino: com os sistemas de RV e RA a criarem as condições para um treino imersivo, reduzindo os procedimentos, os tempos de instrução, os acidentes, as necessidades logísticas e os custos;
  - Logística: com os identificadores de rádio frequência (RFID), sensores de peso e outros dispositivos conectados a fazerem a gestão dos inventários e a reposição automática de *stocks*;
  - Atividades de manutenção: com reparações mais seguras e simplificadas, uma vez que os mecânicos ao mesmo tempo que consultam a documentação técnica, via RA, têm as mãos livres para proceder à reparação e/ou serem guiados, à distância, por outro técnico especialista;
  - Veículos: o emprego de veículos autónomos irá reduzir a dependência do transporte tripulado de alto risco relacionado com o reabastecimento logístico, diminuindo a maior parte das baixas que ocorrem na zona de combate.
- Campos de batalha inteligentes
  - Comando e controlo: combatentes e equipamentos apetrechados com sensores, irão permitir uma visão pormenorizada do campo de batalha e, por isso, uma liderança mais próxima das operações;
  - Cirurgia robótica e triagem médica: com equipas médicas a colaborar remotamente com especialistas, partilhando vídeo e dados relacionados com o estado de saúde dos combatentes, no campo de batalha;
  - Defesa contra armas hipersónicas (i.e. misseis com velocidades Mach 5): com a inteligência artificial e a computação de proximidade poder-se-á receber, analisar e agir rapidamente, com base em elevada quantidade de dados transmitidos a longas distâncias.

A RCM n.º 7-A/2020, de 7 de fevereiro, aprova a estratégia e calendarização da distribuição da 5G, tendo como meta a atingir, até 2030, a cobertura de todo o território com 5G, e estabelece a criação de um grupo de trabalho relativo à segurança das redes 5G (que funciona no âmbito do Conselho Superior de Segurança do Ciberespaço, sob a coordenação e presidência de um representante do Centro Nacional de Cibersegurança), do qual faz parte um representante do Ministério da Defesa Nacional (MDN).

Em comunicado de imprensa da Comissão Europeia e da Presidência Finlandesa do Conselho da UE (Comissão Europeia, 2019c, p. 1) é reconhecido que as redes 5G constituem

a futura espinha dorsal das economias e sociedades, destacando-se a importância de se manter a segurança e a resiliência das redes e serviços de comunicações eletrónicas, relativamente à tecnologia 5G. Com base nos contributos recebidos dos Estados-Membros, o GCSRI publicou, em 29 de janeiro de 2020, um conjunto de cenários de risco relacionados com: as medidas de segurança insuficientes; a cadeia de abastecimento 5G; o *modus operandi* dos principais atores mal-intencionados; as interdependências entre redes 5G e os outros sistemas críticos; os dispositivos dos utilizadores finais (NIS Cooperation Group, 2020).

A OTAN também reconhece a importância das redes 5G e o impacto que as mesmas irão ter na área militar, espelhando num *working papper*, datado de 15 de setembro de 2020, dez cenários de referência para quatro domínios de aplicação: *Computer Information System* projetável para operações expedicionárias, operações táticas terrestres, operações marítimas e comunicações fixas (Bastos, Capela, & Koprulu, 2020). A Letónia, a 13 de novembro de 2020, foi o primeiro país aliado a reportar o primeiro teste europeu do 5G militar, envolvendo o emprego da RA em óculos para o treino médico, operação de sistemas de controlo de UAV, teste de sensores e sistemas de defesa (LSM.LV, 2020).

A nível nacional, verifica-se que não existe um Conceito de Segurança Nacional. No entanto, a RCM n.º 7-A/2020, de 07 fevereiro, estabelece o que se pode designar por estratégia nacional para as redes 5G:

> O país precisa de dispor de redes 5G nos setores que mais fortemente contribuem para as mudanças na competitividade e na qualidade de vida […] e deve fazê-lo de forma que a oportunidade seja concedida a todo o território e a toda a população, para que o 5G não acentue as assimetrias regionais e, pelo contrário, contribua para as combater, alavancando uma transformação digital da sociedade.

Ainda no âmbito da Segurança Nacional, deve-se considerar como documento enquadrante a ENSC 2019-2023 (RCM n.º 92/2019, 23 de maio, 2019) que detalha um conjunto de LA para cada um dos seis eixos de intervenção.

Já no que diz respeito à Defesa Nacional, verifica-se a existência de um Conceito Estratégico de Defesa Nacional (CEDN) que refere que o ciberterrorismo e a cibercriminalidade são ameaças e riscos a ter consideração no ambiente de segurança global, devendo o desenvolvimento da ciberdefesa ser uma das prioridades de maior grau a ter em consideração (RCM n.º 19/2013, 21 de março, 2013, pp. 1984-1992).

O EMGFA e os Ramos têm DEstr próprias onde são estabelecidos OEstr e as respetivas LA (EMGFA e Marinha) e os Objetivos Operacionais (OOp) (Exército e Força Aérea). A implantação das redes 5G irá por certo ter impacto nesses OEstr, principalmente nas LA/OOp relacionados com: investimento, comando e controlo, conhecimento situacional, cibersegurança e ciberdefesa, segurança militar, formação e treino, investigação e desenvolvimento, inovação e transformação, telemedicina, gestão de *stocks*, operação de veículos não tripulados e interoperabilidade.

Nas leituras e pesquisas bibliográficas realizadas não foi identificado qualquer trabalho ou estudo relativo ao impacto das redes 5G nas FFAA portuguesas.

2.2. Modelo de análise

O modelo de análise da investigação seguido (Quadro 1) deriva dos OE e das QD levantadas que, no seu conjunto, permitem atingir o OG e responder à QC.

Sendo as redes 5G o conceito enquadrante, estabeleceu-se como dimensões/variáveis para a caraterização do ambiente externo as orientações da UE e da OTAN conjugadas com as caraterísticas da 5G, enquanto que no ambiente interno se recorreu às componentes estabelecidas no conceito de capacidade militar (Despacho n.º 11400/2014, 3 de setembro, 2014). Os indicadores baseiam-se nos elementos necessários para sintetizar as pressões externas enfrentadas por uma organização e a capacidade interna existente para fazer face a essas pressões (Cadle, Debra, & Turner, 2010).

Quadro 1 – Modelo de análise

<table>
<tr><td>TEMA</td><td colspan="5">O IMPACTO DAS REDES 5G NA SEGURANÇA E DEFESA NACIONAL.</td></tr>
<tr><td>Objeto de estudo</td><td colspan="5">As redes 5G procurando-se saber o seu impacto nas FFAA portuguesas, no contexto das orientações recebidas da UE e OTAN e tendo em consideração as caraterísticas e os campos de aplicação da 5G.</td></tr>
<tr><td>Objetivo Geral (OG)</td><td colspan="5">Formular as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal.</td></tr>
<tr><td rowspan="2">Objetivos Específicos (OE)</td><td colspan="5">Questão Central (QC) Quais são as principais LA a ter em consideração pelas FFAA na implantação das redes 5G em Portugal?</td></tr>
<tr><td>Questões Derivadas (QD)</td><td>Conceitos/ constructos</td><td>Dimensões/Variáveis</td><td>Indicadores</td><td>Técnicas e instrumentos de recolha de dados</td></tr>
<tr><td rowspan="2">OE1
Analisar as orientações da UE e da OTAN relativamente à implantação das redes 5G nos Estados-Membros/Países Aliados.</td><td>QD1
Quais são as oportunidades para as FFAA portuguesas, no âmbito das orientações da UE e da OTAN, relativamente à implantação das redes 5G?</td><td rowspan="4">Redes 5G</td><td rowspan="2">• Orientações da UE
• Orientações da OTAN
• Caraterísticas 5G</td><td>• Oportunidades</td><td rowspan="4">Entrevistas semiestruturadas</td></tr>
<tr><td>QD2
Quais são as ameaças para as FFAA portuguesas, no âmbito das orientações da UE e da OTAN, relativamente à implantação das redes 5G?</td><td>• Ameaças</td></tr>
<tr><td rowspan="2">OE2
Analisar as capacidades das FFAA portuguesas para a implantação das redes 5G.</td><td>QD3
Quais são os pontos fortes das FFAA portuguesas para a implantação das redes 5G?</td><td rowspan="2">Capacidade militar
• Doutrina
• Organização
• Treino
• Material
• Liderança
• Pessoal
• Infraestruturas
• Interoperabilidade</td><td>• Pontos fortes</td></tr>
<tr><td>QD4
Quais são os pontos fracos das FFAA portuguesas para a implantação das redes 5G?</td><td>• Pontos fracos</td></tr>
</table>

3. Metodologia e método

Neste capítulo apresenta-se a metodologia seguida na investigação nas componentes relativas à filosofia, ao raciocínio, à estratégia, ao desenho e à recolha e análise de dados. Ainda neste capítulo explana-se a população de estudo e a técnica de recolha de dados para resposta às QD e à QC.

3.1. Metodologia

A posição ontológica[6] adotada foi a construtivista, na qual o objeto de estudo ainda está em evolução, sendo o conhecimento fruto da interação entre os atores sociais e o seu meio, na atualidade e no contexto das FFAA (Bryman, 2012, p. 33). O posicionamento epistemológico[7] foi interpretativista, onde se defende que o fenómeno "[…] não pode nem deve ser estudado a partir dos princípios, ferramentas e técnicas das ciências naturais" (Santos & Lima, 2019, p. 18).

O processo de raciocínio foi indutivo partindo da observação de factos particulares, recolhidos na UE, OTAN, MDN, Gabinete Nacional de Segurança (GNS), EMGFA, Ramos e Autoridade Nacional de Comunicações (ANACOM), para através da sua análise obter uma generalização que permita formular as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal, ou seja, "[…] generaliza a toda uma classe de acontecimentos (ou população) aquilo que foi provado em alguns casos" (Santos & Lima, 2019, p. 19), pretendendo-se chegar a conclusões racionais ou prováveis (Oliveira, 2018).

A estratégia de investigação foi a qualitativa, que vai ao encontro do objetivo de se entender o fenómeno através das perspetivas de um número restrito de participantes (Flick, 2013, p. 23), visando investigar o impacto das redes 5G com base na recolha de dados junto das entidades que têm maior relação com o assunto, admitindo que as mesmas se relacionam com o fenómeno de forma subjetiva.

O procedimento metodológico foi o estudo de caso, já que se procurou "[…] recolher informação detalhada sobre uma única unidade de estudo […]" (Freixo, 2011, cit. (Santos & Lima, 2019, p. 36).

Em resumo, e de acordo com o modelo de apresentado por Saunders et al. (2009, p. 108), na Figura 4, sistematiza-se a metodologia adotada:

---

[6] "A parte da filosofia que estuda a natureza do ser, a existência e a realidade" (Santos & Lima, 2019, p. 15).
[7] "A parte da filosofia que estuda a origem, a estrutura, os métodos e a validade do conhecimento" (Santos & Lima, 2019, p. 16).

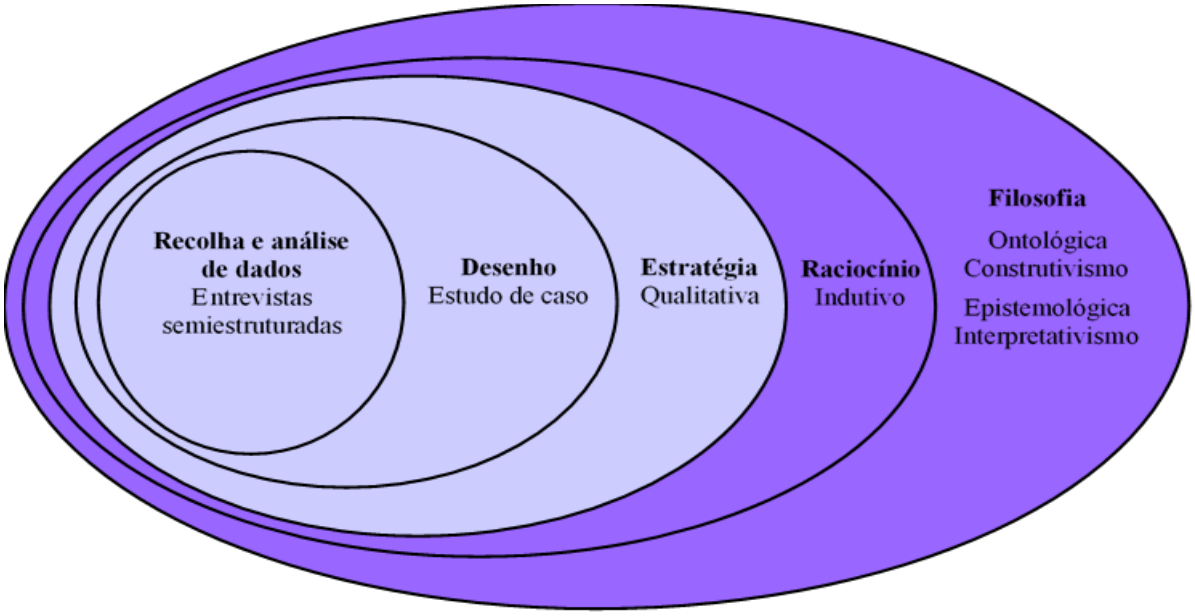


Figura 4 – "Cebola" da Investigação

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

3.2. Método

3.2.1. Participantes e procedimento

A população do estudo foram as entidades que exercem funções de elevada responsabilidade e reconhecidos especialistas nas matérias relacionadas com as redes 5G – segurança nacional, cibersegurança, comunicações nas FFAA, investigação e ensino académico de sistemas de comunicações móveis, estudo e desenvolvimento de políticas associadas à adoção das redes 5G na OTAN, e atividades regulatórias das comunicações eletrónicas em Portugal.

Na obtenção das respostas às QD participaram 13 oficiais das FFAA e civis (Apêndice B, Entrevista n.º 1) escolhidos de forma deliberada (amostra não-probabilística intencional) (Santos & Lima, 2019, p. 69), constituindo um grupo relativamente homogéneo para ser provável alcançar a saturação (Rego, Cunha, & Junior, 2018, p. 53).

De entre esse grupo, selecionaram-se os Oficiais Generais para participar na confirmação da resposta à QC: Diretor-Geral do GNS, Representante do MDN no grupo de trabalho relativo à segurança das redes 5G, Diretor da Direção de Comunicações e Sistemas de Informação do EMGFA (DIRCSI), Superintendente das Tecnologias da Informação da Marinha, Diretor da Direção de Comunicações e Sistemas de Informação (DCSI) do Exército e Diretor da DCSI da Força Aérea (Apêndice B, Entrevista n.º 2).

3.2.2. Instrumentos de recolha de dados

A técnica de recolha de dados para resposta às QD foi a entrevista semiestruturada (Santos & Lima, 2019, p. 83) nomeadamente através das quatro primeiras perguntas abertas do Guião de Entrevista n.º 1 (GE1) (Apêndice B), pré-validadas por especialistas da área de metodologia científica do IUM e submetidas a um pré-teste por dois elementos do curso, procedendo-se à sua análise antes da elaboração definitiva da entrevista (Sarmento, 2013, pp. 30-46). A quinta questão teve por finalidade obter dados para a elaboração das LA.

No sentido de validar as LA que dão resposta à QC e satisfazem o OG, foram realizadas entrevistas confirmatórias, Guião de Entrevista n.º 2 (GE2) (Apêndice C), aos decisores de topo na Segurança Nacional e nas FFAA (Sarmento, 2013, p. 33).

Durante a realização das entrevistas, todos os entrevistados prescindiram do direito à confidencialidade da sua identidade e das suas respostas, obtendo-se autorização para gravar a entrevista para sua posterior análise e submetendo-se posteriormente o seu conteúdo para validação por parte dos entrevistados. O conteúdo das entrevistas foi utilizado como fonte, para citações no trabalho (Sarmento, 2013, pp. 30-46), nos termos do n.º 4, do art.º 31.º do Regulamento Geral de Proteção de Dados (Lei n.º 58/2019, de 8 de agosto).

Com exceção de duas entrevistas, em que após contato telefónico, se receberam as respostas por e-mail, todas as entrevistas foram realizadas por via telemática recorrendo à aplicação *Microsoft Teams*, não afetando a validade da investigação, uma vez que que se manteve a excecionalidade e a especificidade do grupo de entrevistados.

3.2.3. Técnica de tratamento dos dados

Os dados recolhidos nas entrevistas foram tratados qualitativamente através de uma análise categorial, que consistiu numa operação de classificação que analisou a totalidade do texto, constituindo unidades de contexto (UnCont), unidades de registo (UnReg), unidades de enumeração (UnEn) e categorias (Cat), apresentando-se os resultados em quadros de UnCont e UnReg (com codificação numérica e cromática) e quadros de análise de conteúdo por cada questão da entrevista (Sarmento, 2013, pp. 53-56). No final da análise categorial foram retiradas as conclusões: (i) GE1 - evidenciando e enfatizando as UnReg que tiveram uma frequência maior ou igual a 50% (parcialmente confirmadas) e 80% (confirmadas), respetivamente; (ii) GE2 - evidenciando a percentagem de concordância e as UnReg com uma frequência maior ou igual a 50% (Sarmento, 2013, pp. 14-15 e 66).

A QC foi respondida através de uma análise *SWOT - Strengths, Weaknesses, Opportunities, Threats* (traduzidas, respetivamente, para pontos fortes, pontos fracos,

oportunidades e ameaças) a partir das UnReg evidenciadas e enfatizadas nas respostas dadas às QD, e correlacionando os pontos fortes e os pontos fracos existentes no ambiente interno das FFAA, com as oportunidades e as ameaças, encontradas no ambiente externo às FFAA. Essa correlação permitiu formular LA para: tirar o máximo partido dos pontos fortes aproveitando ao máximo as oportunidades; minimizar os efeitos negativos dos pontos fracos aproveitando as oportunidades; rentabilizar os pontos fortes mitigando as ameaças; minimizar ou ultrapassar os pontos fracos evitando as ameaças. De seguida, as LA foram organizadas de acordo com os vetores que constituem uma capacidade militar (doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade), identificando-se as Entidades Primariamente Responsáveis (EPR) por cada LA. Finalmente, e tendo em consideração os dados recolhidos no GE2, as LA sofreram uma melhoria incorporando UnReg que tiveram uma frequência maior ou igual a 50%.

O tratamento de dados realizou-se com recurso a uma folha de cálculo *Excel*.

4. Apresentação dos dados e discussão dos resultados

Este capítulo encontra-se estruturado em cinco subcapítulos, de forma a dar resposta a cada uma das QD e à QC, apresentando a análise de conteúdo das entrevistas efetuadas. Assim, quatro subcapítulos correspondem às QD, os dois primeiros relativos ao ambiente externo e os dois seguintes relativos ao ambiente interno. O último subcapítulo é reservado para a QC, formulando-se as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal.

As entrevistas em guião e as UnCont respeitantes a cada entidade entrevistada estão vertidas nos Apêndices C e D, respetivamente, sendo que os resultados da análise de conteúdo de cada uma das questões são apresentadas nos subcapítulos seguintes.

