



ESCOLA NAVAL

ta tante de bi-faire



Daniela Filipa Miranda da Silva

O mar como um ambiente de competição estratégica global: a segurança dos cabos submarinos no mundo do Ciberespaço

**Dissertação para o grau de Mestre em Ciências Militares Navais, na
especialidade de Marinha**



**Alfeite
2024**



ESCOLA NAVAL

talant de biëfaire



Daniela Filipa Miranda da Silva

O mar como um ambiente de competição estratégica global: a segurança dos cabos submarinos no mundo do Ciberespaço

**Dissertação para obtenção do grau de Mestre em Ciências Militares Navais,
na especialidade de Marinha**

Orientação de: Capitão-de-fragata Baptista de Sousa

Coorientação de: Capitão-de-mar-e-guerra Palmeiro Ribeiro

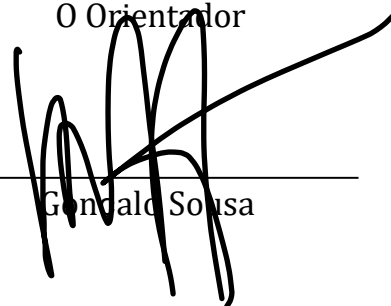
Coorientação de: Professor Doutor Sandro Mendonça

O Aluno Mestrando

Assinado por: **Daniela Filipa Miranda da Silva**
Num. de Identificação: 14041980
Data: 2024.08.27 17:08:24+01'00'

Daniela Silva

O Orientador



Gonçalo Sousa

Alfeite

2024

“I can’t change the direction of the wind, but I can adjust my sails to always reach my destination”.

Jimmy Dean

Aos meus pais, à minha irmã e ao meu namorado,
pelo amor e pelo apoio incondicional, que tudo fazem por mim
e por estarem sempre presentes, seja em que circunstância for.

Agradecimentos

Após estes cinco anos de Escola Naval, nesta ilustre casa mãe que fará sempre parte do meu percurso acadêmico, encontro-me, finalmente, a terminá-lo. Apresento os meus sinceros agradecimentos, aos demais que contribuíram para que não faltasse dedicação, conhecimento e orientação durante esta fase.

Primeiramente gostaria de expressar a minha gratidão ao meu Orientador, CFR EN-MEC Gonçalo Nuno Baptista de Sousa, pela honra e prazer que me deu, em me ter orientado, apesar de todos os desafios que foi tendo presentes ao longo da sua vida, sempre se demonstrou muito presente e disponível para me orientar da melhor forma possível. Pela partilha dos seus múltiplos conhecimentos e valorosos conselhos, fundamentais para a concretização desta Dissertação. A sua incansável orientação foi imprescindível, expressando-lhe assim, um especial agradecimento.

Aos meus Coorientadores, o CMG M Palmeiro Ribeiro e o Professor Doutor Sandro Mendonça, muito obrigado pela partilha e por todo o conhecimento que me transmitiram.

Expresso um especial agradecimento ao Professor Hugo Policarpo, pela sua disponibilidade, tendo sido imprescindível. Muito obrigada por toda a partilha de conhecimentos e pela dedicação demonstrada.

Agradeço ao Professor Doutor Duarte Lynce de Faria, ao Sr. Engenheiro José Barros e ao Dr. Rui Pereira pela disponibilidade prestada e pela partilha de conhecimentos.

Aos meus pais, por serem a base da minha existência, por acreditarem sempre em mim, pela educação, valores e por se terem dedicado à minha formação.

Ao meu namorado, pelo amor incondicional, apoio, dedicação, pela partilha mútua e eterna, por todos estes anos juntos, por tudo.

À minha irmã, sempre presente e sempre pronta para me ajudar no que for preciso, pelo amor, compreensão e por sermos seres iguais e únicos. Ao meu cunhado, por todo o apoio e motivação.

À minha família e amigos, um especial agradecimento, por tudo. Sem todos vocês, não teria sido possível.

Aos meus camaradas do Curso Fernão de Magalhães, por estes cinco anos.

Por fim, expresso a minha gratidão a todos aqueles que, de alguma forma, direta ou indiretamente, contribuíram para a realização deste trabalho.

Resumo

O facto de Portugal exercer jurisdição sob a maior área marítima atlântica da Europa, reforça a necessidade de proteção e segurança dos Cabos Submarinos (CSs), ao nível da segurança marítima e da cibersegurança, uma vez que circulam através destas infraestruturas críticas cerca de 99% do tráfego transatlântico de dados, fazendo parte da crescente dependência tecnológica a nível mundial.

Os Estados dependem fortemente destes cabos no que respeita a interesses de segurança e soberania nacionais, estando estes relacionados com o domínio do ciberespaço, a fim de garantir a sustentabilidade da Sociedade da Informação (SI).

A presente Dissertação de Mestrado, incide essencialmente sobre a segurança dos CSs no mundo do ciberespaço, estando este vulnerável no que toca à cibersegurança da Humanidade devido às ciberameaças, cada vez mais presentes no mundo tecnológico, na medida em que qualquer entidade pode ser alvo de um ciberataque.

Como forma de melhorar a proteção dos CSs, insere-se nesta temática, o projeto *Fibersense*, através de uma tecnologia muito promissora, eficaz e de baixo custo em comparação com as já existentes. Atualmente, o mundo encontra-se em expansão tecnológica, sendo importante salientar o desenvolvimento deste projeto que contribuirá de uma forma bastante significativa para a monitorização, vigilância e deteção submarinas, através desta tecnologia de fibra ótica.

Os resultados obtidos através do uso desta tecnologia de *Distributed Acoustic Sensing* (DAS) ao longo deste projeto pretendem comprovar que a sensibilidade, operacionalidade e fiabilidade do sinal acústico são detetados, garantindo a necessidade de resiliência dos Cabos de Fibra Ótica (CFO) submarinos essenciais para o Conhecimento Situacional Marítimo.

Para proceder à elaboração desta Dissertação, foram pesquisados inúmeros artigos, datados entre 1983 e 2024, nas seguintes bases de dados: *ScienceDirect*, *Google Scholar*, *b-on*, *RCAAP*, *Elsevier*, *ResearchGate* e *IEEE*.

Palavras-chave: Cabos Submarinos, Ciberespaço, Cibersegurança, *Distributed Acoustic Sensing*, Conhecimento Situacional Marítimo

Abstract

The fact that Portugal exercises jurisdiction over the largest Atlantic maritime area in Europe reinforces the need for the protection and security of Submarine Cables (SCs), in terms of maritime security and cybersecurity, since around 99% of them circulate through these critical infrastructures of transatlantic data traffic, being part of the growing technological dependence worldwide.

States depend heavily on these cables regarding to national security and sovereignty interests, which are related to the domain of cyberspace, in order to guarantee the sustainability of the Information Society (IS).

This Master's Dissertation essentially focuses on the security of SCs in the world of cyberspace, which is vulnerable in terms of the cybersecurity of Humanity due to cyber threats, increasingly present in the technological world, as any entity can be the target of a cyberattack.

As a way of improving the protection of SCs, the Fibersense project was inserted into this theme, through a very promising, effective and low-cost technology compared to existing ones. Currently, the world is experiencing technological expansion, and it is important to highlight the development of this project, which will contribute in a very significant way to underwater monitoring, surveillance and detection, through this fiber optic technology.

The results obtained using this Distributed Acoustic Sensing (DAS) technology throughout this project aims to demonstrate the sensitivity, operability and reliability of the acoustic signal to be detected, guaranteeing the need for resilience of submarine Fiber Optic Cables (FOC) essential for the Maritime Situational Awareness.

To proceed with the preparation of this Dissertation, numerous articles were searched, dated between 1983 and 2024, in the following databases: ScienceDirect, Google Scholar, b-on, RCAAP, Elsevier, ResearchGate and IEEE.

Keywords: Submarine Cables, Cyberspace, Cybersecurity, Distributed Acoustic Sensing, Maritime Situational Awareness

Índice

Agradecimentos	VIII
Resumo	X
<i>Abstract</i>	XII
Índice de Figuras	XVII
Índice de Gráficos	XIX
Índice de Tabelas	XXI
Lista de Abreviaturas, Siglas e Acrónimos	XXII
Introdução	1
1.Revisão da Literatura e Enquadramento Conceptual	3
1.1. Contexto Histórico: os cabos submarinos e as comunicações internacionais submarinas	3
1.2. Ligação dos cabos submarinos em Portugal	6
1.3. Constituição e funcionamento dos cabos submarinos	9
1.4. Instalação, conectividade e viabilidade dos cabos submarinos	13
2.Mapeamento geográfico dos cabos submarinos	19
2.1. Enquadramento Jurídico e Cooperação Internacional	21
2.2. A importância da posição geoestratégica de Portugal	24
2.3. A presente conflitualidade e a competição estratégica global	29
3.Segurança dos cabos submarinos	33
3.1. Cibersegurança e segurança marítima	36
3.2. Políticas e Regulamentações no caso de ataques aos cabos submarinos .	40
3.3. Propostas de atuação que garantam a segurança dos cabos submarinos	52
4.Ciberespaço: Organização, Segurança e Defesa	57
4.1. Operações militares no ciberespaço com ligação à OTAN e à Marinha Portuguesa	59
4.2. Criptografia, autenticação e proteção dos dados	65

5.Projeto	<i>Fibersense</i>
.....	69
5.1. Introdução à tecnologia DAS.....	69
5.2. Descrição e objetivos do projeto.....	71
5.3. Especificações do projeto	71
5.3.1. Tanque de Arquitetura Naval.....	72
5.3.2. Cabo de Fibra Ótica submarino.....	73
5.3.3. Altifalante subaquático	73
5.4. Funcionamento do projeto	74
5.4.1. Descrição dos Testes A e dos Testes B.....	75
5.5. Processamento de dados.....	78
5.6. Interpretação dos resultados	79
5.7. Análise final dos resultados	95
Conclusão	101
Limitações do Estudo.....	104
Sugestões de Estudos Futuros	105
Referências Bibliográficas	107
Apêndices.....	127
Apêndice A- Ficheiros transferidos do <i>software</i> DAS da <i>AP Sensing</i>	127
Apêndice B- Código em linguagem de programação <i>python</i> utilizado	129
Apêndice C- Tabela do <i>Excel</i> relativa aos Testes A, posição 1	131
Apêndice D- Código em linguagem de programação <i>python</i> utilizado, relativo aos Testes A, posição 1.....	159
Anexos.....	161
Anexo A- Especificações do Cabo de Fibra Ótica utilizado no projeto	161
Anexo B- Especificações do modelo do altifalante subaquático LL916C	163
Anexo C- Certificado de participação no XI Curso de “Cibersegurança e Gestão de Crises no Ciberespaço”.....	165

Índice de Figuras

Figura 1 - A primeira ligação transatlântica entre a Europa e a América em 1858 .	3
Figura 2 - Primeiro cabo submarino de fibra ótica transatlântico (TAT-8).....	5
Figura 3 - Evolução dos cabos submarinos: fibra ótica, coaxial e telegráfico	5
Figura 4 - Atlantic CAM e as presentes placas tectónicas	8
Figura 5 - Os mais recentes cabos submarinos amarrados em Portugal	9
Figura 6 - Cabo submarino de fibra ótica	10
Figura 7 - Funcionamento e ligação dos cabos submarinos	11
Figura 8 - Segmento seco e molhado do cabo submarino	12
Figura 9 - Configuração do cabo submarino	13
Figura 10 - Processo de instalação de um cabo submarino no leito marinho com recurso da charrua	16
Figura 11 - Instalação de um cabo submarino no leito marinho com recurso a um mergulhador.....	16
Figura 12 - Mapa dos cabos submarinos do ano de 2024	19
Figura 13 - Cabos submarinos operacionais ligados a Portugal correspondentes a 2024	20
Figura 14 - Zonas Marítimas de acordo com a CNUDM.....	22
Figura 15 - Representação da Zona Económica Exclusiva.....	26
Figura 16 - A centralidade Atlântica de Portugal	28
Figura 17 - Cabos submarinos operacionais no Atlântico Norte correspondentes a 2024	30
Figura 18 - Cabos submarinos operacionais no Atlântico Sul correspondentes a 2024	30
Figura 19 - Ilustração do tanque em estudo.....	72
Figura 20 - Gerador de ondas.....	73
Figura 21 - Altifalante subaquático.....	74
Figura 22 - Disposição dos Testes A com o altifalante subaquático na posição 1....	76
Figura 23 - Disposição dos Testes A com o altifalante subaquático na posição 2....	76
Figura 24 - Disposição dos Testes B com o altifalante subaquático na posição 1 ...	77
Figura 25 - Disposição dos Testes B com o altifalante subaquático na posição 2 ...	78
Figura 26 - FBE Data para os Testes A e posição 1.....	81
Figura 27 - FBE Data para os Testes A e posição 2.....	86
Figura 28 - FBE Data para os Testes B e posição 1	89
Figura 29 - FBE Data para os Testes B e posição 2	92

Índice de Gráficos

Gráfico 1 - Média das energias em função da amplitude de potência dos Testes A em P1 (escala linear).....	83
Gráfico 2 - Média das energias em função da amplitude de potência dos Testes A em P1 (escala logarítmica)	84
Gráfico 3 - Média das energias em função da amplitude de potência dos Testes A em P2 (escala linear).....	88
Gráfico 4 - Média das energias em função da amplitude de potência dos Testes A em P2 (escala logarítmica)	88
Gráfico 5 - Média das energias em função da amplitude de potência dos Testes B em P1 (escala linear).....	90
Gráfico 6 - Média das energias em função da amplitude de potência dos Testes B em P1 (escala logarítmica)	91
Gráfico 7 - Média das energias em função da amplitude de potência dos Testes B em P2 (escala linear).....	93
Gráfico 8 - Média das energias em função da amplitude de potência dos Testes B em P2 (escala logarítmica)	94
Gráfico 9 - Média das energias em função da posição dos Testes A em P1	95
Gráfico 10 - Média das energias em função da posição dos Testes A em P2	96
Gráfico 11 - Média das energias em função da posição dos Testes B em P1	97
Gráfico 12 - Média das energias em função da posição dos Testes B em P2	97

