INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2021/2022

TRABALHO DE INVESTIGAÇÃO INDIVIDUAL

SEGURANÇA NAS REDES 5G – ESTRATÉGIA NACIONAL E INTERNACIONAL

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.

Isidro Miguel Mendes Lopes

MAJOR, INFANTARIA PARAQUEDISTA

INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

SEGURANÇA NAS REDES 5G – ESTRATÉGIA NACIONAL E INTERNACIONAL

MAJOR, INFANTARIA PARAQUEDISTA

Isidro Miguel Mendes Lopes

Trabalho de Investigação Individual do CEMC 2021/2022

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

SEGURANÇA NAS REDES 5G – ESTRATÉGIA NACIONAL E INTERNACIONAL

MAJOR, INFANTARIA PARAQUEDISTA

Isidro Miguel Mendes Lopes

Trabalho de Investigação Individual do CEMC 2021/2022

Orientador: MAJOR, TRANSMISSÕES

Tiago Filipe Abreu Moura Guedes

Pedrouços 2022

Declaração de compromisso Antiplágio

Eu, **Isidro Miguel Mendes Lopes**, declaro por minha honra que o documento intitulado "**SEGURANÇA NAS REDES 5G – ESTRATÉGIA NACIONAL E INTERNACIONAL"** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditor do **Curso de Estado-Maior Conjunto 2021/2022** no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

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

Assinado por: **Isidro Miguel Mendes Lopes**
Num. de Identificação: 12400096
Data: 2022.06.15 12:04:08+01'00'

Pedrouços**, 04** de **maio** de **2022**

CHAVE MÓVEL

Isidro Miguel Mendes Lopes

Agradecimentos

A elaboração deste trabalho de investigação constituiu um desafio tão gratificante como exigente, beneficiando de um conjunto de prestimosos contributos, sejam eles do foro profissional ou pessoal e que importa aqui salientar.

As minhas primeiras palavras, de agradecimento e elevado apreço, dirigem-se ao meu orientador, Major de Transmissões Tiago Filipe Abreu Moura Guedes, pelo acompanhamento, serenidade, disponibilidade e vontade em ajudar, mas acima de tudo, pela confiança que me transmitiu.

Pela disponibilidade demonstrada e visão enquadradora, apoiando a reflexão e debate dos tópicos estruturantes deste trabalho, foi importante poder contar com os contributos do Sr. Diretor-Geral do Gabinete Nacional de Segurança Contra-Almirante António Gameiro Marques, do Sr. Representante do Ministério da Defesa Nacional no grupo de trabalho relativo à segurança das redes 5G Comodoro Rui Manuel Alves Francisco, do Diretor de Operações da ANACOM – Açores Sr. João Frederico Beleza Vaz e do Sr. Major de Transmissões, *Security by Design Expert* (*Cibersecurity engineer*) na EDP, Nuno Casteleiro de Goes.

Aos meus camaradas do Curso de Estado-Maior Conjunto 2021/2022, pela amizade e partilha nesta jornada, sob o desígnio sempre "***Firmes e Constantes***", mas com particular apreço e reconhecimento de verdadeira amizade, J. Miranda, R. Carvalho, H. Alvarenga, H. Rodrigues, J. Marques, A. Martins.

Por último, para quem realmente importa e são o verdadeiro pilar da minha essência militar, a minha família. Pelo seu incondicional apoio e motivação, sem a retaguarda suportada por vocês, nada disto seria possível, a minha esposa Sandra Cotrim e os meus filhos Miguel e Margarida. Estou consciente que este público agradecimento nunca será suficiente para agradecer toda a compreensão e paciência, que mesmo nos momentos de maior ausência, sempre me forneceram todo o seu amor incondicional e estabilidade familiar necessária.

Índice

Índice de Anexos

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

A tecnologia das redes 5G pretende revolucionar o modo como a sociedade interage entre si e o meio envolvente, constituindo-se como um forte instrumento da transição digital devido às características que apresenta.

A intensificação da virtualização nas redes 5G conduzirá a uma evolução das ameaças à segurança e a uma superfície de ataque mais ampla e multifacetada, tornando-se crucial garantir a Cibersegurança e a resiliência destas redes.

Propondo contributos para a Estratégia de segurança nas redes 5G no âmbito das Forças Armadas portuguesas, este estudo analisa as potencialidades e as vulnerabilidades de segurança das redes 5G e as estratégias desenvolvidas para a sua implementação.

Para este efeito, utilizou-se o raciocínio indutivo utilizando uma estratégia qualitativa e um desenho de estudo de caso num horizonte temporal transversal com recurso a análise documental, bem como entrevistas a especialistas da Cibersegurança nacional.

Dos resultados obtidos pode concluir-se que as redes 5G, apesar das suas potencialidades, necessitam de definição de estratégias de implementação, com vista à segurança, principalmente nas Forças Armadas portuguesas, por forma mitigar os riscos associados, garantindo a confidencialidade, a integridade, a disponibilidade, a autenticidade, a resiliência e a privacidade das mesmas.

Palavras-chave: Redes 5G, Cibersegurança, Estratégias, Potencialidades Vulnerabilidades, Oportunidades, Ameaças.

Abstract

The network 5G´s technology aims to revolutionize the way that society interacts each other as well the environment that surrounds it, constituting a strong instrument of digital transition due to the characteristics that constitute it.

The intensification of virtualization in 5G networks will lead to an increase of threats to security and a wider, multifaceted attack surface. In this way it is crucial to ensure cybersecurity and the resilience of these networks.

Proposing contributions to the Security Strategy in 5G networks within the Portuguese Armed Forces, this study analyzes the security strengths and weakness of 5G networks, and also, the strategies developed for their implementation.

For this purpose, inductive reasoning was used within a qualitative strategy and a case study design in a cross-sectional time horizon using documentary analysis as well as interviews with national cybersecurity specialists.

Due the results obtained it is possible to concluded that the 5G networks, despite the potential that it has, is necessary and crucial to define strategies to implement a security awareness, especially in the Portuguese Armed Forces, to mitigate the associated risks, ensure confidentiality, integrity, availability, authenticity, resilience, and privacy of these kind of networks.

Keywords: 5G Networks, Cybersecurity, Strategies, Strengths, Weakness, Opportunities, Threats.

Lista de abreviaturas, siglas e acrónimos

3G	Terceira geração de comunicações móveis
3GPP	*3rd Generation Partnership Project*
4G	Quarta geração de comunicações móveis
5G	Quinta geração de comunicações móveis
A	
ANACOM	Autoridade Nacional de Comunicações
C	
CE	Comissão Europeia
CRS	Congressional Research Service
CSSC	Conselho Superior de Segurança do Ciberespaço
D	
DDoS	*Distributed Denial of Service*
DoD	*Department Of Defense*
E	
eMBB	*enhanced Mobile Broadband*
EUA	Estados Unidos da América
F	
FFAA	Forças Armadas
G	
GNS	Gabinete Nacional de Segurança
I	
IA	Inteligência Artificial
IoT	*Internet of Things*
ITU	*International Telecommunication Union*
L	
LE	Linhas de Esforço
M	
MA	Medidas de Apoio
ME	Medidas Estratégicas
mMTC	*massive Machine Type Communications*
MT	Medidas Técnicas

N

NCIA	*NATO Communications and Information Agency*
NTIA	*National Telecommunications and Information Administrations*

O

OE	Objetivo Específico
OG	Objetivo Geral
OTAN	Organização do Tratado do Atlântico Norte

P

PKI	*Public Key Infrastructure*

Q

QC	Questão Central
QD	Questão Derivada

R

RCM	Resolução de Conselho de Ministros

S

SWOT	*Strengths, Weaknesses, Opportunities, Threats*

T

TCE	Tribunal de Contas Europeu
TII	Trabalho de Investigação Individual

U

UE	União Europeia
uRLLC	*Ultra Reliable Low Latency Communications*

1. Introdução

A atualidade é caracterizada por um mundo impulsionado pelas novas disruptivas tecnologias, o que tem causado um significativo impacto na construção e transformação na forma como a sociedade vive e interage. Nesse alinhamento, a pandemia do SARS-CoV-2, demonstrou que a conectividade é essencial para as pessoas e empresas, tendo-se verificado um aumento do tráfego da internet de cerca de 30 % (International Telecommunication Union [ITU], 2020).

As redes de comunicações eletrónicas, em especial as redes de capacidade muito elevada, têm desempenhado um papel crucial na resposta à crise pandémica, permitindo assegurar o teletrabalho, o ensino à distância, a prestação de cuidados de saúde, a comunicação pessoal e o entretenimento.

Consequentemente, este progresso traduz-se igualmente na necessidade de desenvolvimento de dispositivos ao nível estrutural que os sustentem. Surge assim a Quinta Geração de Comunicações Móveis (5G), a tecnologia que transformará os dispositivos inteligentes em superdotados, pois a velocidade da rede 4G já não é suficiente para suportar estas dinâmicas por se encontrar no limite da sua capacidade (Ahmad, et al., 2017).

A implantação e operacionalização das redes 5G irá disponibilizar novas capacidades de serviços e constituir-se como elemento facilitador de sectores essenciais da sociedade, nomeadamente, da energia, transportes, financeiro, saúde, bem como, dos sistemas de controlo industriais (Resolução de Conselho de Ministros [RCM] n.º 7-A/2020, 2020).

Naturalmente, garantir a Cibersegurança das redes 5G é uma questão de importância estratégica para a defesa dos interesses essenciais de segurança de qualquer Estado, num momento em que os ciberataques aumentam e são mais sofisticados. Neste contexto, prevê-se que possam ser particularmente graves as consequências de perturbações sistémicas e generalizadas devido à futura dependência dos inúmeros serviços críticos em relação às redes 5G (Recomendação União Europeia (EU) 2019/534, 2019).

O recente relatório da *Microsoft Digital Defense Report* indica que no último ano, o país que mais ciberataques sofreu foi os Estados Unidos da América (EUA), representando 46% de todos os ciberataques. Portugal, ainda que com apenas 1% dos ciberataques, também aparece na lista (Figura 1) (Microsoft, 2021).

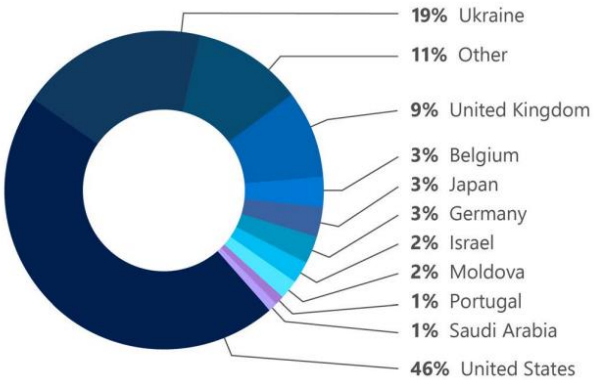


Figura 1 - Países com maior índice de ciberataques sofridos (Jul20-Jun21)
Fonte: Disponível em Microsoft (2021, p. 53).

O mesmo relatório da Microsoft (*op. cit.*) revela que, no mesmo período, o setor do Governo foi o mais atingido neste âmbito (Figura 2).

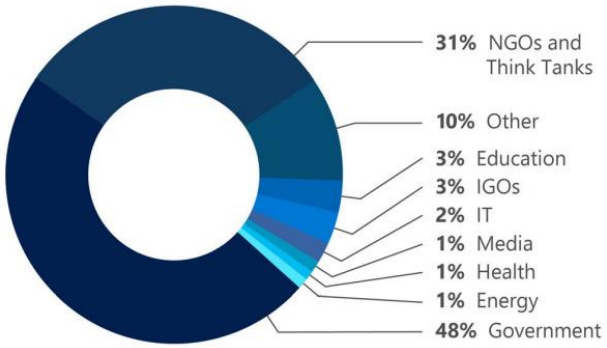


Figura 2 - Setores com maior índice de ciberataques sofridos (Jul20-Jun21)
Fonte: Disponível em Microsoft (2021, p. 53).

Face ao exposto, a compreensão deste fenómeno que se intitula como a era da hiperconectividade, representa um verdadeiro desafio da atualidade à sociedade. Pela abrangência nos diversos domínios da sociedade e na incerteza das reais implicações transformacionais, materializa-se desta forma a necessidade de investigação e assumido especial acuidade e oportunidade.

Diante da problemática de que existem poucos artigos e estudos científicos significativos a nível nacional, de um modo geral sobre as redes 5G e, em particular, sobre a sua segurança, esta investigação debruça-se sobre as Estratégias Nacionais e Internacionais para a sua implementação, circunscrevidas ao desígnio da segurança nas redes 5G e na forma como as Forças Armadas (FFAA) podem acolher e acompanhar esta nova era digital, configurando estratégias de segurança naquilo que são as suas especificidades e exigências militares.

Este tema insere-se no ramo do conhecimento das Ciências Militares, na área das Técnicas e Tecnologias Militares (Art.º 5º do Decreto-Lei n.º 249/2015 de 28 de outubro de

2015, p. 9300), na subárea da Ciberdefesa/Cibersegurança (Academia das Ciências de Lisboa, s.d.).

O objeto de estudo da presente investigação são as redes 5G, analisando as ameaças e vulnerabilidades associadas a esta nova tecnologia e as estratégias que estão a ser delineadas no âmbito da sua segurança.

A delimitação da investigação respeita a taxonomia apresentada por Santos et al. (2019, p. 42) pelo que se encontra delimitada: i) domínio temporal, a investigação reportar-se desde 2016 à atualidade (2021/2022), correspondente aos documentos de referência analisados, nomeadamente às diretivas e recomendações emanadas, ao nível nacional e internacional, sobre a implementação das redes 5G; ii) domínio espacial, incide sobre as orientações, diretivas e recomendações emanadas ao nível nacional (na componente da Cibersegurança), UE, Organização do Tratado do Atlântico Norte (OTAN) e os EUA na componente para a segurança das redes 5G. Relativamente ao conteúdo, a investigação foca-se nos conceitos das redes 5G e campos de aplicação militar, nas estratégias e recomendações de segurança para as redes 5G estabelecidas pelos EUA, UE, OTAN e Portugal.

No que concerne ao Objetivo Geral (OG) e os Objetivos Específicos (OE) formulados são apresentados no Quadro 1.

Quadro 1 - Objetivos da Investigação

Objetivo Geral
Propor contributos para a Estratégia de Segurança nas Redes 5G no âmbito das FFAA Portuguesas
Objetivos Específicos
OE 1: Descrever as potencialidades e vulnerabilidades de segurança nas redes 5G.
OE 2: Analisar as Estratégias de Segurança para as redes 5G.

Em linha com os objetivos elencados, foi definida a seguinte Questão Central (QC):

Que contributos podem ser integrados na Estratégia de Segurança nas redes 5G no âmbito das FFAA Portuguesas?

A estrutura do presente trabalho de investigação individual (TII), para além da presente introdução (primeiro capítulo), organiza-se em seis capítulos a que acrescem as conclusões. O segundo capítulo, apresenta a revisão da literatura, conceitos estruturantes e o modelo de análise. No terceiro identifica o percurso metodológico utilizado, participantes e procedimento, instrumento de recolha e técnicas de tratamento de dados. No quarto descreve as características das redes 5G, identificando-se as potencialidades e as vulnerabilidades de segurança das redes 5G. No quinto analisam-se as estratégias de segurança para as redes 5G dos países/organizações como os EUA, UE, OTAN e Portugal. No sexto apresentam-se os contributos colhidos da análise feita nas respostas às Questões Derivadas (QD) e,

consequentemente, dada resposta à QC apresentando-se contributos para a Estratégia de segurança para as redes 5G, no âmbito das FFAA portuguesas.

Nas conclusões, sintetizam-se o procedimento metodológico e os resultados obtidos, identificando contributos de seguranças para as redes 5G nas FFAA portuguesas. Como corolário deste trabalho, apresentam-se recomendações e sugestões para investigações futuras.

2. Enquadramento teórico e conceptual

O presente capítulo apresenta a revisão da literatura, os conceitos estruturantes, nomeadamente as redes 5G, Cibersegurança, Segurança das redes e dos sistemas de informação, Estratégia e culmina com o modelo de análise.

2.1 Revisão da Literatura

Nas últimas décadas, as redes de comunicação sem fios móveis sofreram uma mudança extraordinária. A geração sem fios móvel geralmente refere-se a uma mudança na natureza do sistema, velocidade, tecnologia, frequência, capacidade de dados, latência, etc. Cada geração tem alguns padrões, diferentes capacidades, novas técnicas e novas funcionalidades que a diferenciam da anterior. Para compreender para onde caminha o desenvolvimento nesta área, é importante visualizar o percurso que estas redes tiveram desde a sua origem até ao momento atual e que potencialidades ofereciam aos utilizadores em cada um desses períodos, conforme se visualiza na Figura 3 (Bhandari, Devra, & Singh, 2017).

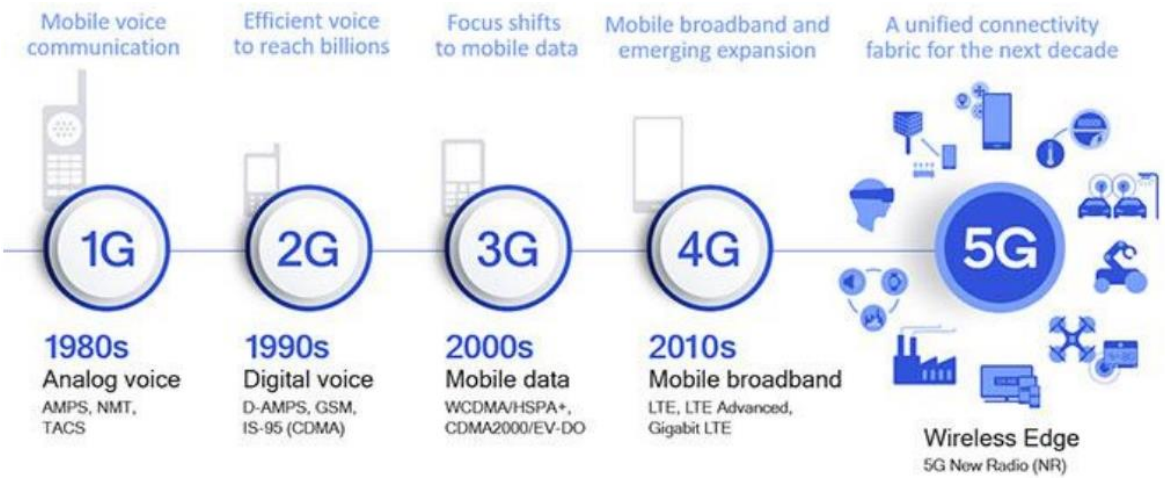


Figura 3 - Evolução das gerações móveis
Fonte: Disponível em Lodha (2020).

As redes de comunicações móveis tiveram o seu início em 1979, com a primeira geração constituída por dispositivos e comunicações analógicos, utilizando apenas chamada de voz. Em 1991 surge a segunda geração que passa a ser uma tecnologia digital, pois começa a suportar também mensagens de texto. A tecnologia móvel de terceira geração (3G) apareceu em 1998, trazendo consigo dados móveis e veio fornecer uma maior taxa de transmissão de dados, maior capacidade e apoio multimédia. A quarta geração foi introduzida em 2008 anunciando a era da internet móvel. Esta rede integra o 3G com internet fixa para suportar a internet móvel sem fios. Os anos da década de 2020-2030 serão dedicados à implementação e desenvolvimento da quinta geração móvel (5G), trazendo consigo uma nova fronteira tecnológica móvel (Bhandari, Devra, & Singh, *op. cit.*), com uma velocidade 100 vezes superior à rede 4G, maior fiabilidade, maior quantidade de

dispositivos conectados, latência insignificante e que se traduzirá num elevado impacto em todas as indústrias, tornando os transportes mais seguros, os cuidados de saúde remotos, a agricultura de precisão, a logística digitalizada, entre outros (Figura 4) (Qualcomm Technologies, Inc., 2022).

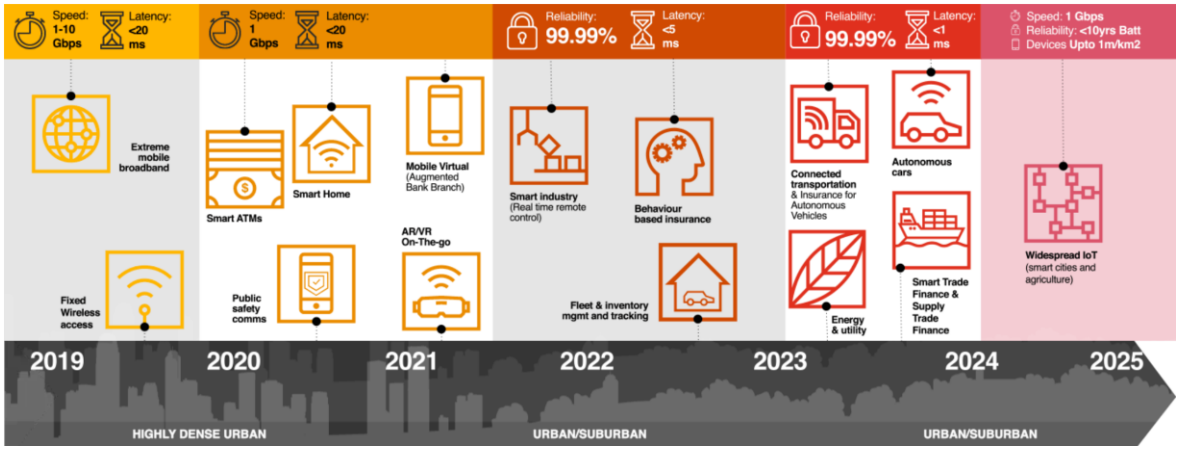


Figura 4 - A evolução 5G
Fonte: Disponível em PwC (2022).