As 13 entrevistas relativas às QD decorreram em janeiro e fevereiro de 2020, tendo uma sido conjunta a dois especialistas do GNS e outra anulada para não desvirtuar os dados recolhidos, uma vez que um dos entrevistados só respondeu à primeira questão alegando não ter conhecimento suficiente sobre as FFAA para responder às restantes. Assim, são utilizadas 12 entrevistas, oito a oficiais das FFAA com elevadas responsabilidades no assunto (66,7%) e quatro a altos responsáveis civis da área técnica e científica (33,3%), cumprindo-se o mínimo para obter a saturação, segundo Rego *et al*. (2018, p. 53).

4.1. QD1 - Quais são as oportunidades para as FFAA portuguesas, no âmbito das orientações da UE e da OTAN, relativamente à implantação das redes 5G?

As oportunidades para as FFAA portuguesas, tendo em consideração as orientações da UE e da OTAN, baseiam-se nas respostas obtidas à primeira questão do GE1. Quatro oportunidades foram referidas por mais de 50% dos entrevistados (Tabela 1): (i) o desenvolvimento de aplicações 5G específicas para as FFAA; (ii) a edificação de redes 5G privadas (*network slicing*), que podem por exemplo serem utilizadas para ligações de troços de rede física ou para operações onde não exista outro tipo de rede; (iii) a operação remota de veículos e equipamentos, que podem eles próprios atuar de maneira autónoma mediante determinados requisitos pré-definidos; (iv) as características intrínsecas da própria tecnologia 5G, ligadas à sua latência, velocidade, volume de informação e capacidade de ligação de elevada quantidade de equipamentos e dispositivos.

Tabela 1 − UnReg da questão 1/GE1

Cat		UnReg	Entrevistados												UnEn	
			1	2	3	4	5	6	7	8	9	10	11	12	∑	%
OPORTUNIDADES	1.1	Cooperação com outros países						X	X		X	X		X	5	41,67%
	1.2	Normalização/estandardização pela UE/NATO	X		X					X				X	4	33,33%
	1.3	Desenvolvimento da Inteligência Artificial e *machine learning* para aplicação militar					X	X	X			X	X		5	41,67%
	1.4	Realidade virtual e realidade aumentada para formação, treino e operações	X		X						X	X	X		5	41,67%
	1.5	Desenvolvimento de aplicações 5G específicas para as FFAA		X	X	X	X	X	X		X	X	X		9	**75,00%**
	1.6	Novos equipamentos/armamento	X												1	8,33%
	1.7	Edificação de redes 5G privadas		X	X		X	X		X	X	X	X	X	9	**75,00%**
	1.8	Saúde *online*	X					X	X	X	X				5	41,67%
	1.9	Gestão de *stocks*, de frotas e manutenção *online* (componente logística)	X		X		X		X						4	33,33%
	1.10	Operação remota de veículos e equipamentos	X		X		X	X	X	X	X	X	X		9	**75,00%**
	1.11	Segurança inteligente					X		X						2	16,67%
	1.12	Diminuição de despesas/orçamentos						X		X	X				3	25,00%
	1.13	Caraterísticas da tecnologia 5G		X	X			X	X	X	X		X	X	8	**66,67%**

Assim, devem ser consideradas as seguintes oportunidades para as FFAA portuguesas:

- O desenvolvimento de aplicações 5G específicas para as FFAA;
- A edificação de redes 5G privadas;
- A operação remota de veículos e equipamentos;
- As caraterísticas da tecnologia 5G.

Desta forma é obtida a resposta à QD1.

4.2. QD2 - Quais são as ameaças para as FFAA portuguesas, no âmbito das orientações da UE e da OTAN, relativamente à implantação das redes 5G?

A análise das ameaças para as FFAA portuguesas, tendo em consideração as orientações da UE e da OTAN, recorre aos dados recolhidos das respostas à segunda questão do GE1 e que se traduzem nas UnReg apresentadas na Tabela 2.

A interferência de Estados Terceiros, designadamente através da cadeia de abastecimentos, é uma ameaça que se destacada com 83,33% na frequência de resposta. Conforme refere A. Marques (entrevista via *Microsoft Teams*, 18 de janeiro de 2021):

> Existem fornecedores da tecnologia 5G que atendendo ao modelo de governação que as respetivas empresas têm e ao valor do 5G em termos do impacto que vão ter na sociedade, que terão que ser acutelados no que respeita às áreas de soberania, em particular a defesa e em particular específico as FFAA.

Tabela 2 – UnReg da questão 2/GE1

Cat	UnReg	Entrevistados												UnEn	
		1	2	3	4	5	6	7	8	9	10	11	12	∑	%
AMEAÇAS	2.1. Interferência de Estados Terceiros	X	X	X	X	X		X	X	X	X	X		10	**83,33%**
	2.2. Ciberataques e cibercriminalidade		X	X		X	X	X		X				6	**50,00%**
	2.3. Indisponibilidade de financiamento												X	1	8,33%
	2.4. Fraca qualidade dos produtos	X	X	X					X			X	X	6	**50,00%**
	2.5. Dependência do único fornecedor						X					X	X	3	25,00%
	2.6. Ações de sabotagem			X		X	X			X		X		5	41,67%
	2.7. Quebra de segurança no acesso à rede									X				1	8,33%
	2.8. Insuficiência de legislação/supervisão		X	X					X	X		X		5	41,67%
	2.9. Diminuição do espectro militar	X										X		2	16,67%
	2.10. Ações de ciberespionagem			X		X		X		X				4	33,33%
	2.11. Tecnologia disruptiva/imaturidade da tecnologia	X	X	X			X	X			X	X		7	**58,33%**
	2.12. Lentidão na tomada de decisões na UE e NATO	X	X	X		X						X		5	41,67%

Na análise destacam-se ainda como ameaças: (i) o facto da tecnologia 5G ser disruptiva e ainda estar em desenvolvimento, criando algumas vulnerabilidades (58,33%); (ii) o incremento dos ciberataques e da cibercriminalidade, devido ao aumento da superfície de ataque com mais equipamentos e dispositivos ligados em rede (50,00%); (iii) a fraca qualidade dos produtos, tanto a nível de *software* como de *hardware* (50,00%).

Deste modo as ameaças que as FFAA portuguesas devem ter em consideração são:

- A interferência de Estados Terceiros;
- O facto da 5G ser uma tecnologia disruptiva e imatura;
- Os ciberataques e cibercriminalidade;
- A fraca qualidade dos produtos.

Desta forma obtém-se a resposta à QD2 e consequentemente, com os resultados obtidos anteriormente na QD1, cumpre-se o OE1.

4.3. QD3 - Quais são os pontos fortes das FFAA portuguesas para a implantação das redes?

A Tabela 3 espelha os pontos fortes para as FFAA portuguesas elencados pelos entrevistados, dos quais 66,67% destacaram: (i) a existência de um conjunto de competências e conhecimentos relativos às comunicações, de forma multifacetada e baseada num conhecimento feito da prática; (ii) a capacidade das FFAA superarem e recuperarem de adversidades (resiliência organizacional).

Tabela 3 – UnReg da questão 3/GE1

Cat	UnReg		Entrevistados												UnEn	
			1	2	3	4	5	6	7	8	9	10	11	12	∑	%
PONTOS FORTES	3.1	Cultura orientada para cumprimento da missão	X	X	X		X					X	X	X	7	**58,33%**
	3.2	Competências e conhecimentos existentes	X	X	X	X	X	X	X					X	8	**66,67%**
	3.3	Existência de infraestruturas seguras para instalação de equipamentos									X	X			2	16,67%
	3.4	Treino e formação em simuladores									X	X		X	3	25,00%
	3.5	Resiliência organizacional		X		X	X	X	X	X			X	X	8	**66,67%**
	3.6	Existência de uma cultura de segurança	X	X	X							X	X	X	6	**50,00%**
	3.7	Capacidade de comando e controlo			X			X		X	X				4	33,33%
	3.8	Capacidade de ciberdefesa (centro de ciberdefesa)			X							X		X	3	25,00%
	3.9	Estabelecimento de parcerias para desenvolver inovações										X			1	8,33%
	3.10	Existência de frequências reservadas/próprias						X				X			2	16,67%
	3.11	Digitalização das FFAA								X					1	8,33%
	3.12	Diálogo com outras Instituições do Estado e Internacionais			X										1	8,33%

Com 58,33% dos entrevistados a mencioná-la, salienta-se a existência de uma cultura orientada para o cumprimento da missão e, finalmente, 50,00% dos entrevistados evidenciam a cultura de segurança embebida nas FFAA como um ponto forte.

Em resumo, os pontos fortes das FFAA portuguesas para a implantação das redes são:

- As competências e os conhecimentos existentes no seio das FFAA;
- A resiliência organizacional das FFAA;
- A existência de uma cultura orientada para cumprimento da missão;
- A existência de uma cultura de segurança nas FFAA.

Desta forma obtém-se a resposta à QD3 cumprindo-se parcialmente o OE2, que ficará completo com a resposta à QD4.

4.4. QD4 - Quais são pontos fracos das FFAA portuguesas para a implantação das redes 5G?

Da Tabela 4 ressalta que todos os entrevistados consideram a falta de recursos humanos especializados/qualificados como um ponto fraco das FFAA para a implantação das redes 5G, como referiu L. Camelo (entrevista por *e-mail*, 8 de fevereiro de 2021):

> Importa igualmente salientar que estas tecnologias emergentes e disruptivas carecem de pessoal com competências altamente especializadas e que exigem formação de elevada complexidade, dispendiosa e dilatada no tempo, com

tempos de retorno de investimento muito longos, que não são consentâneos com a normal rotação do pessoal militar no desempenho de funções.

Tabela 4 – UnReg da questão 4/GE1

Cat	UnReg	Entrevistados												UnEn	
		1	2	3	4	5	6	7	8	9	10	11	12	∑	%
PONTOS FRACOS	4.1 Falta de recursos humanos especializados/ qualificados	X	X	X	X	X	X	X	X	X	X	X	X	12	**100%**
	4.2 Redes com classificação de segurança elevada										X	X		2	16,67%
	4.3 Falta/obsolescência de sistemas e equipamentos				X	X			X			X	X	5	41,67%
	4.4 Necessidade absoluta de comunicações										X			1	8,33%
	4.5 Insuficiência de recursos financeiros	X	X	X		X	X	X	X		X	X	X	10	**83,33%**
	4.6 Inexistência de normas técnicas/doutrina			X		X	X			X	X	X	X	7	**58,33%**
	4.7 Necessidade de interoperabilidade			X				X			X	X	X	5	41,67%
	4.8 Falta de consciencialização das chefias	X	X	X		X		X		X	X	X		8	**66,67%**
	4.9 Falta de capacidade para tratar a informação					X						X		2	16,67%

Muito importante é verificar que outro ponto fraco das FFAA portuguesas, com 83,33% dos entrevistados a referi-lo, é a falta de alocação de verbas para fazer face à implantação das redes 5G, como menciona L. Bastos (entrevista via *Microsoft Teams*, 21 de janeiro de 2021) "A limitação de recursos financeiros, também constitui um constrangimento para as FFAA […]".

São ainda de destacar como pontos fracos, com 66,67%, o facto das chefias responsáveis pelas decisões ao mais alto nível ainda não terem uma consciencialização das implicações da implantação das redes 5G, suas possibilidades e limitações, visualizando essa implantação como um assunto meramente tecnológico, e com uma frequência de 58,33%, a inexistência de doutrina ou normas técnicas relativamente ao ecossistema 5G.

Conclui-se que os quatro pontos fracos das FFAA portuguesas para a implantação das redes 5G são:

- A falta de recursos humanos especializados/qualificados em 5G;
- A insuficiência de recursos financeiros para implementação das redes 5G;
- A falta de consciencialização das chefias relativamente à implantação das redes 5G;
- A inexistência de normas técnicas/doutrina relacionadas com o 5G.

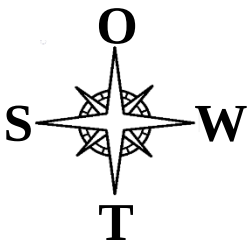
Desta forma obtém-se a resposta à QD4 e em conjunto com a resposta à QD3 cumpre-se o OE2.

4.5. QC - Quais são as principais LA a ter em consideração pelas FFAA na implantação das redes 5G em Portugal?

4.5.1. Análise SWOT

A Análise SWOT aplicada às respostas obtidas na QD1, QD2, QD3 e QD4, ou seja, às oportunidades, às ameaças, aos pontos fortes e aos pontos fracos, respetivamente, permitiu formular os quatro grupos de LA a ter em consideração na implementação das redes 5G nas FFAA (Quadro 2).

Quadro 2 – Análise SWOT

 **Ambiente Externo** / **Ambiente Interno**	**PONTOS FORTES (S)** S1 - Competências e conhecimentos existentes S2 - Resiliência organizacional S3 - Cultura orientada para cumprimento da missão S4 - Existência de uma cultura de segurança	**PONTOS FRACOS (W)** W1 - Falta de recursos humanos especializados/qualificados W2 - Insuficiência de recursos financeiros W3 - Falta de consciencialização das chefias W4 - Inexistência de normas técnicas/doutrina
OPORTUNIDADES (O) O1 - Desenvolvimento de aplicações 5G específicas para as FFAA O2 - Edificação de redes 5G privadas O3 - Operação remota de veículos e equipamentos O4 - Caraterísticas da tecnologia 5G	**CRESCIMENTO** SO1 - **CRIAR** cenários de emprego operacional do 5G nas FFAA (S1, S2, S3) x (O1, O2, O3) SO2 - **CONSOLIDAR** a interoperabilidade 5G nas FFAA e com os países aliados (S1, S2, S4) x (O1, O2, O3, O4)	**OTIMIZAÇÃO** WO1 - **CONSTITUIR** grupos de acompanhamento especializados em 5G (W1, W3, W4) x (O1, O4) WO2 - **ADEQUAR** os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações (W1, W2) x (O2, O4)
AMEAÇAS (T) T1 - Interferência de Estados Terceiros T2 - Tecnologia disruptiva/ imaturidade da tecnologia T3 - Ciberataques e cibercriminalidade T4 - Fraca qualidade dos produtos	**DINAMIZAÇÃO** ST1 - **ENVOLVER** as chefias no processo de implantação do 5G nas FFAA (S2, S3, S4) x (T2) ST2 - **EXPLORAR** a utilização segura de redes 5G próprias (S1, S2, S4) x (T1, T3, T4)	**PROTEÇÃO** WT1 - **POTENCIAR** a formação em cibersegurança/ciberdefesa e a especialização em 5G (W1, W2, W3, W4) x (T1, T3, T4) WT2 - **PROMOVER** a evolução sustentada das soluções tecnológicas 5G (W2) x (T3, T4)

As LA formuladas são descritas da seguinte forma:

- *CRIAR cenários de emprego operacional do 5G nas FFAA* – de modo a obter conhecimento, identificar necessidades, potencialidades e vulnerabilidades, que possibilitem a criação de conceitos nas FFAA relativamente ao 5G;
- *CONSOLIDAR a interoperabilidade 5G nas FFAA e com os países aliados* – de forma a existir interoperabilidade nas comunicações dentro da rede e com os equipamentos e dispositivos a ela ligados, garantindo todos os requisitos de segurança;
- *CONSTITUIR grupos de acompanhamento especializados em 5G* – que integrem especialistas e operacionais, de forma transversal ao MDN, EMGFA e Ramos, que sigam os assuntos relativos ao 5G, no âmbito civil e militar, e produzam pareceres, estudos, normas e análises;
- *ADEQUAR os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações* – de modo a criarem-se mecanismos que garantam a fixação desses efetivos especializados responsáveis pela parametrização das aplicações, serviços e equipamentos;
- *ENVOLVER as chefias no processo de implantação do 5G nas FFAA* – com a finalidade de evitar que o tema seja reconhecido apenas como um assunto meramente técnico, mas sim como um ativo estratégico, criando as condições para a tomada de decisão informada e potenciando o emprego da capacidade 5G;
- *EXPLORAR a utilização segura de redes 5G próprias* – de forma a potenciar as ligações da rede física, designadamente na interligação das comunicações estratégicas com as comunicações táticas, incluindo a *Internet of Battlefield Things*, efetuando uma gestão e um controlo da rede de forma autónoma e garantindo uma adequada interligação com outras redes, quando aplicável;
- *POTENCIAR a formação em cibersegurança/ciberdefesa e a especialização em 5G* – de modo a fazer face à imaturidade da tecnologia e ao aumento da superfície de ataque cibernético, reforçando a capacidade de ciberdefesa das FFAA;
- *PROMOVER a evolução sustentada das soluções tecnológicas 5G* – garantindo os recursos financeiros e materiais necessários para o desenvolvimento e manutenção de uma capacidade conjunta, apoiando a Investigação, Desenvolvimento e Inovação (ID&I).

Como resultado da análise SWOT desenvolvida, procurou-se que as LA formuladas fossem organizadas e apresentadas de acordo com os vetores que constituem uma capacidade militar (doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade), de forma a tornar mais lógica a sua implementação.

Paralelamente, aprofundou-se o trabalho identificando as Entidades Primariamente Responsáveis (EPR) por cada LA, de modo a que essas entidades fiquem cientes das tarefas que serão necessárias desenvolver para implementar esta capacidade (Quadro 3).

Quadro 3 – LA a considerar pelas FFAA

VETOR CAPACIDADE	LINHAS DE AÇÃO	EPR
DOUTRINA	LA1 - CRIAR cenários de emprego operacional do 5G nas FFAA	EMGFA+Ramos
ORGANIZAÇÃO	LA2 - CONSTITUIR grupos de acompanhamento especializados em 5G	EMGFA+Ramos
TREINO	LA3 - POTENCIAR a formação em cibersegurança/ciberdefesa e especialização em 5G	EMGFA+Ramos
MATERIAL	LA4 - PROMOVER a evolução sustentada das soluções tecnológicas 5G	EMGFA+Ramos
LIDERANÇA	LA5 - ENVOLVER as chefias no processo de implantação do 5G nas FFAA	EMGFA+Ramos
PESSOAL	LA6 - ADEQUAR os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações	Ramos
INFRAESTRUTURAS	LA7 - EXPLORAR a utilização segura de redes 5G próprias	EMGFA
INTEROPERABILIDADE	LA8 - CONSOLIDAR a interoperabilidade 5G nas FFAA e com os países aliados	EMGFA+Ramos

4.5.2. Análise das entrevistas

A análise da quinta questão do GE1 (Tabela 5), relativa às ações a serem acauteladas pelas FFAA na implantação das Redes 5G, 75% dos entrevistados refere a constituição de um grupo de acompanhamento do 5G, o que reforça a necessidade da LA2.