Índice de Tabelas

Tabela 1 - Cibersegurança e Ciberdefesa relação com atores e tipos de crime, adaptado de Estruturas de Coordenação Nacional no Ciberespaço.....	40
Tabela 2 - Tipos de ameaças consoante a natureza.....	43
Tabela 3 - Dados reduzidos do Teste A na posição 1	82
Tabela 4 - Valor médio total por coluna.....	85
Tabela 5 - Dados reduzidos do Teste A na posição 2	87
Tabela 6 - Valor médio total por coluna.....	89
Tabela 7 - Dados reduzidos do Teste B na posição 1.....	90
Tabela 8 - Valor médio por coluna	91
Tabela 9 - Dados reduzidos do Teste B na posição 2.....	93
Tabela 10 - Valor médio por coluna	94

Lista de Abreviaturas, Siglas e Acrónimos

ACMA – *Atlantic Cable Maintenance & Repair Agreement*

ACST – ACOS STRAT

AIS – Sistema de Identificação Automático (do inglês *Automatic Identification System*)

AJP – *Allied Joint Publication*

ANACOM – Autoridade Nacional das Comunicações

ANETIE – Associação Nacional das Empresas das Tecnologias de Informação e Eletrónica

AP – Amplitude de Potência

AP Sensing – *Advanced Photonic Sensing*

AT&T – *American Telephone and Telegraph*

AUV – Veículo Autónomo Subaquático (do inglês *Autonomous Underwater Vehicle*)

BMH – *Beach Manhole*

BD – *Big Data*

BU – *Branching Units*

CAM – Continente, Açores, Madeira

CCD – Centro de Ciberdefesa

CCDCOE – *NATO Cooperative Cyber Defence Centre of Excellence* (Centro de Excelência para a Ciberdefesa Cooperativa da OTAN)

CCICE – Centro de Comunicações e Informação, Ciberespaço e Espaço

CCOM – Comando Conjunto para as Operações Militares

CEDN – Conceito Estratégico de Defesa Nacional

CEMA – Chefe de Estado Maior da Armada

CERT – *Computer Emergency Response Team*

CFO – Cabo de Fibra Ótica

CIRC – *Computer Incident Response Capability*

CISMIL – Centro de Informações e Segurança Militares

CLS – *Cable Landing Station*

CNCS – Centro Nacional de Cibersegurança

CNPCE – Conselho Nacional de Planeamento Civil de Emergência

CNUDM – Convenção das Nações Unidas sobre o Direito do Mar (do inglês *United Nations Convention on the Law of the Sea* – UNCLOS)

COCiber – Comando de Operações de Ciberdefesa

COI – Comissão Oceanográfica Intergovernamental

COMNAV – Comando Naval

CPNI – Centro de Proteção Nacional de Infraestruturas (do inglês *Centre for the Protection of National Infrastructure*)

CSs – Cabos Submarinos

CSIRT – *Computer Security Incidents Response Team*

CSRIC – *Communications Security, Reliability and Interoperability Council*

CSSC – Conselho Superior de Segurança do Ciberespaço

C2 – Comando e Controlo

DAS – Detecção Acústica Distribuída (do inglês *Distributed Acoustic Sensing*)

DCs – *Data Centers*

DGPM – Direção-Geral de Política do Mar

DITIC – Direção de Tecnologias de Informação e Comunicações

DL – *Deep Learning* (Aprendizagem Profunda)

DoD – *Department of Defense*

DOTMLPI-I – Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade

DR – Diário da República

DWDM – *Dense Wavelength Division Multiplexer*

EES – Estratégia Europeia de Segurança

EMA – Estado Maior da Armada

EMGFA – Estado Maior General das Forças Armadas

EMSA – *European Maritime Safety Agency*

EN – Escola Naval

ENISA – Agência da União Europeia para a Cibersegurança (do inglês *European Union Agency for Cybersecurity*)

ENSC – Estratégia Nacional de Segurança do Ciberespaço

EUA – Estados Unidos da América

FFAA – Forças Armadas

FOCC – *Foreign Owned or Controlled Companies*

FPC – Fundação Portuguesa das Comunicações

GB – *Gigabyte*

GPS – Sistema de Posicionamento Global (do inglês *Global Positioning System*)

GRP – Governo da República Portuguesa

HMS – *Her Majesty's Ship*

IA – Inteligência Artificial

IC – Infraestrutura Crítica

ICPC – *International Cable Protection Committee*

IDN – Instituto da Defesa Nacional

IOC – *Intergovernmental Oceanographic Commission*

IPMA – Instituto Português do Mar e da Atmosfera

ISO/ IEC – *International Organization for Standardization/ International Electrotechnical Commission*

ISPS Code – Código Internacional para a Proteção dos Navios e das Instalações Portuárias (do inglês *International Ships and Port Facility Security Code*)

IXP – *Internet Exchange Point*

JTF – Força Tarefa Conjunta (do inglês *Joint Task Force*)

MDN – Ministério da Defesa Nacional

m – Metros

ML – *Machine Learning* (Aprendizagem Automática)

NMS – *Network Management System*

NOAA – *National Oceanic and Atmospheric Administration*

OCAD – Órgão Central de Administração e Direção

OMM – Organização Meteorológica Mundial

OMI – Organização Marítima Internacional

ONGs – Organizações Não-Governamentais

ONU – Organização das Nações Unidas

OTAN – Organização do Tratado do Atlântico Norte (do inglês *North Atlantic Treaty Organization* – NATO)

PCA – Publicações de Comunicações da Armada

PFE – *Power Feed Equipment*

PIC – Proteção de Infraestruturas Críticas

PICI – Proteção das Infraestruturas Críticas da Informação

PJ – Polícia Judiciária

PLATCON – Plataforma continental

PoP – *Point of Presence*

RA – Revista da Armada

RCM – Resolução do Conselho de Ministros

RGPD – Regulamento Geral sobre a Proteção de Dados

ROV – Veículos Controlados Remotamente (do inglês *Remotely Operated Vehicle*)

SAR – Busca e Salvamento Marítimo (do inglês *Search And Rescue*)

SCI – Infraestrutura de Cabos Submarinos (do inglês *Submarine Cables Infrastructure*)

SI – Sociedade da Informação

SIC – Sistemas de Informação e Comunicações

SICA – Sistemas de Informação e Comunicação Automatizados

SIED – Serviço de Informações Estratégicas de Defesa

SIM – Serviço de Informações Militares

SIRP – Sistema de Informações da República Portuguesa

SMART – Monitorização Científica e Telecomunicações Fiáveis (do inglês *Scientific Monitoring And Reliable Telecommunications*)

SOLAS – *Safety Of Life At Sea*

STI – Superintendência das Tecnologias da Informação

SUA *Convention* – Convenção para a Supressão de Atos Ilícitos Contra a Segurança da Navegação Marítima (do inglês *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation*)

TAT – *Trans-Atlantic Telephone*

TELCON – *The Telegraph Construction and Maintenance Company*

TI – Tecnologias da Informação

TIC – Tecnologias da Informação e Comunicação

UE – União Europeia

UIT – União Internacional das Telecomunicações (do inglês *International Telecommunication Union* – ITU)

UNCLOS – Convenção das Nações Unidas para o Direito do Mar (do inglês *United Nations Convention on the Law of the Sea*)

UNEP – *United Nations Environment Programme* (em português Programa das Nações Unidas para o Ambiente – PNUA)

UNESCO – *United Nations Educational, Scientific and Cultural Organization*

ZEE – Zona Económica Exclusiva

Introdução

A posição geoestratégica do espaço marítimo impõe grandes desafios no que concerne à segurança e defesa a nível nacional. Nestes espaços marítimos encontram-se infraestruturas vitais para a circulação de comunicações eletrónicas internacionais e para a *internet* em particular, que carecem de uma adequada vigilância e segurança marítima.

Os Cabos Submarinos (CSs) representam a espinha dorsal da comunicação global (Deloitte Technology, 2021), pois, cerca de 99% do tráfego internacional de dados é feito através desta rede de cabos (Bischof et al., 2018; Bueger et al., 2022). Há cerca de 150 anos que estas infraestruturas se tornaram o próprio meio de comunicação transoceânica. Desde o aparecimento dos CSs, o que remota para o século XIX, que estes foram acompanhando as mudanças do conhecimento tecnológico, de inovação e adaptação às necessidades crescentes de um mundo em progressiva e contínua globalização (Rollo, 2013), na medida em que foram evoluindo até ao presente século XXI. Atualmente, já existem tecnologias muito mais avançadas de fibra ótica (Thomas et al., 2015). Estes cabos têm sido, ao longo dos anos, fundamentais para a globalização e troca de informações, mas com a crescente dependência da sociedade moderna em relação aos serviços digitais, a segurança dos CSs tornou-se uma preocupação crítica. Estes são conhecidos, por esse motivo, como infraestruturas críticas de comunicações a nível mundial. Mesmo segundo esta citação, “Além da utilização para fins civis, os países dependem dos CSs para a segurança nacional” (Bueger et al., 2022, p. 12), a segurança destas infraestruturas é questionada devido aos riscos, como ciberameaças ou ciberataques e, ainda, ataques físicos. Contudo, a cibersegurança é considerada uma prioridade nacional na resposta às ciberameaças. A cibersegurança uma vez que se define como a proteção de sistemas, redes e dados contra ciberataques, é essencial para a integridade de IC incluindo os CSs. Posto isto, torna-se uma preocupação constante devido ao fracasso na proteção do fluxo das informações (Nunes, 2022; Weiss & Jankauskas, 2019).

A presente investigação justifica-se pelo contributo que pretende oferecer quanto ao tema da segurança dos CSs, explorando, desenvolvendo e sugerindo medidas de proteção para a preservação destas infraestruturas de grande relevância. Além disso, busca analisar e investigar diversos assuntos a nível global relacionados com este tema. Resultando deste facto, a grande Questão Central presente nesta Dissertação, de uma

forma intrínseca no texto: “Considerando os cabos submarinos no domínio do ciberespaço, como infraestruturas críticas de comunicação, estarão estes devidamente seguros na atual era digital?”

Quanto à metodologia seguida, na presente Dissertação, a sustentação teórica baseou-se primeiramente numa criteriosa e exaustiva recolha de informações tendo em consideração todos os objetivos definidos, com o intuito de serem cumpridos e também para a síntese da bibliografia existente sobre o tema proposto, propondo, ainda estratégias para melhorar a segurança destas infraestruturas.

Relativamente à organização da presente Dissertação, encontra-se estruturada em cinco capítulos principais, sendo: a Revisão da Literatura e Enquadramento Conceptual, de modo a estudar com profundidade a história dos CSs, o Mapeamento geográfico dos cabos submarinos, em que se estuda de uma forma mais objetiva, as questões interligadas com a conflitualidade, assim como o posicionamento estratégico e a cooperação internacional relacionada com estas infraestruturas. No capítulo seguinte, a Segurança dos cabos submarinos, analisa-se de forma precisa e concreta a proteção destas infraestruturas. De seguida, o capítulo referente ao Ciberespaço: Organização, Segurança e Defesa, que é meramente explicativo tendo em conta o nome do capítulo e, por último, um capítulo referente ao Projeto *Fibersense*. Contendo, no final do presente trabalho, as conclusões em que se abordam limitações do estudo e sugestões de estudos futuros relacionados com a área em questão.

Salienta-se ainda o facto de toda a estrutura da presente Dissertação ser seguida de acordo com as “Normas para a elaboração de dissertações, trabalhos de projeto ou relatórios” de 2015 e a referência bibliográfica utilizada ter sido, segundo o *APA Style*¹.

¹ American Psychological Association (APA), *Publication Manual*, 6th edition, Washington, 2010.

1. Revisão da Literatura e Enquadramento Conceptual

1.1. Contexto Histórico: os cabos submarinos e as comunicações internacionais submarinas

Em meados do século XIX surgiram várias descobertas na Europa, destacando-se as descobertas científicas e os avanços na área da matemática que promoveram o uso das telecomunicações pelo mundo através dos Cabos Submarinos (CSs) (Carter et al., 2009). A história dos CSs e das comunicações intercontinentais passa por três diferentes eras de progressão, com o aparecimento dos cabos telegráficos, no século XIX, seguidamente, no século XX, com o aparecimento dos cabos coaxiais e, por último, com os cabos de fibra ótica, também no século XX até à atualidade (Msongaleli, 2015; Carter et al., 2009; Burns, 2009).

Assim, em 1850, surgiu o primeiro cabo telegráfico submarino que ligou França a Inglaterra (Reino Unido) através do estreito de Dover (Canal da Mancha) (Matis, 2012; Hayes & Schwartz, 2008; Brake, 2019). Este tipo de cabo era composto somente por um condutor de cobre revestido por um isolante e o retorno do sinal transmitido era feito através do mar (Carvalho, 2023).

A rede mundial de CSs começou a ser criada desde então, tendo sofrido diversas melhorias ao longo do tempo até que, no ano de 1858, instalaram um cabo telegráfico no oceano Atlântico, a primeira ligação transatlântica, representada na **Figura 1**. Esta instalação permitiu a comunicação entre a Europa e a América, tendo esta ligação apenas funcionado durante um curto período (três semanas) (Clark, 2016).

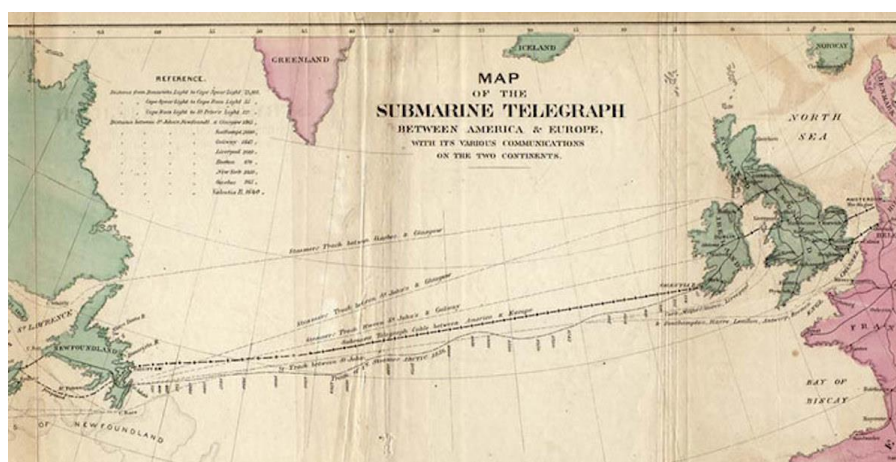


Figura 1 - A primeira ligação transatlântica entre a Europa e a América em 1858

(Retirado de English, 2020)

Este cabo telegráfico submarino transatlântico foi posteriormente substituído em 1866, possuindo uma velocidade de comunicação oitenta vezes superior à do cabo anteriormente instalado, tendo ligado pela primeira vez os dois continentes de uma forma duradoura e eficaz (Hayes & Schwartz, 2008). Ainda durante o ano de 1858, existiam mais de trinta conexões submersas regionais, sendo a mais extensa a do Mar Negro (Finn & Yang, 2009).