Segundo a Comissão Europeia (CE) (2021), as redes 5G estão a ser definidas como a futura espinha dorsal da sociedade e da economia global, cada vez mais digitalizadas. O maior uso da virtualização nas redes 5G conduzirá a uma evolução das ameaças à segurança e a uma superfície de ataque mais ampla e multifacetada, tornando-se crucial garantir a Cibersegurança e a sua resiliência.

No âmbito da UE, encontram-se claramente definidas as funções e responsabilidades relativamente às redes 5G, conforme podemos observar na Figura 5.

	Comissão e agências da UE	Autoridades dos Estados-Membros	Operadores de redes móveis e fornecedores de tecnologia 5G
Reserva e atribuição de faixas pioneiras na tecnologia 5G		✓	
Definição da política da UE em matéria de redes 5G	✓	✓	
Implantação das redes 5G			✓
Investimento e financiamento	✓	✓	✓
Segurança nacional		✓	
Segurança das redes 5G		✓	✓
Apoio e coordenação das ações dos Estados-Membros	✓		

Figura 5 - Funções e responsabilidades da UE relativamente às redes 5G
Fonte: Adaptado a partir de Tribunal de Contas Europeu (TCE) (2022).

Em 2019, os Estados-Membros da UE, em colaboração com a CE, adotaram a Recomendação 2019/534 sobre Cibersegurança das redes 5G, onde invoca a todos os Estados-Membros para que ao nível nacional, completassem as avaliações de risco das redes 5G e que efetuassem a revisão dos requisitos de segurança e dos procedimentos de gestão de risco (CE, 2019).

Já a Recomendação 2020/1307 (2020), pretendeu que os Estados-Membros trabalhassem em conjunto numa avaliação de risco, para a elaboração de uma *Connectivity Toolbox* ("caixa de ferramentas" da conetividade) comum, com a agregação de medidas de mitigação de riscos de Cibersegurança no que diz respeito às redes 5G. Na Figura 6, poderemos visualizar os principais documentos estratégicos e metas relacionadas com a implantação e a segurança das redes 5G.

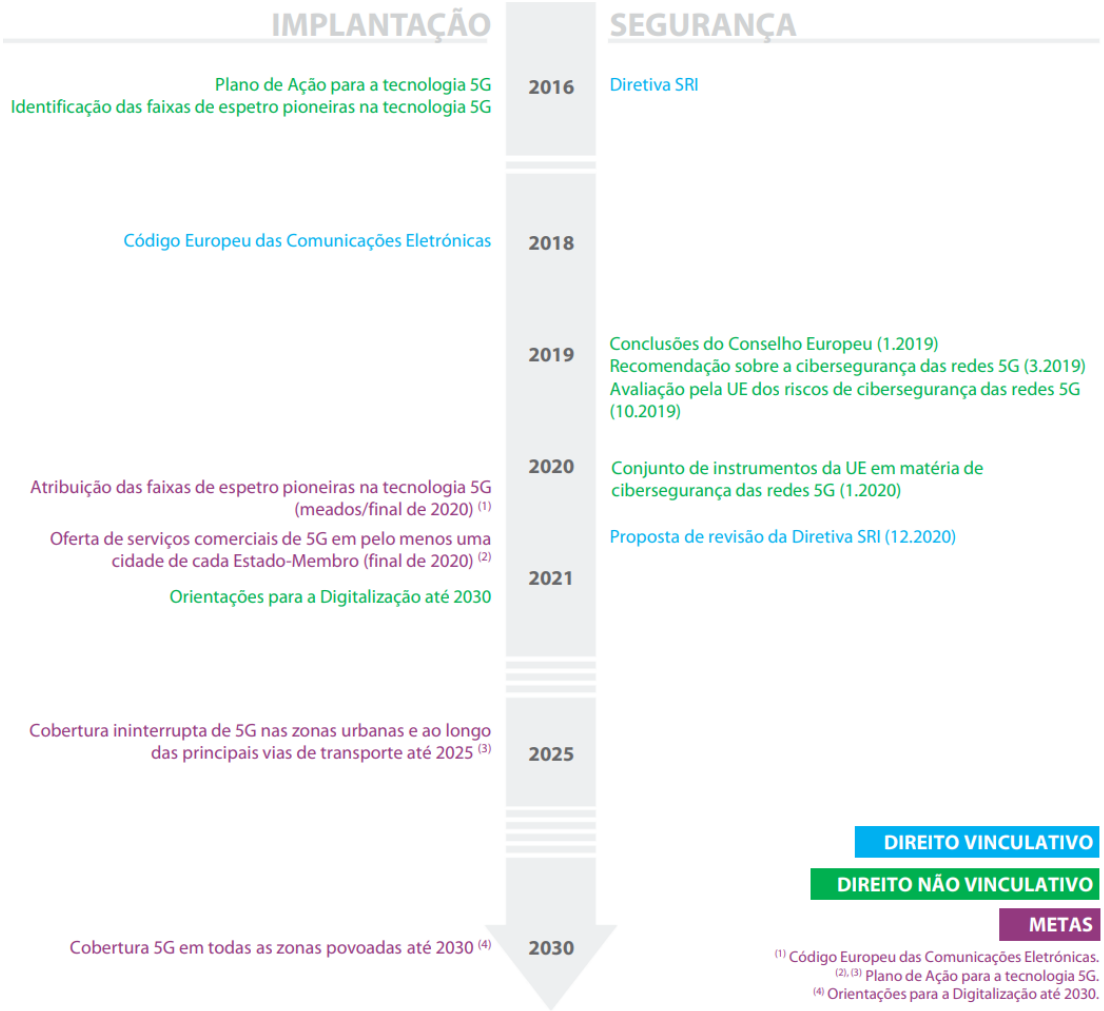


Figura 6 - Documentos estratégicos e metas das redes 5G da UE
Fonte: Disponível em TCE (2022).

Para a OTAN, a próxima geração de telecomunicações também identifica questões importantes como, as políticas para a alocação de espectro 5G as definições de normas sobre as aplicações de distribuição em tempo real de pacotes de dados massivos rececionados. Em algumas das suas recentes declarações públicas, destacou o papel central do 5G em questões de segurança e defesa no futuro próximo (Gilli, 2020).

Para os EUA, o 5G é uma tecnologia estratégica crítica, nesse sentido, afirmam que as nações que dominarem as tecnologias de comunicação avançadas e de conectividade omnipresente terão uma vantagem económica e militar a longo prazo. A ubiquidade da

conectividade de alta velocidade também transformará a maneira como as FFAA dos EUA irão operar no futuro (Department of Defense [DoD], 2020).

De acordo com o DoD (2020), os soldados do amanhã usarão redes 5G locais e expedicionárias para transferir grandes quantidades de dados, para conectar sensores e armas distantes numa rede do campo de batalha densa e resiliente. Este novo ambiente operacional, rico em dados, alimentará algoritmos poderosos que permitirão aos comandantes militares compreender, moldar e adaptarem-se melhor (*situational awareness*) a ambientes físicos e de informação complexos e disputados. As comunicações de baixa latência permitirão novas gerações de sistemas de armas não tripulados e autónomos em todos os domínios. O soldado terá acesso a dados inimagináveis, colocando-o na vanguarda tática, de modo que até mesmo unidades pequenas podem alcançar efeitos estratégicos. Para os EUA, os seus militares devem aprender a utilizar a conectividade fornecida pelo 5G para operar com a velocidade, precisão e eficiência necessárias, por forma a permanecerem eficazes e com capacidade de sobrevivência no futuro.

Portugal difundiu a RCM n.º 7-A/2020, que reconhece as redes 5G como uma importante ferramenta para a transição digital. A mesma resolução aprova a estratégia e calendarização da sua distribuição e estabelece a criação de um grupo de trabalho relativo à sua segurança que funciona no âmbito do Conselho Superior de Segurança do Ciberespaço (CSSC), sob a coordenação e presidência de um representante do Centro Nacional de Cibersegurança. Desse grupo de trabalho resultou um relatório relativo à segurança 5G com o objetivo de avaliar as medidas já implementadas em Portugal, tendo posteriormente sido avaliadas as medidas constantes da *EU Toolbox of risk mitigating measures* à luz da avaliação de risco nacional, no âmbito da Cibersegurança das redes 5G (CSSC, 2020).

2.1.1 Redes 5G

A União Europeia define as redes 5G como,

> […] um 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. (Recomendação (UE) 2019/534, 2019)

2.1.2 Cibersegurança

O conceito de Cibersegurança surge, da necessidade de se garantir a segurança no complexo ambiente do ciberespaço, consistindo:

> "[…] no 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, de 05 de junho, 2019)

2.1.3 Segurança das redes e dos sistemas de informação

> […] entende-se a capacidade das redes e dos sistemas de informação para resistir, com um dado nível de confiança, a ações que comprometam a confidencialidade, a integridade, a disponibilidade, a autenticidade e o não repúdio dos dados armazenados, transmitidos ou tratados, ou dos serviços conexos oferecidos por essas redes ou por esses sistemas de informação, ou acessíveis através deles. (CSSC, 2020)

2.1.4 Estratégia Militar

Entende-se por Estratégia Militar a definição sugerida por Couto (2020, p. 247) "como a ciência e arte de desenvolver e utilizar as FFAA com vista à consecução de objetivos fixados pela Política".

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

2.2 Modelo de Análise

O modelo de análise[1] elaborado apresenta os conceitos estruturantes, as dimensões, variáveis e indicadores em estudo que permitiram desenvolver a investigação de forma estruturada, lógica e coerente, culminando com a consecução do OG.

A construção do modelo de análise, teve como sustentação o conteúdo proveniente da revisão de literatura e da entrevista exploratória. Este primeiro momento permitiu tomar contacto com a realidade a investigar e foi determinante para estruturar o modelo de análise nas suas dimensões. As variáveis estão associadas às características das redes 5G e nos domínios de aplicação da segurança destas redes. Por último os indicadores, foram definidos para identificar contributos para a estratégia de segurança nas redes 5G.

[1] Vide Apêndice B – Modelo de Análise.

3. Metodologia e método

Neste capítulo apresenta-se a metodologia aplicada na investigação referente ao seu raciocínio, estratégia, desenho e à recolha e análise de dados. Explica-se qual a técnica de recolha de dados e qual a população de estudo que contribui para as respostas às QD e à QC.

3.1 Metodologia

Para atingir o OG, o método científico escolhido foi o raciocínio indutivo para que através da "observação de factos particulares", recolhidos na UE, OTAN, EUA, Ministério da Defesa Nacional, Gabinete Nacional de Segurança (GNS) e Autoridade Nacional de Comunicações (ANACOM), se efetue uma análise para obter uma generalização que permita propor contributos para as Estratégias de Segurança que as FFAA devem ter em consideração aquando da implantação das redes 5G (Santos & Lima, 2019, p. 20).

A estratégia de investigação seguida foi a qualitativa, sem se preocupar com medições e análises estatísticas (Vilelas, 2009, cit. por Santos & Lima, 2019, p. 27). Procurou-se valorizar o enquadramento teórico e o trabalho de campo junto de especialistas, visando investigar as reais implicações para a implementação das Estratégias de Segurança das redes 5G no domínio Militar.

O desenho de pesquisa utilizado foi o estudo de caso, num horizonte temporal transversal, pois para alcançar o OG foi investigado uma única unidade de estudo, as redes 5G, no que à segurança diz respeito (Santos & Lima, 2019, pp. 36–37).

3.2 Método

3.2.1 Participantes e procedimento

No quadro dos participantes, realizaram-se quatro entrevistas semiestruturadas a entidades que exercem funções de elevada responsabilidade e reconhecidos especialistas[2] nas matérias relacionadas com as redes 5G, nomeadamente nas áreas da Cibersegurança e Ciberdefesa.

O procedimento adotado, a população foi escolhida de forma deliberada (amostra não-probabilística intencional), em que o tamanho dependeu do juízo do investigador (Santos & Lima, 2019, pp. 69-70).

3.2.2 Instrumentos de recolha de dados

Considerando a respetiva abordagem qualitativa e a especificidade do objeto de investigação, optou-se pela utilização de técnicas de recolha de dados baseadas principalmente na análise documental e de conteúdo sobre a temática, que, irá servir para

[2] Vide Apêndice E.

dar respostas às QD, que irão resultar num conhecimento detalhado sobre as vulnerabilidades e potencialidades das redes 5G e sobre as Estratégias de Segurança ao nível nacional e internacional das mesmas.

Posteriormente para complementaridade, realizaram-se entrevistas semiestruturadas (Santos & Lima, 2019, pp. 83-86; Sarmento, 2013, p. 34) constituídas por sete questões. As três primeiras direcionadas para a QD1, as últimas quatro, direcionadas para a QD2. As entrevistas semiestruturadas permitiram validar a adequabilidade e a importância das estratégias de segurança para as redes 5G, servindo de suporte para a resposta à QC.

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).

3.2.3 Técnicas de recolha de dados

A técnica de recolha deu prioridade à recolha e análise de fontes documentais e não documentais, para criar uma base de conhecimento que permitiu elencar as estratégias para segurança das redes 5G. De modo a completar a análise documental, foram realizadas entrevistas semiestruturadas, para aprofundar o objeto de estudo e assim responder às QD com maior assertividade (Quivy & Campenhoudt, 1998, p. 121).

Os dados recolhidos foram tratados qualitativamente relativamente à documentação disponível sobre a temática, conforme as dimensões abordadas e equacionadas no modelo de análise já exposto, segundo três fases organizadas em: pré-análise; a exploração do material; o tratamento dos resultados, a inferência e a interpretação (Bardin, 2004, p. 89).

A análise das entrevistas foi efetuada de acordo com a metodologia proposta por Sarmento (2013, pp. 29–63), pretendendo-se não só “descrever as situações, mas também interpretar o sentido em que foi dito” (Guerra, 2006, p. 69), tendo-se optado por fazer a citação direta, no corpo da presente investigação, das posições e expressões que permitem reforçar os contributos adiantados pela investigação ou aprofundar o tema abordado (França, 2000, p. 113).

4. As características das redes 5G

> *"From my perspective, 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years and, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today to secure tomorrow".* Christopher Krebs, Director, CISA, 2020

O desenvolvimento das redes 5G e de toda a sua tecnologia enquadrante, vem perspetivar que a quantidade de informações trocadas em rede tenha um volume sem precedentes (Figura 7).

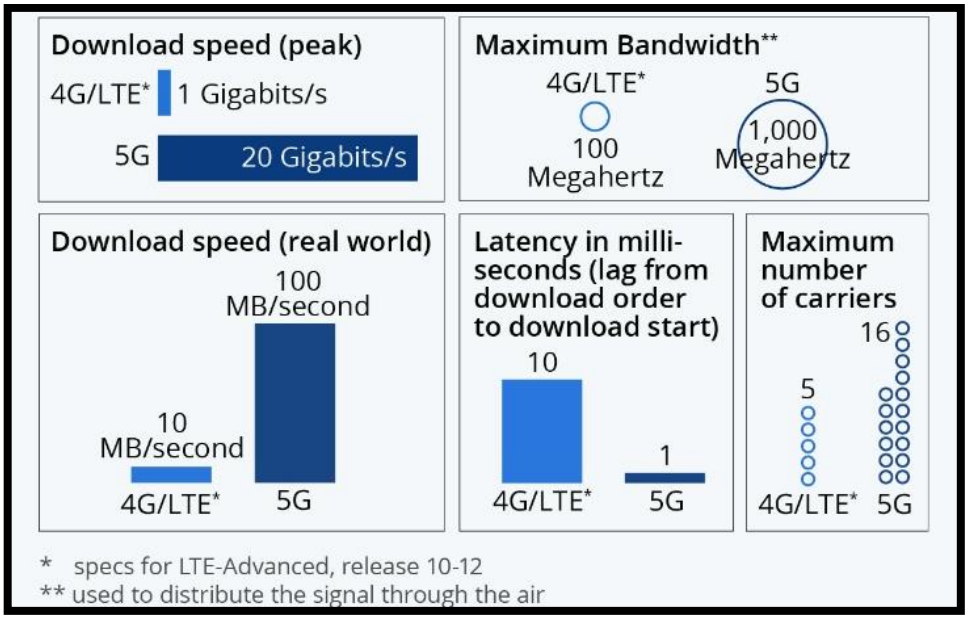


Figura 7 - Comparação das principais especificações de desempenho de redes 4G e 5G
Fonte: Adaptado a partir de Buchholz (2021).

A tecnologia 5G apresenta características que a tornam num poderoso instrumento da transição digital, de desenvolvimento e competitividade das economias, de coesão social e territorial, de melhoria e transmutação do modo de vida, de inovação social e da qualidade dos serviços públicos, com um impacto positivo para a sociedade, como se poderá percecionar pela representação gráfica na Figura 8 (RCM, 2020).

A tecnologia 5G foi traçada para sustentar um enorme número de dispositivos conectados, de natureza diversa, ligados em rede, além de permitir ligações de elevada largura de banda e latências muito reduzidas, suportando nomeadamente aquilo que denominamos de "Internet das Coisas", ou em inglês, *Internet of Things* (IoT) (ANACOM, 2020b), tendo-se verificado entre todos os entrevistados a identificação destas características como benéficas e diferenciadoras das redes antecessoras.

Figura 8 - 5G e o impacto positivo para a sociedade
Fonte: Adaptado a partir de Iberdrola, S.A (2021).

A ANACOM (2020a), salienta como principais características das redes 5G, i) maior velocidade e capacidade da rede **(eMBB)**; ii) massificação da comunicação entre dispositivos **(mMTC)**; iii) Conectividade permanente e mais fiável **(uRLLC)**; e iv) redes mais flexíveis e ajustadas aos serviços, em que as redes 5G permitirão a implementação de várias redes virtuais sobre uma infraestrutura de rede física única (*network slicing*) tornando-a mais flexível e ajustada aos serviços a disponibilizar[3].

Da análise das entrevistas efetuadas sobre esta matéria, A. Marques (entrevista presencial, 18 de abril de 2022) destaca que "A tecnologia 5G pode ser de tal maneira impactante, que ela por si só é um *enabler* de uma série de capacidades […]". Já R. Francisco (entrevista presencial, 18 de abril de 2022) prefere salientar "[…] redução do consumo de energia dos diversos dispositivos […] uma conectividade em tempo real. A baixa latência é claramente importante para as operações militares."

As características eMBB, mMTC e uRLLC estão representadas na Figura 9, assim como algumas das aplicações associadas a essas características.

[3] Vide Apêndice A.

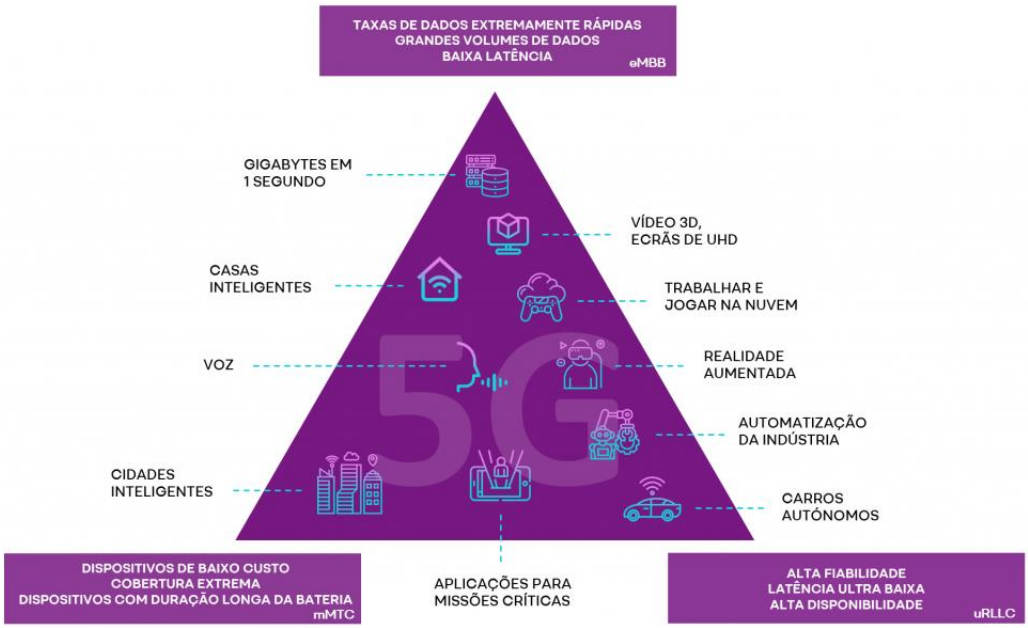


Figura 9 - Características eMBB, mMTC e uRLLC
Fonte: Disponível em ANACOM (2020a).