Tabela 5 – UnReg da questão 5/GE1

Cat	UnReg	Entrevistados												UnEn	
		1	2	3	4	5	6	7	8	9	10	11	12	∑	%
AÇÕES A ACAUTELAR	5.1 Constituição de grupo de acompanhamento	X	X	X	X		X	X		X	X		X	9	**75,00%**
	5.2 Alocação de recursos financeiros	X	X				X	X		X				5	41,67%
	5.3 Formação e atualização de recursos para apoiar implantação da tecnologia	X					X	X	X					4	33,33%
	5.4 Abordagem tendo como *framework* a edificação de uma capacidade (DOTLPMI[2])			X		X	X	X						4	33,33%
	5.5 Gestão eficiente dos recursos humanos								X					1	8,33%
	5.6 Garantir a segurança e a certificação dos componentes							X	X			X		3	25,00%
	5.7 Lançamento de projetos de I&D							X						1	8,33%

As entrevistas confirmatórias (GE2) permitiram confirmar totalmente as oito LA formuladas na resposta à QC, merecendo a concordância de todos os entrevistados (Tabela 6).

Tabela 6 – UnReg por LA/GE2

Cat	UnReg	Entrevistados						UnEn	
		1	3	4	5	6	7	∑	%
LA1	6.1 Concordo	X	X	X	X	X	X	6	**100%**
	6.2 Cenários limitados e pragmáticos	X	X	X		X	X	5	**83,33%**
	6.3 LA não especifica do 5G				X			1	16,67%
LA2	8.1 Concordo	X	X	X	X	X	X	6	**100%**
	8.2 Dependência do EMGFA	X	X				X	3	**50,00%**
	8.3 Estrutura 5G		X					1	16,67%
	8.4 Não exclusivo do 5G				X			1	16,67%
	8.5 Não é importante/prioritário					X		1	16,67%
LA3	12.1 Concordo	X	X	X	X	X	X	6	**100%**
	12.2 Especialização	X	X					2	33,33%
	12.3 Não exclusivo do 5G			X	X			2	33,33%
LA4	13.1 Concordo	X	X	X	X	X	X	6	**100%**
	13.2 Envolvimento FFA, Indústria e Academia	X	X				X	3	**50,00%**
	13.3 Difícil execução			X				1	16,67%
	13.4 Não exclusivo do 5G/Não prioritário				X	X		2	33,33%
LA5	10.1 Concordo	X	X	X	X	X	X	6	**100%**
	10.2 Multidisciplinar				X			1	16,67%
LA6	9.1Concordo	X	X	X	X	X	X	6	**100%**
	9.2 Garantir a formação	X		X			X	3	**50,00%**
	9.3 Estrutura 5G			X				1	16,67%
	9.4 Não exclusivo do 5G				X	X		2	33,33%
LA7	11.1 Concordo	X	X	X	X	X	X	6	**100%**
	11.2 Dependência dos cenários	X						1	16,67%
	11.3 Autonomia		X	X		X		3	**50,00%**
	11.4 Difícil execução						X	1	16,67%
LA8	7.1 Concordo	X	X	X	X	X	X	6	**100%**
	7.2 Incluir parceiros das FFAA	X	X	X	X		X	5	**83,33%**
	7.3 Capacidade conjunta	X					X	2	33,33%

Concluiu-se ainda o seguinte:

- LA1 – 83,33% dos entrevistados referiu que os cenários levantados devem ser pragmáticos e deve ser focado o estudo naqueles que são considerados os mais remuneradores e prováveis para as FFAA;
- LA2 – 50,00% dos entrevistados indicou que o grupo de acompanhamento deve estar funcionalmente dependente do EMGFA;
- LA4 – 50,00% dos entrevistados mencionou a importância de se incluir na descrição da LA o envolvimento das FFAA, da indústria e da academia;
- LA6 – 50,00% dos entrevistados considerou que devem ser obtidas competências técnicas especializadas;

- LA7 – 50,00% dos entrevistados referiu que esta LA será a forma de garantir a autonomia das FFAA, essencial para a operação em áreas remotas e em situações em que as FFAA tenham que prestar apoio de comunicações móveis;
- LA8 – 83,33% dos entrevistados acrescentou que, para além dos países aliados, devem ser incluídas outras entidades nacionais com quem as FFAA poderão operar (e.g. Autoridade Nacional de Proteção Civil).

Tendo em consideração a pertinência do referido por pelo menos 50% dos entrevistados, relativamente a aspetos que não estão contemplados nas LA formuladas, foram introduzidas melhorias (assinaladas a **negrito**) nos títulos das seguintes LA:

- LA1 - *CRIAR cenários* **verosímeis** *de emprego operacional do 5G nas FFAA*;
- LA8 - *CONSOLIDAR a interoperabilidade 5G nas FFA*A, **com parceiros nacionais que operam com as FFAA** *e com os países aliados*;

bem como na descrição das seguintes LA:

- LA2 - que integrem especialistas e operacionais, de forma transversal ao MDN, EMGFA e Ramos, **que na dependência do EMGFA** sigam os assuntos relativos ao 5G, no âmbito civil e militar, e produzam pareceres, estudos, normas e análises;
- LA4 - garantindo os recursos financeiros e materiais necessários para o desenvolvimento e manutenção de uma capacidade conjunta, apoiando a ID&I **e envolvendo a indústria e a academia**;
- LA6 - de modo a criarem-se mecanismos que garantam **a formação** e a fixação desses efetivos especializados responsáveis pela parametrização das aplicações, serviços e equipamentos;
- LA7 - de forma a potenciar as ligações da rede física, designadamente na interligação das comunicações estratégicas com as comunicações táticas, incluindo a *Internet of Battlefield Things*, efetuando uma gestão e um controlo da rede de forma autónoma **e independente**, garantindo uma adequada interligação com outras redes, quando aplicável;

Desta forma obtém-se a resposta à QC e cumpre-se o OG, formulando-se as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal.

5. Conclusões

Como sublinhado pelo Comissão Europeia (2020c), a pandemia COVID-19 demonstrou que é essencial dispor-se de uma conectividade rápida e omnipresente, sendo que as redes de capacidade muito elevada têm desempenhado um papel crucial na resposta à crise provocada pela mesma, assegurando o teletrabalho, o ensino à distância, a prestação de cuidados de saúde, a comunicação pessoal e o entretenimento. Este tipo de conectividade generalizada, a *gigabits*, será decisiva para a retoma económica da Europa, abrangendo os domínios da saúde, da educação, dos transportes, da logística e dos meios de comunicação social, e irá contribuir significativamente para a oferta de serviços de fácil acesso e a preços minorados, possibilitando a eliminação do fosso digital.

A nível militar, a implantação das redes 5G irá proporcionar benefícios transversais relativamente as atividades desenvolvidas em tempo de paz e às missões executadas em campanha, e que passam por aspetos relacionados com a segurança física das instalações, formação e treino, manutenção de equipamentos, telemedicina, operação de veículos não tripulados, comando e controlo das missões, entre outras.

A UE e a OTAN têm sido as organizações, das quais Portugal faz parte, que mais têm desenvolvido estudos e recomendações relativamente à implantação das redes 5G, e deverão continuar a ser aquelas que devem ter um papel mais preponderante na definição de estratégias no âmbito da temática do 5G. Por outro lado, a nível nacional e ao nível das FFAA, existe um conjunto de documentação, como sejam o CEDN, a ENSC e as DEstr do EMGFA e dos Ramos, no qual é feita referência a aspetos relacionados com a cibersegurança e ciberdefesa. Esta documentação deve constituir a base para se mitigarem os riscos associados à implantação das redes 5G, uma vez que a superfície de ataque irá aumentar consideravelmente, relativamente às redes 4G, tendo em consideração o elevado número de dispositivos que irão estar conectados às redes 5G.

A presente investigação teve como OG, *formular as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal*, tendo sido delimitada nos domínios: espacial, ao âmbito da Segurança Nacional na componente de Segurança no Ciberespaço e ao âmbito da Defesa Nacional, na componente militar; temporal, à atualidade; e no conteúdo, às caraterísticas da 5G e campos de aplicação militar, às orientações estabelecidas pela UE e OTAN, às LA estabelecidas na ENSC, aos OEstr estabelecidos nas DEstr do EMGFA e Ramos e ao impacto das redes 5G na capacidade militar.

O procedimento metodológico adotado seguiu um posicionamento ontológico construtivista e epistemológico interpretativo. A investigação recorreu ao raciocínio indutivo utilizando uma estratégia qualitativa e um desenho de estudo de caso.

A técnica de recolha de dados utlizada foi as entrevistas semiestruturadas, dirigidas a um conjunto de decisores de topo e especialistas que estão a lidar com os assuntos relativos ao 5G, privilegiando-se a qualidade de amostra em detrimento da sua densidade. Uma primeira entrevista, dirigida a 13 entidades, teve como principal finalidade recolher dados relativos à caraterização do ambiente externo e do ambiente interno. Já a segunda entrevista, envolvendo os seis decisores de topo na Segurança Nacional e nas FFAA, realizou-se após a análise SWOT, com a finalidade de validar as LA formuladas.

De forma a atingir o OG, estabeleceram-se dois OE. O OE1, que visou analisar as orientações da UE e da OTAN relativamente à implantação das redes 5G nos Estados-Membros/Países Aliados, foi atingido através das respostas obtidas na QD1 quanto às oportunidades e na QD2 relativa às ameaças. Da recolha de dados efetuada através das entrevistas e sua análise categorial cromática, espelhando as UnReg acima 50%, resultou o apuramento de quatro oportunidades e quatro ameaças (Figura 5). Relativamente à caraterização do ambiente externo, com uma frequência de resposta superior a 80%, destacou-se a ameaça respeitante à interferência de Estados Terceiros, sendo que todas as restantes ameaças e oportunidades apuradas tiveram resultados entre os 50,00% e os 75,00%.

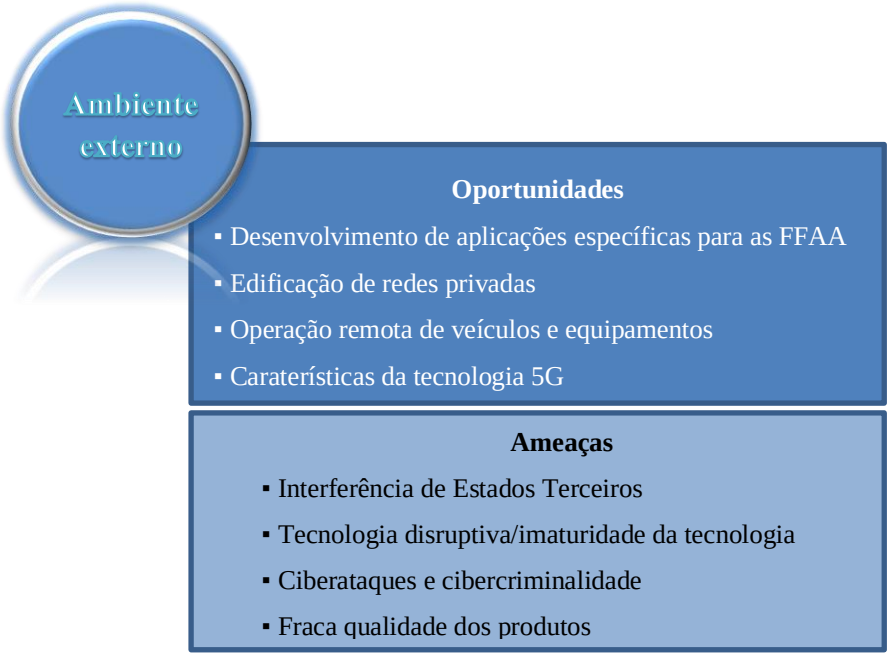


Figura 5 – Análise do ambiente externo

Para análise das capacidades das FFAA portuguesas para a implantação das redes 5G foi estabelecido o OE2, que foi cumprido através das respostas obtidas na QD3 quanto aos pontos fortes e QD4 relativa aos pontos fracos.

Resultante da informação recolhida das entrevistas foi possível estabelecer quatro pontos fortes e quatro pontos fracos que obtiveram a concordância de mais de metade dos entrevistados (Figura 6), destacando-se os pontos fracos relacionados com a falta de recursos especializados/qualificados e a insuficiência de recursos financeiros, que obtiveram 100% e 83,33% das respostas, respetivamente.

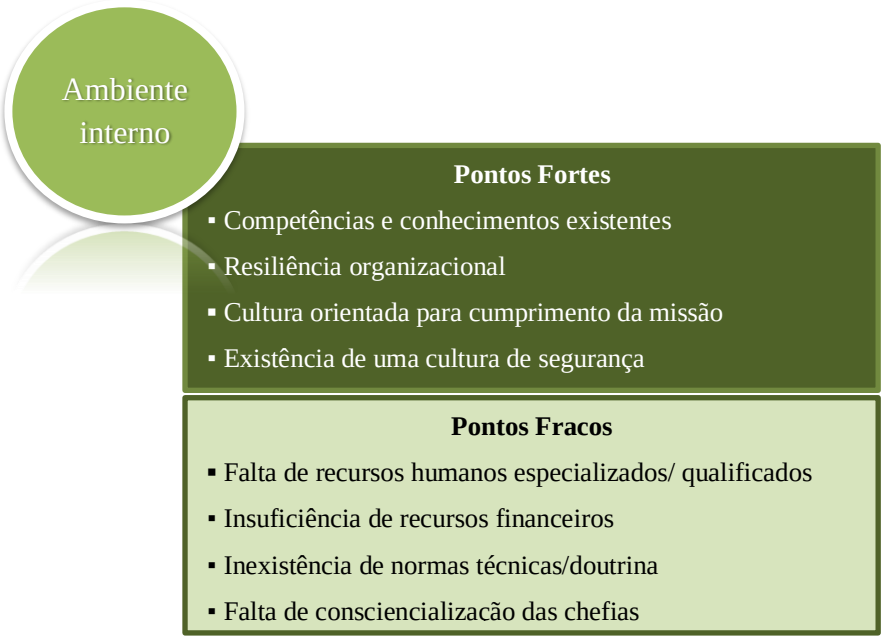


Figura 6 – Análise do ambiente interno

Para cumprimento do OG, *Formular as LA que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal*, a investigação foi orientada no sentido de responder à QC através de uma análise SWOT, com base nas conclusões da QD1, QD2, QD3 e QD4. Dessa análise formularam-se oito LA, que foram posteriormente submetidas a validação, através de entrevistas confirmatórias.

Nas entrevistas confirmatórias todos os entrevistados concordaram com as LA, mas sugeriram algumas alterações ao nível do título e/ou da descrição, as quais foram consideradas pertinentes sempre que referidas por pelo menos 50% dos entrevistados.

As LA revistas são as seguintes:

⇒ **LA1**: *CRIAR cenários verosímeis de emprego operacional do 5G nas FFAA*, de modo a obter conhecimento, identificar necessidades, potencialidades e

vulnerabilidades, que possibilitem a criação de conceitos nas FFAA relativamente ao 5G;

⇒ **LA2**: *CONSTITUIR grupos de acompanhamento especializados em 5G***,** que integrem especialistas e operacionais, de forma transversal ao MDN, EMGFA e Ramos, que na dependência do EMGFA sigam os assuntos relativos ao 5G, no âmbito civil e militar, e produzam pareceres, estudos, normas e análises;

⇒ **LA3**: *POTENCIAR a formação em cibersegurança/ciberdefesa e a especialização em 5G*, de modo a fazer face à imaturidade da tecnologia e ao aumento da superfície de ataque cibernético, reforçando a capacidade de ciberdefesa das FFAA;

⇒ **LA4:** *PROMOVER a evolução sustentada das soluções tecnológicas 5G*, garantindo os recursos financeiros e materiais necessários para o desenvolvimento e manutenção de uma capacidade conjunta, apoiando a ID&I e envolvendo a indústria e a academia;

⇒ **LA5**: *ENVOLVER as chefias no processo de implantação do 5G nas FFAA*, com a finalidade de evitar que o tema seja reconhecido apenas como um assunto meramente técnico, mas sim como um ativo estratégico, criando as condições para a tomada de decisão informada e potenciando o emprego da capacidade 5G;

⇒ **LA6**: *ADEQUAR os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações*, de modo a criarem-se mecanismos que garantam a formação e a fixação desses efetivos especializados responsáveis pela parametrização das aplicações, serviços e equipamentos;

⇒ **LA7**: *EXPLORAR a utilização segura de redes 5G próprias*, de forma a potenciar as ligações da rede física, designadamente na interligação das comunicações estratégicas com as comunicações táticas, incluindo a *Internet of Battlefield Things*, efetuando uma gestão e um controlo da rede de forma autónoma e independente, garantindo uma adequada interligação com outras redes, quando aplicável;

⇒ **LA8**: *CONSOLIDAR a interoperabilidade 5G nas FFAA, com parceiros nacionais que operam com as FFAA e com os países aliados*, de forma a existir interoperabilidade nas comunicações dentro da rede e com os equipamentos e dispositivos a ela ligados, garantindo todos os requisitos de segurança.

Seguidamente, as LA foram reorganizadas de acordo com os vetores de capacidade, identificando-se a respetiva EPR associada a cada LA (Figura 7), de forma a tornar mais lógica e racional a sua implementação. Com este procedimento respondeu-se à QC e consequentemente cumpriu-se o OG.

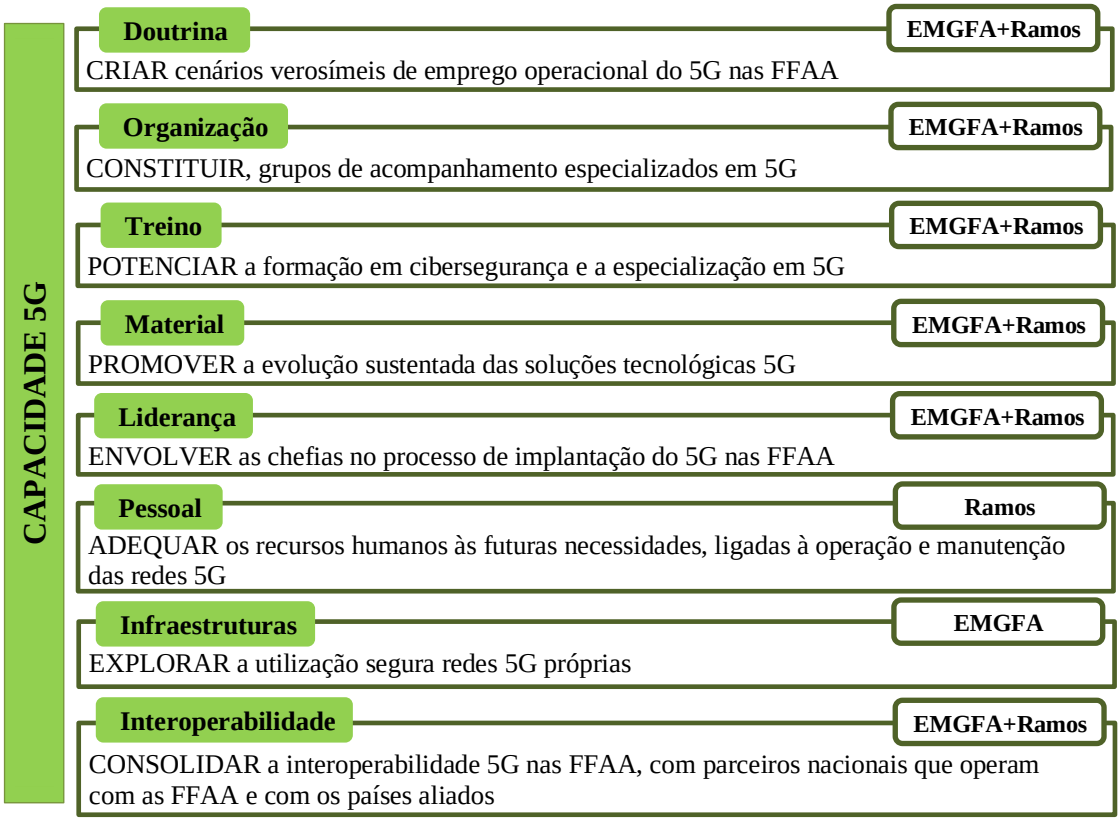


Figura 7 – LA por vetor de capacidade e EPR

Em termos de contributos para o conhecimento, as LA formuladas irão permitir que as FFAA tirem o máximo rendimento das redes 5G, mitigando os riscos associados à sua implementação e utilização. A adoção destas LA, pelas diversas entidades das FFAA, permitirá evitar ineficiências e disfunções e potencializará o desenvolvimento do uso militar da 5G.