Contudo, ao longo do século XX, os cabos telegráficos submarinos foram perdendo o interesse, dado que, havia a necessidade de aumentar a capacidade de comunicações internacionais. Estes cabos tiveram uma grande concorrência, a telegrafia sem fios e as primeiras comunicações telefônicas via rádio, tendo sido substituídos pelos cabos coaxiais submarinos, que permitiam, além da transmissão do serviço telegráfico, a transmissão do serviço telefônico. No ano de 1956, foi colocado o primeiro cabo submarino coaxial transatlântico, o *Trans-Atlantic Telephone 1* (TAT-1) (Hayes & Schwartz, 2008; Vilela, 2016; FPC, 2022). Cabo esse dotado de uma maior capacidade de comunicação, possuindo maior amplificação de sinal ao longo da rota do cabo, localizada em repetidores submarinos e ainda, uma menor atenuação e dispersão (FPC, 2022). A criação deste cabo exigiu um grande investimento efetuado por um consórcio entre três empresas, uma americana *American Telephone and Telegraph* (AT&T), uma inglesa *General Post Office* e uma canadiana *Canadian Overseas Telecommunications Corporation*, permitindo a ligação da Escócia à Terra Nova (Canadá). Esta ligação possibilitou assim, uma amplificação de sinal através de repetidores submarinos, o que tornou o sinal mais robusto e com menos perdas significativas de sinal (Vilela, 2016). O TAT-1 operou sem nenhuma falha durante vinte e dois anos (Hayes & Schwartz, 2008).

Posteriormente, com a necessidade crescente de melhorar e aumentar as comunicações internacionais, em 1988, foi instalado o primeiro cabo submarino de fibra ótica transatlântico, TAT-8, utilizando pares de fibras óticas para melhorar drasticamente a largura de banda de transmissão do sinal, como se pode observar na **Figura 2**, projetado para empregar a técnica de Multiplexação Densa por Divisão de Comprimento de Onda (DWDM), fazendo a interligação entre os Estados Unidos da América (EUA) com a Grã-Bretanha e a França (Beaufils, 2000; FPC, 2017). A técnica DWDM é uma tecnologia inventada com o propósito de aumentar a largura de banda das redes de fibra existentes e combinar os sinais dos dados provenientes de diferentes fontes num único par de fibras óticas, mantendo a separação completa do fluxo de dados. O sistema TAT-8 (**Figura 2**) tinha a capacidade de suportar quarenta mil conversas telefônicas simultâneas, usando a

tecnologia digital (FPC, 2017; Dutton, 1998).



Figura 2 - Primeiro cabo submarino de fibra ótica transatlântico (TAT-8)

(Retirado de FPC, 2017)

No decorrer dos anos, o mundo dos CSs sofreu um enorme crescimento devido não só ao desenvolvimento tecnológico e conhecimento científico, como também ao aparecimento da fibra ótica, registado como um grande marco na história dos CSs (Davenport, 2012).

A **Figura 3** destaca a crescente e necessária evolução que os CSs foram sofrendo ao longo do tempo, onde se pode observar, respetivamente, um cabo de fibra ótica submarino, um cabo submarino coaxial e um cabo telegráfico submarino, salientando que a única diferença entre os três cabos consiste no género do condutor de sinais (Vilela, 2015; Carvalho, 2023).



Figura 3 - Evolução dos cabos submarinos: fibra ótica, coaxial e telegráfico

(Adaptado de Vilela, 2015)

1.2. Ligação dos cabos submarinos em Portugal

No século XIX, as restrições tecnológicas demandavam pontos de retransmissão, enquanto a localização geográfica dos territórios portugueses se impunha devido à elevada importância estratégica como ponto de convergência e de interligação. O posicionamento geoestratégico de Portugal, que irá ser abordado no decorrer da presente dissertação, caracteriza-se como uma vantagem, tendo um papel crucial nas ligações transatlânticas por CSs (Carvalho, 2023).

Devido a esta vantagem, em 1870, foi lançado o primeiro cabo telegráfico submarino pertencente à *Falmouth Gibraltar and Malta Telegraph Company, Ltd.*, do grupo de empresas *The Telegraph Construction and Maintenance Company* (TELCON), pelo navio HMS *Hibernia*. O lançamento do CS foi feito a partir de Carcavelos, chegando a *Porthcurno*, Inglaterra, onde após alguns dias se efetuou a união definitiva do cabo com 824 milhas náuticas de extensão (Vilela, 2016; Matos, 2020). Anos antes houve várias tentativas de assinaturas de contratos para a instalação de CSs, mas sempre sem sucesso (Vilela, 2016).

As ligações telegráficas não só com Inglaterra e Gibraltar, mas também com Malta, Índia e China foram originadas na primeira exploração dos dois cabos (Gibraltar-Carcavelos e Carcavelos-*Porthcurno*), permitindo assim a continuidade da rede mundial de CSs (Vilela, 2016; Carvalho, 2023).

Aproveitando esta conjuntura, Portugal integrou-se numa rede global em constante evolução, desenvolvendo várias soluções para atender às exigências de crescimento do tráfego com os territórios sob administração e o tráfego terminal internacional. Carcavelos (Continente), Horta (Açores), Funchal (Madeira) e São Vicente (Cabo Verde), devido à posição geográfica, em pleno oceano Atlântico e a meio caminho entre a América do Norte e a Europa, foram as principais estações portuguesas de CSs internacionais (FPC, 2022).

Em 1999, foi criado o Anel Continente-Açores-Madeira (Anel CAM), desenvolvido para atender à necessidade de comunicação no país (ligação doméstica que complementava as outras ligações terrestres no Continente, nos Açores e na Madeira), ocupando metade do Atlântico Norte (RCM n.º 19/2013, 2013; Mendes, 2020; Howe et al., 2019), de modo a permitir que “A geografia do espaço nacional, definida pelo «triângulo estratégico» formado pelo território continental e pelos arquipélagos da Madeira e dos Açores, valoriza, naturalmente, a Europa e o Atlântico. A história confirma

a vocação universalista de Portugal” (RCM n.º 19/2013 de 5 de abril, 2013, p. 1985). Devido à extensa dimensão da Zona Económica Exclusiva (ZEE), torna-se importante a constante monitorização e vigilância marítima a fim de proteger toda a envolvente, incluindo o próprio sistema *Atlantic CAM*. Para este fim, em complemento à utilização de sensores submersos no *Atlantic CAM* como um SMART Cable, encontra-se em estudo a tecnologia do DAS, referente ao projeto *Fibersense*, no qual se encontra em estudo a capacidade para apoiar a monitorização e vigilância marítima das águas costeiras, abrangendo parte da ZEE² e poderá vir a ter capacidade para a criação de um sistema de alerta quanto à deteção dos navios que a atravessem.

Uma vez que os CSs têm um prazo de vida útil, normalmente, de 25 anos por contrato, segundo a (RCM n.º 104/2022 de 2 de novembro, 2022)³ “A obsolescência dos referidos cabos está estimada ocorrer nos anos de 2025 (entre Portugal continental e Madeira), 2024 (entre Portugal continental e Açores) e 2028 (entre Açores e Madeira), pelo que preparar a sua substituição atempada constitui prioridade essencial” (RCM n.º 104/2022 de 2 de novembro, 2022, p. 8), estima-se que, em 2026, com a liderança das Infraestruturas de Portugal, se encontre em funcionamento o novo Anel CAM, o *Atlantic CAM*, como se pode observar na **Figura 4**. Este sistema terá uma componente inovadora, *Scientific Monitoring And Reliable Telecommunications* (SMART), de acordo com o determinado pelo Governo da República, que, segundo uma comunicação do Governo dos Açores:

“constituindo-se o novo Anel, como o maior observatório subaquático do mundo, que irá permitir o estudo de matérias ligadas ao mar, aos fenómenos sísmicos, aos fenómenos vulcânicos e às alterações climáticas, favorecendo a fixação de comunidades científicas nas regiões autónomas e potenciando o desenvolvimento de projetos e da economia regional” (Governo dos Açores, 2022).

A fim de garantir tanto a interligação entre os três, como a deteção sísmica e a monitorização climática e ambiental (Barros, 2024; Governo dos Açores, 2022; RCM n.º 104/2022, 2022).

² Uma vez que a ZEE corresponde à zona marítima até 200 milhas da linha de costa.

³ A Resolução do Conselho de Ministros n.º 104/ 2022 é um diploma legal que autoriza, desde o dia 2 de novembro de 2022, “a Infraestruturas de Portugal, S.A., a lançar procedimentos pré-contratuais e contratuais necessários à implementação do sistema de cabos submarinos que integram o *Atlantic CAM*” (RCM n.º 104/2022 de 2 de novembro, 2022, p. 8).

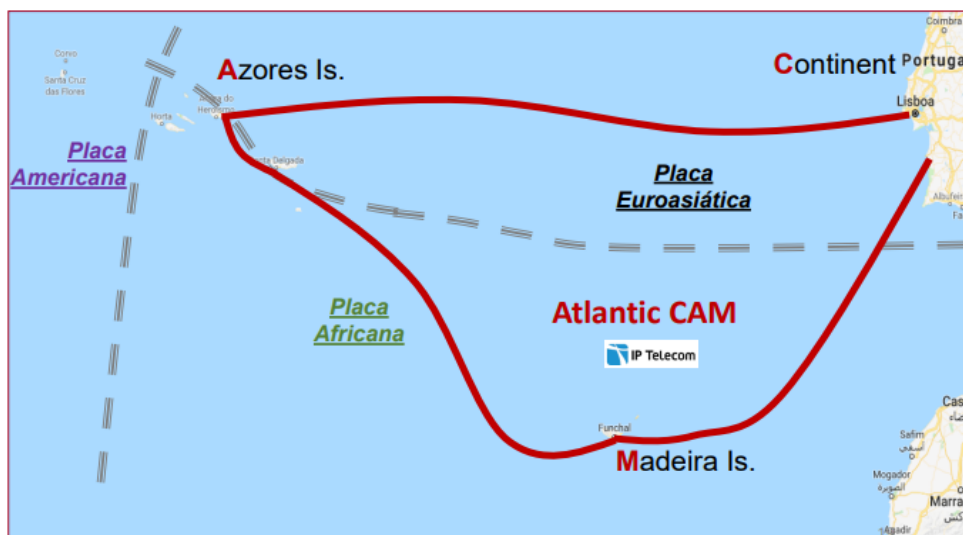


Figura 4 - Atlantic CAM e as presentes placas tectónicas

(Retirado de Barros, 2024, p. 10)

O facto do *Atlantic CAM* poder estar situado próximo de três placas tectónicas (Placa Americana, Placa Euroasiática e Placa Africana) e possuir a componente SMART, possibilita a capacidade de emissão de avisos precoces à população no que concerne a ocorrência de tsunamis e sismos (Barros, 2024). Esta tecnologia consiste numa grande evolução no que respeita à capacidade de avaliação e de alarme de potenciais fenómenos naturais, devido aos conjuntos de sensores de temperatura e sensores de pressão que auxiliam na medição da coluna de água. Acrescenta-se ainda a existência de acelerómetros para deteção da vibração sísmica, estando estes espalhados pelo anel, sendo capazes de detetar os movimentos dos fundos oceânicos (Barros & Bernardino, 2024).

A iniciativa SMART é liderada por uma Força Tarefa Conjunta (JTF) composta por três organizações das Nações Unidas: a União Internacional de Telecomunicações (ITU), a Organização Meteorológica Mundial (OMM) e a Comissão Oceanográfica Intergovernamental da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO-IOC). A JTF é responsável por traçar um caminho para a implementação de capacidades de monitorização, através da iniciativa neste parágrafo abordada, em novas instalações de cabos em todo o mundo, ou seja, promover a utilização de CSs SMART (Howe et al., 2019; ANACOM [Autoridade Nacional de Comunicações], 2021).

De modo a contextualizar a ligação dos CSs em Portugal, é crucial mencionar a mais recente tecnologia de CSs que amarram em Portugal, sendo os seguintes: o

ELLALINK que foi estabelecido em 2021, o EQUIANO estabelecido em 2023, o 2AFRICA estabelecido no presente ano de 2024 e estão ainda previstos amarrar em Portugal, no futuro, até 2026 (inclusive), os seguintes CSs, o MEDUSA *Submarine Cable System* e o Olisipo em 2025 e ainda, o PISCES, o *Atlantic CAM* e o NUVEM com previsão para 2026, como se pode observar na **Figura 5** (Barros, 2024).