A sua fiabilidade e a segurança são essenciais para as atividades económicas e societais e, em especial, para o funcionamento dos serviços e infraestruturas consideradas críticas para a dinâmica global da sociedade (Figura 10), afigurando-se assim fundamental salvaguardar a segurança e a integridade das redes e serviços de comunicações eletrónicas (ANACOM, 2020b).

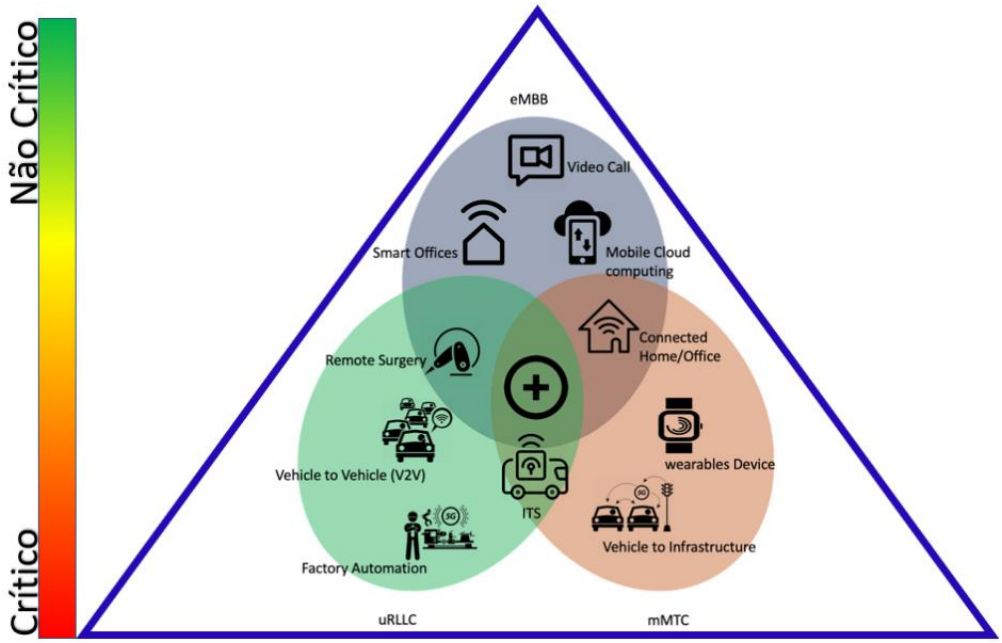


Figura 10 - Diagrama do nível de criticidade do espectro da rede 5G
Fonte: Adaptado a partir de Barzegar (2020).

A dimensão, a regularidade e o impacto dos incidentes de segurança estão a aumentar e compõe uma ameaça relevante para o funcionamento das redes e dos sistemas de informação, tornando-se cada vez mais um alvo de ações prejudiciais deliberadas e com o

objetivo de danificar ou a interromper a operação dos sistemas (Diretiva UE 2016/1148, 2016).

Este tipo de incidentes podem impedir o exercício das atividades económicas, gerar perdas financeiras, minar a confiança dos utilizadores e causar graves prejuízos à economia (Diretiva UE 2016/1148, *op. cit.*).

4.1 Potencialidades de segurança das redes 5G

As redes 5G potenciam melhor segurança através de padrões e *design* (arquitetura) incorporados, bem como uma melhor utilização da encriptação. Podemos também esperar que as capacidades de Inteligência Artificial (IA) sejam implementadas para monitorizar e responder a ameaças[4], e o papel das soluções de software sejam reforçados para permitirem aos operadores de rede, através de corte de rede ou da sua virtualização, isolar as ameaças por forma a não comprometer segurança das redes 5G (Keiser, 2020).

De acordo com Keiser (*op. cit.*) os benefícios das redes 5G para a segurança são:

- **Segurança na Arquitetura**, em que as redes 5G são a primeira rede móvel a ter segurança incorporada desde o início como parte do processo das normas. Vão passar a integrar camadas de segurança do núcleo centralizado para a rede de acesso via rádio e redes virtuais. Esta potencialidade também é considerada pelos entrevistados número 1 e 3.
- **Encriptação melhorada**, as redes 5G utilizarão a Infraestrutura de Chaves Públicas (PKI – *Public Key Infrastructure*) para encriptação com mais facilidade do que os operadores de rede 4G. O PKI refere-se à fundação de princípios de segurança que incluem encriptação, assinaturas, autenticação e certificados. Também utilizará a encriptação *International Mobile Subscriber Identity* (IMSI) para mascarar o identificador de utilizador único de um telemóvel antes de ser enviado para a rede móvel 5G — protegendo contra criminosos virtuais e outros atores maliciosos.
- **Latência Reduzida**, o facto de as redes 5G baixarem a latência também apresenta oportunidades de segurança. As ferramentas de encriptação geralmente reduzem a velocidade de acesso introduzindo um passo adicional, por isso as partes muitas vezes renunciam o uso de encriptação no interesse de manter os sistemas mais rápidos. A redução da latência deve, então, significar o

[4] Anexo A – Os tipos de ameaças

aumento da utilização da encriptação e a melhoria global da segurança. Esta potencialidade foi referida por todos os entrevistados.

O mesmo autor identifica ainda mais três soluções emergentes ao nível da segurança das redes 5G:

– **IA**, é provável que esta potencialidade desempenhe um papel importante na segurança cibernética das redes 5G, à medida que as ameaças se tornam mais complexas e a quantidade de dados supera a capacidade dos humanos de se protegerem contra elas.

– ***Network Slicing,*** é a compartimentação da rede e representa o isolamento dos operadores uns dos outros ao usar uma parte da infraestrutura da rede 5G. Esta compartimentação da rede, ou virtualização da rede, também será proeminente no 5G, fornecendo principalmente às empresas de *software* um papel crucial e com maior preponderância do que nas gerações anteriores de redes móveis (Figura 11).

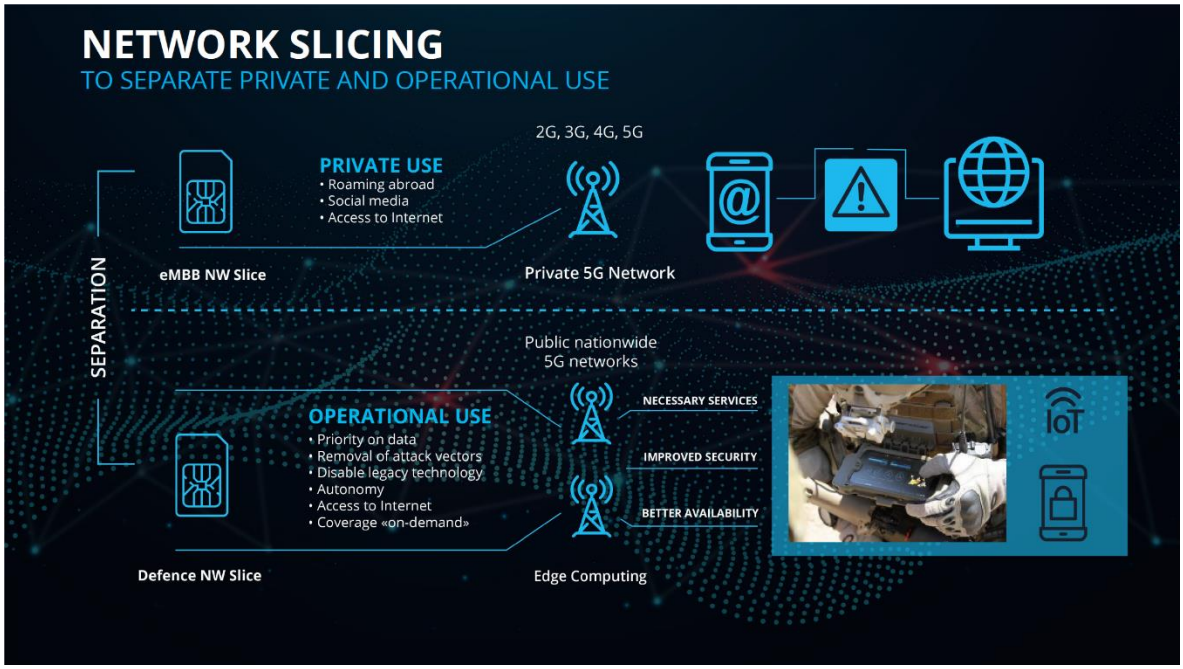


Figura 11 - Exemplo de *Network Slicing*
Fonte: Disponível em Helweg (2022).

– **Protocolo *Diameter***, embora seja uma aspiração, alguns especialistas em segurança esperam que a mudança para o 5G, promova o uso do protocolo *Diameter*, que é um padrão internacional usado para autenticar e autorizar comunicações e a troca de dados entre aplicativos de *software* baseados na Internet em redes móveis e é mais resiliente a ataques. Contém opções mais confiáveis, seguras e flexíveis para a movimentação de dados em redes móveis.

4.2 Vulnerabilidades na segurança 5G

A tecnologia 5G representa também novos e alargados riscos de segurança devido ao aumento exponencial dos dispositivos em rede, consequentemente do tráfego, à acessibilidade das pequenas infraestruturas de telecomunicações e à crescente dependência dos diversos dispositivos e aplicações (Keiser, 2020).

Keiser (*op. cit.*) identifica três vulnerabilidades ao nível da segurança das redes 5G:

- **Volume de dados transferidos**, espera-se que as ameaças à segurança aumentem exponencialmente, uma vez que a tecnologia 5G é amplamente alargada, com o aumento exponencial do número de dispositivos conectados e por consequência o aumento do tráfego de dados. Esta vulnerabilidade é salientada por N. Goes (entrevista por *e-mail*, 01 de maio de 2022) quando refere, "O maior volume de dados transferidos vai complicar esta tarefa, pois vai tornar mais difícil detetar tráfego malicioso, correlacionar eventos […]"
- **IoT e ataque de Distributed Denial of Service (DDoS),** o afluxo de novos dispositivos cria o potencial de *bots* massivos para serem agrupados e lançarem nefastos ciberataques globais. Outro risco é o aumento do potencial para direcionar um aumento disruptivo do tráfego de rede. Os ataques DDoS não são problemas inerentes à tecnologia 5G, uma vez que tais ataques já estão a ocorrer. No entanto, com o aumento da largura de banda e alvos disponíveis (dispositivos IoT), a eficácia dos ataques DDoS podem aumentar com a adoção da tecnologia 5G. Esta característica que se identifica também como uma vulnerabilidade, é referenciada por R. Francisco (*op. cit.*) "Desvantagens será a reduzida fiabilidade dos inúmeros dispositivos conectados […]", e também por N. Goes (*op. cit.*) "O crescimento no número de dispositivos conectados aumenta a potencial "superfície de ataque"[…]".
- **Acessibilidade de Pequenas Células**, em que, o que diferencia as pequenas células 5G da infraestrutura tradicional não é apenas pelo seu tamanho. A tecnologia 5G depende, pelo menos em parte, do espectro de alta frequência que não pode viajar até o espectro de baixa frequência usado para dados 3G/4G/*Long Term Evolution*. Este aspeto vai requer repetidores persistentes para transmitir informações e a acessibilidade de dispositivos de pequenas células levanta suas próprias ameaças.

– **Confiança na conectividade**, pois o aumento de dispositivos conectados inevitavelmente criará maiores dependências nessa infraestrutura, e dispositivos mal protegidos podem estar propensos à exploração. Esta característica é identificada por todos os entrevistados, quando dizem que tem de certificar fornecedores e operadores para trabalharem em conjunto.

4.3 Síntese conclusiva

Destarte, e em resposta à QD 1 "Quais as potencialidades e vulnerabilidades de segurança das redes 5G?", importa salientar que as soluções de segurança atuais já são uma mescla entre a segurança na ponta (dispositivo) e a segurança no núcleo (rede). As redes 5G é a infraestrutura de rede sem fios mais segura construída até à data, embora a grande quantidade de dispositivos recém-conectados traga os seus próprios desafios de segurança, o que não se verificava nas gerações de comunicações móveis anteriores.

Os inúmeros dispositivos IoT são na sua maioria baratos, de fácil conexão à rede de comunicações e com uma estrutura de segurança inexistente ou muito vulnerável, traduzindo-se assim numa ameaça potencial à segurança do utilizador e da própria rede.

Uma boa segurança de rede significa reduzir a superfície de ataque e, em seguida, permitir que as pessoas certas através dos dispositivos certos acedam aos serviços certos numa rede e mantenham tudo e todos os outros fora.

Uma estratégia de segurança bem pensada é indispensável. Somente aqueles que podem identificar e eliminar as vulnerabilidades, falhas de segurança, ambientes maliciosos, sistemas operacionais desatualizados no tempo, são capazes de evitar falhas e manipulações graves no futuro. A melhor proteção possível contra ciberataques é uma solução de segurança incorporada na própria aplicação IoT.

Assim como potencialidades de segurança das redes 5G destaca-se, i) Segurança na Arquitetura; ii) Encriptação melhorada; iii) Latência Reduzida; iv) IA; v) *Network Slicing* e vi) Protocolo *Diameter*.

As vulnerabilidades identificadas para a segurança das redes 5G são: i) volume de dados transferidos; ii) IoT e DDoS; iii) Acessibilidade de Pequenas Células; e iv) Confiança na conectividade.

Considera-se assim respondida a QD 1 e consequentemente atingido o OE 1.

5. As Estratégias de Segurança para as redes 5G

> *"Cyberattacks can be more dangerous to the stability of democracies and economies than guns and tanks".* Jean-Claude Juncker, Munique Security Report, 13/09/2017

Neste capítulo, aborda-se as estratégias de segurança para as redes 5G, desenvolvidas e em implementação pelos países/organizações, nomeadamente, os EUA, a UE, a OTAN e Portugal.

5.1 Estados Unidos da América

A Estratégia Nacional do Governo dos EUA para garantir a implementação e a segurança das redes 5G, passa por garantir a segurança das suas infraestruturas, interna e externamente. As infraestruturas 5G serão um alvo atrativo para criminosos e adversários geopolíticos, devido ao grande volume de dados que transmitem e processam, bem como, pelo apoio que as redes 5G irão fornecer às infraestruturas críticas (Trump, 2020).

De acordo com a avaliação do *Defense Innovation Board*, as Companhias de Comunicações Chinesas e fabricantes destas tecnologias, recebem regularmente subsídios (por exemplo, terreno subsidiado para instalações) e encontram-se bem posicionados como fornecedores globais da tecnologia 5G. A *Huawei* assinou contratos para a construção de infraestrutura 5G em cerca de 30 países, incluindo Islândia, Turquia e Reino Unido (Congressional Research Service [CRS], 2022).

Nesta sequência, e de acordo com o CRS (2022) alguns especialistas receiam que as vulnerabilidades em equipamentos chineses possam ser usadas para conduzir ciberataques ou espionagem militar/industrial. Estes especialistas afirmam que as vulnerabilidades introduzidas advêm de más práticas comerciais de muitas empresas chinesas. No entanto, notam que as vulnerabilidades também podem ser introduzidas intencionalmente para fins maliciosos. A Lei Nacional de Informações da China, de 2017, declara que "qualquer organização e cidadão deve, de acordo com a lei, apoiar, prestar assistência e cooperar no trabalho de informações nacional, e proteger o sigilo de qualquer trabalho de informações nacional que tenham conhecimento" (CRS, 2022). Assim, para diversos analistas, esta lei é interpretada como uma exigência às empresas chinesas para cooperarem com os serviços de informações, incluindo a instalação de *backdoors* para fornecer dados privados ao governo chinês.

Outros analistas argumentam que ter qualquer equipamento chinês na rede poderá colocar potenciais preocupações ao nível da segurança, o que os leva a argumentar que os

EUA devem limitar a partilha de informações com qualquer país que opere equipamentos 5G fornecidos por fabricantes chineses (CRS, *op. cit.*).

Em resposta a estas questões de segurança para as redes 5G, os EUA, em março de 2020, desenharam a Estratégia Nacional para a segurança do 5G. Esta Estratégia cumprirá os objetivos da Estratégia Nacional da Cibersegurança com quatro linhas de esforço (LE) (Figura 12) (Trump, 2020; National Telecommunications and Information Administration [NTIA], 2021):

Figura 12 - Estratégia Nacional dos EUA para a segurança das redes 5G
Fonte: Adaptado a partir de NTIA (2021).

– LE 1: Facilitar o lançamento do 5G a nível nacional:

Estabelece uma nova iniciativa de investigação e desenvolvimento com o objetivo de gerar avançadas capacidades de comunicação e *networking*, por forma a alcançar segurança, resiliência, segurança, privacidade, cobertura de 5G e a um custo acessível. Com este esforço pretende-se alavancar parcerias público-privadas abrangendo o governo, a indústria, o ensino, os laboratórios nacionais e os aliados internacionais. Neste sentido, foram identificadas duas atividades (NTIA, 2021):

- Atividade 1.1 – Investigação, Desenvolvimento e Formação para alcançar e manter a liderança dos EUA no 5G.
- Atividade 1.2 – Identificar os incentivos e opções para alavancar os fornecedores dos parceiros internacionais e domésticos fidedignos.

– LE 2: Avaliar os riscos de Cibersegurança e identificar os princípios fundamentais de segurança das capacidades e infraestruturas 5G:

Orienta-se para identificar e avaliar riscos e vulnerabilidades para infraestruturas 5G, baseando-se nas capacidades existentes na avaliação e gestão do risco da cadeia de abastecimento. Envolverá igualmente o desenvolvimento de critérios para fornecedores de confiança e a aplicação de um modelo de gestão de risco da cadeia de fornecimento de

fornecedores para permitir a tomada de decisão de aquisição conscientes da segurança. Nesta LE foram identificadas cinco atividades (NTIA, 2021):

- Atividade 2.1 – Avaliação de risco de fornecedores nacionais e internacionais.
- Atividade 2.2 – Avaliar ameaças, vulnerabilidades e riscos para infraestruturas 5G.
- Atividade 2.3 – Identificar lacunas de segurança e ameaças aos EUA e às cadeias de abastecimento de parceiros estratégicos.
- Atividade 2.4 – Avaliação da competitividade global e vulnerabilidades (económicas) dos fabricantes/fornecedores dos EUA.
- Atividade 2.5 – Identificar/desenvolver/aplicar princípios de segurança para infraestruturas 5G nos EUA.

– LE 3: Abordar os riscos para a segurança económica e nacional dos EUA durante o desenvolvimento e implantação de infraestruturas 5G em todo o mundo:

Abordar os riscos para a segurança económica e nacional dos EUA durante o desenvolvimento e implementação das infraestruturas 5G em todo o mundo. Como parte deste esforço, os EUA identificarão os incentivos e políticas necessários para colmatar as lacunas de segurança identificadas em estreita coordenação com o setor privado. Uma atividade igualmente importante diz respeito à identificação e avaliação de fornecedores de "alto risco" em infraestruturas 5G dos EUA. Neste contexto, foram também identificadas cinco atividades (NTIA, 2021):

- Atividade 3.1 – Identificar incentivos e políticas para colmatar lacunas de segurança.
- Atividade 3.2 – Identificar incentivos e políticas para garantir a viabilidade económica da base industrial dos EUA.
- Atividade 3.3 – Abordar o risco de ter fornecedores de "alto risco" na infraestrutura 5G dos EUA (olhar para o futuro).
- Atividade 3.4 – Envolvimento do setor privado na segurança 5G.
- Atividade 3.5 – Estabelecer processos de aquisição para facilitar requisitos de informação classificada para a infraestrutura 5G.

– LE 4: Promover o desenvolvimento global responsável e a implantação de infraestruturas 5G seguras e fiáveis:

Aborda a divulgação diplomática e o envolvimento na defesa da adoção e implementação de medidas de segurança 5G que proíbam o uso de fornecedores não fidedignos em todas as partes das redes 5G (NTIA, 2021).

Será necessária uma coordenação estreita e continuada entre o Governo dos EUA, o setor privado, os parceiros académicos e países aliados para garantir a adoção de políticas, normas, orientações e estratégias de aquisição que reforcem a diversidade dos fornecedores 5G e fomentem a concorrência no mercado, promovendo o desenvolvimento e implementação de redes 5G abertas, baseadas em padrões e interoperáveis. Assim, identificaram-se seis atividades (NTIA, 2021):

- Atividade 4.1 – Envolvimento Diplomático para Mitigação de Riscos, Normas e Princípios de Segurança.
- Atividade 4.2 – Prestar Assistência Técnica a Parceiros Internacionais.
- Atividade 4.3 – Opções para mitigar o risco de segurança de equipamentos não fidedignos dos parceiros internacionais.
- Atividade 4.4 – Promover a liderança dos EUA no desenvolvimento de padrões internacionais para as redes 5G, incluindo através do setor privado e do envolvimento internacional.
- Atividade 4.5 – Ambientes de teste conjuntos com parceiros internacionais.
- Atividade 4.6 – Políticas e estratégias para a competitividade do mercado global e diversidade de segurança nas infraestruturas 5G.