Tendo em consideração as LA formuladas e as EPR que lhe estão associadas, é recomendável que esta investigação seja dada a conhecer ao EMGFA e aos Ramos.

Em relação às limitações da investigação, destacam-se os constrangimentos relacionados como a pandemia COVID-19, o que impossibilitou os contactos presenciais para a realização das entrevistas. Assim, 17 entrevistas ocorreram via telemática, através da aplicação *Microsoft Teams*, e duas por contacto telefónico, seguido de receção das respostas por e-mail. Também a escassa informação e conhecimento da utilização das redes 5G, no

âmbito militar nacional, mesmo por parte dos especialistas militares, dificultou uma análise mais profunda do ambiente interno, designadamente por parte dos dados disponibilizados pelos entrevistados.

A validação das conclusões da investigação e a fiabilidade dos resultados foram fruto da qualidade das respostas obtidas nas entrevistas e da materialização concreta das categorias de análise, tendo sido realizada uma validação interna dos objetivos de estudo e elaborada uma classificação das UnReg.

No respeitante a estudos futuros, e considerando que as redes 5G terão implantação nacional, a nível civil e militar, sugere-se: a curto prazo, o estabelecimento dos cenários de emprego operacional do 5G nas FFAA, o planeamento dos objetivos a atingir, bem como os prazos temporais decorrentes dos mesmos; a médio prazo: o estudo mais aprofundado dos campos de aplicação militar das redes 5G nas FFAA portuguesas, através do consolidação dos cenários de emprego; a longo prazo e após implantação das redes 5G, proceder à recolha dos dados relativos à sua utilização, de modo a estabelecerem-se as melhores estratégias para cada um dos campos da sua utilização.

A recomendação de ordem prática que pode ser feita nesta área, é que sendo as redes 5G um recurso essencial e crítico para o futuro desenvolvimento das FFAA, é necessário que os diferentes patamares de comando e chefia lhe atribuam a devida importância e prioridade, devendo ser estabelecidas diretivas claras nesse sentido.

A presente investigação regeu-se pelos valores, princípios éticos e morais estabelecidos pelo IUM, seguindo-se as normas de citação e referenciação em vigor nesse Instituto.

Referências Bibliográficas

Academia das Ciências de Lisboa. (s.d.). Definição/conceito de ciências militares. *Anexo A à informação*.

Bastos, L., Capela, g., & Koprulu, A. (2020). *Potential of 5G technologies for military application.* NATO Communications and Information Agency.

Booz Allen Hamilton Holding Corporation. (s.d.). *Establishing a secure and resilient 5G ecososystem - Report*. Retirado de https://www.boozallen.com/c/insight/publication/5g-report.html

Bryman, A. (2012). *Social Research Methods* (4th ed.). New York: Oxford University Press. Retirado de https://www.academia.edu/30520568/Social_Research_Methods_4th_Edition_by_Alan_Bryman_pdf

Cadle, J., Debra, P., & Turner, P. (2010). *Business Analysis Techniques: 72 Essential Tools for Success.* Swindon: British Informatics Society Limited. Retirado de https://www.academia.edu/11176141/Business_Analysis_Techniques_72_Essential_Tools_for_Success

Centro de Computação Gráfica - Investigação & Desenvolvimento Tecnológico. (2019). *Cloud computing vs fog computing vs. edge computing na era da internet das coisas industrial*. Retirado de https://www.ccg.pt/cloud-computing-vs-fog-computing-vs-edge-computing-na-internet-das-coisas-industrial/

Centro Nacional de Cibersegurança. (2020). *A Internet das Coisas (IoT – Internet of Things)*. Retirado de https://www.cncs.gov.pt/a-internet-das-coisas-iot-internet-of-things/

Comissão Europeia. (2019c). Estados-Membros publicam relatório sobre a avaliação coordenada dos riscos da segurança das redes 5G na UE. *Comunicado de imprensa*. Retirado de https://ec.europa.eu/commission/presscorner/detail/pt/ip_19_6049

Comissão Europeia. (2019d). Cibersegurança das redes 5G. *Recomendação (UE) 2019/534 da Comissão*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32019H0534&from=EN

Comissão Europeia. (2020a). Conjunto de instrumentos da UE para a cibersegurança das redes 5G. *Factsheet*. Retirado de https://ec.europa.eu/digital-single-market/en/news/eu-toolbox-5g-security

Comissão Europeia. (2020b). Implantação segura de redes 5G na UE – Aplicação do conjunto de instrumentos da UE. *COM(2020) 50 final. Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao*

Comité das regiões. Retirado de https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=COM:2020:0050:FIN

Comissão Europeia. (2020c). Relativa a um conjunto de instrumentos comuns a nível da União destinados a reduzir o custo da implantação de redes de capacidade muito elevada e a assegurar um acesso ao espetro de radiofrequências 5G. *Recomendação (UE) 2020/1307 da Comissão*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32020H1307&from=PT

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

Damião, R. (2019). *City as a service*. Retirado em 12 de novembro de 2020, de IT-insight: https://www.itinsight.pt/news/in-deep/city-as-a-service

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,1ª Série, 211. Lisboa: Ministério da Defesa Nacional. Retirado de https://dre.pt/application/file/a/70842580

Despacho n.º 11400/2014, 3 de setembro. (2014). Diretiva Ministerial de Planeamento de Defesa Militar. Retirado de https://dre.pt/application/file/a/56725594

Dias, Á. L., Varela, M., & Costa, J. L. (2013). *Excelência Organizacional*. Bnomics.

Fachada, C.P.A., Ranhola, N.M.B., Marreiros, J.P.R, & Santos, L. A. (2020). Normas de Autor no IUM (3ª ed., revista e atualizada). *IUM Atualidade, 7*. Lisboa: Instituto Universitário Militar.

Flick, U. (2013). *Introdução à metologia de pesquisa: um guia para iniciantes* (4th ed.). Porta Alegre: Penso editora Ltda. Retirado de https://www.ets.ufpb.br/pdf/2013/2%20Metodos%20quantitat%20e%20qualitat%20-%20IFES/Bauman,%20Bourdieu,%20Elias/Livros%20de%20Metodologia/Flick%20-%20Introducao%20%C3%A0%20Metodologia%20da%20Pesquisa.pdf

Fonseca, J. N. (2010). O conceito de Segurança Nacional perspectivado para 2030. *Trabalho de Investigação Individual do CPOG 2009/2010*. Lisboa: Instituto de Estudos Superiores Militares.

Gilli, A., & Bechis, F. (2020). *NATO and the 5G challenge*. Retirado de https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html

Hernández, D. C. (2020). *5G, una carrera por la hegemonía y el futuro con muchos beneficios. Documento MARCO IEEE 07/2020*. (ieee.es, Editor) Retirado de http://www.ieee.es/en/Galerias/fichero/docs_marco/2020/DIEEEM07_2020DAVCOR_5G.pdf

Iberdrola. (2020a). *Estamos cientes dos desafios e das principais aplicações da Inteligência Artificial?* Retirado de https://www.iberdrola.com/inovacao/o-que-e-inteligencia-artificial

Iberdrola. (2020b). *Realidade Aumentada: o mundo real com outros olhos*. Retirado de https://www.iberdrola.com/inovacao/o-que-e-realidade-aumentada

Iberdrola. (2020c). *Realidade Virtual: outro mundo ao alcance de seus olhos*. Retirado de https://www.iberdrola.com/inovacao/realidade-virtual

Infopédia - Dicionários Porto Editora. (s.d.). *Siginificado das palavras*. Retirado de https://www.infopedia.pt/dicionarios/lingua-portuguesa

IUM. (2020a). Procedimentos relativos à elaboração de trabalhos de investigação realizados no âmbito de cursos que não atribuem grau académico. *NEP/INV-001 (A1)*. Lisboa: Instituto Universitário Militar.

IUM. (2020b). Estrutura e regras de citação e referênciação de trabalhos escritos a realizar no Instituto Universitário Militar. *NEP/INV-003 (A3)*. Lisboa: Instituto Universitário Militar.

Lei n.º 46/2018. (2018). Regime jurídico da segurança do ciberespaço. *Diário da República n.º 155/2018, Série I de 2018-08-13*. Lisboa. Retirado de https://dre.pt/web/guest/home/-/dre/116029384/details/maximized?print_preview=print-preview

LSM.LV. (2020). *Latvia launches first 5G military test site in Europe.* Latvia Defense. Retirado de https://eng.lsm.lv/article/society/defense/latvia-launches-first-5g-military-test-site-in-europe.a381607/

Machado, N. (2018). *Domótica: o que é e quais as vantagens*. Retirado de https://www.e-konomista.pt/domotica/

NIS Cooperation Group. (2020). *Cybersecurity of 5G networks - EU Toolbox of risk mitigating measures*. Retirado de https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures

Oliveira, M. A. (2018). *Raciocínio indutivo*. Retirado de https://www.infoescola.com/filosofia/raciocinio-indutivo/

Pujol, F., Manero, C., Carle, B., & Remis, S. (2021). *5G Observatory Quarterly Report 10.* Bruxelas: Comissão Europeia. Retirado de http://5gobservatory.eu/wp-content/uploads/2021/01/90013-5G-Observatory-Quarterly-report-10.pdf

Ramalho, P. (2000). A crise internacional - a sua Gestão. Em *Revista Estratégia* (Vol. XII). Lisboa: Editorial Presença.

RCM n.º 19/2013, 21 de março. (2013). Conceito Estratégico de Defesa Nacional. *Diário da República n.º 67/2013, Série I de 2013-04-05*, 1981 - 1995. Lisboa: Presidência do Conselho de Ministros. Retirado de https://dre.pt/pesquisa/-/search/259967/details/maximized

RCM n.º 7-A/2020, 7 fevereiro. (2020). Aprova a estratégia e calendarização da distribuição da quinta geração de comunicações móveis. *Diário da República n.º 27/2020, 1º Suplemento, Série I de 2020-02-07*. Lisboa: Presidência do Conselho de Ministros. Retirado de https://dre.pt/home/-/dre/129106697/details/maximized

RCM n.º 92/2019, 23 de maio. (2019). Estratégia Nacional de Segurança do Ciberespaço 2019-2023. *Diário da República n.º 108/2019, Série I de 2019-06-05*. Lisboa: Presidência do Conselho de Ministros. Retirado de https://dre.pt/web/guest/home/-/dre/122498962/details/maximized?print_preview=print-preview

Rego, A., Cunha, M. P., & Junior, V. M. (2018). Quantos participantes são necessários para um estudo qualitativo? Linhas práticas de orientação. *Revista de Gestão dos Países de Língua Portuguesa*. Retirado de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-44642018000200004

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

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

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students 5th Edition* (5th ed.). Essex: Pearson Education Limited. Retirado de https://www.academia.edu/23374295/Research_Methods_for_Business_Students_5th_Edition

What You Need to Know about 5G. (s.d.). Retirado de Free WiFi Hotspot: https://www.free-wifi-hotspot.com/what-you-need-to-know-about-5g/

Yasmin. (2019). *Upload e Download*. Retirado de https://definicao.net/upload/

Apêndice A – Corpo de Conceitos

Ameaça – qualquer acontecimento ou ação (em curso ou previsível) que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais ou morais, sendo o produto entre uma possibilidade e uma intenção (Couto, 1988, p. 329). No âmbito da análise SOWT as "Ameaças" (*Threats*) devem ser considerados como aspetos externos negativos com potencial para prejudicar uma organização (Cadle, Debra, & Turner, 2010, p. 15).

Análise externa – estudo de uma organização com a finalidade de escolher os fatores externos que têm mais potencialidade de influenciar uma organização, tendo em consideração a sua probabilidade de ocorrência e o seu grau impacto na organização (Dias, Varela, & Costa, 2013, p. 298).

Análise interna – estudo de uma organização em termos dos seus pontos fortes e dos seus pontos fracos (Dias, Varela, & Costa, 2013, p. 322).

Análise *SWOT* – técnica utilizada para sintetizar as pressões externas enfrentadas por uma organização e a capacidade interna existente para fazer face a essas pressões. A nível interno são diagnosticados os pontos fortes (*Strenghts*) e os pontos fracos (*Weakness*) e a nível externo são diagnosticadas as oportunidades (*Opportunities*) e as ameaças (*Threats*) (Cadle, Debra, & Turner, 2010).

Capacidade Militar – "entende-se por capacidade militar o conjunto de elementos que se articulam de forma harmoniosa e complementar e que contribuem para 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" (Despacho n.º 11400/2014, 3 de setembro, 2014).

Ciberdefesa – consiste na atividade que visa assegurar a defesa nacional no, ou através do, ciberespaço (RCM n.º 92/2019, 23 de maio, 2019).

Cibersegurança – conjunto de medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação, das redes e sistemas de informação no ciberespaço, e das pessoas que nele interagem (RCM n.º 92/2019, 23 de maio, 2019).

Computação de proximidade (*edge computing*) – é um paradigma de computação distribuída que aproxima a computação e o armazenamento de dados no local onde são necessários, a fim de melhorar os tempos de resposta e economizar largura de banda (Comissão Europeia, 2020b, p. 3).

Computação em nuvem (*Cloud Computing*) − pode ser definida como um modelo de disponibilização e utilização de Tecnologias de Informação e Comunicação, que permite o acesso remoto, através da internet, a um leque de recursos de computação partilhados em forma de serviços (Centro de Computação Gráfica - Investigação & Desenvolvimento Tecnológico, 2019).

Defesa Nacional – "conjunto de medidas tanto de carácter militar como político, económico, social e cultural que, adequadamente coordenadas e integradas, e desenvolvidas global e sectorialmente, permitem reforçar a potencialidade da Nação e minimizar as suas vulnerabilidades, com vista a torná-la apta a enfrentar todos os tipos de ameaça que, directa ou indirectarnente, possam pôr em causa a Segurança Nacional" (Ramalho, 2000, p. 171).

Divisão de rede (*network slicing*) – permite um elevado grau de separação entre as diferentes camadas de serviço (*service layers*) na mesma rede física, aumentando assim as possibilidades de oferta de serviços diferenciados em toda a rede (Comissão Europeia, 2020b, p. 3).

Inteligência artificial – é a combinação de algoritmos projetados para criar máquinas que tenham as mesmas capacidades que o ser humano (Iberdrola, 2020a).

Internet das Coisas (*IoT*) – compreende todos os aparelhos e objetos que se encontram habilitados a estarem permanentemente ligados à Internet, sendo capazes de se identificar na rede e de comunicar entre si (Centro Nacional de Cibersegurança, 2020).

Oportunidades (***Opportunities***) – são aspetos externos positivos com potencial para beneficiar uma organização (Dias, Varela, & Costa, 2013, p. 318).

Pontos fortes (***Strengths***) – são as capacidades internas positivas de uma organização (Cadle, Debra, & Turner, 2010, p. 15) que constituem uma vantagem face a outras organizações (Dias, Varela, & Costa, 2013, p. 342).

Pontos fracos (***Weaknesses***) – são os fatores internos negativos capazes de diminuir as hipóteses de sucesso de uma organização (Cadle, Debra, & Turner, 2010, p. 15).

Realidade aumentada (RA) – é uma tecnologia que permite sobrepor elementos virtuais à nossa visão da realidade. Enquanto que a RV permite criar um mundo virtual do zero com tudo aquilo que quisermos (ou seja, um mundo fantástico), o que a RA faz é adicionar elementos virtuais (informações adicionais em forma de gráficos ou imagens) no nosso ambiente real (Iberdrola, 2020b).

Realidade virtual (RV) – é um ambiente, gerado por dispositivo informático, com cenas e objetos que parecem reais, fazendo com que os utilizadores se sintam imersos nessa realidade (Iberdrola, 2020c).

Redes 5G – "Conjunto de todos os elementos relevantes da infraestrutura das redes para tecnologias de comunicações móveis e sem fios utilizadas para fins de conectividade e em serviços de valor acrescentado com características de desempenho avançadas, tais como velocidades de débito e capacidade de dados muito elevadas, comunicações de baixa latência, de fiabilidade ultraelevada ou que suportem um grande número de dispositivos conectados. Podem incluir elementos das redes históricas baseados em gerações de tecnologias de comunicações móveis e sem fios anteriores, tais como as tecnologias 4G ou 3G. As redes 5G devem ser entendidas como incluindo todas as partes relevantes da rede." (Comissão Europeia, 2019d)

Risco – é uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação (Lei n.º 46/2018, 2018, p. 4032), sendo o produto entre um perigo e uma vulnerabilidade (Fonseca, 2010, p. 15).

Segurança Nacional – segundo Couto (1988, p. 172), a segurança nacional é a "condição da Nação que se traduz pela permanente garantia da sua sobrevivência em paz e liberdade, assegurando a soberania, independência e unidade, a integridade do território, a salvaguarda colectiva das pessoas e bens e dos valores espirituais, o desenvolvimento normal das tarefas do Estado, a liberdade de ação política dos órgãos de soberania e o pleno funcionamento das instituições democráticas".

Apêndice B – Lista de entidades participantes nas entrevistas

Neste apêndice é apesentada a listagem de entidades que participaram nas entrevistas (Quadro 4). Sendo que a entrevista n.º 1 é relativa às QD e a entrevista n.º 2 diz respeito à QC.