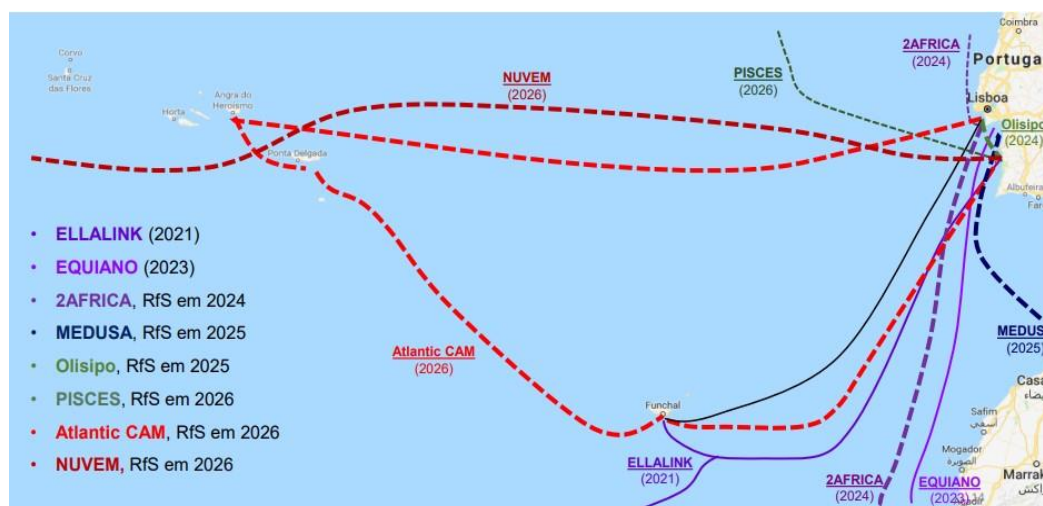


Figura 5 - Os mais recentes cabos submarinos amarrados em Portugal

(Retirado de Barros, 2024, p. 14)

1.3. Constituição e funcionamento dos cabos submarinos

Os atuais CSs possuem uma tecnologia de fibra ótica extremamente fina e caracterizada pela capacidade de transmissão de enormes quantidades de informação em forma de pulsos de luz com uma capacidade de transmissão de dados muito superior à dos satélites (Matis, 2012; Monteiro, 2019; Thomas et al., 2015).

As fibras óticas encontram-se rodeadas por gel podendo ser composto por parafina (composto à base de petróleo), com posteriores camadas de proteção e isolamento que garantem a resistência deste tipo de cabos. Associados às fibras óticas existem condutores de cobre ou alumínio para a alimentação de energia aos repetidores. As fibras óticas e os condutores de energia elétrica são cobertos por um revestimento impermeável de polietileno (ou policarbonato) que impedem a penetração de água. Envolvendo esse revestimento, consoante o nível de proteção mecânica necessária (segundo a profundidade a que o cabo é instalado, isto é, quanto mais profundo, menor a necessidade de proteção mecânica), existe uma armadura protetora de aço possuindo uma grande

resistência. Por fim, as camadas são cobertas por um revestimento externo de polietileno (ou polipropileno), como se pode observar na **Figura 6** (Dutton, 1998; Sechrist, 2010).



Figura 6 - Cabo submarino de fibra ótica

(Adaptado de Bischof et al., 2018, p. 79)

Todos estes materiais garantem diversas qualidades e benefícios, como: boa resistência a efeitos ambientais, isolamento eficaz, boa flexibilidade e excelente resistência à tração e esmagamento (Hopper & Drew, 2009).

A estrutura do CS de fibra ótica deve ser constituída por materiais fortes e leves (Frasca & Galantini, 2023).

O princípio de transmissão nos CSs é extremamente rápido⁴ e eficiente uma vez que o meio de transmissão é constituído por fibras óticas. A fibra ótica é um filamento flexível, composta por sílica (vidro) com uma elevada transparência e revestida por uma camada refletora que permite a reflexão dos sinais luminosos ao longo dos CSs, evitando-se perdas significativas na transmissão do sinal (Eleftherakis & Vicen-Bueno, 2020). Quando um sinal luminoso é transmitido por um *laser*, o sinal convertido num pulso luminoso percorre as fibras sofrendo várias reflexões nas paredes da fibra ótica até chegar ao recetor onde são reconvertidos em dados digitais (Vilela, 2016). Não sendo a fibra 100% transparente, haverá perdas na transmissão, acrescentando perdas pelas reflexões nas próprias paredes das fibras (as reflexões não são absolutas) e o sinal luminoso vai perdendo intensidade ao longo da fibra ótica pois, possuem ainda um comprimento elevado, assim, são necessários repetidores de sinal em intervalos regulares (cerca de 50

⁴ Cerca de 2/3 da velocidade da luz em espaço livre, ou seja, cerca de 200.000 km/s.

a 80 km) para que o sinal transmitido seja regenerado ao longo do trajeto do cabo. Estes repetidores amplificam óticamente o sinal e permitem restabelecer a intensidade mínima do sinal ótico até ao próximo repetidor, e assim sucessivamente até à outra extremidade do cabo (Vilela, 2016). A fonte de alimentação de energia remota do sistema de CSs é fundamental nas *Cable Landing Stations* (CLSs) e o funcionamento dos repetidores dependem das mesmas fontes (Global Marine, 2018).

Uma vez que já se conhecem os constituintes dos CSs, salienta-se a importância de abordar também as CLSs, ou seja, as estações de amarração dos CSs em terra, podendo-se observar na **Figura 7** (Davenport, 2012; Davenport, 2015).

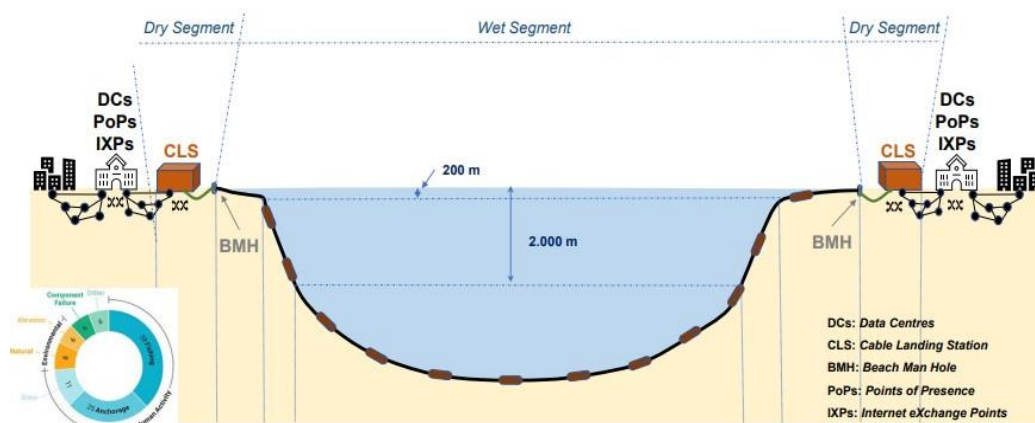


Figura 7 - Funcionamento e ligação dos cabos submarinos

(Retirado de Barros, 2024, p. 30)

Estas estações são portos de entrada e saída de dados. Mais detalhadamente, enviam dados para o mar, recebem dados vindos do mar e enviam-nos para locais em terra onde os dados são armazenados e processados. As CLSs são a interface entre a transmissão de dados entre a terra e o mar, servindo como porta de entrada para redes de comunicações terrestres onde se localizam os *Point of Presence* (PoP), os *Internet Exchange Points* (IXPs) e os *Data Centers* (DCs) que servem os consumidores (Barros, 2024).

As CLSs têm uma elevada importância, não só na baixa latência⁵ (Barros, 2017),

⁵ A latência é caracterizada como o tempo desde que uma solicitação demora para ser transferida de um ponto até ao outro, ou seja, o tempo de processamento e o tempo de propagação de um certo conteúdo (Barros, 2024).

como também, na elevada intensidade de transmissão⁶ dos sinais de telecomunicações internacionais, servindo como porta de entrada para redes de comunicações terrestres através de um PoP onde recebe e transmite sinais para outras ligações submarinas ou terrestres (Communications Security, Reliability and Interoperability Council [CSRIC], 2016; Davenport, 2015; Matis, 2012).

De acordo com o que se encontra representado na **Figura 8**, as CLSs podem ainda incorporar sistemas que permitem fazer a gestão da rede, *Network Management Systems* (NMS) para monitorizar e controlar as operações e o tráfego de dados, assim como o equipamento de alimentação de energia, o *Power Feed Equipment* (PFE) sendo que este fornece a alimentação vinda da estação terminal, em corrente contínua elétrica diretamente através do cabo para alimentar os repetidores dos CSs (Centre for the Protection of National Infrastructure [CPNI], 2006; CSRIC, 2016; Davenport, 2015).

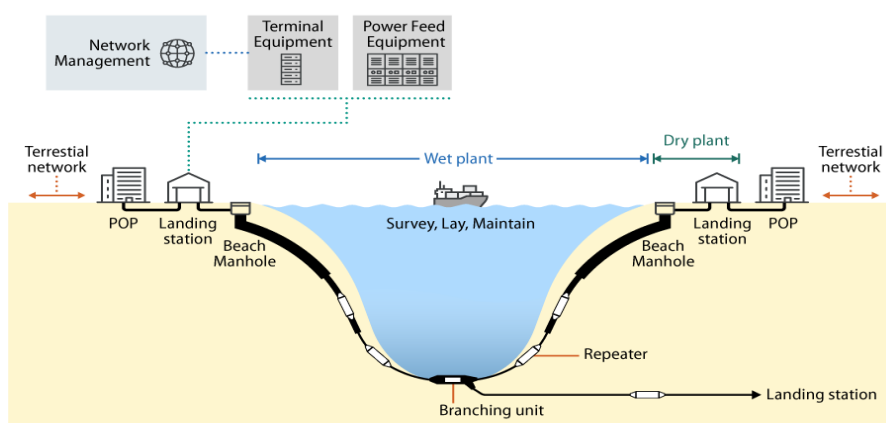


Figura 8 - Segmento seco e molhado do cabo submarino

(Retirado de Gallagher, 2022, p. 5)

Os centros de dados, DCs, estão ligados direta ou indiretamente às CLSs, ou seja, aos CSs, estando os DCs instalados em terra mas sempre desejavelmente próximos das CLSs, interligados às mesmas por redes terrestres (Barros, 2024). Os DCs permitem o armazenamento e processamento de dados (Roach, 2014; Starosielski, 2015).

Os CSs, atendendo à **Figura 7**, na amarração a terra, atravessam a praia (enterrados) e estão ligados a um *Beach Manhole* (BMH)⁷, sendo este a primeira caixa de visita no percurso até chegar à CLS que se identifica como um edifício terminal em terra

⁶ Elevada intensidade de transmissão, neste contexto, significa sem interrupções, com uma transmissão contínua.

⁷ *Beach Manhole* é uma estação de conexão, que se encontra enterrada na costa e que permite a conexão do término do CS, ao cabo terrestre (CSRIC, 2016; Gallagher, 2022).

(CPNI, 2006; Davenport, 2012; Davenport, 2015; Starosielski, 2015).

Atendendo ao facto de pertencerem ainda ao sistema dos CSs, as unidades que se encontram dentro de água, caracterizados como *wet plant* e as unidades que se encontram a seco são as *dry plant*, segundo a **Figura 8**, dos quais fazem parte o troço entre a CLS e o BMH, os cabos propriamente ditos, os repetidores submarinos e as *Branching Units* (BUs). As unidades de ramificação, encontram-se representadas nas **Figura 8** e na **Figura 9**, mas mais detalhadamente na **Figura 9**, onde se compreende a configuração dos CSs de uma forma mais simples. Estas permitem redireccionar os sinais dentro de água e a posterior conexão de vários CSs (CSRIC, 2016; Starosielski, 2015).

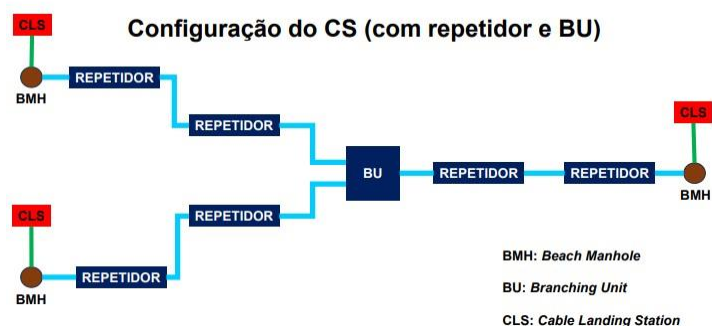


Figura 9 - Configuração do cabo submarino

(Retirado de Barros, 2024, p. 25)

Contudo, após a perceção da ligação dos CSs e atendendo à **Figura 7**, os CSs partindo da CLS, entram no mar muitas vezes enterrados (próximos de terra) e são depositados ou ainda podem ser enterrados a grandes profundidades (na região CAM atinge-se cerca de 5.000 metros (m) de profundidade) (Matis, 2012).

1.4. Instalação, conectividade e viabilidade dos cabos submarinos

Os CSs possuem uma elevada complexidade técnica e possuem ainda diversos componentes com uma elevada tecnologia que exigem um conhecimento específico de engenharia para os projetar, fabricar, instalar, operar e mantê-los em segurança (FPC, 2017; RCM n.º 203-A/2019, 2019). Acrescenta-se a importância e obrigatoriedade de obter um licenciamento para a instalação do CS. Devido à necessidade do respeito pela Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), às elevadas complexidades administrativas nacionais, às considerações geopolíticas, torna-se

necessário que o promotor do CS possua competências específicas sobre aspetos jurídicos que se relacionem com uma autorização de licenciamento. A fim de obter sucesso no projeto, terão que ser tomadas em consideração quatro etapas de instalação dos CSs, sendo as seguintes: planeamento, desenvolvimento do projeto (incluindo o financiamento e contratação do fornecedor), construção, aceitação e a operação em si (Evans, 2009; Roach, 2014).

De uma forma generalizada, o planeamento tem de ser detalhado para determinar e seleccionar a rota mais eficiente e segura para o CS, sendo estes procedimentos feitos tendo também em conta os limites geopolíticos da área, onde a CNUDM possui um papel fundamental nas definições das fronteiras marítimas que existem, assim como os requisitos de permissão dos Estados costeiros (Burnett, 2011). Em suma, no que respeita ao planeamento, é muito importante ter-se em conta os locais de amarração em terra do CS.

Posto isto, com o objetivo de se conhecer melhor o fundo do mar, é necessário recorrer a levantamentos hidrográficos e a cartas de navegação atualizadas, entre outros documentos, para auxiliar na escolha da rota otimizada para a instalação dos CSs. De seguida, é feito um levantamento eficiente e ajustado, através do mapeamento das rotas definidas com o objetivo de minimizar distúrbios marinhos, estudar a batimetria, a geologia do fundo do mar, locais de pesca, locais utilizados por outros CSs ou gasodutos, plataformas eólicas, emissores de centrais de dessalinização, entre outros, locais de atracação e locais de fundeadoiro com recurso não só de um estudo intensivo como através do método de varredura lateral de área por sistemas multifeixe (Diogo, 2004). Estes processos são realizados por navios modificados para o efeito, possuindo especificidades suficientes para transportar e instalar muitos quilómetros de CS (RCM n.º 203-A/2019 de 30 de dezembro, 2019).