No âmbito das implicações para as operações militares, a tecnologia 5G poderá ter uma série de potenciais aplicações militares, nomeadamente para veículos autónomos, Comando e Controlo, logística, manutenção, realidade aumentada e virtual e sistemas *Intelligence, Surveillance e Reconnaissance* (CRS, 2022). Neste context, o *DoD* (2020, p. 2) refere que, *"5G is a critical strategic technology: those nations that master advanced communications technologies and ubiquitous connectivity will have a long-term economic and military advantage."*

O DoD conclui que as redes 5G são importantes porque oferecem um maior desempenho e capacidades adicionais, especialmente para aplicações baseadas em dados e para comunicação máquina-a-máquina. Estas capacidades tornar-se-ão a base para uma nova forma de guerra em rede que reúne sensores e máquinas que irão revolucionar o espaço de batalha e as funções logísticas no apoio às operações (DoD, 2020).

Assim, o DoD (*op. cit.*) delineou uma Estratégia para as redes 5G e um plano de implementação, onde aborda a tecnologia, segurança, normas e políticas. Esta Estratégia está assente em quatro LE, que são:

- Promover o desenvolvimento tecnológico.
- Avaliar, mitigar e operar através de vulnerabilidades 5G.
- Influenciar os padrões e políticas 5G.
- Envolver os parceiros.

Apesar do DoD estar numa fase de testes inicial para a experimentação das aplicações 5G, selecionou 12 instalações militares para efetuar testes e desenvolver esta tecnologia, destacando-se a realidade aumentada e virtual, Comando e controlo de sobrevivência, avaliação da rede 5G para aspetos da segurança, partilha de espectro entre comunicações militares e 5G e por fim conectividade para bases operacionais avançadas e centros de operações táticas (Figura 13) (CRS, 2022).

Figura 13 - Exemplo de aplicações militares em 5G
Fonte: Disponível em DoD (2020).

Contudo, o relatório do Defense Science Board (2019) conclui que pode haver benefícios significativos da utilização da tecnologia 5G na cadeia de fornecimento do DoD, mas as características *cyber, Radio Frequency /Electronic Warfare* e vulnerabilidades virtuais/físicas criam riscos significativos para a missão. Qualquer implementação de redes 5G em infraestruturas do DoD deve ser avaliada em função da criticidade da missão e do risco aceitável.

5.2 União Europeia

Garantir a Cibersegurança das redes 5G é uma questão de importância estratégica para a UE, numa altura em que os ciberataques estão em ascensão, mais sofisticados do que nunca e provenientes de um vasto leque de atores de ameaças, em particular de estados não comunitários ou de outros atores com apoios estatais não declarados. Quanto à segurança das infraestruturas críticas como as redes 5G, a abordagem escolhida, pela primeira vez, foi uma abordagem europeia comum (CE, 2020a).

De salientar que a UE reconheceu que a falta de coordenação nas implementações nacionais das redes 5G iria aumentar o risco de fragmentação nos padrões e na disponibilidade de espectro e que iria "atrasar a criação de massa crítica" para permitir a inovação no mercado único digital (Tirkey, 2020).

Em 2019, o Conselho Europeu apelou a uma abordagem concertada da segurança das redes 5G, aprovando a Recomendação 2019/534 sobre a Cibersegurança das redes 5G. Nesse alinhamento, exorta os Estados-Membros a completarem as avaliações de risco nacional e a reverem as medidas nacionais, assim como, a trabalharem em conjunto numa avaliação coordenada dos riscos e a prepararem uma caixa de ferramentas para eventuais medidas mitigadoras, integrando dessa forma a estratégia digital europeia global (CE, 2019).

A CE (2019) identificou uma série de categorias de riscos de importância estratégica numa perspetiva ilustrada por cenários de risco concretos, que refletem combinações relevantes dos diferentes parâmetros (vulnerabilidades, ameaças e atores de ameaça) no que diz respeito aos diferentes ativos.

O relatório coordenado da avaliação de riscos[5] da UE destaca uma série de aspetos importantes para as redes 5G, nomeadamente as sintetizadas na Tabela 1:

Tabela 1 - Avaliação de risco da UE. Aspetos importantes para as redes 5G

As mudanças tecnológicas introduzidas pela tecnologia 5G irão aumentar a superfície de ataque global e o número de potenciais pontos de entrada para os atacantes.
Estas novas funcionalidades tecnológicas vão dar maior significado à dependência dos operadores de redes móveis em fornecedores terceiros e ao seu papel na cadeia de fornecimento 5G.
Uma grande dependência de um único fornecedor aumenta a exposição e as consequências de uma potencial falha deste fornecedor. Agrava igualmente as potenciais consequências de deficiências ou vulnerabilidades e da sua eventual exploração por parte de atores ameaçados, nomeadamente quando a dependência diz respeito a um fornecedor que apresente um elevado grau de risco.
Algumas das novas utilizações previstas para a tecnologia 5G vão concretizar-se, as redes 5G acabarão por ser uma parte importante da cadeia de fornecimento de muitas aplicações das Tecnologias de Informação e Comunicação críticas, sendo que, como tal, não só os requisitos de confidencialidade e privacidade serão afetados, como também a integridade e disponibilidade dessas redes passará a ser um dos principais problemas de segurança nacional e um grande desafio de segurança do ponto de vista da UE.

Fonte: Adaptado a partir de CE (2020b).

Estes desafios criam um novo paradigma de segurança, tornando necessário reavaliar o atual quadro de política e segurança aplicável ao sector 5G e ao seu ecossistema, tornando essencial que os Estados-Membros tomem as medidas mitigadoras necessárias (CE, 2020b).

Para fazer face aos riscos identificados de forma eficaz e reforçar a segurança e a resiliência das redes 5G, a UE criou um conjunto de medidas-chave de mitigação que podem ser aplicadas a nível nacional e europeu (CE, 2020b), conforme (Figura 14):

[5] Vide Anexo A.

Figura 14 - Medidas-Chave de mitigação de risco da UE
Fonte: Adaptado a partir de CE (2020b).

Neste contexto, o conjunto de instrumentos da UE em matéria de Cibersegurança das redes 5G, contém três tipos de medidas não vinculativas (estratégicas, técnicas e de apoio)[6] como esquematizado na Figura 15.

Figura 15 - Medidas de mitigação de riscos de Cibersegurança nas redes 5G
Fonte: Disponível em European Commission (2021).

A UE, dentro do quadro das Medidas Estratégicas (ME) identificou oito e a serem executadas por vários intervenientes, conforme sintetizado no Quadro 2.

[6] Vide Anexo B.

Quadro 2 - ME da UE para as redes 5G e os seus intervenientes

Medidas	Intervenientes pertinentes				
	Autoridades dos Estados-Membros	Operadores de redes móveis	Comissão Europeia	ENISA	Partes interessadas (incluindo fornecedores)
Medidas estratégicas (ME)					
ME01 – Reforçar o papel das autoridades nacionais	✓	✓			
ME02 – Realizar auditorias aos operadores e exigir informações	✓	✓			
ME03 – Avaliar o perfil de risco dos fornecedores e aplicar restrições aos fornecedores considerados de risco elevado (incluindo as exclusões necessárias para atenuar eficazmente os riscos) no que respeita a ativos essenciais	✓	✓			
ME04 – Controlar a utilização de prestadores de serviços geridos e do apoio de terceira linha dos fornecedores de equipamento	✓	✓			
ME05 – Garantir a diversidade de fornecedores de cada operador de rede móvel através de estratégias de múltiplos fornecedores adequadas	✓	✓			
ME06 – Reforçar a resiliência a nível nacional	✓	✓			
ME07 – Identificar os ativos essenciais e promover um ecossistema 5G diversificado e sustentável na UE	✓		✓		
ME08 – Manter e desenvolver a diversidade e as capacidades da UE nas futuras tecnologias de rede	✓		✓		✓

Fonte: Disponível em TCE (2022).

Assim, os Estados-Membros devem dispor de medidas e de poderes para atenuar os riscos, designadamente (Figura 16):

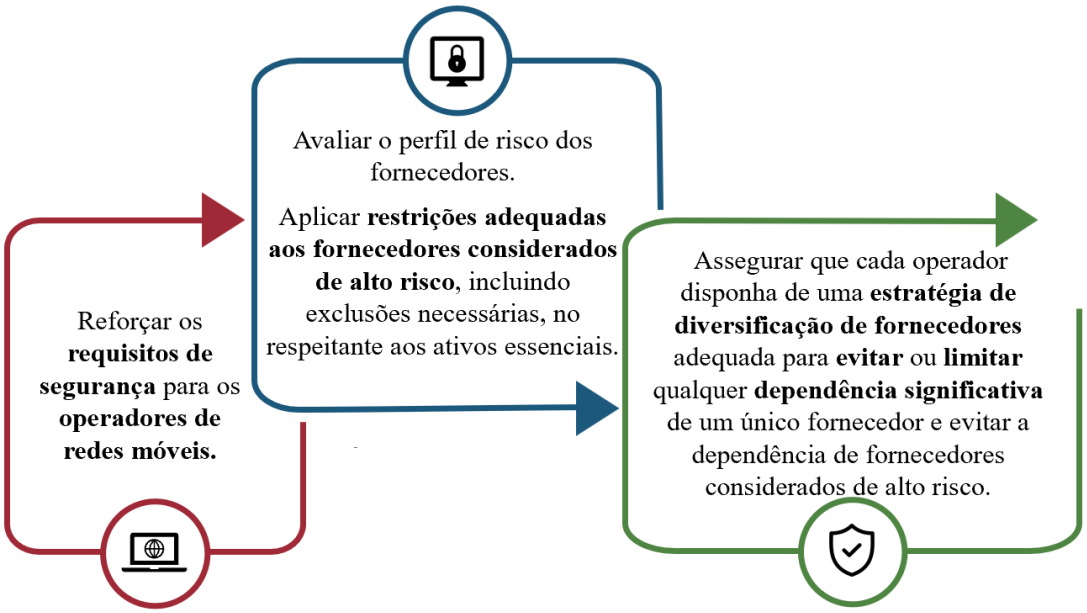


Figura 16 - Medidas e poderes dos Estados-Membros da UE
Fonte: Adaptado a partir de European Commission (2021).

Já a Comissão Europeia, juntamente com os Estados-Membros, deve tomar medidas para: i) manter uma cadeia de abastecimento 5G diversificada e sustentável, a fim de evitar a dependência a longo prazo; e ii) facilitar a coordenação entre os Estados-Membros no que diz respeito à normalização, a fim de alcançar objetivos de segurança específicos, e desenvolver sistemas de certificação pertinentes ao nível da UE (European Commission, 2021) .

5.3 Organização do Tratado do Atlântico Norte

O desenvolvimento, maturação e implementação da rede 5G está em curso a nível global e a OTAN começou a analisar o que isso significará para a Aliança (NATO Communications and Information Agency [NCIA], 2021), nomeadamente quando os

representantes dos países como o Canadá, França, Alemanha, Holanda, Suécia, EUA e Reino Unido participaram numa Equipa Exploratória de investigação nacional com interesse em pesquisar os desafios das comunicações 5G na vertente da Guerra Eletrónica. Esta equipa exploratória criou um Grupo de Tarefas de Investigação para acompanhar os desenvolvimentos e investigar o impacto das principais tecnologias 5G nos sistemas de Cibersegurança da OTAN (Keiser, 2020).

Para a OTAN em particular, será de importância crucial explorar estas novas oportunidades tecnológicas de comando, controlo e comunicações, bem como para outros fins, pois, sem comunicações 5G, será difícil explorar totalmente os *big data*, IA e computação em nuvem no campo de batalha (Gilli & Bechis, 2020). Consideram assim que será importante manter uma vantagem tecnológica para que os decisores da aliança se mantenham informados e tomem as decisões políticas e estratégicas certas (NCIA, 2021).

Atualmente, os especialistas da NCIA estão a analisar o potencial da tecnologia para uso militar e quais os desafios técnicos, conceptuais e arquitetónicos que devem ser abordados para a permitir. No entanto, concluem que, por exemplo, o 5G é demasiado complexo ou vulnerável para ser usado em alguns cenários militares (NCIA, 2021).

A OTAN, sendo uma aliança militar de democracias, não foi concebida para lidar com a política comercial, a liderança industrial e a concorrência no mercado no mundo da alta tecnologia. No entanto, no contexto atual e neste domínio em concreto, a Aliança deve ter o dom de decidir a implementação das estratégias ou políticas a seguir (Gilli, 2020).

Ainda de acordo com Gilli (2020), a Cibersegurança e a Ciberdefesa desempenham um papel crescente no esforço coletivo de defesa da OTAN e trabalhar em conjunto nestas questões não é apenas da maior importância para a Aliança, como também é uma das suas principais responsabilidades.

Devido à partilha de valores comuns e às complementaridades entre as duas organizações, a UE e a OTAN têm um forte interesse em trabalhar em conjunto na implementação das redes 5G. A UE promove a investigação e os investimentos, estabelece parâmetros comuns na atribuição do espectro entre os seus membros, promove a concorrência interna e monitoriza o cumprimento das leis e regulamentos existentes (da privacidade aos direitos fundamentais). Por seu lado, a OTAN pode continuar a trabalhar na Cibersegurança e na Ciberdefesa (Gilli, 2020).

Assim, no seguimento do referido, poder-se-á afirmar que a OTAN não tem uma estratégia definida no que concerne à segurança das redes 5G, tendo sim, recomendações para os seus membros e aliados, em que o Secretário-geral da Aliança deverá considerar as

seguintes ações para catalisar o desenvolvimento de uma estratégia 5G de uma aliança mais robusta e cumprir a Declaração da Cimeira de Londres de 2019 (DaSilva, et al., 2020; Jones, et al., 2020; Pernik, et al., 2021):

- **Segurança da cadeia de abastecimento**, em que a OTAN deverá estabelecer critérios de fiabilidade para os fabricantes de equipamentos 5G de alto risco e prestadores de serviços associados, tendo em vista a mitigação de intenções maliciosas (como a inserção de vulnerabilidades, interceção ou perturbações do fornecimento). A mitigação dos riscos da cadeia de abastecimento requer uma estreita parceria público-privada entre a Aliança, os governos nacionais e a indústria.
- **Segurança da Rede**, os Estados-Membros devem determinar conjuntamente os níveis adequados de segurança da rede e os complementos aos controlos de segurança comercial das redes de nível militar e dos serviços associados. Deve determinar critérios comuns para a certificação de produtos e serviços. Devem ser incentivadas mais investigações no que diz respeito aos desafios técnicos de segurança da rede, incluindo sobre a aplicação dos princípios de Segurança Zero Trust e respetivas ferramentas do setor, encriptação de ponta a ponta para comunicações militares através de redes 5G, autonomia e automatização para monitorização e deteção, e análise e segurança ativadas pela IA.
- **Políticas e Normas**, em que os Estados-Membros devem harmonizar estratégias e políticas nacionais para assegurar redes comerciais e militares 5G. A Aliança deverá considerar o desenvolvimento de uma estratégia para o desenvolvimento de casos militares para a sua utilização 5G, abordando a interoperabilidade dos equipamentos, serviços e o espectro de frequências de rádio. As estratégias deverão identificar o tipo de casos de uso militar implantados em redes comerciais e cenários de implantação de redes 5G privadas (militares/defesa/OTAN). Deve considerar a forma como as atuais normas *3rd Generation Partnership Project* (3GPP) abordam os requisitos de segurança dos militares. Os países da OTAN devem certificar os produtos, processos e serviços associados à tecnologia 5G de acordo com critérios acordados conjuntamente, tendo em conta os sistemas de certificação existentes e avaliando o seu valor e suficiência. Devem assegurar a interoperabilidade das redes nacionais comerciais e militares 5G. Devem considerar o desenvolvimento de normas à

escala da Aliança para redes 5G resistentes, fiáveis, disponíveis e seguras em redes civis e militares e considerar normas militares para redes militares.

- **Investigação, Formação e Treino**, em que a investigação deverá ser aprofundada de modo a explorar as oportunidades que as tecnologias 5G podem proporcionar para melhorar a defesa e dissuasão dos Aliados e os riscos de segurança inerentes a estas redes. Também a sensibilização para os riscos associados tanto às redes públicas (comerciais) como às redes militares 5G deverá continuar a visar públicos específicos (como o público em geral, os parlamentos, os decisores governamentais e industriais e os oficiais militares). As nações da OTAN também devem providenciar estudos para determinar que competências são necessárias nas FFAA e na OTAN para permitir o destacamento de redes militares 5G e garantir a sua segurança.
- **Parcerias**, neste domínio, os países da OTAN devem reforçar a informação atempadamente e a partilha de boas práticas, incluindo avaliação de riscos, relativas às redes 5G comerciais e militares. Para o efeito, as nações devem:
  - Estabelecer pontos de contacto e criar redes de peritos nas organizações governamentais e das FFAA. Devem ser criadas redes de peritos semelhantes com a participação de universidades, instituições de investigação e indústria.
  - Os governos e as FFAA devem ter visibilidade suficiente dos processos, procedimentos e práticas de segurança da cadeia de abastecimento e da rede, dos procedimentos e práticas utilizados pelos fabricantes de tecnologia 5G e fornecedores de serviços associados.
  - As FFAA devem estabelecer parcerias com prestadores de serviços comerciais e fabricantes de equipamentos que lhes permitam avaliar os riscos e assegurar a integridade, segurança, resiliência, privacidade e qualidade dos produtos, sistemas e serviços adquiridos ao longo do seu ciclo de vida.
  - Os prestadores de serviços de rede 5G devem ser encorajados a cooperar com as FFAA, devendo partilhar informações confidenciais sobre questões como as suas avaliações de risco 5G, políticas de segurança e controlos e certificação dos seus componentes de rede.

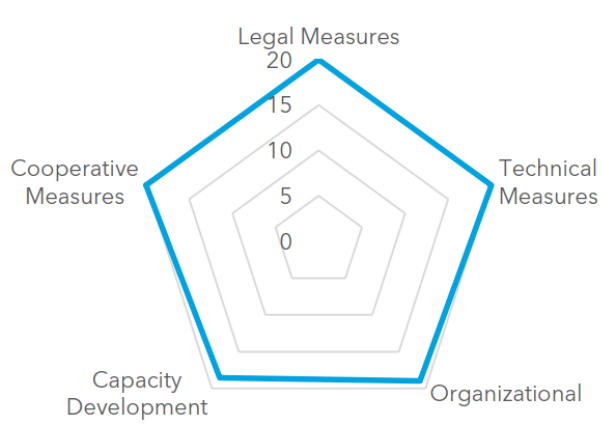
- A OTAN e a UE deverão criar um organismo de consulta informal regular para avaliar em conjunto os riscos e desenvolver medidas de mitigação em dimensões estratégicas, técnicas e de apoio, com base na experiência da UE com avaliações de riscos e na *Toolbox*.

5.4 Portugal

Tendo em consideração as recomendações da UE e da OTAN, cabe ao Governo decidir os objetivos estratégicos para a implementação das redes 5G em Portugal. Este reconhece ser de capital importância que seja garantida a segurança das redes 5G devido ao previsível aumento substancial da dependência da sociedade em geral e de muitos serviços críticos do funcionamento e da segurança destas redes (RCM n.º 7-A/2020, 2020).

O relatório de Índice de Cibersegurança Global mostra que Portugal se encontra bem cotado devido ao facto de ter promulgado novas leis e regulamentos de Cibersegurança, onde aborda áreas como, privacidade, acesso não autorizado e segurança online. Inclusive tem desenvolvido uma estratégia nacional de Cibersegurança que orienta a sua postura global da mesma (Figura 17) (ITU, 2020).

Portugal



Development Level:
Developed Country

Area(s) of Relative Strength
Legal, Technical, Cooperative Measures

Area(s) of Potential Growth
Organizational, Capacity Development Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
97.32	20.00	20.00	18.98	18.34	20.00

Figura 17 - Índice de Cibersegurança Global – Portugal
Fonte: Disponível em ITU (2020, p. 123).

Na Figura 18, descrevem-se os cinco pilares de compromisso para a Cibersegurança que servem de análise a esta avaliação.