Quadro 4 – Entidades participantes nas entrevistas

N.º	Função	Identificação	Data da entrevista
E1	Diretor-Geral do Gabinete Nacional de Segurança	Contra-Almirante António Gameiro Marques	Entrevista n.º 1-18JAN21 Entrevista n.º 2-10MAR21
E2	Coordenador do Centro Nacional de Cibersegurança	Engenheiro Lino Santos	Entrevista n.º 1-25JAN21
E3	Representante do Ministério da Defesa Nacional no grupo de trabalho relativo à segurança das redes 5G	Comodoro Rui Alves Francisco	Entrevista n.º 1-02FEV21 Entrevista n.º 2-16MAR21
E4	Diretor da DIRCSI/EMGFA	Brigadeiro-General João António Campos Rocha	Entrevista n.º 1-28FEV21 Entrevista n.º 2-15MAR21
E5	Superintendente das Tecnologias da Informação da Marinha	Comodoro João Paulo Cancela Roque	Entrevista n.º 1-20JAN21 Entrevista n.º 2-12MAR21
E6	Diretor da DCSI do Exército	Brigadeiro-General Luís Filipe Camelo	Entrevista n.º 1-08FEV21 Entrevista n.º 2-18MAR21
E7	Diretor da DCSI da Força Aérea	Brigadeiro-General Armando Correia de Barros	Entrevista n.º 1-15JAN21 Entrevista n.º 2-16MAR21
E8	Chefe de Divisão - Normalização e Catalogação/ Direção-Geral de Recursos da Defesa Nacional	Coronel Francisco Veiga	Entrevista n.º 1-19JAN21
E9	Investigador no Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento em Lisboa e professor de sistemas de comunicações móveis no Instituto Superior Técnico	Professor Doutor Luís M. J. Sousa Correia	Entrevista n.º 1-19JAN21
E10	Cientista na NCIA responsável pelos assuntos 5G	Engenheiro Luís Bastos	Entrevista n.º 1-21JAN21
E11	Chefe de Segurança Digital, Tecnológica e de Infraestruturas/GNS e Coordenador da Segurança da Informação/GNS	Coronel José Gonçalves TCor Mário Duarte	Entrevista n.º 1-01FEV21
E12	ANACOM - Consultor do Conselho de Administração	Engenheiro Manual Pedrosa de Barros	Entrevista n.º 1-28JAN21
E13 (*)	---	---	---

Nota:

(*) Os dados recolhidos na Entrevista E13 foram considerados não relevantes, optando-se pela sua anulação.

Apêndice C – Guiões de Entrevista

Neste apêndice são apesentados os Guiões das Entrevistas semiestruturadas n.º 1 e n.º 2.

1. Guião de Entrevista n.º 1

Exmo. Senhor,

Sou o Coronel Jorge Pedro, presentemente a frequentar o Curso de Promoção a Oficial General 2020-2021, e estou a realizar um trabalho de investigação individual sobre o tema "O impacto das redes 5G na Segurança e Defesa Nacional", cujo objetivo geral (OG) é "Formular as linhas de ação (LA) que as Forças Armadas devem ter em consideração aquando da implantação das redes 5G em Portugal".

Para se atingir o OG foram definidos dois objetivos específicos (OE):

- OE1 - Analisar as orientações da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN) relativamente à implantação das redes 5G nos Estados-Membros/Países Aliados;
- OE2- Analisar as capacidades das Forças Armadas (FFAA) portuguesas para a implantação das redes 5G.

O percurso assim delineado implica a recolha de dados, por um lado relativamente ao ambiente externo das FFAA portuguesas (no âmbito das orientações da UE e da OTAN) identificando-se as oportunidades e as ameaças que as FFAA portuguesas irão enfrentar relativamente à implantação das redes 5G, e por outro lado relativamente ao ambiente interno das FFAA portuguesas identificando-se os seus pontos fortes e os pontos fracos para a implantação das redes 5G.

Esta entrevista semiestruturada tem como finalidade a recolha de dados para se alcançar os OE1 e OE2, e contributos para o OG, sendo realizada a um conjunto de entidades considerados especialistas conhecedores do tema ou que tenham responsabilidades na implantação das redes 5G, procurando-se ouvir, além das entidades na área da Defesa (Ministério da Defesa Nacional, Estado-Maior-General das Forças Armadas, Marinha, Exército, Força Aérea e OTAN), entidades externas que estão envolvidas nesta temática (Gabinete Nacional de Segurança, Centro Nacional de Cibersegurança, ANACOM e Instituto Superior Técnico).

Peço a autorização para gravar e para referir no trabalho o conteúdo desta entrevista associando o seu nome, respeitando o n. 4, do art.º 31.º do Regulamento Geral de Proteção de Dados (Lei n.º 58/2019, de 8 de agosto), em que os dados obtidos nesta entrevista destinam-se única e exclusivamente ao desenvolvimento desta investigação, respeitando-se os valores e os princípios éticos em vigor no Instituto Universitário Militar. Não sendo essa a sua vontade, garanto a sua confidencialidade e tratarei os dados recolhidos de forma anónima.

Importa mencionar que a sua experiência e conhecimento são fundamentais para a qualidade e relevância desta investigação, pelo que agradeço desde já a sua disponibilidade para colaborar neste trabalho.

A entrevista é constituída por cinco questões, divididas em três grupos (ambiente externo e ambiente interno e LA a considerar). A duração estimada é de 30 minutos de duração.

Caracterização do entrevistado

Entrevista n.º _____
Nome do entrevistado: _____
Entidade: _____Categoria/Posto_____
Cargo/Função:_____
Local: _____ Data: _____
Hora de início: _____Hora de fim: _____

Questões

Primeiro grupo de questões (Q) – Ambiente externo

N.º	Síntese introdutória
Q1 e Q2	A UE tem desenvolvido um conjunto de estudos e recomendações relativamente à implantação das redes 5G nos Estados-Membros, considerando benefícios nas áreas da saúde e da mobilidade, redes elétricas inteligentes, fábricas inteligentes e utilização da realidade aumentada e virtual nos meios audiovisuais e de entretimento. Paralelamente, apresentou um conjunto de cenários de risco relacionados com: (i) as medidas de segurança insuficientes; (ii) a cadeia de abastecimento 5G; (iii) o modus operandi dos principais atores mal-intencionados; (iv) as interdependências entre redes 5G e os outros sistemas críticos; (v) os dispositivos dos utilizadores finais. Já na OTAN os estudos desenvolvidos apontam para quatro domínios de aplicação das redes 5G: *Communications and Information Systems* projetável para operações expedicionárias, emprego em operações táticas terrestres, emprego em operações marítimas e utilização comunicações fixas.

	Indissociável destes estudos estão as caraterísticas das redes 5G com elevadas velocidades e volumes de transmissão de dados, baixa latência, disponibilidade e cobertura quase total, a ligação de um milhão de dispositivos/equipamentos por quilómetro quadrado, a divisão da rede e dos espetros (*network slicing*).
Q1	**Questão 1**
	Que oportunidades considera existirem no ambiente externo às FFAA portuguesas (i.e. aspetos externos positivos com potencial para beneficiar as FFAA), designadamente fruto das orientações da UE e da OTAN, relativamente à implantação das redes 5G?
Q2	**Questão 2**
	Que ameaças considera existirem no ambiente externo às FFAA portuguesas (i.e. aspetos negativos com potencial para prejudicar as FFAA), designadamente fruto das orientações da UE e da OTAN, relativamente à implantação das redes 5G?

Segundo grupo de questões (Q) – Ambiente interno

N.º	**Síntese introdutória**
Q3 e Q4	Genericamente, segundo o Despacho n.º 11400/2014, de 3 de setembro, a capacidade militar é o conjunto de elementos que engloba as componentes de doutrina, organização, treino, material, liderança, pessoal, infraestruturas e interoperabilidade. A implantação das redes 5G poderá ter impacto na capacidade militar, sendo que os campos de aplicação militar mais prováveis onde serão sentidas alterações são: (i) segurança militar (vigilância, deteção e reconhecimento facial); (ii) formação e treino (realidade aumentada e realidade virtual); (iii) logística (veículos autónomos, atividades de manutenção e gestão de stocks); (iv) comando controlo (visão e monitorização pormenorizada do campo de batalha); (v) triagem médica (diagnóstico e cirurgia remota); e (vi) defesa contra armas hipersónicas (i.e. misseis com velocidades superiores a Mach 5).
Q3	**Questão 3**
	Que pontos fortes considera existirem no seio das FFAA portuguesas (i.e. capacidades internas positivas das FFAA que constituem uma vantagem face a outras organizações) que irão beneficiar a implantação das redes 5G?
Q4	**Questão 4**
	Que pontos fracos considera existirem no seio das FFAA portuguesas (i.e. fatores internos negativos capazes de diminuir as hipóteses de sucesso das FFAA) que irão prejudicar a implantação das redes 5G?

Terceiro grupo de questões (Q) – Linhas de ações a considerar

N.º	**Síntese introdutória**
Q5	Neste trabalho procura-se cumprir OG (formular as LA ação que as FFAA devem ter em consideração aquando da implantação das redes 5G em Portugal) através de uma análise SWOT, tendo por base os dados recolhidos nas questões anteriores. É possível que já existam algumas ações que se considerem essenciais para as FFAA, relativamente à implantação das redes 5G.
Q5	**Questão 5**
	Que ações considera que devem ser acauteladas pelas FFAA relativamente à implantação das redes 5G?

Esta entrevista chega ao seu fim restando-me apresentar o meu agradecimento pela sua colaboração, pois sem ela não seria possível realizar esta investigação.

Irei efetuar a redação da entrevista e, logo que pronta, enviar-lhe-ei o conteúdo para aprovação e validação.

Agradeço, uma vez mais a sua atenção e disponibilidade.

2. Guião de Entrevista n.º 2

Exmo. Senhor,

Sou o Coronel Jorge Pedro, presentemente a frequentar o Curso de Promoção a Oficial General 2020-2021, e estou a realizar um trabalho de investigação individual sobre o tema "O impacto das redes 5G na Segurança e Defesa Nacional", cujo objetivo geral é "Formular as linhas de ação que as Forças Armadas devem ter em consideração aquando da implantação das redes 5G em Portugal".

No seguimento da estrutura-guia da investigação e após a recolha e análise de dados, através de entrevistas semiestruturadas, procedeu-se a uma análise SWOT de que resultaram oito linhas de ação (LA) que as Forças Armadas (FFAA) devem ter em consideração na implantação das redes 5G. Estas LA procuram satisfazer cada um dos vetores necessários para o desenvolvimento de uma capacidade.

Esta entrevista semiestruturada tem como finalidade validar as LA formuladas sendo realizada aos decisores de topo na Segurança Nacional e nas FFAA (Diretor-Geral do GNS, representante do MDN no grupo de trabalho relativo à segurança das redes 5G, Diretor de Comunicações e Sistemas de Informação do EMGFA, Superintendente das Tecnologias da Informação da Marinha, Diretor da Divisão de Comunicações e Sistemas de Informação (DCSI) do Exército e Diretor da DCSI da Força Aérea).

A entrevista é constituída por oito questões (uma para cada LA), para as quais se pretende obter uma posição de concordância ou desaprovação (respostas do tipo "sim" ou "não"), no caso de discordância saber o porquê (com a finalidade de melhorar essa LA), estimando-se uma duração de 30 minutos para a sua concretização.

Face ao exposto, solicito autorização para gravar e referir no trabalho o conteúdo desta entrevista, associando o seu nome no respeito do preconizado no n. 4, do art.º 31.º do Regulamento Geral de Proteção de Dados (Lei n.º 58/2019, de 8 de agosto), uma vez que os dados obtidos nesta entrevista se destinam-se, única e exclusivamente, ao desenvolvimento desta investigação, respeitando-se os valores e os princípios éticos em vigor no Instituto Universitário Militar. Não sendo essa a sua vontade, garanto a sua confidencialidade e tratarei os dados recolhidos de forma anónima.

Caracterização do entrevistado

Entrevista n.º _____
Nome do entrevistado: _____
Entidade: _____Categoria/Posto_____
Cargo/Função:_____
Local: _____ Data: _____
Hora de início: _____Hora de fim: _____

Questões

Síntese introdutória

1. Matriz SWOT

Ambiente Externo	Ambiente Interno: PONTOS FORTES (S)	PONTOS FRACOS (W)
	S1 - Competências e conhecimentos existentes S2 - Resiliência organizacional S3 - Cultura orientada para cumprimento da missão S4 - Existência de uma cultura de segurança	W1 - Falta de recursos humanos especializados/qualificados W2 - Insuficiência de recursos financeiros W3 - Falta de consciencialização das chefias W4 - Inexistência de normas técnicas/doutrina
OPORTUNIDADES (O) O1 - Desenvolvimento de aplicações 5G específicas para as FFAA O2 - Edificação de redes 5G privadas O3 - Operação remota de veículos e equipamentos O4 - Caraterísticas da tecnologia 5G	**CRESCIMENTO** SO1 - **CRIAR** cenários de emprego operacional do 5G nas FFAA (S1, S2, S3) x (O1, O2, O3) SO2 - **CONSOLIDAR** a interoperabilidade 5G nas FFAA e com os países aliados (S1, S2, S4) x (O1, O2, O3, O4)	**OTIMIZAÇÃO** WO1 - **CONSTITUIR** grupos de acompanhamento especializados em 5G (W1, W3, W4) x (O1, O4) WO2 - **ADEQUAR** os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações (W1, W2) x (O2, O4)
AMEAÇAS (T) T1 - Interferência de Estados Terceiros T2 - Tecnologia disruptiva/ imaturidade da tecnologia T3 - Ciberataques e cibercriminalidade T4 - Fraca qualidade dos produtos	**DINAMIZAÇÃO** ST1 - **ENVOLVER** as chefias no processo de implantação do 5G nas FFAA (S2, S3, S4) x (T2) ST2 - **EXPLORAR** a utilização segura de redes 5G próprias (S1, S2, S4) x (T1, T3, T4)	**PROTEÇÃO** WT1 - **POTENCIAR** a formação em cibersegurança/ciberdefesa e a especialização em 5G (W1, W2, W3, W4) x (T1, T3, T4) WT2 - **PROMOVER** a evolução sustentada das soluções tecnológicas 5G (W2) x (T3, T4)

Questão 1
Concorda que "CRIAR cenários de emprego operacional do 5G nas FFAA", de modo a obter conhecimento, identificar necessidades, potencialidades e vulnerabilidades, que possibilitem a criação de conceitos nas FFAA relativamente ao 5G, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 2
Concorda que "CONSOLIDAR a interoperabilidade 5G nas FFAA e com os países aliados", de forma a existir interoperabilidade nas comunicações dentro da rede e com os equipamentos e dispositivos a ela ligados, garantindo todos os requisitos de segurança, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 3
Concorda que "CONSTITUIR grupos de acompanhamento especializados em 5G", que integrem especialistas e operacionais, de forma transversal ao MDN, EMGFA e Ramos, que sigam os assuntos relativos ao 5G, no âmbito civil e militar, e produzam pareceres, estudos, normas e análises, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 4
Concorda que "ADEQUAR os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações", de modo a criarem-se mecanismos que garantam a fixação desses efetivos especializados responsáveis pela parametrização das aplicações, serviços e equipamentos, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 5
Concorda que "Concorda que "ENVOLVER as chefias no processo de implantação do 5G nas FFAA" com a finalidade de evitar que o assunto seja reconhecido apenas como um assunto meramente técnico, mas sim como um ativo estratégico, criando as condições para a tomada de decisão informada e potenciando o emprego da capacidade 5G, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 6
Concorda que "EXPLORAR a utilização segura de redes 5G próprias" de forma a potenciar as ligações da rede física, designadamente na interligação das comunicações estratégicas com as comunicações táticas, efetuando uma gestão e controlo da rede de forma autónoma, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 7
Concorda que "POTENCIAR a formação em cibersegurança/ciberdefesa e a especialização em 5G", de modo a fazer face à imaturidade da tecnologia e ao aumento da superfície de ataque cibernético, reforçando a capacidade de ciberdefesa das FFAA, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?
Questão 8
Concorda que "PROMOVER a evolução sustentada das soluções tecnológicas 5G" garantindo os recursos financeiros e materiais necessários para o desenvolvimento e manutenção de uma capacidade conjunta, apoiando a ID&I, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?

Esta entrevista chega ao seu fim restando-me apresentar o meu agradecimento pela sua colaboração pois ela acrescenta muito valor aos resultados obtidos nesta investigação.

Irei efetuar a redação da entrevista e, logo que pronta, enviar-lhe-ei o conteúdo para aprovação e validação.

Muito agradecido pela sua colaboração e apoio.

Apêndice D – Unidades de contexto

Neste Apêndice são apresentadas as UnCont obtidas de cada um dos entrevistados, para cada uma das questões da Entrevista n.º 1 (QD) e da Entrevista n.º 2 (confirmação da resposta à QC).