O levantamento tem de ser muito pormenorizado, contendo dados relativos à profundidade da água, topografia do fundo, o tipo e a espessura dos sedimentos, medições da corrente, marés e ondulação para avaliar a estabilidade do fundo do mar, pois, o movimento dos sedimentos e as condições oceânicas podem afetar o assentamento do CS assim como a futura necessidade de manutenção dos CSs (o acesso ao mesmo terá de ser facilitado em caso de necessidade de reparação), para além dos perfis sísmicos do fundo. O levantamento é feito ao longo de uma rota otimizada e desejada, com recurso de sonares

e Sistema de Posicionamento Global (GPS), para caracterizar completamente essa área evitando potenciais perigos provocados pelo Homem ou ainda, zonas ambientalmente prejudiciais que podem não ter sido identificadas a partir da informação existente (Davenport, 2012).

De seguida, antes dos CSs serem instalados no mar, estes são submetidos a testes rigorosos em terra para garantir a sua integridade e desempenho total. Após a elaboração destes testes é que os *cable ships*, os navios especificados para a instalação e reparação dos CSs, ao iniciarem o processo de instalação do cabo, navegam lentamente, com uma velocidade que depende da profundidade a que o cabo é assente, da topologia do solo, do tipo de CS, entre outros fatores e o cabo deve ser lançado a ré⁸ do navio (Barros, 2024). A colocação e estabilidade do cabo na água vai sendo afetada pelas condições marítimas e por qualquer variação nas operações do navio, portanto, deve ser desenrolado muito lentamente para permitir que o CS seja depositado no leito marinho. Em zonas sensíveis onde é necessário a inspeção visual, monitorização ou controlo do cabo e da área onde o mesmo é colocado, exige o uso de equipamentos ou Veículos Operados Remotamente (ROV). Os ROV podem ainda realizar trabalhos mecânicos como movimentação de objetos, por exemplo. Neste sentido, de modo a proceder-se à monitorização e vigilância marítima, depois da instalação do cabo, poderia ser utilizada a tecnologia associada ao Projeto *Fibersense*, como mencionado anteriormente, sendo mais aprofundado no decorrer da presente Dissertação.

Salienta-se ainda que as posições dos CSs, junto à costa, são marcadas nas cartas de navegação a fim de garantir a consciencialização para evitar qualquer desastre por parte dos navios ou embarcações que naveguem na área. Quanto à localização exata, em alto mar, não é fornecida nem publicada, dificultando a localização dos mesmos (Bueger et al., 2022).

Dependendo da profundidade, estes podem ser enterrados com recurso da *plough machine*, conhecida por charrua (como se pode observar na **Figura 10**) e, se necessário, por um mergulhador, como se pode observar o processo através da **Figura 11** (Carter et al., 2009; Evans, 2009).

⁸ Parte posterior do navio.

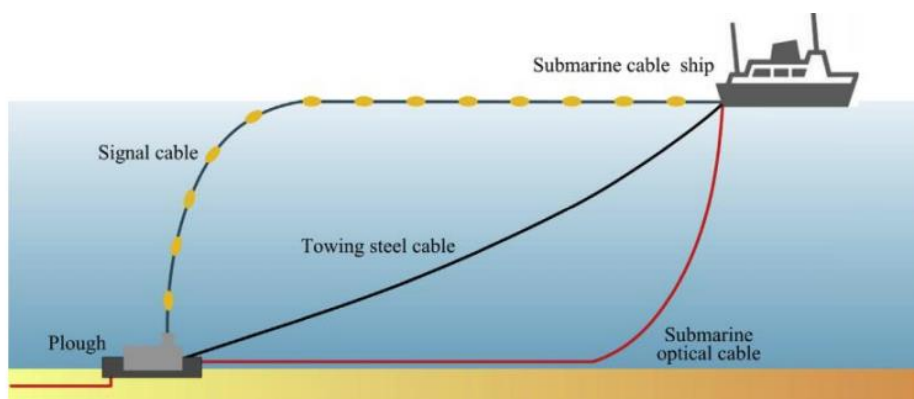


Figura 10 - Processo de instalação de um cabo submarino no leito marinho com recurso da charrua

(Retirado de Ye et al., 2018, p. 188)

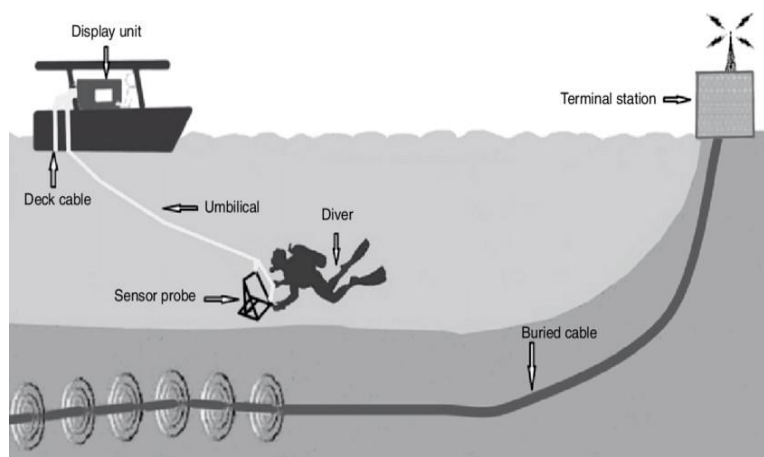


Figura 11 - Instalação de um cabo submarino no leito marinho com recurso a um mergulhador

(Retirado de Szyrowski et al., 2013, p. 134)

Os promotores/ operadores, através do conhecimento específico de engenharia que possuem acerca de CSs, devem encontrar-se a bordo do navio, observar minuciosamente e avaliar o progresso da instalação do cabo utilizando como base o planeamento da rota projetada e otimizada, podendo realizar ajustes, se necessário (Carter et al., 2009). Uma vez colocado no fundo do mar, o cabo é sinalizado por boias na chegada a terra, estando as extremidades do CS conectadas a terra através do BMH, encontrando-se este posteriormente ligado à CLS, o que pressupõe a gestão integral do sistema de telecomunicações (Davenport, 2012).

Por fim, durante o período de funcionamento de vida útil dos CSs, pode ser necessário proceder-se à manutenção ou até mesmo a reparações causadas por ruturas. O reparo envolve geralmente a localização da zona afetada, retirar o cabo do fundo do mar e substituição daquele local por outro novo (Recomendação (UE) 2024/779 de 26 de fevereiro, 2024). As empresas responsáveis pelos CSs assim como os Estados dependentes do funcionamento desse cabo têm interesse que as suas operações de reparação sejam realizadas o mais rapidamente possível, uma vez que as interrupções nos CSs podem afetar potencialmente as telecomunicações nacionais e internacionais, a *internet* e ainda a economia a nível global (Atlantic Cable Maintenance & Repair Agreement [ACMA], s.d.).

2. Mapeamento geográfico dos cabos submarinos

Atualmente, a rede de Cabos Submarinos (CSs) representa um grande número de infraestruturas subaquáticas. À exceção da Antártida, o único continente que ainda não possui CSs, permanece dependente da comunicação por via satélite (Shvets, 2017).

A nível global, destacam-se quatro áreas principais que dominam a geoestratégia dos CSs, sendo áreas com maior profusão dos mesmos, as seguintes: os EUA, área Américo-Atlântica, a Europa e a Ásia (Barros & Bernardino, 2024), como se pode observar na **Figura 12** a sua afluência nas zonas mencionadas.

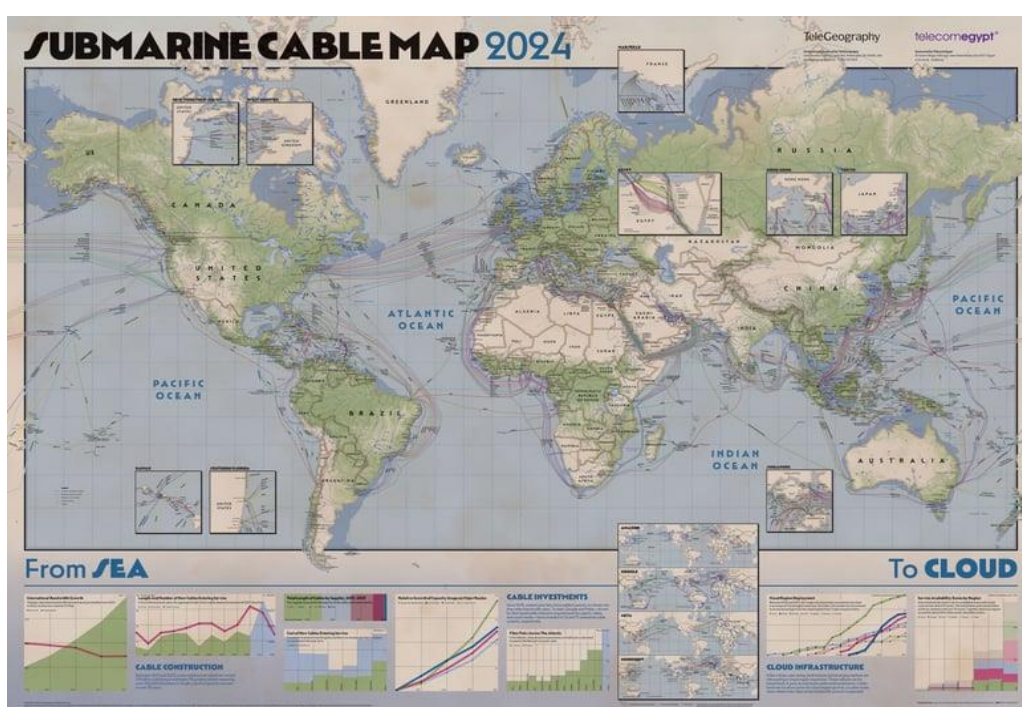


Figura 12 - Mapa dos cabos submarinos do ano de 2024

(Retirado de TeleGeography, 2024)

Conforme mencionado no capítulo anterior, os CSs desempenham um papel muito importante nas comunicações internacionais e nacionais, portanto, importa reconhecer o contributo tanto no que concerne ao desenvolvimento da Sociedade da Informação (SI)⁹,

⁹ Sociedade da Informação, um conceito primeiramente referido pelo economista *Fritz Machlup*, no livro, publicado no ano de 1962, *The Production and Distribution of Knowledge in the United States*. Posteriormente, foi desenvolvido por *Peter Drucker*, no ano de 1966, no livro *The Age of Discontinuity*. Este autor aborda pela primeira vez numa abordagem uma “sociedade pós-industrial em que o poder da economia – que, segundo o autor, teria evoluído da agricultura para a indústria e desta para os serviços – estava agora assente num novo bem precioso: a informação” (Crawford, 1983, pp. 380-385).

como para a ligação entre diferentes geografias (Barros, 2021; Eleftherakis & Vicen-Bueno, 2020).

Após a consulta da base de dados da TeleGeography, no ano de 2023, Portugal possuía doze amarrações de CSs internacionais e sete ligações óticas nacionais, ou seja, um total de dezanove CSs com ligação a Portugal (TeleGeography, 2023).

No que se refere ao presente ano, 2024, segundo a mesma fonte, Portugal possui dezassete CSs operacionais, dos quais dez são amarrações internacionais e sete ligações óticas nacionais, realçando o facto de que estão previstos cinco novos CSs, como abordado anteriormente, no subcapítulo **1.2** (TeleGeography, 2024).

Na **Figura 13** pode-se observar as diversas ligações operacionais de CSs portuguesas em ligação com outros países que permitem assim grande parte da comunicação a nível global.

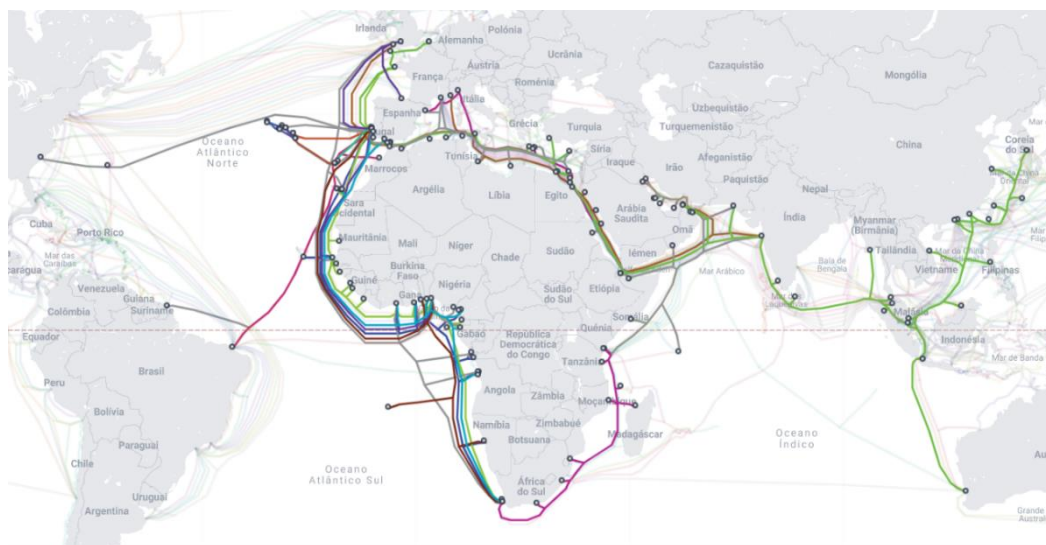


Figura 13 - Cabos submarinos operacionais ligados a Portugal correspondentes a 2024

(Retirado de TeleGeography, 2024)

Conforme afirma o autor José Barros, “Portugal tem uma posição geoestratégica que é ímpar no mundo” (Barros & Bernardino, 2024), devido à excelente localização geográfica que possui, foi até meados de 2021 o único país no Mundo que esteve ligado diretamente a todos os continentes, à exceção da Antártida. Neste momento, não existe nenhum país no Mundo interligado diretamente por CSs a todos os Continentes, devendo Portugal voltar a possuir essa posição com a entrada em operação do NUVEM que interligará Portugal à América do Norte (Barros, 2021; Matos, 2020).