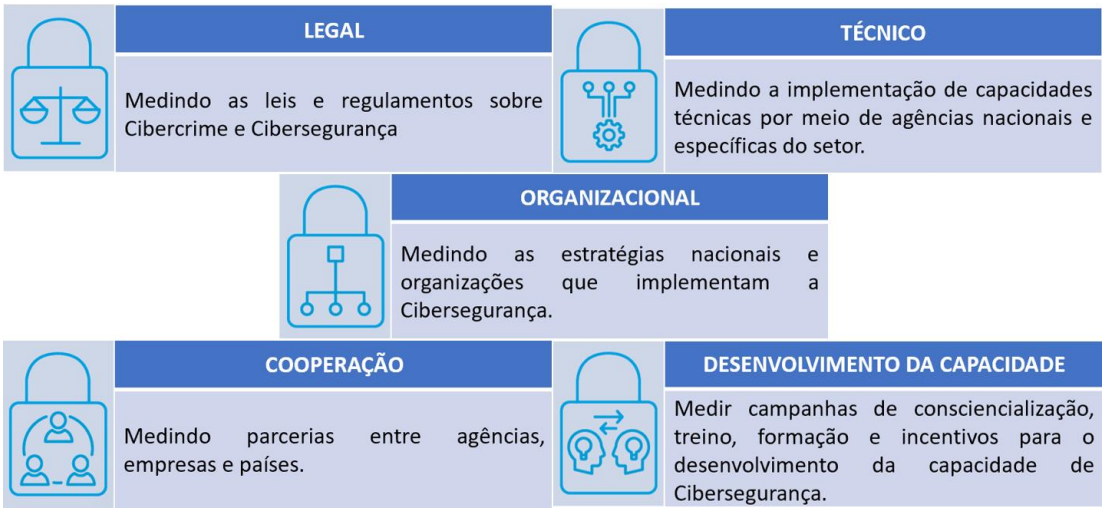


Figura 18 - Compromissos de Cibersegurança em cinco pilares
Fonte: Adaptado a partir de ITU (2020, p. vii).

No entanto, num relatório de avaliação de risco no âmbito da Cibersegurança, Portugal por dispor de infraestruturas *Huawei*, foi avaliado com uma situação que poderá degradar as relações EUA-Portugal (Quadro 3).

Quadro 3 - Avaliação de risco no âmbito da Cibersegurança – Portugal

Region/ Country	Statement made by	Statement
Portugal	Ajit Varadaraj Pai, Chairman of the US Federal Communication Commission	He met representatives of the Portuguese government for talks on the security of the 5G network in Portugal. US representatives reiterated that the security of critical communication infrastructures was paramount and that Huawei's presence in Portugal could ultimately damage US-Portugal relations.

Fonte: Adaptado a partir de Tirkey (2020, p. 39).

Na sequência da Recomendação (UE) n.º 534/2019, da CE, relativa à Cibersegurança das redes 5G promoveu a realização de uma avaliação de risco nacional, participando também na avaliação de risco ao nível da UE. Com base nas avaliações efetuadas, identificou-se um conjunto de medidas estratégicas, técnicas e ações[7] comuns a adotar para corrigir e mitigar os riscos de segurança detetados (RCM n.º 7-A/2020, *op. cit.*).

As avaliações destas medidas estratégicas tiveram por base as seguintes vulnerabilidades identificadas (Figura 19):

[7] Vide Anexo B.

Figura 19 - Vulnerabilidades de âmbito 5G identificadas por Portugal
Fonte: Adaptado a partir de CSSC (2020, pp. 23-24).

Neste seguimento e tendo por base as oito medidas estratégicas da UE, Portugal desenvolveu oito ações principais por forma a implementar as medidas de segurança adequadas à atenuação dos riscos em matéria de Cibersegurança, sendo elas (CSSC, 2020, p.36):

- Avaliação contínua de Risco Nacional da Cibersegurança das redes e comunicações eletrónicas.
- Criação de um mecanismo de autorização prévia para a utilização de equipamentos no âmbito das redes 5G.
- Criação do Sistema Nacional de Certificação em Cibersegurança.
- Reforço da segurança e fiabilidade das infraestruturas nacionais de comunicações eletrónicas.
- Implementação da legislação complementar ao regime jurídico de segurança do ciberespaço.
- Reforço dos requisitos de segurança das Redes e Serviços de Comunicações Eletrónicas.
- Reforço das obrigações das empresas e da supervisão.
- Reforço do Regime de Segurança e Emergência de Comunicações.

5.5 Síntese conclusiva

No seguimento do referido e respondendo à QD 2 "Quais as Estratégias de Segurança para redes 5G?", resumem-se no Quadro 4.

Quadro 4 - Quadro resumo das Estratégias de Segurança para as redes 5G

País / Organização	Estratégias de Segurança para redes 5G
EUA	Governo: – Facilitar o lançamento do 5G a nível nacional. – Avaliar os riscos de Cibersegurança e identificar os princípios fundamentais de segurança das capacidades e infraestruturas 5G. – Abordar os riscos para a segurança económica e nacional dos EUA durante o desenvolvimento e implantação de infraestruturas 5G em todo o mundo. – Promover o desenvolvimento global responsável e a implantação de infraestruturas 5G seguras e fiáveis. DoD: – Promover o desenvolvimento tecnológico. – Avaliar, mitigar e operar através de vulnerabilidades 5G. – Influenciar os padrões e políticas 5G. – Envolver os parceiros.
UE	– Reforçar o papel das autoridades nacionais. – Realizar auditorias aos operadores e exigir informações. – Avaliar o perfil de risco dos fornecedores e aplicar restrições aos fornecedores considerados de risco elevado (incluindo as exclusões necessárias para atenuar eficazmente os riscos) no que respeita a ativos essenciais. – Controlar a utilização de prestadores de serviços geridos e do apoio de terceira linha dos fornecedores de equipamento. – Garantir a diversidade de fornecedores de cada operador de rede móvel através de estratégias de múltiplos fornecedores adequadas. – Reforçar a resiliência a nível nacional. – Identificar os ativos essenciais e promover um ecossistema 5G diversificado e sustentável na EU. – Manter e desenvolver a diversidade e as capacidades da UE nas futuras tecnologias de rede.
OTAN	– Segurança da cadeia de abastecimento. – Segurança da Rede. – Políticas e Normas. – Investigação, Formação e Treino. – Parcerias.
Portugal	– Avaliação contínua de Risco Nacional da Cibersegurança das redes e comunicações eletrónicas. – Criação de um mecanismo de autorização prévia para a utilização de equipamentos no âmbito das redes 5G. – Criação do Sistema Nacional de Certificação em Cibersegurança. – Reforço da segurança e fiabilidade das infraestruturas nacionais de comunicações eletrónicas. – Implementação da legislação complementar ao regime jurídico de segurança do ciberespaço. – Reforço dos requisitos de segurança das Redes e Serviços de Comunicações Eletrónicas. – Reforço das obrigações das empresas e da supervisão. – Reforço do Regime de Segurança e Emergência de Comunicações.

Considera-se assim respondida a QD 2 e consequentemente atingido o OE 2.

6. Contributos para a Estratégia de Segurança nas Redes 5G nas FFAA

Até ao final do ano de 2023, as instalações militares prioritárias devem estar dotadas com redes 5G, conforme definido pelo membro do Governo responsável pela área da defesa nacional (RCM n.º 7-A/2020, 2020).

Assim, para assegurar a adaptação das FFAA às redes 5G, os contributos para a sua Estratégia Segurança foram deduzidos através de uma análise SWOT[8] - *Strengths, Weaknesses, Opportunities, Threats* (traduzidas, respetivamente, para pontos fortes, pontos fracos, oportunidades e ameaças) para responder à QC, correlacionando os pontos fortes e os pontos fracos existentes no ambiente interno da segurança das redes 5G, com as oportunidades e as ameaças, encontradas no ambiente externo para a segurança das redes 5G.

Contudo, as redes 5G apresentam muitos fatores de ambiente interno e externo com impacto nesta estratégia em análise. Todavia, por uma questão de sistematização, apenas são elencados no máximo cinco fatores em cada quadrante. Nessa ótica, recorreu-se às análises de situação constantes nas respostas às QD1 e QD2.

Como resultado da análise SWOT desenvolvida, procurou-se que os contributos[9] identificados para uma Estratégia de Segurança nas redes 5G fossem organizados e apresentados 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 (Quadro 5), tendo em consideração os pontos fortes aproveitando ao máximo as oportunidades e minimizar os efeitos negativos dos pontos fracos para mitigar as ameaças.

Quadro 5 - Contributos para a Estratégia de Segurança das redes 5G

VETOR CAPACIDADE	Contributos
DOUTRINA	C1 - CRIAR a capacidade 5G nas FFAA
ORGANIZAÇÃO	C2 - CONSTITUIR uma estrutura de Ciberdefesa especializada em 5G
TREINO	C3 - POTENCIAR a Investigação, desenvolvimento e inovação em Ciberdefesa e a especialização em segurança das redes 5G
MATERIAL	C4 - PROMOVER a implementação sustentada das redes 5G nos diversos domínios das FFAA
LIDERANÇA	C5 - ENVOLVER as chefias no processo de implantação das redes 5G nas FFAA
PESSOAL	C6 - ADEQUAR os recursos humanos às futuras necessidades, ligadas à implementação e manutenção da resiliência das redes 5G
INFRAESTRUTURAS	C7 - APROFUNDAR a cooperação com os fornecedores certificados
INTEROPERABILIDADE	C8 - REFORÇAR a interoperabilidade das redes 5G nas FFAA e com os países aliados

[8] Vide Apêndice E.
[9] "C" - Abreviado no Quadro 5 como codificação de contributos.

Da análise das entrevistas, estes contributos também são corroborados pelos entrevistados. De acordo com R. Francisco (*op. cit.*), este afirma que "a edificação desta Tecnologia 5G, como uma capacidade e que desta forma permita exponenciar a segurança nas redes 5G." e salientada também por A. Marques (*op. cit.*) aquando da resposta às Q1 e Q2.

No vetor Organizacional, A. Marques (*op. cit.*) destaca a importância de "haver uma estrutura que faça a *Governance* da sua implementação nos Ramos das FFAA […] tem que ter uma nova organização." Já para o vetor Treino, a opinião dos entrevistados é unânime, ao referirem que as FFAA têm uma grande cultura e experiência na área da formação e que é vital formar os seus militares e civis com o *know-how* sobre esta matéria que é recente, que está em constante desenvolvimento, onde é preciso saber implementá-la, mantê-la, usá-la e evoluí-la. Neste sentido R. Francisco (*op.cit.*) diz "Outra estratégia é apostar na formação das pessoas, em pessoas qualificadas, na sensibilização desde os operadores às chefias, que vai permitir mitigar estas vulnerabilidades de segurança.".

Ao nível do vetor Material, N. Goes (*op. cit.*) ressalva que "A sua utilização poderá ser feita em ambientes restritos, com âmbitos bem definidos […]". Já J. Vaz (entrevista via Teams, 22 de abril de 2022) refere que "as redes 5G não devem ser já implementadas nas FFAA, porque é uma tecnologia que tem de ganhar maturidade, especialmente as tecnologias comerciais". Para o vetor Liderança, é o entrevistado R. Francisco (*op.cit.*) que afirma que é preciso envolver as chefias, "[…]na sensibilização desde os operadores às chefias […]".

No vetor Pessoal, A. Marques (*op. cit.*), infere que deve "haver pessoas que conheçam o que é o 5G, que saibam repará-la, mantê-la, usá-la, que definam cenários para a sua utilização operacional, que pensem se devem ou não haver infraestruturas próprias nas FFAA para haver redes locais de 5G." Nas Infraestruturas, todos os entrevistados indicam que deve existir cooperação com os fornecedores, países aliados e organizações, por forma a garantir uma estrutura 5G segura e resiliente. N. Goes (*op. cit.*) refere que "A relação de confiança entre todos deve ser muito alta, extremamente coordenada e governada."

Por fim, e não menos importante, a Interoperabilidade é vista por todos como um dos pontos fulcrais para garantir estas sinergias na implementação do 5G e das suas medidas de segurança. Nomeadamente R. Francisco destaca que uma "Outra oportunidade é o incremento da interoperabilidade entre parceiros e forças."

Considera-se que a sistematização apresentada dos contributos dá resposta à QC e, paulatinamente, materializa o cumprimento do OG proposto.

7. Conclusões

> *Next generation telecommunications will affect every aspect of society, from transportation to healthcare, as well as our military operations.* NATO Secretary General Jens Stoltenberg – Defence Ministers Meeting, Brussels, 25 October 2019

As redes 5G formarão a espinha dorsal da economia digital, em que os avanços de hoje prometem uma tecnologia transformadora, fundamental para permitir a próxima revolução digital. O 5G proporcionará benefícios maciços para o futuro desenvolvimento económico e competitividade nacional, incluindo algumas aplicações militares. As redes 5G são muito mais do que simplesmente uma interação mais rápida da tecnologia 4G. Os seus benefícios incluem a alta velocidade, baixa latência e alta produção, que permitem fluxos de dados a uma velocidade e volume muito maiores do que as redes 4G de hoje.

Espera-se que esta tecnologia potencie significativamente todos os sectores da sociedade e, em particular, os que são críticos para a segurança nacional, como os cuidados de saúde, os transportes e a energia, incluindo os governos e os seus cidadãos. Infelizmente, com os muitos benefícios gerados também surgem vulnerabilidades de segurança incalculáveis. Nomeadamente, a crescente dependência das sociedades nestas tecnologias poderá ter graves implicações em termos de segurança nacional e social se as redes 5G e os dados em que confiam forem perturbados ou comprometidos.

Os dados são por isso, uma das mercadorias mais valiosas do nosso tempo, usadas para fins civis, comerciais e militares pelos governos e pelo sector privado em todo o mundo.

Isto reforça a importância das infraestruturas das redes 5G serem seguras, resilientes e íntegras, no que diz respeito à segurança nacional e consequentemente de interesse estratégico.

Estes desenvolvimentos invocam grandes riscos para importantes interesses públicos e têm implicações na segurança nacional. Na atualidade, os atores mal-intencionados operam no ciberespaço, com a intenção de minar a coesão das sociedades e paralisar o bom funcionamento dos Estados ou das empresas. Nas sociedades digitalizadas, isto pode ter consequências graves, pelo que é vital implementar medidas de segurança adequadas e mecanismos baseados no risco para ajudar a garantir a confidencialidade, integridade, a disponibilidade de dados para reduzir o risco de corrupção de dados, aumentar a confiança na informação e garantir as proteções de privacidade adequadas.

A segurança nas redes 5G não pode ser considerada uma questão puramente técnica. Uma infraestrutura segura e resiliente requer estratégias nacionais adequadas, políticas sólidas, um quadro legal abrangente, pessoal dedicado, formado e instruído de forma adequada.

O procedimento metodológico escolhido, seguiu o raciocínio indutivo utilizando uma estratégia qualitativa e um desenho estudo de caso num horizonte temporal transversal, pois para alcançar o OG foram analisadas duas Organizações Internacionais, um país de referência nesta matéria e Portugal.

A técnica de recolha de dados assentou na análise de fontes documentais e não documentais, que possibilitou criar uma base de conhecimento que sustentou os contributos para a Estratégia de Segurança nas redes 5G. Por forma a complementar a análise às fontes bibliográficas, realizaram-se entrevistas semiestruturadas a especialistas nacionais na área de Cibersegurança e Ciberdefesa, permitindo um tipo de investigação para verificação e aprofundamento do objeto em estudo.

Desta análise foi possível apresentar as potencialidades de segurança das redes 5G nomeadamente, i) Segurança na Arquitetura; ii) Encriptação melhorada; iii) Latência Reduzida; iv) IA; v) *Network Slicing*; e vi) Protocolo *Diameter*, e as suas vulnerabilidades como, i) volume de dados transferidos; ii) IoT e DDoS; iii) Acessibilidade de Pequenas Células; e iv) Confiança na conectividade.

Tendo por foco a análise às estratégias para a implementação das redes 5G no geral e segurança das mesmas em particular, de uma forma global as estratégias mais relevantes para a segurança das redes 5G são: i) Avaliação contínua de Risco Nacional da Cibersegurança das redes e comunicações eletrónicas; ii) Criação de um mecanismo de autorização prévia para a utilização de equipamentos no âmbito das redes 5G; iii) Criação do Sistema Nacional de Certificação em Cibersegurança; iv) Reforço da segurança e fiabilidade das infraestruturas nacionais de comunicações eletrónicas; v) Implementação da legislação complementar ao regime jurídico de segurança do ciberespaço; vi) Reforço dos requisitos de segurança das Redes e Serviços de Comunicações Eletrónicas; vii) Reforço das obrigações das empresas e da supervisão; viii) Reforço do Regime de Segurança e Emergência de Comunicações; ix) Facilitar o lançamento do 5G a nível nacional; x) Envolver os parceiros.

Como corolário da investigação e em resposta à QC (Que contributos podem ser integrados na Estratégia de Segurança nas redes 5G no âmbito das FFAA Portuguesas?) foi desenhada uma matriz SWOT, recorrendo às oportunidades, às ameaças, aos pontos fortes e

aos pontos fracos para formular os quatro grupos de contributos a ter em consideração para a estratégia de segurança das redes 5G, nomeadamente, o grupo do crescimento, da dinamização, da otimização e da defesa.

Com o resultado da análise SWOT desenvolvida, procurou-se que estes contributos fossem organizados e apresentados de acordo com os vetores que constituem uma capacidade militar, conforme a seguir se indicam:

- Doutrina: CRIAR a capacidade 5G nas FFAA;
- Organização: CONSTITUIR uma estrutura de Ciberdefesa especializada em 5G;
- Treino: POTENCIAR a Investigação, Desenvolvimento e Inovação em Ciberdefesa e a especialização em segurança das redes 5G;
- Material: PROMOVER a implementação sustentada das redes 5G nos diversos domínios das FFAA;
- Liderança: ENVOLVER as chefias no processo de implantação das redes 5G nas FFAA;
- Pessoal: ADEQUAR os recursos humanos às futuras necessidades, ligadas à implementação e manutenção da resiliência das redes 5G;
- Infraestruturas: APROFUNDAR a cooperação com os fornecedores certificados;
- Interoperabilidade: REFORÇAR a interoperabilidade das redes 5G nas FFAA e com os países aliados.

Assim, como **principais contributos para o conhecimento** uma perspetiva detalhada das potencialidades e vulnerabilidades da segurança das redes 5G. Uma perspetiva global das estratégias desenvolvidas pelos EUA, UE, OTAN e Portugal para a implementação das redes 5G com enfoque na sua segurança. Por fim, os contributos que podem ser integrados para uma futura estratégia a definir pelas FFAA para a implementação das redes 5G na organização, de forma a exponenciar o rendimento destas redes, mitigando os riscos associados, e garantir confidencialidade, a integridade, a disponibilidade, a autenticidade, a resiliência e a privacidade destas redes 5G.

Como possível **limitação da investigação** naturalmente pelo objeto de estudo ser muito recente e da não obtenção dos contributos via entrevista da estrutura do EMGFA, que não permitiu incluir uma análise da visão estratégica prevista a que, a esta matéria diz respeito.

No que concerne a **estudos futuros**, sugere-se uma investigação detalhada dos programas de implementação das redes 5G em desenvolvimento nas diversas FFAA de países aliados, como os EUA, Noruega, Estónia, Polónia e Lituânia.

A recomendação de ordem prática que decorre deste trabalho, prende-se com a necessidade de se constituir equipas e parcerias militares e civis de modo a adquirir um maior conhecimento das redes 5G, acompanhar o desenvolvimento e a aplicabilidade desta tecnologia a fim de criar condições de estruturar uma estratégia de implementação desta capacidade (redes 5G) nas FFAA. Será um passo importante, na medida em que permitirá às FFAA acompanhar o desenvolvimento tecnológico, modernizarem-se e serem interoperáveis com as forças congéneres.

Referências bibliográficas

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

Ahmad, I., Kumar, T., Liyanage, M., Okwuibe, J., Ylianttila, M., & Gurtov, A. (2017). 5G Security: Analysis of Threats and Solutions. *IEEE Conference on Standards for Communications and Networking (CSCN)*. Finland: Centre for Wireless Communications, University of Oulu. doi:10.1109/CSCN.2017.8088621

ANACOM. (2020a). *Sobre o 5G*. Obtido em 04 de dezembro de 2021, de portal 5G. Retirado de https://portal5g.pt/5g/

ANACOM. (2020b). *Segurança 5G*. Obtido de portal 5G. Retirado de https://portal5g.pt/temas/seguranca/#id_0

Bardin, L. (2004). *Análise de Conteúdo.* Lisboa: Edições 70.

Barzegar, H. (2020). *5G three main use cases with examples of associated applications*. Retirado de https://www.researchgate.net/profile/Hamid-R-Barzegar/publication/343115757/figure/fig4/AS:925409420013570@1597646207996/5G-three-main-use-cases-with-examples-of-associated-applications-17.ppm

Bhandari, N., Devra, S., & Singh, K. (2017). Evolution of Cellular Network: From 1G to 5G. *International Journal of Engineering and Techniques, 3*, pp. 98-105 [versão PDF]. Retirado de https://oaji.net/articles/2017/1992-1515158039.pdf

Buchholz, K. (2021). *5G Dwarfs All of 4G's Specs*. Retirado de https://www.statista.com/chart/17506/5g-and-4g-comparison/

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. (2019). 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). Secure 5G deployment in the EU - Implementing the EU toolbox. *Communication from the Commission to the European parliament, the Council, the European Economic and Social Committee and the Committee of the regions*. Retirado de https://digital-strategy.ec.europa.eu/en/library/secure-5g-deployment-eu-implementing-eu-toolbox-communication-commission?msclkid=b1f3659cc48711ec9baf705408a161b0

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. (2021). *Conjunto de instrumentos da EU para a cibersegurança das redes 5G : um conjunto de medidas sólidas e abrangentes para uma estratégia coordenada a nível da UE que garanta a segurança das redes 5G.* Luxemburgo: Serviço das Publicações da União Europeia. Retirado de https://data.europa.eu/doi/10.2759/212439

Congressional Research Service. (2022). *National Security Implications of Fifth Generation (5G) Mobile Technologies [versão PDF]*. Washington, D.C: Autor. Retirado de https://sgp.fas.org/crs/natsec/IF11251.pdf

Conselho Superior de Segurança do Ciberespaço. (2020). *Relatório do Grupo de Trabalho relativo à segunrança das redes 5G.* Lisboa: Autor.