1. Guião de Entrevista n.º 1

Quadro 5 – UnCont da questão 1/GE1

Questão Q1: Que oportunidades considera existirem no ambiente externo às FFAA portuguesas (i.e. aspetos externos positivos com potencial para beneficiar as FFAA), designadamente fruto das orientações da UE e da OTAN, relativamente à implantação das redes 5G?		
E	**UnCont**	**UnReg**
E1	"Oportunidades no âmbito geral inerentes à natureza das FFAA […] impulsionadas na transformação por via genética devido a introdução de um novo sistema […] adaptando os processos de manutenção, formação, treino e mesmo a forma como ela se organiza […]. Oportunidades no âmbito específico […] nos domínios militares puros […] desde a forma como conduzimos operações, dentro e fora do território nacional […] que tem que ser aproveitadas, pois podem tornar-se ao invés de uma vantagem uma desvantagem […] na componente de operações, logística, médica, seguimento de dispositivos e sistemas, monitorização permanente do combatente, operação remota de veículos não tripulados […]. À semelhança do que tem sido histórico nas FFAA, a introdução de um novo equipamento/tecnologia é por si só potenciador de um conjunto de transformações, ou seja, procede-se à inovação por via da componente genética […]. As FFAA irão beneficiar da normalização/estandardização que irá ser estabelecida a montante, designadamente pela UE e OTAN […] e que poderá ser adaptada para normativos internos a nível do EMGFA e dos Ramos […]."	1.6 1.4 1.9, 1.8 1.10 1.2
E2	"Penso que o enfoque não deve ser nas redes 5G propriamente ditas, mas nas possibilidades que estas vêm trazer de novas aplicações que resultam de um conjunto de caraterísticas da tecnologia 5, que a torna completamente distinta das anteriores […] essencialmente a capacidade de transmissão, que permite aplicações com elevada qualidade de vídeo, em tempo real, a diminuição da latência, com novas aplicações com capacidade em tempo real […] e as características intrínsecas às próprias redes como por exemplo a capacidade de levar o processamento para o *edge* (*edge computing*), ou seja, para o mais próximo possível dos dispositivos que estão ligados ou a capacidade de criar *network slicing*, que é a capacidade de se criar redes virtuais em cima de uma infraestrutura partilhada […]. As novas aplicações terão um leque alargado de finalidades trazendo vantagens conforme o modelo de negócio."	1.13 1.7 1.5
E3	"[…] As oportunidades, de uma forma mais global, são as próprias características que as redes 5G nos vão trazer, da sua latência, velocidade, volume de informação, entidades que podem estar interconectadas […]. A nível externo é necessariamente a relação com a União Europeia e com a NATO […] e o apoio que poderemos obter dessas organizações, já materializado em alguns trabalhos que se têm feito […]. Depois temos as oportunidades relacionadas com a capacidade em si própria e que vão desde a formação, uma maior rapidez de reação no comando e controlo […] esta tecnologia aplica-se em todos os aspetos, quer na componente logística […] na operação de veículos autónomos […] ou na criação de redes próprias nas FFAA […]. O desenvolvimento de algumas aplicações […] principalmente ao nível tático […] que irá beneficiar mais desta tecnologia que a componente estratégica, face aos timings de cada uma das componentes."	1.13 1.2 1.4 1.9,1.10 1.7,1.5
E4	"[…] A Autoridade Nacional das Comunicações, o Conselho Superior de Segurança do Ciberespaço, assim como a indústria que dará corpo à tecnologia necessária para as FFAA possam usar operacionalmente […]."	1.5
E5	"As possibilidades do 5G são imensas como o acesso em locais remotos onde não existem ligações físicas, o controlo de veículos autónomos não tripulados, de transmissão de mais informação, mais dados, basicamente é fazer o que nós fazemos hoje mas com um *upgrade* significativo em termos de largura de banda que podemos utilizar […] poderemos utilizar redes 5G internas, muitas delas *ad hoc*, para ligações de troços de rede física, para operações no terreno, entre navios isolados […] ou seja muitas possibilidades que se constituirão como vantagens […] obviamente que há sítios onde as preocupações de segurança e privacidade são superiores como será o caso da saúde […] poderemos utilizar o 5G para tudo […] desde a gestão de *stocks*, controlo de veículos não tripulados, manutenção *online*, segurança inteligente, inteligência artificial, desenvolvimento de aplicações, etc."	1.10 1.7 1.9 1.10,1.11 1.3 1.5

E6	"Necessariamente existirá um conjunto de oportunidades que as FFAA portuguesas irão usufruir, do envolvimento crescente da União Europeia, Organização do Tratado do Atlântico Norte e das indústrias tecnológicas no âmbito da implantação das redes 5G. As redes 5G têm como pilares fundamentais, um elevado débito de dados (até 10 Gbps), níveis de latência extremamente reduzidos (1 ms), aumento significativo do número de dispositivos ligados por unidade de área, elevada disponibilidade (99,999%) e redução muito significativa do consumo de energia dos equipamentos (90%), especificidades que, per si, impactam no modus operandi das FFAA, em particular da sua componente terrestre […]. A tecnologia associada às redes 5G, sendo uma tecnologia emergente e disruptiva, necessariamente um dos vetores da revolução digital, terá certamente um forte impacto no estilo de vida das pessoas, no funcionamento das sociedades e organizações, com resultados inovadores nas áreas da robótica, telemedicina, computação quântica, meios de transporte autónomos, inteligência artificial […] constituirá assim que os que integram a OTAN, em estreita cooperação com a UE, desenvolvam sinergias, por via de uma cooperação estreita nos domínios da investigação e desenvolvimento, garantindo a interoperabilidade, através de adequados processos de normalização e implementação de standards, originando assim por via de economia de escala, redução dos custos de investimento […]. Os progressos alcançados pela inovadora tecnologia 5G […] resultarão, num futuro próximo, em arquiteturas mais proficientes para apoiar a condução de operações militares das forças envolvidas em operações, em ambientes conjuntos e combinados, garantindo a essencial interoperabilidade e incrementando a capacidade de comando e controlo, com recurso a uma rede de comunicações eficaz, mais resiliente e de elevada disponibilidade […] importa igualmente procurar acompanhar alguns projetos-piloto, lançados na OTAN, designadamente na NATO *Communications and Information Agency* (NCIA), com vista ao desenvolvimento específico de aplicações militares para as tecnologias 5G."	1.1 1.13 1.8, 1.10 1.3 1.1 1.2 1.12 1.7 1.5
E7	"[…] O potencial desta nova tecnologia está exatamente no que ela pode proporcionar em termos de utilização militar […], entre outras possibilidades, tornar realidade efetiva o emprego de veículos remotamente controlados e a cirurgia à distância, bem como o desenvolvimento de aplicações específicas para as FFAA ligadas à inteligência artificial, tais como, entre outras, o desencadeamento, de forma automática, de ações com base no reconhecimento facial, bem como a análise de dados ao nível do *big data*, cumprindo ainda destacar, no domínio das aplicações e relativamente à logística de suporte às máquinas em operação no campo de batalha, a gestão de stocks e a manutenção online , sendo certo que, para conseguirmos operar e tirar o máximo rendimento das redes 5G, devemos cooperar e obter o apoio de outros países."	1.13 1.10, 1.8 1.5, 1.3 1.11 1.9 1.1
E8	"[…] A NATO deve ser vista como elemento de confiança mútua entre nações, indispensável para que as operações corram como planeado […] proporcionará o desenvolvimento da economia de defesa […] que deve mostrar-se como potenciadora do desenvolvimento da economia nacional […]. Para uso em teatros de operações no exterior do território nacional, possivelmente em que o nível de penetração da tecnologia é baixo ou inexistente, temos que pensar em garantir que as FFAA cultivam a sua rede autónoma 5G, incorporando-a nas suas comunicações estratégicas e fazendo-a interligar com as comunicações táticas […] as caraterísticas do 5G acabam por ser uma vantagem possibilitando por exemplo […] extrair um ferido da frente de combate […] que poderá ter sensores instalados no seu equipamento individual que despoletam esse alerta e que acionam um drone, que guiado pela tecnologia faz a extração do combatente […].Teremos vantagens ao nível da modernização tecnológica."	1.2 1.12 1.7 1.13 1.8 1.10
E9	"Uma das grandes diferenças do 5G, relativamente a gerações anteriores é que terá novas tecnologias de rede que nos permitem constituir redes virtuais [*network slicing*] possibilitando que entidades externas aos operadores tenham redes próprias […] deixando de existir as limitações que acontecem agora com as VPN […]. As FFAA vão ter a possibilidade de contratar as tais redes virtuais, a um ou mais operadores, e a gestão das redes, no sentido de que serviços vão lá ser colocados, quem tem acesso a eles e outras possibilidades, pode ser feito pelas próprias FFAA e não pelo operador […] permitindo constituir um sistema tipo SIRESP, próprio das FFAA […]. Em ambientes exteriores ao território nacional, onde existem forças militares projetadas de vários países, irá permitir o uso partilhado da rede, sem que existam procedimentos de grande complexidade […]. Significa também que as FFAA não precisam de investir em infraestruturas pois aproveitam as que os operadores têm […]. As características do 5G irão melhorar o uso de aplicações	1.7 1.1 1.12 1.13,1.5

	militares […] controlo remoto de equipamentos […] cirurgia remota […] realidade virtual e aumentada, por exemplo através dos óculos dos combatentes ver os mapas do edifício […] tudo isto, potencialmente, com custos muito mais baixos."	1.10, 1.8 1.4 1.12
E10	"O 5G é a evolução do 4G e tudo o que está para trás, mas com um paradigma completamente diferente […] pela primeira vez os standards da tecnologia foram desenvolvidos com base em industrias verticais, portanto, definiu-se os requisitos e desenvolveu-se a tecnologia em torno desses requisitos […] fazendo coisas muito diferentes, como ligar máquinas a máquinas, de forma muito eficiente, até permitir o controlo remoto de equipamentos, usando redes móveis, etc., […] mas o 5G trás tecnologia nova, aplicações novas, com interesse militar […] com possibilidade dos militares utilizarem redes publicas para suportar comunicações militares […] o 5G irá permitir o chamado *network slicing*, em que uma rede seja partida por redes virtuais completa e verdadeiramente diferentes […] em que o próprio utilizador implementa, gera e controla essa rede através de software […] com conjunto de novas aplicações militares com tecnologia 5G […]. Relativamente à interoperabilidade, o 5G poderá ser visto, em ambiente militar, como uma forma fácil de Nações diferentes, em ambiente multinacional, contactarem umas com as outras […]. Se as FFAA tiverem sistemas 5G táticos próprios que se movem com os soldados, poderão utilizar a realidade aumentada e virtual nas suas operações […]. Se países trabalharem em conjunto e cooperarem, poderá haver mercado para o desenvolvimento da inteligência artificial para aplicação militar e outras tecnologias de uso militar, interoperáveis."	1.3 1.10 1.5 1.7 1.5 1.1 1.4 1.1 1.3
E11	"A implementação em Portugal das redes 5G, surge como uma oportunidade para as FFAA criarem a sua própria rede 5G […]. A utilização de aeronaves não tripuladas […] no apoio das Operações Militares […]. As características do 5G que são intrínsecas ao produto, a baixa latência, o volume de dados, a velocidade e o facto de se poder ter milhares de equipamentos ligados, entre outras, são vantagens às quais não podemos ficar alheios […] levaria a uma constante procura das melhores soluções para o cumprimento da missão, através da criação e desenvolvimento de aplicações especificas para as FFAA aliadas por exemplo a possível utilização de *clouds* proprietárias das FFAA, ou á inteligência artificial, assente numa capacidade de virtualização, potenciaria a capacidade natural das Força Armadas e estimularia a continua miniaturização e consequente criação de equipamentos muito mais fáceis de usar e de transportar. […] ou à utilização de inteligência artificial, assente numa capacidade de virtualização […]."	1.7 1.10 1.13 1.5 1.3 1.3 1.4
E12	"[…] as vantagens estão nas características da tecnologia 5G […] ter acesso a uma rede dedicada, que começa numa determinada faixa espectral, o chamado *network slicing* […] as alianças são muito importantes, desde que elas sejam sãs, na lógica de partilha de informação e de partilha da ameaça […]. A forma de obtermos interoperabilidade é irmos para a OTAN e União Europeia, pois aí existe uma massa critica que têm interesse para os fabricantes."	1.13 1.7 1.1 1.2

Quadro 6 – UnCont da questão 2/GE1

Questão Q2: Que ameaças considera existirem no ambiente externo às FFAA portuguesas (i.e. aspetos negativos com potencial para prejudicar as FFAA), designadamente fruto das orientações da UE e da OTAN, relativamente à implantação das redes 5G?		
E	**UnCont**	**UnReg**
E1	"As orientações da União Europeia, para já, vão no sentido de mitigar eventuais ameaças […] e garantir por exemplo, que sistemas de 5G cumpram requisitos de segurança […]. A maior ameaça é a eventual lentidão com que as decisões são tomadas na UE […]. Existem fornecedores da tecnologia 5G que atendendo ao modelo de governação que as respetivas empresas têm e ao valor do 5G em termos do impacto que vão ter na sociedade, que terão que ser acutelados no que respeita às áreas de soberania, em particular a defesa e em particular específico as FFAA […] A ameaça maior decorre da natureza da própria tecnologia, por ser muito intrusiva […] A cedência de espetro que estava reservado para uso militar, para as redes 5G, poderá ser uma ameaça […]."	2.4 2.12 2.1 2.11 2.9
E2	"Uma ameaça transversal […] é um aumento da superfície de ataque, com mais ciberataques e cibercriminalidade […]. Uma outra ameaça diz respeito ao *edge computing* […]. Depois temos as vulnerabilidades que são horizontais às novas tecnologias, desde logo a sua imaturidade […] a imaturidade dos produtos que são disponibilizados no mercado […] a capacidade de adaptação dos próprios instrumentos regulatórios e de supervisão […] e ainda aquelas ameaças relacionadas com a tecnologia, nomeadamente as relativas às cadeias de	2.2 2.10 2.11 2.4 2.8 2.1

	abastecimento e à capacidade de garantir a integridade dos produtos e dos serviços para estas infraestruturas.”	
E3	“O mais importante das ameaças é termos consciência delas, para tomarmos as mediadas adequadas […] e claramente que a primeira está relacionada com a segurança […] nos equipamentos […] abrindo portas a outros vetores de ameaça como sejam os ciberataques, a cibercriminalidade, a ciberespionagem, ações de sabotagem, etc. […] por exemplo a interferência de Estados terceiros, *sniffing* das nossas redes e informações […]. Como em qualquer outra tecnologia a sua imaturidade também é uma ameaça, aqui agudiza-se mais a questão pelo volume de dados que são tratados […] podendo haver intencionalidade da tecnologia não funcionar conforme deveria […] funcionando de modo ameaçador, encoberto na própria tecnologia […]. Teremos que ter mecanismos para proceder à certificação dos produtos, por exemplo garantido que eles não têm *backdoors*, não têm em si, embebidos, iniciativas propositadas para nos extrair informação ou para entrar dentro da nossa organização […]. O facto de não haver decisões atempadas, nacionais ou internacionais, relativamente à aplicabilidade da tecnologia, à segurança, etc.[…].”	2.4 2.2 2.10,2.6 2.1 2.11 2.8 2.12
E4	“As ameaças nas redes 5G serão as mesmas que já existem hoje, onde se destacam os atores estatais, com objetivos políticos ou económicos, pela sua capacidade humana e material.”	2.1
E5	“[...] a interferência de Estados terceiros será uma ameaça igual ao que se verifica […] ciberataques, cibercriminalidade, ciberespionagem, etc. porventura uma rede com maior capacidade possa dificultar os efeitos de *denial of service*, tudo o resto, é o que já vem a acontecer […] a lentidão da tomada de decisões a nível nacional e internacional poderá também ser um ameaça […].”	2.1 2.2, 2.10 2.6 2.12 .
E6	“[…] O 5G, pelas suas características intrínsecas, irá permitir interligar, para além das pessoas individualmente, uma vasta rede de sensores, transportes autónomos, equipamentos robóticos, sistemas de telemedicina, através de inteligência artificial, o que acarretará riscos de segurança acrescidos. Um ciberataque a estes sistemas, provocaria eventualmente a disrupção de infraestruturas críticas nos países afetados e consequentemente originaria riscos para a segurança interna dos estados […] riscos que poderia representar a hegemonia de fornecedores exteriores à Aliança […] proporcionar o acesso a grupos de cibercrime e atores hostis.”	2.11 2.2 2.6 2.5 2.2
E7	“[…] o 5G é uma tecnologia disruptiva que também pode ser usada por regimes autoritários de interesses contrários aos das referidas coligações e, sobretudo, com capacidade de interferir com o acesso de outros Estados a aspetos críticos da cadeia logística que sustenta a utilização desta tecnologia […] a utilização desta tecnologia comporta, desde o primeiro momento, vulnerabilidades, nomeadamente no que concerne à exposição a ciberataques, […] tornando ainda mais imperativo que a ciberdefesa e a cibersegurança sejam assuntos de elevada prioridade, quer a nível civil, que a nível militar. […].”	2.11 2.10 2.1 2.2
E8	“Deve existir a preocupação de salvaguardar a segurança da informação […] corremos o risco de ter componentes que entraram no processo de fabrico e mais tarde no abastecimento que não são de fontes confiáveis […] isto agravado pela nossa cultura de adquirir o mais barato, pode acarretar a aquisição de tecnologia que não é fiável […].”	2.8 2.1 2.4
E9	“A questão da segurança das comunicações terá que ser acautelada […] principalmente através de sistemas de cifra […] evitando que entidades exteriores tenham acesso à informação […] através dos equipamentos instalados pelos operadores, ou nas ações de manutenção/upgrade que estes possam realizar […] e com certeza irão manter-se as atuais ameaças, como sejam os ciberataques e a cibercriminalidade, ações de ciberespionagem e de sabotagem, entre outras.”	2.8 2.1 2.7 2.2,2.10 2.6
E10	“Devido às caraterísticas que o 5G pode permitir […]. Devemos considerar que a interferência de Estados terceiros será uma ameaça muito concreta.”	2.11 2.1
E11	“[…] Nesse sentido a segurança e a qualidade em qualquer dos equipamentos, produtos ou serviços a utilizar nesta rede, só pode ser garantido por uma avaliação da integridade do código antes da entrada em funcionamento, naquilo que na gíria se designa por *software quality analysis* […]. Uma outra preocupação a ter em conta é o possível preenchimento do espectro eletromagnético, o que poderá dificultar o nível de comunicações, principalmente quando se trata de serviços de comunicação mais antigos […]. Em termos de ameaça, antecipa-se ainda o potenciar da facilidade para criar disrupções via *distributed denial of service* […]. Um outro ponto a ter em conta será a existência de muito mais *players*, ou seja, mais interessados, sejam eles clientes ou fornecedores, o que irá obrigar a uma maior supervisão, mudanças ao nível dos acessos, seja ao nível da segurança e à identificação de	2.4 2.8 2.9 2.6 2.5 2.8

	quem está a ceder e a quê, esta situação tende a criar pressão também no nível de qualidade contratado com qualquer um dos operadores. Relativamente à dependência um fornecedor único, fragilidade que preocupava muitos países e instituições, ela foi no presente ultrapassada através da criação de algumas políticas e regras na União Europeia para a adoção de redes 5G, e que Portugal continua a implementar […]. A imaturidade da tecnologia poderá vir a constituir-se como uma ameaça, uma vez que cria algumas vulnerabilidades […]. No caso nacional podemos considerar que a insuficiência de legislação poderá ser um obstáculo ou melhor poderá constituir-se como uma ameaça […]. A dependência nacional da componente legislativa, seja da Comunitária ou da NATO, é uma constante realidade que tem atrasado toda uma regulamentação nacional, face à adoção de novas estratégias ou tecnologias […]. Para finalizar, a interferência de estados terceiros é e será sempre uma ameaça […].”	2.5 2.11 2.8 2.12 2.1
E12	“A China detém um número muito significativo de patentes chave para a implantação do 5G […] não sendo membro da União Europeia, da OTAN, da OCDE, surge como uma força colossal ao nível das Nações Unidas e da Organização Mundial do Comércio […]. O dado mais empírico que se vê, ao nível de fonte livre, é uma acusação do centro de testes do Reino Unido relativamente ao *software* de má qualidade de uma empresa chinesa […]. A definição da estratégia militar tem que começar pelo paradigma financeiro, ou seja, à luz do recurso financeiro existente (qual o orçamento existente?) como vou fazer a alocação dos recursos […] de outro modo temos somente uma abordagem teórica.”	2.5 2.4 2.3