Existem, à data, no Continente, quatro locais de amarração, Carcavelos, Seixal, Sesimbra e Sines. O Arquipélago dos Açores possui em cada uma das nove ilhas, um local de amarração, em Vila do Porto, Ponta Delgada, Angra do Heroísmo, Graciosa, Velas, Faial, São Mateus, Flores e Corvo, enquanto o Arquipélago da Madeira possui no Funchal e em Porto Santo (Barros & Bernardino, 2024; Carvalho, 2023; TeleGeography, 2024).

2.1. Enquadramento Jurídico e Cooperação Internacional

No que se refere aos CSs, entre o ano de 1884 e 1982, enquanto direitos e obrigações dos Estados, foram adotados quatro instrumentos legais internacionais: a Convenção Internacional para a Proteção dos Cabos Submarinos de 1884; a Convenção sobre o alto mar de 1958; a Convenção sobre a Plataforma Continental (PLATCON) de 1958; e a Convenção das Nações Unidas sobre o Direito do Mar de 1982 (Davenport, 2015).

A Convenção de 1884, é uma Convenção independente, criada com o objetivo de proteger os CSs instalados fora das águas territoriais (Burnett, 2011). Relativamente às Convenções de 1958 e à de 1982, dirigem-se ao Direito do Mar no que concerne a diversos aspetos com este relacionados. Das quatro Convenções, a CNUDM de 1982 tem realce dado que pretendeu estabelecer “com a devida consideração pela soberania de todos os Estados, uma ordem jurídica para os mares e oceanos” (Resolução da Assembleia da República n.º 60-B/97 de 14 de outubro, 1997, p. 3). De acordo com o autor:

“A CNUDM identificou e caracterizou diversos espaços marítimos onde os países costeiros têm diferentes competências, tanto ao nível da soberania como da jurisdição. Os espaços referidos foram *as águas interiores, o mar territorial, a zona contígua, a Zona Económica Exclusiva (ZEE) e a plataforma continental*. Os espaços marítimos que num dado âmbito não estão sob jurisdição ou soberania de qualquer país foram designados por *alto mar* quando se referem à coluna de água, e por *área* quando se referem ao solo e subsolo marinho” (Pacheco, 2014, p. 112).

Contudo, destaca-se como um resultado marcante desta Convenção, a definição de três diferentes zonas marítimas: as águas territoriais, a ZEE/ PLATCON e o alto mar, como se pode observar na figura seguinte (**Figura 14**).

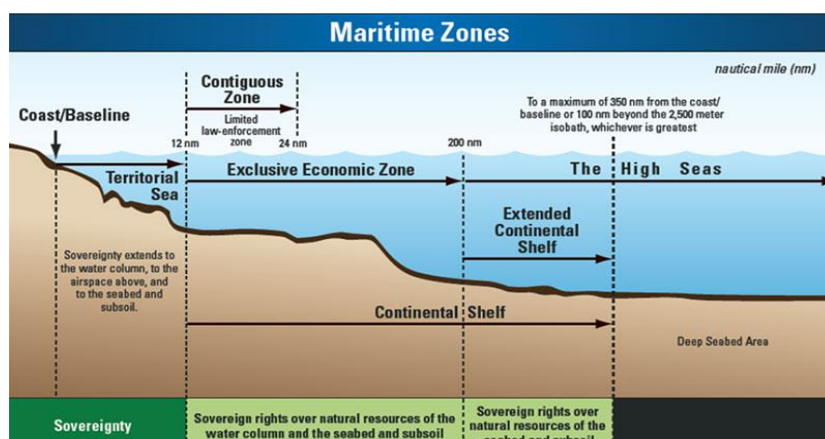


Figura 14 - Zonas Marítimas de acordo com a CNUDM

(Retirado de Bohan, 2018)

Esta convenção, possui na constituição artigos referentes aos direitos e obrigações de cabos e ductos submarinos, nomeadamente, a colocação, proteção, reparação e manutenção, de acordo com o regime jurídico das águas territoriais (segundo a CNUDM de 1997, artigos: 21.º, 79.º, 87.º, 112.º, 113.º, 114.º, 297.º): como comprovado, pelo estabelecido no artigo 79.º, n.º 1 da CNUDM que “Todos os Estados têm o direito de colocar cabos e ductos submarinos na PLATCON, competindo ao Estado costeiro estabelecer as condições para que estes passem no seu território ou no seu mar territorial” (Resolução da Assembleia da República n.º 60-B/97 de 14 de outubro, 1997, p. 5486 (18)).

Todavia, Portugal contém na constituição de mar uma extensa área de CSs, segundo a RCM68 (2021) “Portugal tem jurisdição sobre cerca de metade das águas marinhas da União Europeia (UE), em espaços adjacentes ao continente europeu, e sobre uma vasta área de solo e subsolo marinhos no Atlântico Nordeste” (RCM n.º 68/2021 de 4 de junho, 2021, p. 23), por forma a que, “A geografia de Portugal e a evolução do direito internacional marítimo, particularmente durante o século XX, levaram a que o País reclamasse sob sua soberania e jurisdição extensas áreas marítimas” (Pacheco, 2014, p. 120), devido à vasta dimensão que ocupam, necessitam de estar bem protegidas. O Estado tem um papel fundamental neste âmbito, pois estabeleceu “A Estratégia Nacional para o Mar 2021-2030 (ENM 2021-2030) está ancorada nestes instrumentos internacionais e contribui para os seus objetivos, reforçando, ao mesmo tempo, o mar como espaço de soberania” (RCM n.º 68/2021 de 4 de junho, 2021, p. 26).

Relativamente à Cooperação Internacional, principalmente no que toca às fragilidades do enquadramento jurídico internacional, existe a necessidade de reforçar os mecanismos de cooperação, nomeadamente, da segurança dos CSs. Surge, assim, em 1958, o *Cable Damage Committee*, que em 1967 viria a adotar a designação de *International Cable Protection Committee* (ICPC) para uma melhor perceção da finalidade do comité (Shvets, 2020). No entanto, uma vez que este organismo só reunia os detentores e os operadores de CSs, em 2010, a organização foi alargada aos Governos nacionais e a diversos órgãos da indústria marítima (operadores de navios, fornecedores de sistemas e empresas de prospeção), ou seja, de agências públicas. Esta permissão das novas adesões deveu-se à necessidade do trabalho conjunto a fim de garantir a proteção e a segurança dos CSs. Uma outra causa foi para “maximizar as proteções da Convenção das Nações Unidas sobre o Direito do Mar (UNCLOS), que é o base legal para a expansão, manutenção e modernização da rede de cabos submarinos” (ICPC, s.d., p. 1). Embora as entidades abordadas façam parte do organismo, ainda se uniram outros órgãos da Organização das Nações Unidas (ONU), outras organizações internacionais e Organizações Não-Governamentais (ONGs) com o fim de promover a conscientização sobre os cabos, fornecendo as melhores práticas de proteção e estabelecendo acordos internacionais eficazes para a proteção dos CSs (Cabral, 2022).

O ICPC procura promover a proteção dos CSs, assim como estabelecer recomendações negociadas internacionalmente para a instalação, proteção e manutenção dos CSs, monitorizando a evolução dos tratados internacionais e da legislação nacional, em suma, garantindo a proteção e salvaguarda dos interesses dos sistemas de CSs (Carter et al., 2009). Possui uma base de dados jurídica exclusiva, a fim de melhorar as funções dos membros desta organização, onde se pode fazer a recolha da informação mais importante e atualizada sobre os CSs relativamente a leis nacionais, documentos e recomendações do ICPC (Shvets, 2020).

Atualmente, de acordo com a informação retirada da Lista de Membros do ICPC, de março de 2024, fazem parte desta organização 220 Membros provenientes de diversos continentes e representantes dos diferentes atores da indústria, fabricantes, instaladores, operadores, Governos, autoridades regulatórias, entre outros, sob o domínio do direito internacional (ICPC, 2024; Wopschall, 2017). Este comité atua como ator não estatal e exerce ainda uma governação transnacional de particular significado público (Shvets, 2020). No que concerne à governação global dos CSs, os atores não estatais que

desempenham um papel de Estados, atuam através de organizações internacionais na ausência de regulamentação legal. Estes atores desempenham ainda um papel significativo na área dos CSs, proporcionando novas perspetivas relevantes relativas a fenómenos de cooperação internacional (Bogdandy et al., 2009; Kulick, 2012; Sampford et al., 2015; Santuraki, 2019).

Desde a criação da ONU, a União Internacional das Telecomunicações (UIT) tornou-se numa das agências especializadas desta organização para as Tecnologias de Informação e Comunicação (TIC) (Gotschalg, 2009; ANACOM, 2020). Existem ainda a nível regional acordos bilaterais e multilaterais de manutenção e reparação realizados relativos aos CSs, ao encargo dos vários operadores a quem pertencem os cabos (ACMA, s.d.).

Contudo, de modo a reforçar a cooperação internacional, advoga-se o reforço do ICPC e um envolvimento crescente de Organizações como a UE e a Organização do Tratado do Atlântico Norte (OTAN) na proteção dos CSs (Cabral, 2022).

Segundo a ENM 2021-2030, “O triângulo marítimo português (continente, Madeira e Açores) constitui 48% da totalidade das águas marinhas sob jurisdição dos Estados-Membros da UE em espaços adjacentes ao continente europeu” (RCM n.º 68/2021 de 4 de junho, 2021, p. 25), assim, é possível concluir que têm de garantir tanto a proteção do ambiente marinho e das infraestruturas que forem nesses locais instaladas, nas quais se inserem os CSs, assim como de toda a informação que neles circula, pois considera-se vital para a segurança das comunicações a nível global.

2.2. A importância da posição geoestratégica de Portugal

Portugal apresenta, geopoliticamente, uma posição singular, de acordo com a Resolução do Conselho de Ministros de 1968, onde se afirma que:

“A relação singular entre Portugal e o Atlântico é um fator crucial para que o País valorize, consolide e reforce relações de cooperação com outros Estados, garanta a soberania em toda a sua área marítima e participe ativamente em processos conjuntos que visem garantir a segurança nas áreas de interesse nacional e internacional” (RCM n.º 68/2021 de 4 de junho, 2021, p. 39).

Embora não deixe de ser importante a relação de cooperação com os outros Estados, “Portugal detém na sua herança marítima e na sua centralidade atlântica um posicionamento geoestratégico que lhe permite continuar a apostar na sua maritimidade e na sua potencialidade enquanto *hub* atlântico nas cadeias logísticas globais de base marítima” (RCM n.º 68/2021 de 4 de junho, 2021, p. 49).

Em relação à posição geográfica, é o país mais ocidental da Europa, estando localizado entre Espanha e o oceano Atlântico (Jesus, 2020). A dimensão deste oceano é imensa, é o segundo maior do mundo, de acordo com a ENM 2013-2020, convencionada para a gestão do espaço marítimo nacional:

“Porém, quando considerada a sua dimensão marítima, Portugal é um país imenso e um dos grandes países marítimos do mundo, com um acrescido potencial geoestratégico, geopolítico e económico. A esta imensa dimensão marítima correspondem grandes desafios e, sobretudo, oportunidades sem precedentes para Portugal” (RCM n.º 12/2014 de 12 de fevereiro, 2014, p. 1315).

Segundo Miguel Pacheco, “Portugal é um dos maiores países marítimos do mundo, especialmente no que se refere à zona económica exclusiva e à plataforma continental” (Pacheco, 2014, p. 105). Atendendo à **Figura 13**, pode-se observar a quantidade de ligações de CSs que atravessam a ZEE, estando a ZEE representada na **Figura 15**. Segundo José Barros e Luís Bernardino, a médio prazo, cerca de 20% dos CSs globais deverão atravessar a ZEE portuguesa, isto comprova o valor do país no que concerne ao espaço marítimo (Barros & Bernardino, 2024; TeleGeograpy, 2023). Ainda relacionado com este tema, encontra-se em análise o pedido de extensão da PLATCON, onde, se o mesmo for concedido favoravelmente pela ONU, alargará a área de jurisdição nacional para quase 4 milhões de km² (Albuquerque et al., 2012).

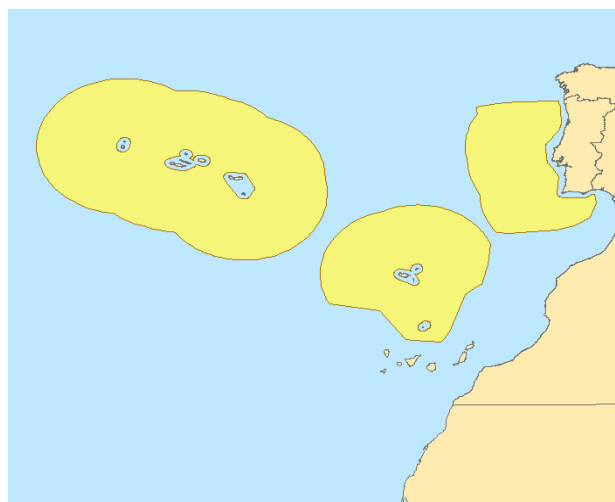


Figura 15 - Representação da Zona Económica Exclusiva

(Retirado de Instituto Hidrográfico, 2015)

Munido do potencial geoestratégico, Portugal é um dos países com a maior ZEE da Europa (fazendo ainda parte desta, a zona contígua) (MDN, 2006). A ZEE estende-se por 1,7 milhões de km² e desempenhou, a par com os EUA, um papel essencial no estabelecimento da aliança e na defesa do Atlântico Norte, que se conhece por OTAN (Adhitama, 2019).