Couto, A. (2020). *Elementos de Estratégia - apontamentos para um curso* (1ª ed.). Lisboa: Leya.

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

DaSilva, L., Reed, J., Shetty, S., Park, J., Wijesekera, D., & Wang, H. (2020). *Securing 5G: NATO's Role in Collaborative Risk Assessment and Mitigation [versão PDF].* Bruxelas: The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Retirado de https://ccdcoe.org/uploads/2020/12/4-Securing-5G_ebook.pdf

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

Defense Science Board. (2019). *Defense Applications of 5G Network Technology [versão PDF]*. Washington, D.C.: Autor. Retirado de https://apps.dtic.mil/sti/pdfs/AD1078719.pdf

Department of Defense. (2020). *5G Strategy Implementation Plan - Advancing 5G Technology & Applications Securing 5G Capabilities [versão PDF]*. Washington, D.C.: Autor. Retirado de https://www.cto.mil/wp-content/uploads/2020/12/DOD-5G-Strategy-Implementation-Plan.pdf

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.

Diretiva (UE) 2016/1148. (2016). Relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. *Jornal Oficial da União Europeia*. O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. Retirado de https://www.cncs.gov.pt/docs/diretiva-2016.pdf

European 5G Observatory. (2022). *5G Scoreboard*. Obtido de European 5G Observatory. Retirado https://5gobservatory.eu/observatory-overview/5g-scoreboards/

European Commission. (2021). FACTSHEET / INFOGRAPHIC - The EU toolbox for 5G security. *Shaping Europe's digital future*. European Commission. doi:10.2759/212439

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.

França, J. (2000). *Manual para normalização de publicações técnico-científica* (4ª ed.). Belo Horizonte: UFMG.

Gilli, A. (2020). NATO and 5G: what strategic lessons? *NATO Defense College (2020)*. Retirado de http://www.jstor.org/stable/resrep25095

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

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

Helweg, M. (2022). *5G is a game changer for the military*. Retirado de https://datarespons.com/5g-is-a-game-changer-for-the-military/

Hernández, D. C. (2020). *5G, una carrera por la hegemonía y el futuro con muchos beneficios. Documento MARCO IEEE 07/2020*. 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

Iberdrola, S.A. (2021). *POR QUE UTILIZAR O 5G?* Obtido de Iberdrola - CONHEÇA TUDO SOBRE O 5G. Retirado de https://www.iberdrola.com/inovacao/o-que-e-5g-vantagens

Instituto Universitário Militar. (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.

International Telecommunication Union. (2020). *Global Cybersecurity Index 2020*. Geneva: Autor. Retirado de https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jones, J., Brzezinski, I., Lute, D., & Wheeler, R. (2020). *NATO Must Move Out Smartly on 5G*. Retirado de https://www.defenseone.com/ideas/2020/08/nato-must-move-out-smartly-5g/167687/

Keiser, A. (2020). The Race to 5G: Securing the win [versão PDF]. *NSI Law and Policy paper*. Retirado de http://nationalsecurity.gmu.edu/wp-content/uploads/2020/07/The-Race-to-5G.pdf

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

Lodha, S. (2020). *The previous generations of mobile networks are 1G, 2G, 3G, and 4G*. targetupsc. Retirado de https://targetupsc.in/post3/the-previous-generations-of-mobile-networks-are-1g-2g-3g-and-4g

Microsoft. (2021). *Microsoft Digital Defense Report.* Autor. Retirado de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

National Telecommunications and Information Administration. (janeiro de 2021). National Strategy to Secure 5G Implementation Plan [versão PDF]. Washington, DC: United States Department of Commerce. Retirado de https://www.ntia.gov/5g-implementation-plan

NATO Communications and Information Agency. (2021). *NATO tech Agency explores the potential of 5G for the Alliance*. Obtido de NCI Agency. Retirado de https://www.ncia.nato.int/about-us/newsroom/nato-tech-agency-explores-the-potential-of-5g-for-the-alliance.html

Pernik, P., Jančárková, T., Kaska, K., Ruuto, U., Gheorghevici, C.-M., & Beckvard, H. (2021). *Research Report Supply Chain and Network Security Network Security Networks [versão PDF]*. Bruxelas: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Retirado de https://ccdcoe.org/uploads/2021/10/Report_Supply_Chain_and_Network_Security_for_Military_5G_Networks.pdf

PwC. (2022). *Business. Supercharged with 5G.* [Página *online*] Retirado de https://www.pwc.com/gx/en/industries/tmt/5g.html

Qualcomm Technologies. (2022). *Everything you need to know about 5G.* [Página *online*]. Retirado de https://www.qualcomm.com/5g/what-is-5g

Quivy, R., & Campenhoudt, L. V. (1998). *Manual de Investigação em Ciências Sociais.* Lisboa: Gradiva.

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

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

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

Recomendação (UE) 2020/1307. (2020). Relativa a um conjunto de instrumentos comuns a nível da União destinados a reduzir o custo da implantação de redes 5G. *Jornal*

Oficial da União Europeia. Bruxelas: Comissão Europeia. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32020H1307&from=PT

Resolução de Conselho de Ministros n.º 7-A/2020. (7 de fevereiro de 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

Resolução de Conselho de Ministros n.º 92/2019, de 05 de junho. (2019). *Estratégia Nacional de Segurança do Ciberespaço 2019-2023.* Diário da República, 1.ª série, N.º 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.

Santos & Lima. (2019). *Orientações Metodológicas para a elaboração de trabalhos de investigação* (2.ª ed., revista e atualizada ed.). Lisboa: Instituto Universitário militar.

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

Teles, T. M. (2015). Cibersegurança, deteção de outeliers. *(Tese de Dissertação de Mestre em Ciências Militares Navais). Escola Naval*.

Tirkey, A. (2020). *The 5G Dilemma: Mapping Responses Across the World [versão PDF]*. New Delhi: Observer Research Foundation. Retirado de https://www.orfonline.org/wp-content/uploads/2020/05/ORF_Monograph_5G_Dilemma.pdf

Trend Micro Incorporated. (2022). *Distributed Denial of Service*. Retirado de Trend Micro: https://www.trendmicro.com/vinfo/us/security/definition/distributed-denial-of-service

Tribunal de Contas Eurupeu. (2022). *Lançamento da tecnologia 5G na UE: atrasos na implantação das redes e questões de segurança ainda por resolver.* Luxemburgo: Autor. Retirado de https://www.eca.europa.eu/Lists/ECADocuments/SR22_03/SR_Security-5G-networks_PT.pdf

Trump, D. J. (2020). National Strategy to secure 5G [versão PDF]. Washington, DC, EUA: The White House. Retirado de https://trumpwhitehouse.archives.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf

Anexo A — Avaliação de riscos da UE: cenários de risco

A avaliação coordenada dos riscos de segurança das redes 5G ao nível da UE identifica nove riscos principais, agrupados em cinco cenários de risco.

Quadro 6 - Avaliação de riscos da UE - cenários de risco

I — Cenários de risco relacionados com medidas de segurança insuficientes	R1 — Má configuração das redes R2 — Falta de controlos de acesso
II — Cenários de risco relacionados com a cadeia de abastecimento 5G	R3 — Fraca qualidade dos produtos R4 — Dependência de um único fornecedor em determinadas redes ou falta de diversidade a nível nacional
III — Cenários de risco relacionados com o *modus operandi* dos principais perpetradores	R5 — Interferência de Estados através da cadeia de abastecimento 5G R6 — Exploração de redes 5G pela criminalidade organizada ou por organizações criminosas que visem os utilizadores finais
IV — Cenários de risco relacionados com interdependências entre as redes 5G e outros sistemas críticos	R7 — Perturbação significativa de infraestruturas ou serviços críticos R8 — Falha generalizada das redes devido à interrupção do fornecimento de eletricidade ou de outros sistemas de apoio
V — Cenários de risco relacionados com dispositivos dos utilizadores finais	R9 — Exploração da IdC (Internet das coisas), de telemóveis ou de dispositivos inteligentes

Fonte: Disponível em CE (2021, p. 2).

Anexo B — Medidas da UE para a implementação do 5G

Figura 20 - Medidas Estratégicas da UE
Fonte: Adaptado a partir de CSSC (2020, pp. 25-28).

Já no que concerne às MT e Medidas de Apoio (MA), e intervenientes, a UE identificou as espelhadas na Figura 22.

Medidas	Intervenientes pertinentes				
	Autoridades dos Estados-Membros	Operadores de redes móveis	Comissão Europeia	ENISA	Partes interessadas (incluindo fornecedores)
Medidas técnicas (MT)					
MT01 – Garantir a aplicação dos requisitos de base em matéria de segurança (conceção e arquitetura de redes seguras)	✓	✓			
MT02 – Garantir e avaliar a aplicação de medidas de segurança nas normas 5G existentes	✓	✓			✓
MT03 – Assegurar controlos de acesso rigorosos	✓	✓			
MT04 – Aumentar a segurança das funções de rede virtualizadas	✓	✓			
MT05 – Garantir a segurança da gestão, do funcionamento e do controlo das redes 5G	✓	✓			
MT06 – Aumentar a segurança física	✓	✓			
MT07 – Reforçar a integridade, a atualização e a gestão de correções do *software*	✓	✓			
MT08 – Reforçar as normas de segurança nos processos dos fornecedores através de condições robustas de aquisição	✓	✓			✓
MT09 – Utilizar a certificação da UE em componentes das redes 5G, equipamentos dos clientes e/ou processos dos fornecedores	✓	✓	✓	✓	✓
MT10 – Utilizar a certificação da UE noutros produtos e serviços informáticos não específicos da tecnologia 5G (dispositivos conectados, serviços de computação em nuvem)	✓		✓	✓	✓
MT11 – Reforçar a resiliência e os planos de continuidade	✓	✓			✓
Medidas de apoio (MA)					
MA01 – Rever ou desenvolver orientações e boas práticas sobre segurança de redes	✓	✓		✓	
MA02 – Aumentar as capacidades de ensaio e auditoria a nível nacional e da UE	✓		✓	✓	
MA03 – Apoiar e definir a normalização no domínio da tecnologia 5G	✓	✓	✓	✓	✓
MA04 – Desenvolver orientações sobre a aplicação de medidas de segurança nas normas 5G existentes	✓			✓	
MA05 – Garantir a aplicação de medidas normalizadas de segurança técnica e organizacional através de um sistema de certificação específico a nível da UE	✓			✓	✓
MA06 – Intercâmbio de boas práticas sobre a aplicação de medidas estratégicas, em particular dos quadros nacionais para a avaliação do perfil de risco dos fornecedores	✓				
MA07 – Melhoria da coordenação na resposta a incidentes e gestão de crises	✓			✓	
MA08 – Realizar auditorias às interdependências entre as redes 5G e outros serviços de importância crítica	✓				
MA09 – Reforçar os mecanismos de cooperação, coordenação e partilha de informações	✓			✓	
MA10 – Garantir que os projetos no âmbito da tecnologia 5G apoiados com financiamento público têm em conta os riscos de cibersegurança	✓		✓		

Figura 21 - MT e MA da UE para as redes 5G e os seus intervenientes
Fonte: Disponível em TCE (2022).

Anexo C — 5G EU toolbox of risk mitigating measures

MEASURES	Indicative implementation timeframe: Short-term	Medium-term	Long-term	Potential implementation factors: Resource costs	Sector specific economic impact	Sector specific economic impact	Broader economic / societal impact	SPECIFIC MEASURES	RISKS: R1: Misconfiguration of networks	R2: Lack of access controls	R3: Low product quality	R4: Dependency on a single supplier	R5: State interference through 5G supply chain	R6: Exploitation of 5G networks by org. crime	R7: Significant disruption of crit. Infras. services	R8: Massive failure due to power interruption	R9: IoT exploitation
STRATEGIC MEASURES																	
a) Regulatory powers	✓			✓	✓	✓	✓	SM 01									
								SM 02									
b) Third party suppliers	✓			✓	✓	✓	✓	SM 03									
								SM 04									
c) Diversification of suppliers	✓	✓		✓	✓	✓	✓	SM 05									
								SM 06									
d) Sustainability and diversity of 5G supply and value chain	✓	✓	✓	✓	✓	✓	✓	SM 07									
								SM 08									
TECHNICAL MEASURES																	
a) Network security – baseline measures	✓			✓	✓			TM 01									
								TM 02									
b) Network security – 5G specific measures	✓			✓	✓			TM 03									
								TM 04									
								TM 05									
								TM 06									
								TM 07									
c) Requirements related to suppliers' processes and equipment		✓	✓	✓	✓	✓		TM 08									
								TM 09									
								TM 10									
d) Resilience and continuity	✓			✓	✓			TM 11									

Expected effectiveness: Very low — Very high

Figura 22 - Visão simplificada das medidas no plano de mitigação do risco
Fonte: Disponível em Comissão Europeia (2020).

The estimated degree of expected effectiveness takes into account the original risk and the expected residual risk after applying the measure, and using the following scale:

• Very High: The measure is considered effective to a very high degree, meaning that it is expected to almost completely mitigate the related risks.

• High: The measure is considered highly effective, meaning that it is expected to significantly mitigate the related risks.
• Medium: The measure is considered somewhat effective, meaning that it is expected to mitigate the related risks to some extent.
• Low: The measure is considered hardly effective, as it is expected to mitigate the related risks only marginally.

In addition, for each measure, the table on mitigation plans (annex 1, table 2) indicatively identifies other parameters and characteristics, with a view of assisting Member States in selecting and implementing measures, namely:

• Potential implementation factors (both positive and negative), namely:
  o Resource costs
  o Sector-specific economic impacts (for operators or for suppliers)
  o Broader economic and/or societal impacts
• Indicative timeframes for taking the necessary steps to implement the measures, expressed using the following scale:
  o Short term: 0-2 years
  o Medium term: 2-5 years
  o Long term: >5 years

STRATEGIC MEASURES		
a) Regulatory powers		
Id	**Measure**	**Description**
SM01	**Strengthening the role of national authorities**	This should include regulatory powers for national authorities, to be able to: - impose strengthened obligations on operators, for example concerning the security of the signalling/management plane; - use ***ex-ante*** powers to restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment, taking into account among other things: ▪ Security of critical and sensitive parts of 5G networks; ▪ Security of the equipment itself or the environment (deployment, interconnections, etc.); ▪ Risk of interference by a third country in the 5G supply chain; ▪ Risk of major dependency on a single supplier by individual MNOs or nationally ▪ Risks for national security.
SM02	**Performing audits on operators and requiring information**	In exercising their powers under Article 41(2) of the EECC[32], competent authorities should: - Audit, or require audits, of MNOs, if needed at an in-depth technical level, for example of critical components and/or sensitive parts of the 5G networks; - Require operators to provide detailed and up-to-date information about their plans for the sourcing of 5G equipment and for the involvement of third party suppliers;

		- Require operators to document and maintain a description on how the baseline technical network security measures are implemented[33].
b) Third party suppliers		
SM03	**Assessing the risk profile of suppliers and applying restrictions for suppliers considered to be high risks-including necessary exclusions to effectively mitigate risks- for key assets**	- Establish a framework with clear criteria, taking into account the risk factors identified in paragraph 2.37 of the EU coordinated risk assessment[34] and adding country-specific information (e.g. threat assessment from national security services, etc.), for national competent authorities and MNOs to: - Perform rigorous assessments of the risk profile of all relevant suppliers at national level and/or EU level (for example jointly with other MS or other MNOs); -Based on the risk profile assessment, apply restrictions- including necessary exclusions to effectively mitigate risks- for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network management and orchestration functions, and access network functions);. - Take steps to ensure that MNOs have adequate controls and processes in place to manage potential residual risks, such as regular supply chain audits and risk assessments, robust risk management, and/or specific requirements for suppliers based on their risk profile.
SM04	**Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support**	Establish a legal/regulatory framework which places limit on the types of activity and conditions under which MNOs are able to outsource particular functions to Managed Service Providers (MSPs), for both physical and virtual infrastructure, including: - Applying restrictions in particular in sensitive parts of the 5G networks, such as the security and network operations functions and where MSPs are considered to be high risk suppliers within the meaning of SM03; - For functions outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given to perform those functions.
		For equipment manufacturers' third line support during the design, deployment and/or operation of networks, impose strict access controls especially for critically sensitive components and/or sensitive parts of the network and in particular for suppliers considered to be high risk within the meaning of SM03.
c) Diversification of suppliers		
SM05	**Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies**	Ensure that each MNO has an appropriate multi-vendor strategy taking into account the technical constraints and interoperability requirements of the different parts of a 5G network: - To avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile); - To avoid dependency on suppliers considered to be high risk within the meaning of SM03.
SM06	**Strengthening the resilience at national level**	Ensure that there is an adequate balance of suppliers at national level to ensure that there is resilience in case there is an incident with one operator and/or one supplier, taking into account the variations in geography and population in individual Member States.
d) Sustainability and diversity of 5G supply and value chain		
SM07	**Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU**	- Build on the EU's Foreign Direct Investment screening mechanism to improve the monitoring of FDI investments across the 5G value chain (e.g. through a mapping of key 5G assets, the use of monitoring tools and exploring specific guidelines), in order to better detect foreign investments in the 5G value chain that may pose a threat to the security or public order of more than one EU MS. Critical infrastructure, public security, access to and control of information and cybersecurity are well embedded under the scope of this (FDI) Regulation, allowing the evaluation of investments taking into account factors such as the risk profile of buyers/companies. - Should dependencies along the 5G value chain arise as a result of trade distorting market behaviour by producers falling under the scope and conditions of the relevant EU anti-dumping and/or anti-subsidy rules – and should these be notified via an ad hoc complaint or in exceptional circumstances via the European Commission's own initiative – then such behaviour could be investigated and acted upon through the EU's trade defence measures.

SM08	**Maintaining and building diversity and EU capacities in future network technologies**	Develop policies which create optimal conditions for European technological firms and foster innovation in key technology areas to promote a diverse, sustainable and secure European 5G eco-system, including by: – Developing the proposed EU Institutionalised partnership in the field of NGI/6G ("Smart Networks and Services")[35] to ensure there is a sufficient degree of diversity of suppliers and sufficient knowledge and supply capacity in the EU across the telecoms value chain; - Developing EU capacities and therefore also avoid dependencies by supporting disruptive and ambitious research & innovation. This relates to the implementation of the various EU funding programmes, in particular Horizon Europe, the Digital Europe Programme and the Connecting Europe Facility (CEF) (e.g. through initiatives such as 5G Corridors for Connected and Automated Mobility); - Bringing together knowledge, expertise, financial resources and economic actors throughout the Union, so as to overcome potential important market or systemic failures along the value chain (IPCEI), and further specific industry initiatives.

Figura 23 - Descrição das Medidas Estratégicas
Fonte: Adaptado a partir de Comissão Europeia (2020).

TECHNICAL MEASURES		
a) Network security – baseline measures		
Id	**Measures**	**Description**
TM01	**Ensuring the application of baseline security requirements (secure network design and architecture)**	Ensure that MNOs implement existing security best practices and recommendations non-specific to 5G networks on, for instance product development, configuration, day-to-day network management, incident management, security updates[36], for instance by imposing and reviewing risk assessment plans by MNOs. Ensure that MNOs keep up-to-date information on security policy, including operational information, as well as linked to change and incident management procedures for key network and information systems.
TM02	**Ensuring and evaluating the implementation of security measures in existing 5G standards**	Ensure that MNOs and their suppliers implement the existing security measures in the relevant 5G technology standards (e.g. 3GPP)and use it as a minimum security baseline for MNOs, so as to ensure that also the optional parts of these standards, relevant for security, are adequately implemented
b) Network security – 5G specific measures		
TM03	**Ensuring strict access controls**	Ensure that MNOs implement adequate, flexible and verifiable technical measures to ensure that: - Strict network access controls are applied; - The principle of least privilege is applied, ensuring that various rights in the network (e.g. access rights between network functions, network administrators' rights, virtualization configuration) are minimized; - The segregation of duties principle is applied; - Procedures are in place to ensure that these rules are in effect all the time and evolve with the network. In setting the access control policies, particular care should be taken to ensure that remote access by third parties, especially suppliers considered to be high risk, is minimized and/or avoided whenever possible. When remote access is necessary, for example to address service outages, the MNO should apply appropriate authentication[37], authorization, logging and auditing so as to have a clear visibility on access to data and configuration changes or network alterations.
TM04	**Increasing the security of virtualised network functions**	Ensure that MNOs follow security best practices for network function virtualisation. Note that there may be settings, for example when a network function is highly critical or when it is handling highly sensitive information, where virtualization is not appropriate and in such settings physical separation may be necessary.