Quadro 7 – UnCont da questão 3/GE1

Questão Q3: Que pontos fortes considera existirem no seio das FFAA portuguesas (i.e. capacidades internas positivas das FFAA que constituem uma vantagem face a outras organizações) que irão beneficiar pela implantação das redes 5G?		
E	**UnCont**	**UnReg**
E1	“Um ponto forte é a cultura das FFAA orientada para a missão […] mas há outras: a nossa capacidade técnica […]. É uma cultura que reflete séculos de história […] e que se inicia logo nos primeiros tempos em que se entra para as fileiras […] A segurança e a cibersegurança, como é natural, está embebido nesta cultura.”	3.1 3.2 3.6
E2	“A cultura de segurança e de avaliação de risco existentes nas FFAA deverão constituir-se como um ponto forte relativo à implantação das redes 5G nas FFAA […] e depois as FFAA têm uma grande capacidade de adaptação, tem recursos para estudar e planear estes processos de inovação tecnológico […]. De uma forma generalista poderemos afirmar que a cultura militar orientada para o cumprimento da missão também poderá constitui-se como um ponto forte […].”	3.6 3.5 3.2 3.1
E3	“Esta tecnologia irá trazer benefícios no comando e controlo, uma vez que manipula redes de sensores inteligentes e, portanto, vai usufruir muito, em tempo real, do esclarecimento da componente estratégica e ao nível tático […] dentro do campo de batalha e entre o campo de batalha e o suporte logístico […] ou inter-forças […]. Claro que a existência de uma cultura de missão, o espírito de missão, é um ponto forte. Também as nossas competências ao nível da área de comunicações e *networking* […] a existência de uma cultura de liderança e de segurança […] a capacidade de ciberdefesa já existente […] a nossa capacidade de dialogar com organizações internacionais e nacionais […] os nossos conhecimentos que cruzam tecnologia e segurança, um conhecimento multifacetado, um conhecimento feito da prática.”	3.7 3.1 3.2 3.6 3.8 3.12 3.2
E4	“A criação da capacidade de Ciberdefesa nas FFAA, demonstrou que a instituição militar é capaz de se organizar para estabelecer uma estratégia e um plano de ação para a sua implementação. A própria Ciberdefesa é um dos pontos fortes para o acompanhamento das ameaças no ciberespaço e para a criação de condições para que as operações militares sejam mais seguras na utilização das redes 5G.”	3.5 3.2
E5	“O primeiro ponto forte, diria, é nós sabermos edificar uma capacidade […] e mais, nós somos orientados para a missão, sem nos desviarmos dos objetivos a atingir […] com resiliência e perenidade […].”	3.2 3.1 3.5
E6	“Uma das oportunidades que as FFAA têm de potenciar, prende-se com o aproveitamento da informação residente na OTAN […]. No entanto, a maior vantagem reside no facto de, no seio das FFAA, ser mais fácil, por via da sua caraterização organizacional, fazer implementar táticas, técnicas, procedimentos e tecnologias afins com apreciável grau de celeridade. No futuro, assumirá relevância fulcral garantir as oportunidades que a tecnologia 5G poderá disponibilizar para o comando, controlo, traduzido num mais profícuo apoio de	3.2 3.5 3.7

	combate em CSI às operações militares. Considera-se igualmente importante que seja acautelado pelo EMGFA, junto da entidade da Autoridade Nacional das Comunicações (ANACOM), a reserva de faixas de frequências […].”	3.10
E7	“Estamos minimamente capacitados para explorar as potencialidades do 5G em contexto militar, na medida em que podemos tirar partido de experiências anteriores, […] bem como fortalecer a nossa resiliência organizacional […].”	3.2 3.5
E8	“As FFAA têm uma cadeia de comando muito bem definida, garantindo uma orientação síncrona num ambiente descentralizado […]. Do ponto de vista do comando e controlo das nossas forças temos vantagens significativas, por exemplo saber a cada momento onde estão os nossos militares no campo de batalha […] a capacidade de se perceber se a operação está a decorrer conforme o planeado ou não […] ou seja permite uma visualização do campo de batalha em tempo real.”	3.5 3.7 3.11
E9	“O controlo das infraestruturas militares poderá ser uma vantagem, relativamente à instalação de antenas e outros dispositivos de rede, pois não acarretará problemas relativos ao pagamento de renda, como previne as questões de segurança do acesso deste nó da rede ao resto da rede, etc. […] um aumento das capacidades de treino […]. A questão da existência de uma hierarquia poderá ser um ponto favor na utilização da rede.”	3.3 3.4 3.7
E10	“A cultura militar orientada para missão poderá ser um ponto forte para a implantação da tecnologia 5G quer nos aspetos relativos às potencialidades, quer naqueles relativos às vulnerabilidades […]. Se houver uma boa cobertura 5G […] poderá haver treino sofisticado […]. A cultura de segurança, de análise de risco e do pensamento estratégico sempre foram pontos fortes da instituição militar […] estando esta mais atenta para os aspetos ligados à ciberdefesa e à cibersegurança […]. As FFAA também têm capacidade de defender infraestruturas físicas estratégicas/criticas […]. A capacidade de facilitar o desenvolvimento de aplicações de uso civil poderá beneficiar os militares pois poderão receber como contrapartidas aplicações para uso militar […]. O facto do 5G estar implementado em várias frequências, que servem para vários mercados, origina a possibilidade de haver equipamentos que já estão desenvolvidos para operar nas frequências que estão reservadas para os militares […].”	3.1 3.4 3.6 3.8 3.3 3.9 3.10
E11	“A resiliência organizacional da Instituição Militar agregado à sua cultura militar, é um dos pontos fortes […]. O chamado *awareness* ou consciencialização, a sensibilidade para uma cultura de segurança, continuam a ser características da Instituição Militar assinaláveis, permitindo de forma independente cumprir os objetivos a que se propõe […]. A componente de análise, analítica e intelectual muito mais voltada para a área de segurança que qualquer entidade civil é garantidamente a nossa mais valia […] a nossa cultura organizacional são a base para o diálogo e a interoperabilidade entre os militares que permite a concretização positiva nas missões que somos chamados a desempenhar.”	3.5 3.6 3.1
E12	“O maior ponto forte das FFAA julgo estar na sua organização ao nível da existência de Estados-Maiores […] na sua função de produção de doutrina […], outra característica das FFAA é a sua capacidade de realizar planeamento […]. O treino é um ponto forte pois é algo que os militares estão habituados […] é do treino que vêm as equipas […] todos os novos cenários de automação, *machine to machine*, etc. poderão colocar alguns desafios ao nível da liderança […]. A nível da capacidade de ciberdefesa tem-se observado um investimento grande […] a vinda da Escola de Comunicações, para Oeiras, reforçou este ponto […] felizmente a cultura de segurança tem-se mantido nas FFAA.”	3.5 3.2 3.1 3.4 3.8 3.6

Quadro 8 – UnCont da questão 4/GE1

Questão Q4: Que pontos fracos considera existirem no seio das FFAA portuguesas (i.e. fatores internos negativos capazes de diminuir as hipóteses de sucesso das FFAA) que se poderão constituir como riscos/vulnerabilidades na implantação das redes 5G?		
E	**UnCont**	**UnReg**
E1	“Pensar-se que é um problema de natureza técnica/tecnológica […] implicando a possa levar mais tempo tirar partido desta nova tecnologia […]. Outro problema é a componente de recursos: financeiros e humanos para lidar com este desafio […]. Sumarizando: o alto comando das FFAA resumir/reduzir as questões do 5G a um assunto de natureza eminentemente tecnológico (que não é) e não termos recursos acautelados, designadamente em sede de LPM para desenvolver essa capacidade […].”	4.8 4.5 4.1 4.8 4.5
E2	“Um dos pontos fracos que vejo é a dificuldade de especialização decorrente da carreira militar (mudança de posto de trabalho/função) conjugada com a dificuldade de contratação	4.1

	de elementos especializados […]. Outro ponto fraco poderá ser a necessidade de maior investimento na Defesa […] do ponto de vista da Defesa devemos olhar para o estado da arte da tecnologia, que inclui o 5G, como ativo estratégico […].”	4.5 4.8
E3	“A falta de recursos humanos e financeiros é ponto fraco que é transversal […] ter forças a falarem umas com as outras e ter que produzir interoperabilidade […] a falta de consciencialização que induz os decisores a saírem do ciclo de decisão […] as coisas para irem para a frente precisam do envolvimento dos decisores ao mais alto nível […] Ao nível da implementação um dos pontos fracos a ser resolvido é a interoperabilidade dentro das FFAA […]. Em termos doutrinários é preciso ter uma doutrina comum de apoio à implantação da capacidade […].”	4.1, 4.5 4.7 4.8 4.7 4.6
E4	“Nas FFAA, como em qualquer organização, o fator humano e o fator material constituem-se sempre como riscos ou vulnerabilidades […].”	4.1, 4.3
E5	“Poderemos ter uma desvantagem que é ter dados a mais para processar […] as limitações serão aquelas que normalmente ocorrem pessoal, material, financeiras […] relativamente à obsolescência dos equipamentos, há partes da tecnologia que serão integráveis, outras terão que ser adquiridas, algumas das quais que ainda terão que ser desenvolvidas […] para implementar um sistema novo a parte tecnológica é a mais fácil de desenvolver e de implementar, a parte procedimental é que muito mais complexa. Assim, reforço que o ponto fraco é a abordagem deste assunto com uma perspetiva meramente tecnológica.”	4.9 4.1 4.5 4.3 4.6 4.8
E6	“Um dos fatores de risco, que será certamente uma vulnerabilidade, consiste no investimento financeiro que esta tecnologia exigirá […] será incrementar decisivamente os mecanismos associados à gestão da qualidade de serviço condição importante à implementação e funcionamento do 5G. Importa igualmente salientar que estas tecnologias emergentes e disruptivas carecem de pessoal com competências altamente especializadas e que exigem formação de elevada complexidade, […] que não são consentâneos com a normal rotação do pessoal militar no desempenho de funções.”	4.5 4.6 4.1
E7	“Em primeiro lugar, pensar-se que a utilização do 5G é um problema de natureza técnica/tecnológica […] quando, na realidade, são da máxima relevância estratégica, já que configuram uma nova arena de confronto […]. Em segundo lugar, para Estados com recursos limitados, humanos e financeiros, a utilização desta tecnologia em teatros de operações distantes só será possível em contexto cooperativo, no âmbito das coligações em que se participar, circunstância que irá tornar ainda mais relevantes as questões relacionadas com a interoperabilidade […].”	4.8 4.1 4.5 4.7
E8	“Esta tecnologia vai necessitar de investimento […] que poderá ter cofinanciamento da União Europeia […] ou temos possibilidade para desenvolver ou adquirir a tecnologia, ou corremos o risco dos Sistemas de Armas que equipam as forças ficarem obsoletos […] deve-se garantir que os recursos humanos são geridos de forma eficiente, apostar na formação e treino específicos garantindo o seu emprego naquilo que é o seu conhecimento.”	4.5 4.3 4.1
E9	“Eu colocaria os pontos fracos a dois níveis: um menor, relativamente à necessidade de existirem militares qualificados […]. O outro nível relacionado com o facto de haver muita tecnologia “escondida” e isto significa que tem toma decisões, se não for bem assessorado, poderá tomar decisões muito erradas […]. É preciso também não esquecer […] recursos financeiros necessários […].”	4.1 4.8 4.5
E10	“Tem que haver dentro das FFAA conhecimento sobre o tema 5G […] podendo advir riscos estratégicos, ao mais alto nível, até à segurança nacional, devido à falta de consciencialização existente […]. Tem que haver pessoal formado e qualificado tecnicamente […] o que ás vezes é agravado com a saída desse pessoal da organização […]. O facto dos militares não serem um cliente normal, que se satisfaz com um requisito de segurança mínimo, poderá constituir um ponto fraco, precisando de colocar níveis adicionais segurança […] podendo entrar no campo da interoperabilidade […]. A limitação de recursos financeiros, também constitui um constrangimento para as FFAA […] deve haver redundância de meios para que as comunicações possam continuar a acontecer mesmo quando existirem falhas ou ataques à rede.”	4.6 4.8 4.1 4.2 4.7 4.5 4.4
E11	“As comunicações atualmente ao serviço das FFAA, muitas delas ainda remontam aos anos noventa, baseadas em estruturas físicas antigas […]. Mas tudo entronca em recursos humanos e financeiros necessários para implementar, gerir e manter […]. Por norma, as chefias tendem a relevar para um segundo plano aquilo que não entende. Para se inverter esta situação terá que ser apresentada de forma clara e objetiva, através de uma demonstração palpável seja das consequências, seja dos benefícios para que as chefias possam decidir em	4.3 4.1 4.5 4.8

	conformidade com os objetivos globais da Organização […]. Sabemos que hoje em dia, as chefias têm uma necessidade cada vez maior de decidir e de forma rápida, e isso normalmente obriga a passar por cima de regras e de aspetos de segurança que poderão prejudicar as FFAA e comprometer a própria decisão […]. A utilização de espectro específico militar permitiria decidir em segurança […] o acesso muito mais rápido e a uma maior quantidade de informação, que temo que os militares não tenham a capacidade para tratar […] necessitamos de estabelecer normas especificas de certificação para equipamentos, produtos ou serviços […]. O 5G poderá constituir-se como a oportunidade fulcral para as FFAA de criarem uma uniformidade, uma interoperabilidade e uma gestão comum das comunicações, de forma a que possam trabalhar definitivamente em conjunto.”	4.2 4.9 4.6 4.7
E12	“Se optarmos pelo *network slicing* uma lógica de harmonização do acesso espectral vai colocar-se ao nível das forças, quanto mais não seja ao nível da interoperabilidade […] se formos para cenários típicos da OTAN, de operações conjuntas, isto tem que ser resolvido “à cabeça”, em sede de planeamento esta matéria vai ter que ser resolvida. Outro assunto que vai ter que ser acautelado é a estandardização, ou seja, a revisão das normas do 3GPP […] devendo haver um olhar ao nível dos protocolos na OTAN para se determinar se servem o desiderato operacional militar […]. As dificuldades que as FFAA têm em ter o material necessário para as suas missões é um ponto fraco […] isto paralelamente à falta de recursos financeiros […]. A quantidade de pessoal será outro ponto fraco […]. A interoperabilidade é essencial […] é um ponto onde se chega, não é um ponto de partida […] a interoperabilidade será o maior desafio ao nível do desenvolvimento da capacidade.”	4.7 4.6 4.3 4.5 4.1 4.7

Quadro 9 – UnCont da questão 5/GE1

Questão Q5: Que ações considera que devem ser acauteladas pelas FFAA relativamente à implantação das redes 5G?		
E	**UnCont**	**UnReg**
E1	“Constituir um grupo de trabalho, com operacionais e pessoal de transmissões (técnico), que acompanhasse os assuntos relativos ao 5G, ao nível do EMGFA, mas com a participação dos Ramos, para se perceber como as FFAA se devem posicionar para tirar proveito desta nova tecnologia, analisando o que se está a fazer noutras FFAA de referência para nós (por exemplo holandesa, alemã, inglesa e espanhola) produzindo um relatório […]. No próximo ciclo de planeamento e de revisão em LPM começar-se a introduzir a edificação da capacidade conjunta de 5G nas FFAA […]. Começar, nos Ramos, a preparar Oficiais e Sargentos neste ecossistema do 5G, de modo a apoiar a implantação desta tecnologia.”	5.1 5.2 5.3
E2	“[…] as FFAA têm que estar atentas ao desenvolvimento desta tecnologia, às possibilidades que esta tecnologia vai permitir, e eu volto a dizer, a integrá-las com outras como a computação avançada, como a computação quântica, como a inteligência artificial, e tirar partido, para a sua missão, deste portefólio (vamos chamar assim) de novas tecnologias, portanto tem obrigatoriamente que investir e deve ser um investimento estratégico.”	5.1 5.2
E3	“Se calhar uma linha de ação é estabelecer um grupo transversal multidisciplinar (uma equipa de projeto) que permita estruturar mais valias da tecnologia, as oportunidades que ela oferece […] pois no final o que queremos é edificar uma capacidade […] e por isso as linhas de ação devem cair dentro dos elementos da capacidade, DOTLPMI[2] […] esta capacidade deverá ter efeitos, em documentos estruturantes, incluindo no Conceito Estratégico de Defesa Nacional […] sendo que é preciso *sponsorship* por parte das lideranças […].”	5.1 5.4
E4	“Ao nível do EMGFA, vamos propor a criação de um Grupo de Trabalho transversal ao MDN (DGRDN e DGPDN), aos Ramos e ao EMGFA, em que o EMGFA deve ter elementos da DIPLAEM, do CCOM e da DIRCSI, por forma a serem definidas as intenções da Defesa de Portugal sobre as diversas temáticas que este assunto levanta aos níveis estratégico, operacional e tático. Por outro lado, devemos continuar a acompanhar as iniciativas nesta área levadas a cabo pela União Europeia e pela NATO.”	5.1
E5	“A capacidade de governação, ou seja, a sua implementação e a sua posterior manutenção […]. Estabelecimento de muitos objetivos intermédios na implementação […] de modo a se obter um processo gradativo de implementação/utilização […] um processo incremental.”	5.4
E6	“O debate sobre 5G na estrutura das FFAA está ainda no seu início e, presumivelmente, alcançará maior relevância na justa medida em que as comunicações militares iniciarem um processo de adaptação e transição para a tecnologia 5G […]. Sem as comunicações assentes em plataformas 5G, não será exequível explorar totalmente o acesso ao conceito *Big Data* e da computação na nuvem, bem como a inteligência artificial, no campo de batalha. Importa	

	que ao nível das FFAA seja debatido e levantadas as consequências desta transição aos vários níveis: material, liderança, pessoal, infraestruturas e interoperabilidade. Esta abordagem será necessária para garantir a identificação do investimento a realizar, a formação do pessoal para aquisição de competências tecnológicas, a par do desenvolvimento de doutrina adaptada a novos conceitos de operações, para explorar as oportunidades proporcionadas por esta tecnologia. As FFAA, deverão estar atentas aos desenvolvimentos a ocorrerem na União Europeia, e em particular na OTAN, com vista a incorporar os novos conceitos que vierem a ser emanados por estas organizações para integração do 5G, quer nas estruturas de comunicações fixas, quer nas táticas. Por último e porque sempre incontornável, a adesão das FFAA só será exequível se, atempadamente, for garantido o necessário financiamento, nomeadamente em sede da Lei de Programação Militar (LPM), a inscrição de verbas que possibilitem o investimento futuro nesta tecnologia, bem como em outras tecnologias emergentes correlacionadas." 5.4 5.3 5.1 5.2
E7	"[…] só será possível tirar partido das oportunidades que o 5G oferece através da edificação de uma capacidade conjunta […] sendo da maior importância que se comece a acompanhar o que se está a fazer em FFAA de referência para nós […]. Este primeiro passo, que se considera dever ser concretizado já no próximo ciclo de revisão da LPM […]. Por um lado, na vertente dos recursos humanos, é necessário, tão cedo quanto possível, preparar as próximas gerações para este novo paradigma tecnológico, começando já a trabalhar nos conteúdos formativos aos diversos níveis, na preparação de Oficiais e Sargentos, para que, no momento da concretização das primeiras iniciativas, já exista um mínimo de familiarização com o novo paradigma […] promover o lançamento de projetos de I&D que possam constituir-se como provas de conceito nas diversas possibilidades de aproveitamento do novo paradigma. […] o conceito de *security by design*, bem como os aspetos de segurança relacionados com a cadeia logística, que são, como vimos, os riscos principais que importa mitigar." 5.4 5.1 5.2 5.3 5.7 5.6
E8	"Eu diria que existem três orientações gerais: primeiro perceber qual a origem dos componentes que vão equipar os sistemas isto para garantir a segurança da informação. A segunda orientação é garantir a gestão eficiente dos recursos humanos e a terceira garantir a formação continua dos operadores dos sistemas de armas." 5.6 5.5 5.3
E9	"Internamente, penso que se deveria criar a tal *awareness* junto de quem toma as decisões, a nível das FFAA, a nível dos vários Ramos, eventualmente através da criação de um grupo de trabalho com os três Ramos, com as pessoas das comunicações, mas também de fora, para que não se torne um grupo demasiado fechado, só de tecnologia [...] que possa acompanhar o desenvolvimento da tecnologia […] percebendo quais as capacidades e o que ela vai permitir, começando a dialogar no exterior com os operadores de telecomunicações e outras entidades que possam ser prestadores de serviços na área militar […] de modo a ter conhecimento das características, potencialidades e vulnerabilidades, e assim tomarem-se as decisões mais acertadas […] e depois há as questões financeiras, que também têm que ser acauteladas." 5.1 5.2
E10	"Eu diria que as FFAA devem manter-se informadas, participarem nas discussões, ou pelo menos, observarem as discussões a nível de cibersegurança, das regras das entidades reguladoras […] por haver essa conotação com o valor estratégico das redes 5G futuras." 5.1
E11	"Avaliar as necessidades de espectro deveria ser uma linha de ação […] não só as necessidades presentes, como as necessidades futuras […]. Outra linha de ação seria o desenvolvimento de redes baseadas em *software* e preparar a introdução dessas redes […] que requerem um controlo mais efetivo e uma segurança mais definida, proactiva e ágil […] sendo necessário que as FFAA verifiquem como se está a fazer a introdução de equipamentos e de *software* […] e perceberem se é passível de ser utilizada para as redes 5G […] são coisas que exigem muito maior controlo do que atualmente se faz e que garantem a segurança que o tráfego vai para onde vai e não vai para onde nós não queremos […]." 5.6
E12	"Através de um grupo de trabalho a chefia devia colocar um objetivo temporal […] por exemplo o estudo de um cenário sob uma plataforma 5G à data tal […].Deveria ser definido o problema em termos de: âmbito [qual o âmbito do 5G que estamos a falar]; qual a profundidade que precisamos que o problema seja analisado; e qual a sua extensão […] devendo a chefia ter a capacidade critica para que os serviços venham com a análise da questão […] a chefia tem que ter o conhecimento e a massa critica para fazer a análise e a síntese […]. A análise deve ser feita nas FFAA e não Ramo a Ramo […]." 5.1