A importância marítima do país, levou à criação de uma ENM, “A Estratégia Nacional para o Mar constitui um instrumento político fundamental para que Portugal possa proteger e valorizar o inestimável recurso que o oceano representa para o nosso país” (MDN, 2006, p. v). Por este motivo, em 2006, foi aprovada em Conselho de Ministros a última versão da ENM 2006-2016, no Dia Nacional do Mar, dia 16 de novembro de 2006, elaborada com o objetivo de aproveitar os recursos marítimos, de forma a evoluir a nível económico e social através de uma “forma sustentável e respeitadora do ambiente” (MDN, 2006, p. 10).

Atualmente, encontra-se em vigor a ENM 2021-2030, aprovada em 2021 (RCM n.º 68/2021 de 4 de junho, 2021), tendo por base o oceano Atlântico, esta estratégia visa fortalecer a presença e destaque de Portugal a nível global, destacando-o como uma nação predominantemente marítima. Amplia a influência económica, impulsionando a prosperidade e o bem-estar da população portuguesa com o propósito de dar resposta aos grandes desafios futuros (Jesus, 2020). De acordo com esta estratégia, Portugal pode ser visto, tendo em conta a dimensão que possui, de duas formas principais. Em relação à dimensão territorial em que é o 111º país do mundo e, pela dimensão Atlântica, em que é

o país com a 20ª maior ZEE do mundo (Pacheco, 2014; Resolução do Conselho de Ministros n.º 68/2021, de 4 de junho, 2021). Ao serem relacionadas estas duas dimensões, pode-se concluir que a área da ZEE é 18 vezes maior que a área do território nacional e equivale a 38% da área da União Europeia. Por outro lado, se tivermos como domínio o ciberespaço, reconhecendo que este tema será aprofundado no decorrer da presente dissertação, pelas características que o definem, os números anteriores têm pouca expressão (Pacheco, 2014).

O posicionamento geoestratégico de Portugal é salientado na ENM 2021-2030 da seguinte forma: “Urge continuar a dar um rumo às políticas do mar e fortalecer o posicionamento geopolítico e geoestratégico de Portugal” (RCM n.º 68/2021 de 4 de junho, 2021, p. 26). Portugal visto ter uma posição geoestratégica claramente conhecida e definida, competências tecnológicas e uma tradição marítima, deve assumir definitivamente as vantagens competitivas e exercer a autoridade do Estado no mar que lhe compete (RCM n.º 68/2021 de 4 de junho, 2021).

Considerando Portugal como “um país oceânico” (RCM n.º 68/2021 de 4 de junho, 2021, p. 25), quanto maior for uma determinada área marítima, maior será a probabilidade de existir potencial de riqueza, adicionando a existência de oportunidades de desenvolvimento económico, social e científico associadas à exploração sustentada do mar que também será maior. “O conhecimento da nossa geografia marítima e a comparação com a dos restantes países costeiros permite-nos, de uma forma prática, ter uma perceção do nosso potencial marítimo e posicionarmo-nos, nos diferentes âmbitos de relacionamento, face ao dos outros” (Pacheco, 2014, p. 107).

Ao se ter em conta a dimensão marítima de Portugal e a periferia face ao continente europeu, o país possui centralidade Atlântica, como se pode confirmar de acordo com a **Figura 16**, “exercendo direitos de soberania ou jurisdição sobre uma das mais extensas regiões marítimas do mundo” (Silva, 2020, p. 91).

Realça-se o facto da figura seguinte conter, de forma representativa, ilustrada a extensão da PLATCON.

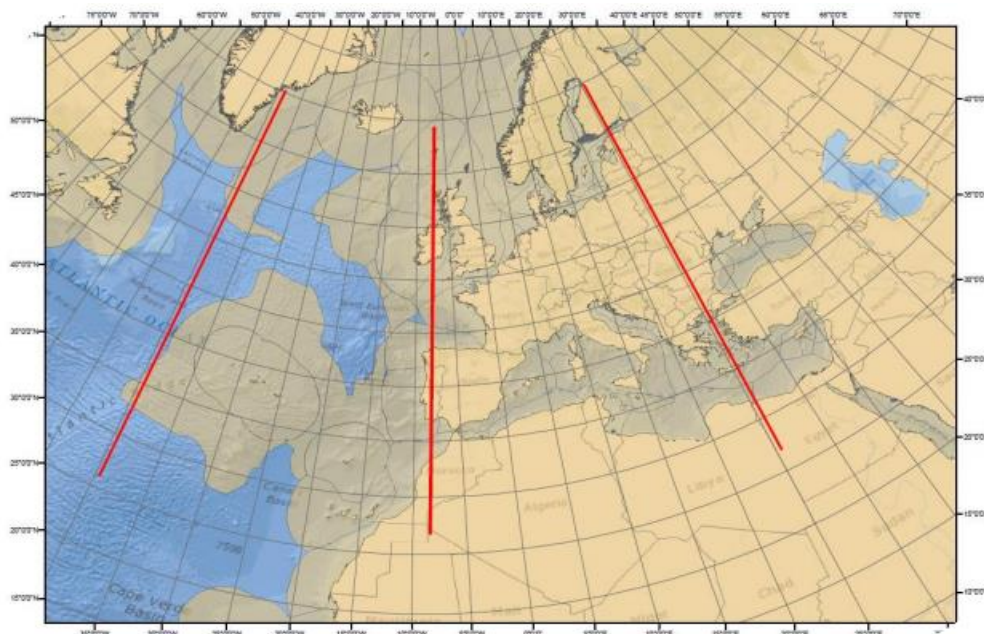


Figura 16 - A centralidade Atlântica de Portugal

(Retirado de Campos, 2013)

Contudo, Portugal, com o poder nacional intrínseco que possui, tem como principais constituintes geográficos: o território emerso e os espaços marítimos sob soberania e jurisdição nacional. Devido à posição geográfica e ao crescente desenvolvimento do direito internacional marítimo, Portugal pôde reivindicar, sob soberania e jurisdição, um conjunto de espaços marítimos de dimensão considerável, consolidando-se como uma potência marítima de relevo (Pacheco, 2014).

A nível estratégico, Portugal tem uma posição geoestratégica valiosa no que toca à intercomunicação marítima e aérea, como aponta o autor. Esta posição geoestratégica do país define-se como:

“um espaço caracterizado pela descontinuidade territorial, de grande dimensão marítima e aérea face à exiguidade terrestre, de limitada profundidade continental, com uma posição periférica no espaço europeu mas central nos espaços euro-americano, euro-africano e face às grandes linhas de comunicações marítimas e aéreas” (Correia, 2002, p. 83).

O que se torna muito relevante face às ambições marítimas dos Estados costeiros. Estes concentram-se no transporte e comércio marítimo, na pesca, na defesa de costa

contra um ataque inimigo e na projeção de força sobre outro Estado costeiro (Pacheco, 2014).

Não obstante, considerando as dimensões atlântica e europeia, Portugal deve afirmar-se como uma nação marítima reconhecida globalmente e promover a segurança das zonas marítimas que estão ao encargo do país. Por detalhe, os CSs não são exceção (RCM n.º 68/2021 de 4 de junho, 2021).

2.3. A presente conflitualidade e a competição estratégica global

Os CSs atuam como sistema nervoso central da *internet* global, sendo estrategicamente muito importantes por permitirem ligações intercontinentais, pois têm de circular em águas internacionais, não estando protegidos pela legislação nacional do país em questão (CCDCOE, 2019).

Ao efetuar-se uma comparação dos mapas de CSs entre o Atlântico Norte (**Figura 17**) e o Atlântico Sul (**Figura 18**), é de notar que existe um número muito mais elevado de rotas transatlânticas¹⁰ no Atlântico Norte. O Atlântico Sul, uma vez que não possui muitas ligações, demonstra a fragilidade e o impedimento do avanço tecnológico e do desenvolvimento da própria capacidade de defesa cibernética pois está dependente relativamente à estrutura dos CSs existentes no Atlântico Norte para tal (Medeiros & Pinto, 2022).

¹⁰ As rotas dos CSs seguem as rotas de maior trocas comerciais, Este/ Oeste no Atlântico Norte (América do Norte - Europa) e Norte/ Sul, em todo o Atlântico (Europa – Ásia e América do Norte – América do Sul).

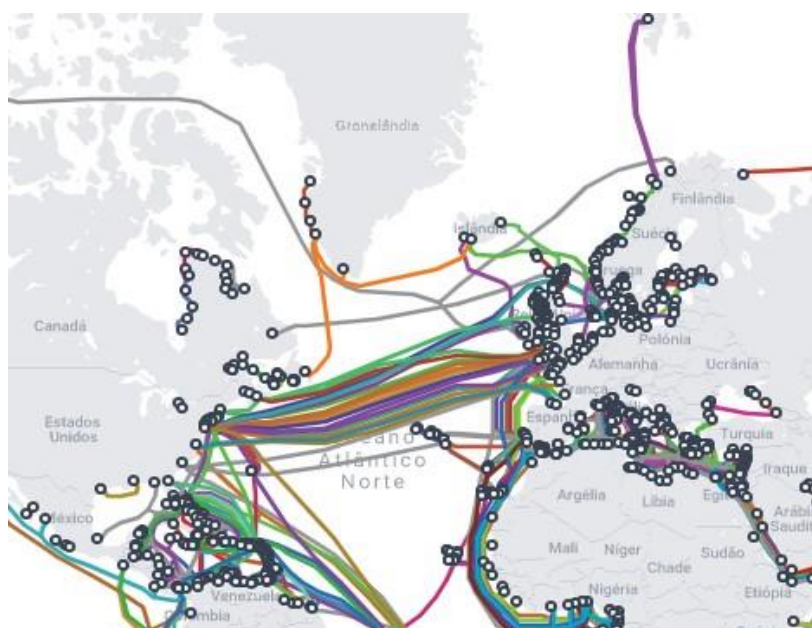


Figura 17 - Cabos submarinos operacionais no Atlântico Norte correspondentes a 2024
(Retirado de TeleGeography, 2024)



Figura 18 - Cabos submarinos operacionais no Atlântico Sul correspondentes a 2024
(Retirado de TeleGeography, 2024)

Por outro lado, os cabos presentes no Atlântico Sul oferecem mais alternativas do que outros oceanos como o Oceano Pacífico ou o Oceano Índico e são significativamente mais expressivos. Algumas redes, embora sejam atlânticas, estão restringidas às regiões

próximas do continente, circulando sobre o território marítimo de alguns países (Medeiros & Pinto, 2022).

O controlo das atividades dos CSs tem de estar em conformidade com a jurisdição geográfica dos regulamentos federais, estaduais e locais que promulgam as disposições da CNUDM na legislação nacional de cada país, no que toca às atividades relacionadas com os CSs, nos mares territoriais e na ZEE. Por outro lado, para os países que não ratificam a CNUDM, têm de seguir e cumprir com a legislação nacional existente (Carter et al., 2009).

De uma forma muito superficial e de modo a não existir intrusão nem evasão relativamente a este tema, os CSs são utilizados como ferramentas de auxílio entre países em conflito: “No entanto, estes cabos têm sido objeto de disputa ostensiva entre nações em potencial conflito ou como instrumentos de guerra” (Medeiros & Pinto, 2022, p. 1), o que promove não só a utilização como a condução de missões diplomáticas e a coordenação de operações militares, portanto, estes cabos refletem uma grande preocupação a nível mundial. Esta preocupação deve-se ao facto da possível ocorrência de atos hostis ou até de ataques cibernéticos para obter as informações que neles circula, que será abordado mais tarde nesta dissertação, para um esclarecimento mais aprofundado (Medeiros & Pinto, 2022).

No que toca à conflitualidade, os países que possuem uma maior capacidade de utilização do terreno submarino terão sempre vantagem no decorrer das fases primitivas de um conflito, mas também estão mais suscetíveis de sofrerem um ataque aos próprios CSs (Clark, 2016), uma vez que, “Quanto maior for a extensão da finalidade militar de um cabo submarino, maior será a sua probabilidade de ser alvo de um conflito” (Bueger et al., 2022, p. 23).

Um Estado, perante um conflito com outro, se quiser obter vantagem militar direta, superioridade geopolítica ou ainda uma sabotagem a nível económico, seria facilmente através do corte das comunicações submarinas desse outro, ou seja, o ataque por CS, antes ou ainda durante o próprio conflito. Em resumo, torna-se muito importante, num conflito entre Estados, a proteção tanto dos CSs como das CLS, uma vez que, no caso de ocorrência do mesmo, existe uma forte possibilidade de perda da capacidade de Comando e Controlo (C2) e posterior isolamento das forças militares, roubo de dados, impedimento do controlo de sistemas de alerta e ainda de armas nucleares, apenas através de um ataque coordenado a estas infraestruturas (Clark, 2016).

No que concerne à economia e à sociedade, estas duas dimensões dependem tanto do funcionamento da *internet* como da conectividade internacional de um país, estando, por isso, diretamente relacionadas com a soberania digital que cada um possui. Posto isto, caracterizam-se como sendo a chave para alcançar uma era de digitalização competitiva (Barros, 2024; European Commission, s.d.). Os acessos internacionais estão intimamente ligados à interdependência de um país, sendo que, quanto maior for a diversidade desses mesmos acessos, maior grau de independência será conseguido em termos de conectividade e interligação internacional, podendo ter um maior leque de escolha de condições comerciais e de qualidade de serviço prestado (Barros, 2024).

Contudo, ao avaliar-se o assunto da competição estratégica global, a competição para monitorizar e controlar o mundo submarino, tem tendência a aumentar e pode ser definida por algumas mudanças significativas na forma como a guerra submarina poderá vir a ser conduzida (Bueger et al., 2022). Os CSs de comunicações comerciais são um alvo militar desde os primórdios, mas os CSs que são associados a Bases Navais ou a estações recetoras de satélites, têm certamente mais uso a nível militar, o que as torna também um alvo para outro Estado em potencial conflito (Bueger et al., 2022).

3. Segurança dos cabos submarinos

A presente Era digital originou benefícios e consequências para o mundo, que se está a tornar cada vez mais tecnológico (Wolff, 2021). A *internet* trouxe um efeito revolucionário a nível global que proporciona tanto oportunidades como riscos e ameaças. Embora seja um mecanismo de propagação de informação, um meio colaborativo e independente, faz parte dos sistemas de Tecnologias da Informação e Comunicação (TIC), numa sociedade reconhecida como a Sociedade da Informação (SI) (Castells, 1999; Leiner et al., 1997).