TM05	**Ensuring secure 5G network management, operation and monitoring**	Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU. The NOC and SOC are a vital component of the MNO's infrastructure in implementing and monitoring the measures for secure network management and operation. They should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and IoT). Also ensure that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components.
TM06	**Reinforcing physical security**	Ensure that MNOs reinforce physical protection of critical components and sensitive parts of the 5G networks, taking a risk-based approach for Multi-access Edge Computing (MEC) and base stations[38], for example considering where the components are deployed and used, like a MEC use in hospitals. In reinforcing physical access controls, it is important to ensure that access is granted only to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored, particularly where it concerns critical components and sensitive parts of the 5G networks.
TM07	**Reinforcing software integrity, update and patch management**	Ensure that MNOs deploy adequate tools and processes to ensure software integrity, which reliably identify and keep track of changes and the status of patches, when performing software updates and applying security patches in the 5G networks.
c) Requirements related to suppliers' processes and equipment		
TM08	**Raising the security standards in suppliers' processes through robust procurement conditions**	Ensure that MNOs demand specific security standards from equipment suppliers in the procurement process (e.g. on specific security improvements and demonstrating quality levels, security maintenance of the equipment throughout its lifetime and built-in of security in the product' development processes).
TM09	**Using EU certification for 5G network components, customer equipment and/or suppliers' processes**	The Commission should consider including into the Union Rolling Work Programme[39] relevant EU-wide scheme(s) for critical network components used in the 5G networks and/or for 5G customer equipment (for example, for eSIMs and related cryptographic material) under the EU certification framework. It should also be examined at a later stage whether the certification or supplier's process could also be added to the Union Rolling Work Programme.
TM10	**Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services)**	The Commission should consider including into the Union Rolling Work Programme EU-wide schemes under the EU certification framework for non-5G specific ICT products and services, such as for: - The security of cloud services and related technologies, which are an important part of 5G deployment[40]; - The security of connected (end-user) devices, including IoT.
d) Resilience and continuity		
TM11	**Reinforcing resilience and continuity plans**	Ensure that MNOs reinforce their resilience and continuity plans. MNOs should ensure they have adequate plans in place in case of disaster affecting the ongoing operation of their network, and ensure any critical dependencies are mapped and mitigated as required. MNOs should request similar arrangements within their suppliers and only use suppliers who demonstrate sufficient levels of long-term resilience.

Figura 24 - Descrição das Medidas Técnicas
Fonte: Adaptado a partir de Comissão Europeia (2020).

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 A. C., 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 *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).

Conectividade permanente e mais fiável (uRLLC) - em que a perceção do utilizador do atraso da comunicação (designada por latência) será muito reduzida (ANACOM, 2020a).

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).

Distributed Denial of Service (DDoS) - é um tipo de ataque cibernético que implica ter os atacantes a utilizar uma grande rede de Computadores remotos, chamados *botnets*, para sobrecarregar a ligação ou processador de outro sistema, fazendo com que negue o serviço ao tráfego legítimo que está a receber. Um ataque DDoS foi concebido para interromper ou desligar uma rede, serviço ou site e torná-lo indisponível para pedidos de tráfego legítimos (Trend Micro Incorporated, 2022).

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).

Maior velocidade e capacidade da rede (eMBB) - Estas características permitirão utilizar, com melhor desempenho e experiência de utilização, as aplicações de banda larga móvel já existentes (por exemplo, trabalhar e jogar através da cloud) (ANACOM, 2020a).

Massificação da comunicação entre dispositivos (mMTC) - as redes 5G estão a ser desenhadas de forma a permitir assegurar a ligação em rede entre milhões de dispositivos de natureza diversa e, consequentemente, a massificação da comunicação entre máquinas sem intervenção humana (ANACOM, 2020a).

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).

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).

Apêndice B — Modelo de Análise

Quadro 7 - Modelo de análise

Título		Segurança nas Redes 5G – Estratégia Nacional e Internacional	
Delimitação	**Domínios**	**Espaço**	EUA, UE, OTAN e Portugal
		Conteúdo	Estratégias para a segurança nas redes 5G
		Tempo	2016 a 2021/2022
Metodologia de Investigação	**Posicionamento**	**Ontológico**	Construtivista
		Epistemológico	Interpretativa
	Metodologia de raciocínio		Indutivo
	Estratégia de Investigação		Qualitativa
	Desenho de Pesquisa/Horizonte Temporal		Estudo de caso Transversal
OG	Propor contributos para a Estratégia de Segurança nas Redes 5G no âmbito das FFAA Portuguesas		
QC	Que contributos podem ser integrados na Estratégia de Segurança nas redes 5G no âmbito das FFAA Portuguesas?		

OE	QD	Conceitos	Dimensões	Variáveis	Indicadores	Técnicas de recolha de dados
OE 1: Descrever as potencialidades e vulnerabilidades de segurança nas redes 5G.	**QD 1:** Quais as potencialidades e vulnerabilidades de segurança das redes 5G?	Redes 5G	Características de Segurança	Potencialidades Vulnerabilidades	Resiliência Confidencialidade Integridade Autenticidade (da perspetiva do Software/Hardware)	Análise documental Entrevistas semiestruturadas
OE 2: Analisar as Estratégias de Segurança para as redes 5G.	**QD 2:** Quais as Estratégias de Segurança para redes 5G?	Estratégias Segurança Cibersegurança Redes 5G	EUA UE OTAN Portugal	Vetores de Desenvolvimento	Capacidade militar • Doutrina • Organização • Treino • Material • Liderança • Pessoal • Infraestruturas • Interoperabilidade	

Apêndice C — Guião para entrevistas semiestruturadas

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS
CURSO ESTADO-MAIOR CONJUNTO
2021/2022
Guião de entrevista
Segurança nas Redes 5G – Estratégia Nacional e Internacional

ENQUADRAMENTO

A implantação e operacionalização das redes 5G irá disponibilizar novas capacidades de serviços e constituir-se como elemento facilitador de sectores essenciais da sociedade, nomeadamente, da energia, transportes, financeiro, saúde, bem como, dos sistemas de controlo industriais (RCM n.º 7-A/2020, 2020).

Contudo, todos os países são afetados, em certa medida, pela clivagem digital, e como um facilitador fundamental da economia, da sociedade e do governo, que dependem dos sistemas digitais, garantir a Cibersegurança das redes 5G é uma questão de importância estratégica para a defesa dos interesses essenciais de segurança de qualquer Estado, num momento em que os ciberataques estão a aumentar e são mais sofisticados do que nunca. No que, a esta matéria diz respeito, prevê-se que possam ser particularmente graves as consequências de perturbações sistémicas e generalizadas devido à futura dependência dos inúmeros serviços críticos em relação às redes 5G (Recomendação (UE) 2019/534, 2019).

O presente TII enquadra-se nas Ciências Militares, na área de técnicas e tecnologias militares, nos termos da alínea c) do n.º 5 do Decreto-Lei n.º 249/2015, de 28 de outubro, mais concretamente no que diz respeito à Segurança nas Redes 5G – Estratégia Nacional e Internacional.

No seguimento do desenvolvimento do tema referido anteriormente, o presente trabalho de investigação terá como principal enfoque as Estratégias de segurança das redes 5G, e o seu possível contributo para as Estratégias de Segurança no âmbito das redes 5G para as Forças Armadas Portuguesas.

IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	
Posto / Título:	
Cargo / Função:	
Data:	
Local (se aplicável)**:**	
Hora de início (se aplicável)**:**	
Hora do fim (se aplicável)**:**	

QUESTÕES

As questões de seguida apresentadas foram elaboradas tendo por finalidade responder a um conjunto de indicadores, que se entende permitirem atingir o objetivo geral do trabalho. Contudo face á experiência e conhecimentos de Vossa Excelência, as mesmas podem ser alteradas ou sugeridas outras, se entendido por conveniente.

1. Sendo o 5G uma tecnologia em implementação, que características destacaria como benéficas e quais se destacam no âmbito da segurança?
2. Na sua visão, no quadro da segurança das redes 5G que desafios e oportunidades considera serem mais relevantes para as Forças Armadas Portuguesas (FFAA)/serviços críticos?
3. Na perspetiva da segurança, quais as implicações/vantagens/desvantagens que as redes 5G podem trazer ao domínio das FFAA/serviços críticos?

4. De acordo com a doutrina NATO, os elementos de capacidades são: Doutrina, Organização, Treino, Materiais, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLPII). Sendo a tecnologia 5G inovadora, as redes 5G compreendem inúmeras potencialidades dadas as suas características. No entanto, associado a estas potencialidades advém um conjunto de vulnerabilidades, que no quadro da segurança são uma preocupação prioritária no âmbito da Cibersegurança e da Ciberdefesa. Esta preocupação tem-se traduzido em grupos de trabalho (quer nacional, quer ao nível das organizações internacionais onde Portugal está inserido), em desenvolvimento de normas e recomendações para mitigar estas vulnerabilidades e reforçar a segurança neste campo.
   4.1. Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem **potenciar (pontos fortes)** a segurança das redes 5G aquando em uso nas FFAA?
   4.2. Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem mitigar as **vulnerabilidades (pontos fracos)** da segurança das redes 5G aquando em uso nas FFAA?
   4.3. Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem reduzir o **risco de ameaças** às redes 5G aquando em uso nas FFAA?
   4.4. Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem **criar oportunidades** de segurança às redes 5G aquando em uso nas FFAA?

Obrigada pela colaboração e tempo despendido.

Atenciosamente,

Isidro Miguel Mendes Lopes
Major de Infantaria Paraquedista
Auditor do Curso de Estado-Maior Conjunto 2021/22

INSTITUTO UNIVERSITÁRIO MILITAR

927 678 257
lopes.imm@ium.pt
Rua Pedrouços, 1449-027 Lisboa

Apêndice D — Matriz de entrevistados e síntese de resposta

1. Matriz de entrevistados

Quadro 8 - Matriz de entrevistados

Código	Posto / Título	Nome	Função	Tipo	Data
E1	Contra-Almirante	António Gameiro Marques	Diretor-Geral do Gabinete Nacional de Segurança	Semiestruturada (Presencial [P])	18abr22
E2	Comodoro	Rui Manuel Alves Francisco	Representante do Ministério da Defesa Nacional no grupo de trabalho relativo à segurança das redes 5G	Exploratória (P) Semiestruturada (P)	25nov21 18abr22
E3	Diretor	João Frederico Beleza Vaz	Diretor de Operações da ANACOM Açores	Semiestruturada (Teams)	22abr22
E4	Major de Transmissões	Nuno Casteleiro de Goes	Security by Design Expert (Cibersecurity engineer) na EDP	Semiestruturada (e-mail)	01mai21

2. Síntese de respostas

As entrevistas semiestruturadas a especialistas nacionais de Cibersegurança seguiram o guião apresentado no Apêndice D, apresentando-se no Quadro 6 a síntese das suas respostas.

Quadro 9 - Síntese de respostas dos entrevistados

Entrevistado	Q1 - Sendo o 5G uma tecnologia em implementação, que características destacaria como **benéficas** e quais se destacam no âmbito da segurança?
E1	A tecnologia 5G pode ser de tal maneira impactante que ela por si só **é um *enabler* de uma série de capacidades** como o comando e controlo. Por isso **tem de ser encarada como uma capacidade**, para haver doutrina da sua utilização, um conceito de operações, haver uma estrutura que faça a Governance da sua implementação nos Ramos das FFAA, **haver pessoas que conheçam o que é o 5G**, que saibam repará-la, mantê-la, usá-la, que definam cenários para a sua utilização operacional, que pensem se devem ou não haver infraestruturas próprias nas FFAA para haver redes locais de 5G. As benéficas são aquelas que todos nós já conhecemos e que são uma marca forte do que é, **baixa latência, a capacidade a velocidade, a capacidade endereçar pequenos dispositivos, que dá potencial de densidade no teatro de operações muito grande,** podemos endereçar um centímetro quadrado do teatro de operações onde temos muito mais capacidade para compilar a informação, de obter informação e, portanto, tomar decisões mais atempadas e mais efetivas. Portanto o 5G está baseado **em tecnologias de alto nível de virtualização** e por isso muito do que se passa pode estar em cloud e no teatro de operações, o soldado, os UAV, as aeronaves, os carros de combate podem estar permanentemente ligados à nuvem e receber informações através dessa nuvem. Como já acontece com o F35, como vai acontecer com o KC390. E, portanto, há um **fluxo bidirecional de informação muito mais denso e muito mais rico que dá que dá vantagens a quem a quem tiver essa capacidade nas suas FFAA.** Em termos de segurança tem desafios grandes e que aliás estão identificados **na Toolbox da União Europeia, como as 22 medidas** que endereçam precisamente os riscos de segurança que foram identificados. **Há as medidas estratégicas (SMs)**. Como a **estrutura é toda virtualizada**, se a questão da segurança não estiver acautelada com bastante acuidade pode haver problemas. porque a rede local é virtual, não precisa de ter redes físicas, portanto estou permanentemente ligado à nuvem e é aí que há o agregado de entidades e de endereços que que

	fazem uma rede corporativa e como nós não vemos isso não é tangível, traz potenciais riscos não só de perceção como também efetivos **se não forem acautelados no seu desenho.**
E2	A tecnologia 5G apresenta um conjunto de características que vem potenciar as capacidades das Tecnologias de Informação e Comunicação (TIC), nomeadamente, a **reduzida latência, o aumento considerável da velocidade da transmissão de dados, a quantidade de dispositivos conectados, a redução do consumo de energia dos diversos dispositivos, o aumento da banda larga, maior cobertura, maior disponibilidade** e que vem responder às necessidades da interação digital da sociedade atual. Estas características irão permitir **dotar às aplicações uma conectividade em tempo real**. A baixa latência e claramente para as operações militares é importante.
E3	O 5G já tem uma abordagem de ***security by design*****,** ou seja, quando estas redes são implementadas, é já sobre **o desígnio dos critérios de segurança**. Ao contrário das redes antecessoras. Se as redes 4G eram uma evolução, as **redes 5G são uma revolução**, porque **logo desde o início estas redes são em termos arquiteturais sobre o conceito de segurança. Este modelo do cibersecurity toolbox de implementação do 5G devia ser massificado para outras tecnologias, inclusive para as comunicações militares, mas não do campo de batalha, táticos**. Há uma tendência obviamente de ir para estas tecnologias comerciais porque estão mais amadurecidas em termos tecnológicos, pois são tecnologias que estão validadas.
E4	Existem 3 pontos que gostaria de destacar: o primeiro é a **mobilidade** que uma rede como estas características permite, o que se reveste de extrema importância quando falamos de redes do campo de batalha; outra característica de grande importância é a **velocidade de comunicação** que permite, possibilitando maiores trocas de informação, com ficheiros maiores, **imagem e metadados em tempo real e comunicações permanentes**; por fim a **diminuição de recursos necessários, desde as baterias aos ativos de rede** que deixam de ser necessários acrescentar para permitir a interligação dos equipamentos, permitindo uma maior elasticidade, resiliência e escalabilidade da rede. No seu conjunto, tornam-se uma grande vantagem no campo de batalha e no dia a dia, mudando o paradigma das redes como o era visto até hoje. É criado um entendimento entre equipamentos que **permitem que troquem comunicações entre eles sem necessitar de outra infraestrutura de suporte.**
Entrevistado	Q2 - Na sua visão, no quadro da segurança das redes 5G que **desafios e oportunidades** considera serem mais relevantes para as Forças Armadas Portuguesas (FFAA)/serviços críticos?
E1	Há desafios e oportunidades que são comuns quando se introduz algo que é potencialmente disruptivo. As organizações têm que se mudar, têm que se adaptar a estes novos desafios. Têm que desenvolver **nova doutrina, têm que desenvolver estratégias de formação e de treino, tem que ter uma nova organização. O meu maior anseio é que as FFAA olhem para o 5G como mais um sistema de comunicações, que não o é.** Portanto temos de **alterar a formação das pessoas, as infraestruturas olhar para isto outra vez numa lógica de interoperabilidade**, mas isto tem que ser olhado em todas essas vertentes. E há aí uma oportunidade para pensarmos **como é que nos devemos organizar e sobretudo como é que nos devemos posicionar para tirar partido do 5G nos novos teatros de operações**. Com o exército certamente foi assim quando vieram os novos carros de combate, quando vêm novas armas, onde tem de se d**esenvolver todas essas competências das pessoas, que depois têm que manter, ensinar, desenvolver novos cenários de treino,** e por isso há aí todo um manancial muito grande de inovação.
E2	Considero que será um desafio e em simultâneo uma oportunidade para as FFAA, **a edificação desta Tecnologia 5G, como uma capacidade e que desta forma permitir exponenciar a segurança nas redes 5G.** Ainda no âmbito da segurança, julgo ser um desafio para as FFAA, **o acompanhamento do desenvolvimento permanente do conhecimento desta tecnologia**, das suas potencialidades e vulnerabilidades, e as múltiplas ameaças que estão em constante mutação e adaptação face aos desafios de segurança que se lhes apresentam. **Como oportunidade é a possibilidade de integrar grupos de trabalho da OTAN e EU, que tem expertises na área, com capacidade de investigação e desenvolvimento e parceria com a indústria neste campo, que permitirá alavancar o conhecimento e a experiência adquirida para as FFAA.** Outra oportunidade é **adquirir parceiros com as entidades civis (ANACOM, GNS, entidades relacionadas com a segurança e comunicações), quer para partilha de informações quer para parcerias operacionais**.

	A própria tecnologia é considerada como um desafio e uma oportunidade para a segurança das redes 5G, **pela monitorização em tempo real, pelo desenvolvimento de aplicações de segurança. Outra oportunidade é o incremento da interoperabilidade entre parceiros e forças**.
E3	O que se pode retirar do quadro de segurança das redes 5G, é precisamente a arquitetura em termos de segurança e os protocolos em termos de *open source*, em termos de rádio. As questões relacionadas com a resiliência, que é um conceito a autorregenerar-se em caso de falha, fazer face a um incidente e a continuar as suas funções. O melhor desafio e a melhor oportunidade é olhar para os objetivos da **do cibersecurity toolbox do 5G** e olhar para as **categorias de risco e diversos cenários, analisá-los e verificar as medidas estratégicas de mitigação que identificaram,** nomeadamente da **identificação da fiabilidade de fornecedores, não depender de fornecedores ou que sejam de países geopoliticamente vistos como adversários.** Outro desafio será as **cadeias logísticas,** que possam ser comprometidos no ato da entrega do abastecimento colocando em causa o cumprimento da missão das FFAA.
E4	Atente-se que, a interação da tecnologia 5G em ambiente militar é diferente da utilização no mundo civil. Poderemos tirar partido dos dois âmbitos, mas, havendo necessidade de interação, será feita apenas se daí não venham compromissos à atividade operacional. Esta integração irá **potenciar a capacidade operacional na interligação entre forças diferentes, na cobertura do campo de batalha e na comunicação interna das forças no terreno e ao escalão superior**. Saliento que esta **tecnologia, como um só, dificilmente irá operar**. Potencia sim a troca de **informação, numa base tecnológica de uma arquitetura de redes adhoc**, libertando grande parte das comunicações filares na integração com o escalão superior, nomeadamente no encaminhamento dos dados entre equipamentos, utilizando protocolos de routing próprios. Haverá sempre impactos no tipo de equipamentos a utilizar, na capacidade de emissão desses equipamentos, nos acessos que o utilizador poderá ter à informação que por ele veicula. As orientações da UE e da OTAN prendem-se diretamente com questões de segurança, por ser uma tecnologia nova e pouco conhecida e explorada, mas sobretudo, pela questão da **fidedignidade dos fabricantes**. Foram emanadas um conjunto de medidas e ações que orientam a sua utilização e aquisição. Maioritariamente prendem-se com questões de utilização no mundo civil que podemos adaptar à realidade militar. A sua utilização poderá ser feita em **ambientes restritos, com âmbitos bem definidos, potenciando a atividade operacional, apoiando os militares num teatro de operações e potenciando o comando e controlo, o que permitirá ter uma common operational picture (COP) mais rica e atualizada em operações militares.** A interação com os homens no terreno será melhor, permitindo uma **rede de cobertura mais abrangente, com maior largura de banda**, o que irá permitir uma troca de informação **mais célere, com mais informação e mais rápida**. A utilização do 5G em ambiente operacional torna-se mais critico nas operações de retaguarda, onde os cuidados de utilização estarão mais perto da utilização normal no mundo civil, principalmente por questões de interoperabilidade com parceiros e fornecedores e que, caso não sejam tomadas as devidas cautelas, poderão ser fonte de informação a um opositor.
Entrevistado	Q3 - Na perspetiva da segurança, quais as **implicações/vantagens/desvantagens** que as redes 5G podem trazer ao domínio das FFAA/serviços críticos?
E1	Há uma grande **componente de virtualização, e isso vai permitir que as redes sejam muito mais dinâmicas, virtuais** e ao fazer isso traz desafios grandes de segurança. Enquanto uma pessoa com o computador está ligada à rede pode interromper a ligação, pode cortar o fio, pode cortar a fibra ótica, pode fazer um DoS. No 5G com funciona por radio frequência, tem o risco dos empasteladores ou bloqueadores de sinal.
E2	As vantagens poderá ser **a conectividade das aplicações, serviços, monitorização em tempo real, a própria virtualização da rede, a possibilidade de criar múltiplas redes privadas com várias camadas de segurança, a capacidade de uma maior cobertura**. **A capacidade de maior transmissão de dados e automatização da própria segurança, quer seja ela física ou virtual**. Desvantagens será a possibilidade **fiabilidade dos inúmeros dispositivos conectados, a própria fiabilidade dos fabricantes**, em que todos eles têm de sofrer de uma constante certificação e monitorização, assim **como contratos de prestação de serviços mais rigorosos**, nomeadamente ao nível do **cumprimento dos requisitos/standards de segurança** exigidos. Outra