2. Guião de Entrevista n.º 2

Quadro 10 – UnCont da questão 1/GE2

Questão Q1: Concorda que "CRIAR cenários de emprego operacional do 5G nas FFAA", de modo a obter conhecimento, identificar necessidades, potencialidades e vulnerabilidades, que possibilitem a criação de doutrina nas FFAA relativamente ao 5G, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Sim, eu concordo plenamente. É fundamental criarem-se cenários de emprego operacional do 5G nas FFAA […] Importante será também filtrar esses cenários ou seja, definir os cinco ou seis mais verosímeis. Só com a criação desses cenários, os chamados casos de uso é que depois se vai desenvolver os conceitos de operações, requisitos ao nível dos recursos humanos, técnicos, etc. possivelmente um exercício interessante a ser realizado pela Academia. Como possível metodologia poderia partir-se da criação de cenários hipotéticos, por exemplo do quadro de missões plausíveis que as FFAA têm que desenvolver, que depois através de um conjunto de critérios pré-estabelecidos iriam ser confirmados ou eliminados, concentrando-se depois o estudo nos cenários obtidos […]. Isto tudo sem prejuízo de no final voltar-se novamente ao início do processo, rever e conceber novos cenários. Todo este processo deveria inicialmente focar-se em cenários que não fossem muito inverosímeis, concentrar-se em cenários nos quais as pessoas, que estivessem da debatê-los, tivessem algum conhecimento dos mesmos."	6.1 6.2
E3	"Concordo claramente que se produzam cenários de emprego do 5G. Deduzir os cenários mais importantes para a partir daí retirar um conjunto de informação, como essa que está descrita na pergunta, que pode ser identificada e desenvolvida.."	6.1 6.2
E4	"Sim, concordo é nitidamente uma linha de ação. Os cenários devem ser aqueles que nos são mais importantes e mais necessários."	6.1 6.2
E5	"Sim concordo […] deveria pensar-se neste assunto como algo envolvente, o "nG", porque o que estamos a fazer para o 5G num futuro próximo teremos que fazer para o 6G, ou seja, é um processo que vale a pena manter um acompanhamento permanente […]."	6.1 6.4
E6	"Concordo […] O desejável, será era que ao nível do emprego operacional nos domínios terra, mar e ar fossem criados cenários de maneira a ver qual é "demanda" do 5G relativamente ao impacto nas operações militares […]."	6.1 6.2
E7	"Concordo, isto é quase obrigatório […]. Daí a necessidade de levantamento de cenários, para depois haver uma opção por aqueles que melhor satisfazem os nossos interesses […] que fundamentasse a escolha dos cenários mais remuneradores para as FFAA.."	6.1 6.2

Quadro 11 – UnCont da questão 2/GE2

Questão Q2: Concorda que "CONSOLIDAR a interoperabilidade 5G nas FFAA e com os países aliados", de forma a operacionalizar interoperabilidade nas comunicações dentro da rede e com os equipamentos e dispositivos a ela ligados, garantindo todos os requisitos de segurança, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Sim, concordo com o consolidar a interoperabilidade 5G nas FFAA, com inter-agências e com os países aliados, ou seja acrescentar-se as inter-agências pois assim será coerente com os cenários, uma vez que deverão existir este tipo de cenários, onde as FFAA terão lidar com a Proteção Civil, bombeiros, INEM, etc. […] o 5G deve ser encarado e tratado como uma capacidade conjunta e não vertical da Marinha, do Exército e da Força Aérea, que depois pode ter instâncias específicas fruto de terminado teatro de operações. […]."	7.1 7.2 7.3
E3	"Sim, concordo […] quer nas FFAA quer externamente, com todos os parceiros que possamos interagir em termos operacionais. […]. Talvez o título da LA pudesse ser restruturado por exemplo para "Consolidar a interoperabilidade 5G nas FFAA, com os aliados e outros parceiros" e assim já se abrangia toda a temática."	7.1 7.2
E4	"Concordo […]. A interoperabilidade deve ser alargada a outras entidades, por exemplo à Proteção Civil."	7.1 7.2
E5	"Concordo e deve ser abrangente a outras entidades como por exemplo é o caso da organização da cibersegurança em Portugal que envolve um conjunto alargado de entidades, incluindo centros universitários e, portanto, não exclusivo da Defesa."	7.1,7.2

E6	"Concordo em absoluto. O 5G vai levantar questões primordiais de interoperabilidade […]. Esta linha de ação concordo em absoluto e é o maior desafio do 5G, além da implementação tecnológica, mas isso são equipamentos […]. "	7.1
E7	"Concordo […]. Nesta questão da interoperabilidade, é também importante incluir os parceiros com quem as FFAA poderão operar no contexto nacional, como é o caso das autoridades de proteção civil e forças e serviços de segurança, mesmo que isso torne este problema da interoperabilidade mais complexo […] obrigará seguramente a que se opere sempre com o apoio de outros e de forma conjunta/combinada."	7.1 7.2 7.3

Quadro 12 – UnCont da questão 3/GE2

Questão Q3: Concorda que "CONSTITUIR grupos de acompanhamento especializados em 5G", que integrem especialistas e operacionais, de forma transversal ao MDN, EMGFA e Ramos, que sigam os assuntos relativos ao 5G, no âmbito civil e militar, e produzam pareceres, estudos normas e doutrina, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Concordo com esta linha de ação […]. Este grupo deve estar "ancorado" numa estrutura existente no EMGFA e deve perceber o que a UE e a OTAN estão a fazer no âmbito do 5G, na sua fase inicial […]."	8.1 8.2
E3	"Penso que tem que haver um órgão de governação do 5G a nível nacional e depois cada um dos setores/ministérios deve fazer o seu acompanhamento […] ficando na dependência do EMGFA. Também aqui o texto da LA poderia ser por exemplo "Criar uma estrutura de governação 5G nas FFAA" ficando desta forma mais percetível a LA […]."	8.1 8.2 8.3
E4	"Sim, nós estamos a tentar fazer esse acompanhamento."	8.1
E5	"Também concordo […]. Isto não deve ser exclusivo do 5G, não deve ser limitado a esta tecnologia, tem que se alargar e acompanhar como um todo […]. Valia a pena alargar tecnologias de comunicações móveis."	8.1 8.4
E6	"Concordo, mas não considero importante pois as Forças Armadas, por via da sua organização ao nível do EMGFA e Ramos, já possuem órgãos com competências nestas áreas […]."	8.1 8.5
E7	"[…] é muito importante fazer esse acompanhamento e dinamizar todo este processo […]. Assim sendo, nesta fase inicial, não vejo outra alternativa que não seja estes grupos de acompanhamento ficarem na dependência do EMGFA (DIRCSI e DIPLAEM), pois aí a ligação com o Ministério da Defesa Nacional (DGRDN) será mais eficaz, tudo isto envolvendo também o recém-criado Departamento para a Inovação e Transformação do EMGFA. Ou seja, esta linha de ação possivelmente terá que ser reformulada, para que fique vincado que o EMGFA é o elemento-pivot e este aspeto não fique algo difuso, como me parece estar presentemente."	8.1 8.2

Quadro 13 – UnCont da questão 4/GE2

Questão Q4: Concorda que "ADEQUAR os recursos humanos às futuras necessidades, ligadas à operação e manutenção das redes 5G e respetivas aplicações", de modo a criarem-se mecanismos que garantam a fixação desses efetivos especializados responsáveis pela parametrização das aplicações, serviços e equipamentos, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Claro que concordo […] devendo haver formação para aquisição de competências técnicas especializadas e competências para fazer face aos cenários levantados na questão um […]."	9.1 9.2
E3	"Sim, é claramente importante. Os recursos humanos são a base para que tudo funcione e eles terem o conhecimento adequado e o treino é fundamental."	9.1
E4	"Concordo, no entanto, faria mais sentido ter uma capacidade residente aqui no EMGFA, uma estrutura fixa de forma a se conseguir manter aqui algum conhecimento que possa ser preservado durante vários anos. Talvez esta LA devesse apontar mais para a especialização nas FFAA e a LA da pergunta 7 para o treino."	9.1 9.3 9.2
E5	"Bem eu concordo, mas tenho que reconhecer que é um problema de difícil solução. Está agora a ser desenvolvido um trabalho sobre o que deverá ser a política de recursos humanos para a ciberdefesa nas FFAA, da mesma forma deveria ser feito para tudo o resto. […]."	9.1 9.4

E6	"Eu aqui diria "sim" e não". Sim, porque é efetivamente necessário, mas "não" porque não é um assunto novo […]. Esta necessidade de recursos humanos é verdade, mas não é do 5G, nem é de agora, é sempre que uma tecnologia determina alterações organizacionais […]."	9.1 9.4
E7	"Sim concordo. Tem que se entrar na questão da formação o quanto antes, começando a sensibilizar os Ramos para a inclusão de conteúdos curriculares relacionados com o 5G […]."	9.1 9.2

Quadro 14 – UnCont da questão 5/GE2

Questão Q5: Concorda que "ENVOLVER as chefias no processo de implantação do 5G nas FFAA" com a finalidade de evitar que o assunto seja reconhecido apenas como um assunto meramente técnico, mas sim como um ativo estratégico, criando as condições para a tomada de decisão informada e potenciando o emprego da capacidade 5G, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Se não se tiver em consideração esta Linha de ação corre-se o risco que inicialmente se observou (ainda que agora com menor expressão) para a cibersegurança, ou seja é uma tecnologia e por isso só aos técnicos diz respeito. As chefias têm que ser envolvidas ao mais alto nível para perceberem que o 5G é algo que é estratégico e que pode, se bem aproveitado, fornecer oportunidades e vantagens competitivas no campo de batalha e em qualquer cenário de emprego operacional que outros não terão se não entenderem isto como estratégico. Daí ser muito importante obter resposta à questão um deste questionário relativamente ao levantamento dos cenários de emprego […]."	10.1
E3	"As chefias têm que "apadrinhar" este processo pois doutra forma a urgência e a importância não são interiorizados nos escalões subordinados e isso irá prejudicar muito o desenvolvimento da capacidade. O "apadrinhar" deste tipo de transformações estratégicas, por parte dos dirigentes, é fundamental."	10.1
E4	"Sim, perfeitamente de acordo."	10.1
E5	"Concordo plenamente, tem que ser multidisciplinar."	10.1,10.2
E6	"Concordo, isto é evidente […] é o principal desafio a ser vencido e que poderá catapultar todo o processo."	10.1
E7	"Sim é importante envolver as chefias […]."	10.1

Quadro 15 – UnCont da questão 6/GE2

Questão Q6: Concorda que "EXPLORAR a utilização segura de redes 5G próprias" de forma a potenciar as ligações da rede física, designadamente na interligação das comunicações estratégicas com as comunicações táticas, efetuando uma gestão e controlo da rede de forma autónoma e garantindo uma adequada interligação com outras redes, quando aplicável, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Mais uma vez a resposta a esta questão é sim, mas dependente dos cenários que forem identificados como verosímeis […]. Por exemplo em cenários de emprego de FND onde faz sentido ter redes privadas, uma vez que não existe no teatro de operações redes 5G […] atendendo que as FFAA são o último reduto de ação do Estado, no início da edificação da capacidade, devia-se pensar na possibilidade de criar redes 5G próprias/autónomas, para cenários em que as infraestruturas do pais estivessem muito debilitadas. Só não colocaria este cenário extremo desde já, para mitigar riscos, uma vez que o conhecimento sobre esta tecnologia ainda tem muito campo para melhorar e como tal podemos adquirir algo que depois não serve os nossos propósitos."	11.1 11.2
E3	"A LA em si deve veicular bem a ideia da explicação, ou seja, deve ser dado enfase à autonomia das redes militares 5G. Assim, devia ser feita uma revisão do texto da LA no sentido de ela carregar devidamente o objetivo, como qual concordo […] a palavra "autonomia" devia no mínimo estar no corpo da LA […]. Talvez um LA que dissesse "Garantir a autonomia da exploração segura de redes 5G próprias."	11.1 11.3
E4	"Concordo, principalmente no que diz respeito à operação sem dependência de outrem."	11.1 11.3
E5	"Concordo […] isto é fundamental, se quisermos utilizar isto para a guerra é aqui que está a mais-valia, não no resto."	11.1

E6	"Concordo […] na minha opinião nem que tenha que ser o Exército a garantir este requisito de forma autónoma, ele é fundamental para o ramo e para as operações que desenvolve […]."	11.1 11.3
E7	"Concordo, mas esta será a linha de ação de mais difícil execução, devido ao investimento a ela associado […]."	11.1 11.4

Quadro 16 – UnCont da questão 7/GE2

Questão Q7: Concorda que "POTENCIAR a formação em cibersegurança/ciberdefesa e especialização em 5G", de modo a fazer face à imaturidade da tecnologia e ao aumento da superfície de ataque cibernético, reforçando a capacidade de ciberdefesa das FFAA, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Eu vejo esta questão ligada à questão quatro ou seja, nas diferentes segmentações de especialização que vai ser preciso realizar […]."	12.1 12.2
E3	"Esta LA em complemento da LA da questão 4 […] o importante aqui é a "especialização" […]. Talvez ter algo do género "Potenciar a especialização 5G, em cibersegurança e ciberdefesa [...]."	12.1 12.2
E4	"Concordo, mas importa referir que o 5G não veio trazer nada de novo […]. É necessária que exista formação e especialização, mas não é específico só do 5G."	12.1 12.3
E5	"Tem que se potenciar a formação em cibersegurança e ciberdefesa […] Por isso concordo e não deve ser particular para o 5G mas sim global para tudo o que é novo."	12.1 12.3
E6	"É claro que isto será uma evolução "cultural" do pessoal que já está em exercício […] por isso neste caso a minha resposta é sim relativamente à formação […]."	12.1
E7	"Concordo, isto é o principal *trade-off* que é preciso ter em conta […]."	12.1

Quadro 17 – UnCont da questão 8/GE2

Questão Q8: Concorda que "PROMOVER a evolução sustentada das soluções tecnológicas 5G" garantindo os recursos financeiros e materiais necessários para o desenvolvimento e manutenção de uma capacidade conjunta, apoiando a ID&I, deverá ser uma linha de ação que as FFAA devem ter em consideração? No caso de não concordar, importa-se de justificar a sua discordância e indicar qual a alteração a efetuar?		
E	**UnCont**	**UnReg**
E1	"Eu concordo porque sendo uma tecnologia de tão largo espectro em termos das suas aplicações terá uma taxa de evolução bastante grande. Sem termos esta linha de ação no nosso portfólio só reagimos […]. Tem que se promover a interação e o envolvimento entre as FFAA, a indústria e a academia […]."	13.1 1 3.2
E3	"Eu nesta LA diria antes "Garantir a sustentabilidade" pois dar-se-ia uma maior força a LA no diz respeito ao tempo e seria uma maneira mais curta de se transmitir a sua finalidade. Acho que na descrição desta LA se deveria incluir o envolvimento da indústria e da academia."	13.1 13.2
E4	"Concordo, mas penso que dificilmente iremos conseguir evoluir conforme aqui está escrito […]. É obvio que isto seria interessante, mas muito dificilmente o iremos conseguir concretizar […]"	13.1 13.3
E5	"Sim concordo, mas volto a referir que deve ser visto para além do 5G e não exclusivo deste. Devemos já olhar para além do 5G […]."	13.1 13.4
E6	"Esta questão é como a questão três, ou seja, concordo com o princípio, mas não considero que seja relevante ou que deva ser prioritária […]. A minha não concordância em algumas das questões enunciadas não decorre da importância da temática, pois são questões do bom senso, mas sobretudo com o modo como devemos lidar com os tópicos que encerram procurando relevar o que é importante […]"	13.1 13.4
E7	"Concordo, enfatizando que há que ver a ID&I como um caminho que, no início, face aos poucos recursos que nós temos, pode servir para manter este assunto suficientemente "vivo" durante um período inicial, até que possa ganhar dinâmicas de adoção que dispensem este apoio […]. Assim sendo, é imperativa uma atuação centralizada, ao mais alto nível estratégico, explorando as potencialidades do "triângulo virtuoso" Forças Armadas – Universidade – Indústria". Sugere-se, por exemplo, um concurso para projetos de ID&I financiado pela DGRDN e orientação estratégica pelo EMGFA, em estreita coordenação entre a DGRDN, de características monotemáticas, ou seja, exclusivamente dedicado ao 5G."	13.1 13.2