	desvantagem, é o facto de os EUA serem o maior financiador da OTAN, impor restrições de parcerias com certos fabricantes de tecnologias 5G, invocando questões securitárias.
E3	Sou da opinião que as **redes 5G não devam ser já implementadas nas FFAA**, porque é uma tecnologia que **tem de ganhar maturidade,** especialmente as tecnologias comerciais. Segundo porque a tecnologia LTE, na minha opinião satisfaz os requisitos operacionais da atualidade, e já é uma tecnologia com maturidade. Estas redes LTE em contrapartida não são desenhadas em termos de arquitetura logo à nascença. Portanto tem que haver aqui um equilíbrio. Qualquer operador de redes consegue saber quantos telefones estão ligados numa determinada área, por estarem ligados a um BTS. Conseguem perceber as rotinas diárias, padrões, e esta informação cruzada com a posição geográfica de uma área militar pode trazer vulnerabilidades. Face a isto temos de colocar um layer de segurança. Temos de **dominar muito bem a tecnologia** por forma a mitigar as suas vulnerabilidades. Para implementar uma tecnologia deste nível temos de **fazer a análise de risco**, e aceitar se é viável ou não o risco calculado para os fins que a queremos utilizar. Temos de encriptar as comunicações ao nível militar, ter o *information assurance* e depois garantir a disponibilidade das comunicações. Os militares não podem depender de uma arquitetura civil, tem de ter contingências, pois somos considerados o último reduto de ação, numa situação de emergência, onde tudo colapsa. Esta tecnologia não é por si autónoma, necessita de outras tecnologias.
E4	Trazer novas tecnologias deve permitir que haja melhoria significativa com risco controlado, potenciando a **capacidade de batalha, interoperabilidade, comando e controlo, sobre comunicações mais rápidas, fiáveis, sustentáveis e seguras, com** foco na garantia dos pilares da segurança da informação, nomeadamente **a disponibilidade, confidencialidade e integridade dos dados transmitidos**. Deve também se capaz de lidar com grande volume de dados, ser o mais simples e amiga do utilizador no que toca à utilização, **potenciando um novo conceito de troca de informação no comando e controlo das operações.** O 5G vem permitir que com **equipamentos mais pequenos, uma estrutura de rede mais fácil de instalar, sem meios terceiros, integração à rede de retaguarda mais fácil, com maior velocidade e poupança de energia,** garantir o que normalmente era uma estrutura mais pesada, com mais meios, maior consumo de energia e com larguras de banda algo limitadas, o que permitia chegar até certos escalões, mas que deixava os equipamentos do combatente um pouco à parte. Com este novo paradigma, será possível **ter meios mais pequenos, ao nível do combatente, que permitirão uma troca de informação mais rápida, transmitindo não só dados de importância operacional mas também do próprio combatente.** Gerir todo este conjunto de meios será um desafio a que todos os atores terão de se adaptar. A aquisição de equipamentos que permitam ser resilientes, robustos e fiáveis, levará a que até para os próprios fabricantes seja algo novo a que **terão de dar respostas, garantindo as condições operacionais, de portabilidade, segurança e interoperabilidade, fatores que são comuns tanto às FFAA como aos serviços críticos.** Para interligação com operadores de comunicações ou a uma infraestrutura própria existe o condicionamento dos pontos de ancoragem, que não são móveis, e cuja interoperabilidade e alcances devem ser bem preparados e planeados. A coordenação entre os vários atores (nacionais ou internacionais) terá um papel essencial neste ponto, sejam eles forças conjuntas no domínio do quadro operacional, ou empresas prestadoras de serviço no domínio dos serviços críticos, formando uma rede maior, em que os interesses se cruzam entre atores. **A relação de confiança entre todos deve ser muito alta, extremamente coordenada e governada.**
Entrevistado	Q4.1 - Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem potenciar **(pontos fortes)** a segurança das redes 5G aquando em uso nas FFAA?
E1	Um dos eixos era que isto devia ser uma **iniciativa joint**. Portanto assumida pelo EMFGA, através da nova estrutura que vai ser criada, as comunicações, espaço, informações e Ciberdefesa. Para quê? Para **evitar depois desenvolvimentos assimétricos**, e isto beneficiava os pontos fortes. Isto podia **mitigar vulnerabilidades** que são, **a falta dinheiro, falta de recursos**, de uma **forma global servir de enabler de comando e controlo, gerida pelo EMGFA.**

	Nós já temos uma história de **formação muito sólida nas FFAA**, selecionava-se **um ramo que desse formação de 5G** a todos os ramos e as **particularidades eram dadas no ramo específico**.
E2	As FFAA ao nível da segurança têm uma elevada cultura e experiência, quer pela capacidade Doutrina, Treino, Pessoal, Infraestruturas. Portanto a **integração de elementos de ligação das FFAA no grupo de trabalho relativo à segurança das redes 5G** é um exemplo recente desta forte presença de cultura de segurança nas FFAA. A questão **da formação e treino nesta área nas FFAA** é também um ponto forte nas FFAA.
E3	A arquitetura das redes 5G ser logo à partida contruída segundo critérios de segurança (security by design), com melhoria do desenho acautelando as questões de guerra eletrónica e análise se sinais SGINT.
E4	As tecnologias 5G podem ter uma série de aplicações militares em potencial, particularmente para **veículos não tripulados, C2, logística, manutenção, realidade aumentada e virtual e sistemas ISR** - que beneficiam de larguras de banda maiores e latências mais baixas. Vai permitir também um **aumento do número de sensores no campo de batalha, tanto no terreno como no próprio combatente, e um aumento da visibilidade por parte do C2, aumentando a quantidade e qualidade da COP**, **bem como a capacidade ISR no terreno**. A capacidade de trocar informação com esta tecnologia aumenta significativamente, o que irá permitir processar, explorar e disseminar informações de um número crescente de sensores permitindo aos comandantes acesso oportuno a dados de inteligência acionáveis, melhorando por sua vez a tomada de decisões operacionais, agilizando as ações no terreno.
Entrevistado	Q4.2 - Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem mitigar as vulnerabilidades **(pontos fracos)** da segurança das redes 5G aquando em uso nas FFAA?
E1	As vulnerabilidades maiores para mim é **a cadeia logística**. A Europa tem dois grandes professores 5G, a Nokia e a Erickson, pertencem a dois países que provavelmente em breve vão juntar-se à NATO, mas já são da União Europeia, portanto aí **ficámos com alguma autonomia estratégica.** As vulnerabilidades é não haver entendimento interno sobre isto.
E2	Uma das estratégias poderá ser **a integração e a parceria neste âmbito com a OTAN e EU**, por forma a criar sinergias no desenvolvimento de investigação e conhecimento que permitam mitigar estas vulnerabilidades, inserindo-se nos vetores da Interoperabilidade, doutrina, organização. Outra estratégia poderá ser por começar esta **tecnologia 5G em ambientes controlados/restritos por forma a ganhar a maturidade** desejada desta tecnologia e desta forma passar posteriormente a incluir em ambiente operacional e ao nível tático, inserindo-se aqui nos vetores da Doutrina, organização, treino e liderança. Outra estratégia é **apostar na formação das pessoas, em pessoas qualificadas, na sensibilização desde os operadores às chefias**, que vai permitir mitigar estas vulnerabilidades de segurança. **O Centro de gravidade desta estratégia são os recursos humanos**.
E3	A questão **do espectro da banda larga**, estão todas comercializadas na europa, não deixando espaço para fins militares. Uma das estratégias seria **acautelar uma faixa de frequência (disponibilidade de espetro) para emergências ou fins militares**, e devia ser acautelado não numa lógica nacional, mas sim nível NATO ou da UE. **Definir muito bem o uso do 5G, o fim a que se destina esta tecnologia. Ter em consideração a fiabilidades dos fornecedores.**
E4	A evolução do ambiente militar deve ser capaz de se comunicar, envolver e operar mais rápido para acompanhar as mudanças do ambiente operacional. A tecnologia 5G poderá alavancar este objetivo, permitindo este novo conceito de operações, **possibilitando que maiores volumes de dados sejam partilhados em tempo quase real por sistemas geograficamente dispersos**. No entanto, o 5G também apresenta um sério risco potencial. Se implementarmos a grande maioria dessas redes e sistemas no 5G, pelas suas capacidades e flexibilidade, **podemos criar uma dependência duma tecnologia que nem todos possuem e, cujos fabricantes ainda estão debaixo de grande escrutínio público.** O **crescimento no número de dispositivos conectados aumenta a potencial "superfície de ataque"** para adversários poderem atingir redes táticas e de suporte, o que **exigirá maior vigilância e segurança entre sistemas**. O maior volume de dados transferidos vai complicar esta tarefa, pois vai tornar mais

	difícil detetar tráfego malicioso, correlacionar eventos e o próprio controlo dos nós 5G duma rede, não só pela sua dispersão geográfica, mas, principalmente, pela sua mobilidade e volatilidade. Existem 3 pontos que deverão ser o foco principal, para além da parte **do controlo do tráfego nas redes**, sendo eles a **cadeia logística de suporte**, não só pela interligação com as forças no terreno mas pelo conjunto de sensores que irão ajudar na operação logística; **as próprias redes 5G**, que pelo fato de **não terem nós fixos trarão dores de cabeço no controlo e organização**, pois assento numa malha de nós mutável em permanência e, por fim, os próprios **terminais ou equipamentos, dependendo do fabricante e a da dúvida que sempre irá subsistir sobre a sua idoneidade**, por muitos testes e verificações de segurança que se lhes façam.
Entrevistado	Q4.3 - Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem reduzir o **risco de ameaças** às redes 5G aquando em uso nas FFAA?
E1	O risco das ameaças é nós não fazermos nada disto. As ameaças **é cadeia logística** é a ameaça de Cibersegurança às redes 5G se não **forem bem arquitetadas e pensadas e isso tem que se definir cenários**. Mas o risco de maiores de ameaças é fazer o deployment com o equipamento, cujo a **cadeia logística não seja segura por nós** e depois ao montar a rede **não calcular os riscos de Cibersegurança, desde o desenho da rede até à sua implementação e não ter processos para monitorizar esse risco**.
E2	A **identificação dos fabricantes confiáveis, certificados e autorizados** para uma futura parceria ou mesmo na questão **da interoperabilidade** entre parceiros da OTAN, EU ou forças militares, deverá estar acautelada por forma a reduzir o risco de ameaças, podendo-se enquadrar nas estratégias para os vetores dos matérias, infraestruturas e interoperabilidade. A definição de uma estratégia, genética e estrutural para a implementação das redes 5G.
E3	Os **fornecedores da tecnologia 5G são sempre os mesmos e traz constrangimentos e da fiabilidade dos fornecedores**. Ou a indústria militar começa a produzir e tem custos elevados. As arquiteturas das redes 5G têm de ser bem idealizadas como vão ser implementadas estas redes 5G, e avançar de forma amadurecida. Quando se entra em guerras híbridas e cada vez mais tecnológica temos de **ser conhecedor desta tecnologia**, e em ambiente militar **a guerra eletrónica pode facilmente empastelar estas redes 5G**, e esta situação tem de ser acautelada.
E4	Existe 4 fatores de risco com grande implicação nos vetores DOTMLPII, nomeadamente naquilo que são os padrões e processos internos das organizações. O conjunto de regras de execução de um conjunto de tarefas deve ser o mais igual e transversal possível entre atores, por forma a que haja **uniformização aos vários níveis**, em que as comunicações desempenham um desses papéis. Outro fator importante é a **maturidade dos equipamentos**. Falamos duma tecnologia relativamente nova, com pouca implantação no mercado e no campo de batalha, e cujos equipamentos ainda não foram totalmente testados. Os controlos e medidas de segurança a implementar devem ser os indicados para uma estrutura deste tipo e devem ser **acrescentados outros controlos complementares**, para salvaguarda e monitorização desta nova tecnologia, o que pode criar alguma entropia à implementação dos sistemas e latências nas comunicações. A tecnologia em si tem muitos desafios que são trabalhados e desenvolvidos diariamente ao nível mundial. **De momento não existem indicadores que nos afirmem de forma perentória e inequívoca que não é uma tecnologia segura**. É uma tecnologia nova, com as suas vicissitudes, e que carece de cuidados suplementares na sua implementação. A sua implementação no âmbito das FFAA poderá ser feita, numa fase inicial, **em ambientes muitos restritos, sem interligação ao mundo civil, suportada nas infraestruturas de comunicações militares próprias.** Assim, mesmo que surjam falhas ainda não conhecidas nesta tecnologia, a informação ficará contida nos nossos sistemas, minimizando o risco ao ambiente operacional. De base iremos cumprir as disposições legais que nos permitam interagir com os nossos parceiros, fornecedores e outras entidades. Ao nível operacional, teremos por base o que for determinado pelas organizações e missões em que participamos tendo como ponto principal garantir a segurança dos dados e das forças e a salvaguarda da missão das FFAA e da soberania nacional.

Entrevistado	Q4.4 - Tendo em consideração os vetores DOTMLPII quais as principais Estratégias identificadas ou a identificar, que permitem **criar oportunidades** de segurança às redes 5G aquando em uso nas FFAA?
E1	As oportunidades aqui, nada se faz disto sem **identificar uma os cenários de risco** e Portugal fez este trabalho. E foi com base nesse relatório que é classificado, e é classificado porque identificámos riscos pertinentes a Portugal. E depois resumimos e contribuímos para a Toolbox da União Europeia aquelas vinte e duas medidas. Agora as oportunidades para a segurança e se aquilo for acautelado ao início com segurança, elas provavelmente **são mais resistentes e por estar virtualizada** e, portanto, por conceito tem muito **mais flexibilidade muito mais alternativas** e provavelmente saia **mais seguro** ainda do que do que os anteriores. Portanto a maior oportunidade aqui eu diria **que é pensar segurança desde o início** não como um acrescente à posteriori. Vamos pensar desde o princípio como pensamos outra coisa qualquer que seja necessária para entregar essa capacidade. E, portanto, se a **rede for concebida de forma densa, alternativa, resiliente** é muito mais difícil o atacante fazer interromper a rede.
E2	A identificação dos fabricantes confiáveis, certificados e autorizados para uma futura parceria. **Parecerias com entidades civis, criar interoperabilidade.** Outra oportunidade, **ao nível do vetor liderança**, é o aproveitamento da invasão da Rússia á Ucrânia e aquilo que foi o início da campanha com um ciberataque direcionado a uma rede de satélites usada pelo governo e agências militares da Ucrânia, em que acabou por afetar dezenas de milhares de utilizadores de internet por toda a Europa, **para consciencializar a população na importância do investimento das forças armadas**, na sua modernização e no reforço da segurança, nomeadamente ao nível do ciberespaço.
E3	**Criar uma política de gestão de espetro a nível europeu e da NATO**. Definir a **finalidade do 5G.**
E4	As tecnologias 5G permitem a operação de várias aplicações potenciais, **incluindo comando e controlo, logística, manutenção, treino, inteligência artificial, realidade aumentada e virtual e sistemas ISR – onde** todos podem se beneficiar de melhores velocidades de dados e menor latência. Com estas melhorias é expectável que a rede 5G gere um ecossistema massivo para a Internet das Coisas (IoT), permitindo dar resposta ao aumento exponencial de dispositivos interligados, conjugando as vantagens trazidas pela maior velocidade, terminais mais pequenos e uma menor latência e custo. A variedade de terminais e tipologia das redes 5G vai obrigar a **implementar métodos e controlos de segurança mais robustos, em que a segurança das comunicações, a autenticação do utilizador, mecanismos de cifra,** vão trazer algumas vantagens pois serão implementadas de raíz na própria rede, traduzindo-se numa vantagem. Embora a **guerra eletrónica possa ser um potencial problema, o 5G pode mudar o cenário de defesa com transmissão e receção instantânea de enormes quantidades de dados, diminuindo o tempo de exposição e a possibilidade de interceção.** Dentro das aplicações operacionais, a comunicação crítica é crucial e deve garantir a funcionalidade necessária, um alto grau de robustez, segurança, blindagem de dados e garantir altos tempos de atividade nas operadoras sem fio existentes, suportada pelas várias tecnologias presentes no terreno, entre forças e na própria ligação à retaguarda, suportada pelo mundo IP, permitindo no próprio campo de batalha a segregação entre redes de utilizadores, onde é possível controlar larguras de banda, medidas de segurança, cifra implementada. A **adoção desta tecnologia será fator diferenciador no moderno campo de batalha, onde o fluxo e superioridade de informação, fatores que dependem da confidencialidade, da integridade e da disponibilidade, trarão vantagens competitivas e operacionais a quem dominar e controlar a tecnologia.**

Apêndice E — Análise da matriz SWOT

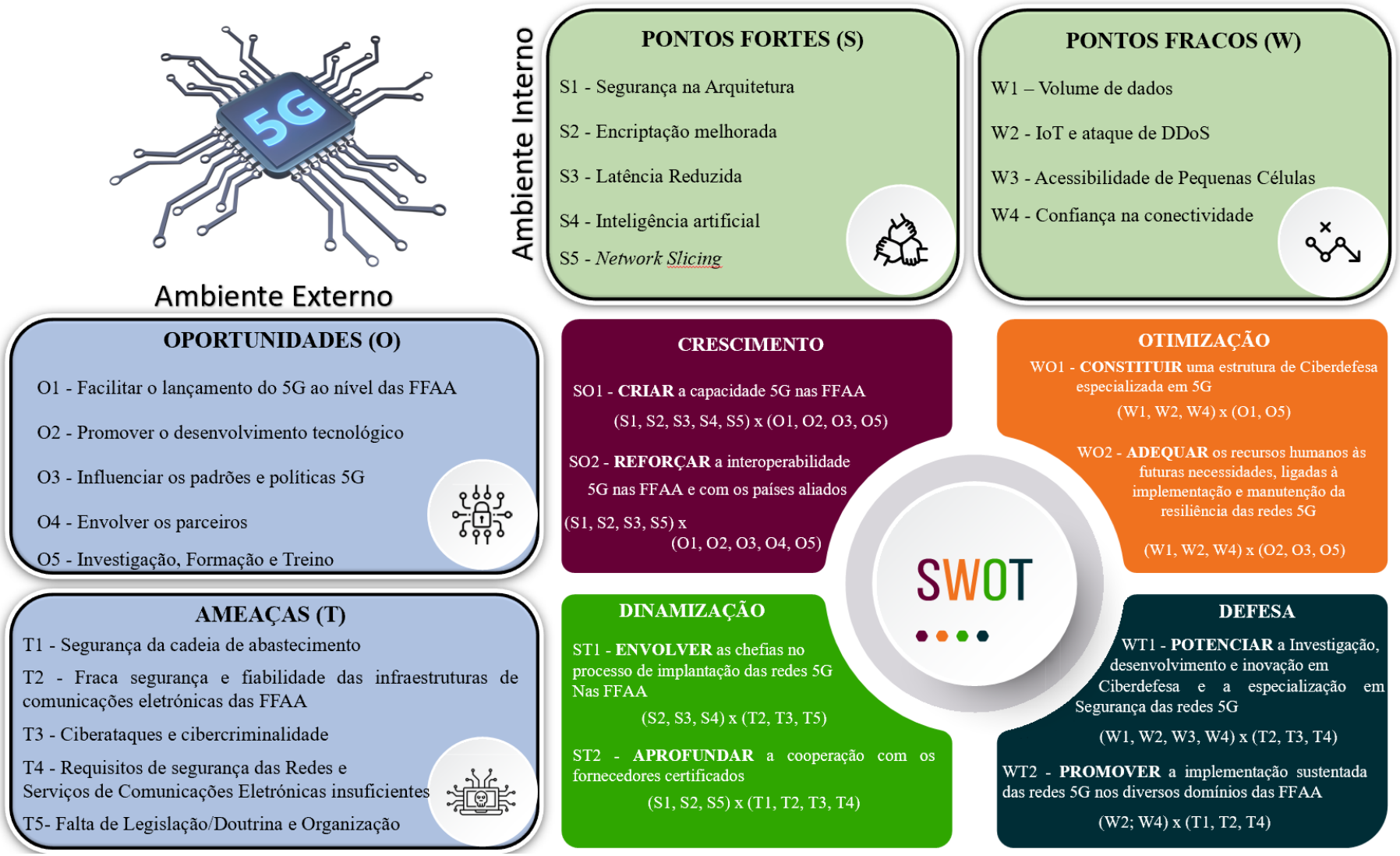


Figura 25 - Análise SWOT