Embora exista uma crescente complexidade dos sistemas de Tecnologias da Informação (TI), associado a um maior fluxo de dados, as novas tecnologias digitais, como a Inteligência Artificial (IA), tornam-se cada vez mais utilizadas, possuindo maior importância, sendo, atualmente, transversais a toda a sociedade (Comissão Europeia, 2021; Roh et al., 2018).

Devido a esta forte utilização da IA, desde o ano de 2020 que este assunto começou a ser debatido pelo Conselho Europeu. Um ano depois, em 2021, a Comissão Europeia propôs o Regulamento da IA. Em 2022, o Conselho da UE definiu a posição do próprio Conselho sobre este Regulamento, em 2023, o Conselho da UE e o Parlamento Europeu chegam a um acordo provisório relativamente a este Regulamento, até que, a 21 de maio de 2024, o Conselho aprovou “O Regulamento Inteligência Artificial da UE” (Conselho da UE e Conselho Europeu, 2024). Este será o primeiro ato legislativo, a primeira lei relativa a esta matéria, podendo “estabelecer uma norma mundial para a regulamentação da IA noutros sistemas jurídicos” (Conselho da UE e Conselho Europeu, 2024), o qual será aplicável a partir de 2026.

A IA tem uma particularidade inigualável na aplicabilidade da automação e inovação, relativamente às capacidades conhecidas no momento. No que toca à interpretação de linguagem, identificação de padrões complexos relativos a qualquer situação e ainda na tomada de decisões baseadas na análise de dados. A IA é caracterizada por possuir vantagens na análise de elevados volumes de dados (Oliveira, 2021; Ordem dos Psicólogos Portugueses, 2023).

O facto da informação ser parte do património mundial e o facto dos Cabos Submarinos (CSs) transportarem cerca de 99% das comunicações digitais transoceânicas (comunicações de dados e de *internet*) entre nações e continentes, torna estas

infraestruturas num ambiente propício para as ameaças cibernéticas, sendo, por este motivo, classificadas como uma prioridade globalmente importante devido à fragilidade e exposição a que estão sujeitas (Brake, 2019; Gallagher, 2022). Inseridas neste tema, realça-se que as comunicações globais, devido às novas tecnologias, estão associadas a uma maior exposição a riscos e ameaças e novas formas de crimes e de alvos, que poderá implicar uma maior exigência para garantir a segurança da humanidade, ou seja, da proteção de dados e da privacidade a nível global (European Liberal Forum, 2023; Frascà & Galantini, 2023; Kettani & Wainwright, 2019; Rego, 2017; Choo, Smith, & McCusker, 2007).

Associado à criação e treino de algoritmos de IA existem o *Machine Learning* (ML), e o *Deep Learning* (DL), embora o DL seja uma derivação do ML, ambos são baseados na aprendizagem de comportamentos humanos (Khanna, 2019). Estes sistemas representam uma tecnologia fundamental para os sistemas de TI atuais e futuros (Apruzzese et al., 2023; Jordan & Mitchell, 2015). Estas técnicas caracterizam-se, de uma forma generalizada, por serem treinadas a partir de grandes volumes de dados, posterior análise eficiente e, por fim, o tratamento dos mesmos, estando associados ao grande fluxo de informações e conexões internacionais que são transportados pelos CSs (Lee, 2019). O ML é uma técnica essencial no que toca ao tratamento do *Big Data* (BD), permitindo o desenvolvimento e evolução de algoritmos ao longo do tempo, o que os torna cada vez mais inteligentes (Kumar & Nagpal, 2018; Palanivinayagam et al., 2021). Sendo o termo BD usado como uma definição consensual, expresso por “*Big Data* é o ativo de informação caracterizado por um volume, velocidade e variedade tão elevados que requerem tecnologia e métodos analíticos específicos para a sua transformação em valor” (De Mauro et al., 2016, p. 127). O DL conhecido como “a tecnologia que está no centro dos recentes desenvolvimentos de IA” (Fundação Calouste Gulbenkian, 2023), apresenta uma maior complexidade relativamente ao ML, pois é conhecido como um sistema artificial capaz de identificar padrões que os humanos não são capazes de interpretar através da utilização de redes neuronais artificiais que permitem a aprendizagem de uma vasta tipologia de dados (Ordem dos Psicólogos Portugueses, 2023). Esta aprendizagem é possível devido à existência das redes neuronais que admitem a introdução destes num determinado algoritmo, em qualquer formato, tornando exequível englobar diversos métodos de aprendizagem na representação dos mesmos. O DL é, por este motivo, mais

versátil do que o ML uma vez que este obriga a inserção dos dados num determinado formato (Jakhar & Kaur, 2019; Khanna, 2019; LeCun et al., 2015).

O DL também apresenta uma maior vantagem quanto à previsão, otimização e discriminação de resultados (Calderon, 2019; Jamadar et al., 2019; Li, 2018).

Posto isto, associado ao progresso tecnológico, está o nível de exigência para garantir a segurança das informações que circulam nos CSs. Embora a sociedade moderna dependa cada vez mais do recurso da IA e das novas tecnologias da globalização das comunicações, a ascensão dos sistemas autónomos, trouxe um «novo paradigma de interdependência», estando este interligado ao crescente nível de importância da Segurança da Informação, em controvérsia com as ameaças digitais em constante evolução (Gregor & LeCun, 2010; LeCun et al., 2015; Kontis, 2022).

Consideram-se os CSs, Infraestruturas Críticas (IC), uma vez que permitem a comunicação mundial (Burnett, 2011; Keupp, 2020; Strohmeier et al., 2020). Em Portugal, IC é definida como:

“a componente, sistema ou parte deste situado em território nacional que é essencial para a manutenção de funções vitais para a sociedade, a saúde, a segurança e o bem-estar económico ou social, e cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções” (Lei n.º 46/2018 de 13 de agosto, 2018, p. 4031).

Assim sendo, para a proteção destas IC, a maioria dos países e Estados que as operam devem ter especial atenção com a segurança uma vez que neles circulam todo o tipo de informações (Conselho da União Europeia, 2024; Comissão Europeia, 2024).

Por último, as TIC tornaram-se um elemento chave e essencial a nível global, contudo, as infraestruturas de comunicações e informações estão sujeitas a ataques maliciosos, uma vez que o Estado depende destas infraestruturas, qualquer ataque ou vaga de ataques, podem vir a afetar gravemente o funcionamento da sociedade atual (Klimburg, 2012).

3.1. Cibersegurança e segurança marítima

Os CSs, considerados IC, necessitam de especial importância no que se refere à segurança, pois, do ponto de vista estratégico, estes cabos são um conjunto ameaçado no mar. Explica-se esta questão de «conjunto ameaçado no mar» através da Recomendação da UE 2024/779 da Comissão Europeia de 26 de fevereiro de 2024, “a importância estratégica de infraestruturas críticas como as redes de telecomunicações e os serviços digitais para um grande número de funções críticas nas nossas sociedades, e o facto de serem um dos principais alvos dos ciberataques” (Recomendação (UE) 2024/779 de 26 de fevereiro, 2024, p. 1).

O facto do fluxo mundial de dados depender destas IC, torna importante que a segurança seja avaliada. Para isso, considera-se o multi-domínio do ciberespaço, (apresenta-se este tema de uma forma mais explícita e completa no capítulo 4 da presente Dissertação), e reconhece-se que possíveis ciberameaças sejam neutralizadas ou impedidas. Estas IC, devido a terem uma elevada importância para o Estado “O conceito estratégico de defesa nacional define os aspetos fundamentais da estratégia global a adotar pelo Estado para a consecução dos objetivos da política de segurança e defesa nacional” (RCM n.º 19/2013 de 5 de abril, 2013, p. 1981), torna-se importante que se adotem políticas corretas para a segurança das mesmas. Ao se considerar o meio em que os CSs estão inseridos e o ciberespaço, obtém-se uma relação entre as duas realidades relativas à segurança dos CSs, a cibersegurança e a segurança marítima (Vichi et al., 2020).

Quanto à segurança marítima, um conceito amplo, sendo esta considerada um subsistema da segurança, divide-se em duas dimensões, pela língua inglesa, *maritime security* (proteção marítima) e *maritime safety* (segurança marítima). De forma a mitigar o conflito que possa existir entre os dois termos mencionados anteriormente, em 2006, adotou-se, no ordenamento jurídico nacional, o significado de proteção para o termo *security* e segurança referente ao termo *safety* (Decreto-Lei n.º 226/2006 de 15 de novembro, 2006).

Posto isto, quando se fala de *maritime security* é importante referir que, no âmbito da Convenção SOLAS de 1974 e enquadrada no Código Internacional para a Proteção

dos Navios e das Instalações Portuárias (ISPS Code¹¹), que entrou em vigor no ano de 2004, conhecido por “o código internacional para a proteção dos navios e das instalações portuárias da Organização Marítima Internacional (OMI), na sua versão atualizada”, *maritime security* objetiva medidas tomadas para a segurança de pessoas e bens, relativamente à proteção de instalações portuárias, navios e cargas, quer ao nível físico como patrimonial, contra ações e atos ilícitos intencionais como ameaças terroristas, pirataria, assaltos à mão armada e violência marítima (Decreto-Lei n.º 226/2006 de 15 de novembro, 2006; Diogo, 2004; EMSA, s.d.).

O termo *maritime safety*, segundo a Convenção SOLAS de 1974 e a *The International Convention for the Prevention of Pollution from Ships 73/78* (Convenção MARPOL 73/78¹²), está direcionado para operações de Busca e Salvamento Marítimo (SAR), ou seja, para a salvaguarda da vida humana no mar, segurança e navegabilidade dos navios, no geral, contribui para a segurança da navegação. De acordo com a CNUDM, tem o objetivo de avaliar, de forma adequada, os fatores de segurança da navegação, proteção e preservação do meio marinho (Diogo & Gouveia, 2005).

A cibersegurança, entende-se por um conjunto de ações e medidas que visam o bem-estar e o regular funcionamento da ação de um Estado e das populações tanto no ciberespaço, como fora dele (Militão, 2014). Ações essas, de prevenção, monitorização, deteção, análise e correção, derivado de ações diretamente a ele acometidas, de modo a garantir integridade, disponibilidade e confidencialidade das TIC e da população que as usa (CNCS, 2024; Solms & Niekerk, 2013). Posto isto, a cibersegurança é considerada uma prioridade nacional na resposta às ciberameaças e uma preocupação constante, uma vez que, o fracasso na proteção do fluxo das informações implica enormes riscos ao nível de todos os setores, sendo, por isso, extremamente importante para a defesa dos Estados (Nunes, 2022; Santos, 2017; Weiss & Jankauskas, 2019).

¹¹ Código ISPS, segundo o Regulamento (CE) n.º 725/2004 do Parlamento Europeu e do Conselho, de 31 de março de 2004, relativo ao reforço da proteção dos navios e das instalações portuárias, no artigo 2.º, ponto 2., define-se como “o Código Internacional de Segurança dos Navios e das Instalações Portuárias da OMI”, tendo entrado em vigor apenas a 1 de julho de 2004 (Regulamento (CE) n.º 725/ 2004 de 31 de março, 2004).

¹² Convenção Internacional para a Prevenção da Poluição por Navios, adotada a 2 de novembro de 1973. Esta Convenção foi alterada pelo Protocolo de 1978 (MARPOL 73/78), tendo entrado em vigor a 2 de outubro de 1983. Conhece-se como a principal convenção internacional relativa à prevenção e minimização da poluição no meio marinho (Decreto do Governo n.º 25/1987 de 10 de julho, 1987).

Em relação à responsabilidade, a cibersegurança tem responsabilidade partilhada entre os cidadãos, entre o setor público e o setor privado, possuindo uma relação direta com atores privados e com os próprios utilizadores, ou seja, não é da responsabilidade exclusiva do Estado (Vichi et al., 2020). Contudo, os atores privados detentores de um determinado CS possuem maior responsabilidade de proteção dos dados que circulam nos CSs do que o próprio Estado (Agência dos Direitos Fundamentais da União Europeia, 2014; Lopes, 2018).

Quanto aos dados que circulam nos CSs, a proteção destes tem dupla responsabilidade, tanto do detentor privado como do próprio Estado. Em relação à cibersegurança, está diretamente relacionada com os atores privados e os próprios utilizadores, enquanto a ciberdefesa considera o Estado como o ator central para a proteção (Galinec et al., 2017; Sunak, 2017).

Importa referir que a cibersegurança está diretamente interligada e associada à ciberdefesa. A ciberdefesa é conhecida pela capacidade de proteção da Soberania do Estado no ciberespaço, através do emprego dos meios para reagir contra ciberataques, prática de missões de Segurança e Defesa Nacionais a fim de preservar e proteger a segurança das comunicações, da informação, ou seja, também dos CSs (Galinec et al., 2017; NATO, 2014). No caso de ataque aos CSs, o Estado é considerado o ator central da proteção do território marítimo, contudo, a ciberdefesa atua de forma a evitar a existência de um ciberataque (Galinec et al., 2017; Nunes, 2012).

Ao se considerar a gestão do risco relacionado com a cibersegurança e a ciberdefesa, as Forças Armadas (FFAA), as Forças de Segurança e os Serviços de Informações têm um papel preponderante na proteção das IC assim como na Segurança e Defesa do Estado, “Os meios militares são uma componente fundamental da segurança do Estado” (RCM n.º 19/2013 de 5 de abril, 2013, p. 1982). De um modo mais preciso, as Forças de Segurança combatem o cibercrime e o hacktivismo e os Serviços de Informações a ciberespionagem e o ciberterrorismo, enquanto as FFAA combatem a ciberguerra:

“Desta forma, considera-se fazer sentido que as Forças de Segurança sejam responsáveis por coordenar a resposta do Estado às atividades relacionadas com o cibercrime e o hacktivismo, que os Serviços de Informações da República atuem

em casos de ciberespionagem e ciberterrorismo e que as Forças Armadas tenham que intervir para fazer face a ações de ciberguerra” (Nunes, 2012, p. 115).

Ao abordar um exemplo concreto, a escuta através dos CSs é classificada como uma operação cibernética, uma vez que, o tráfego mundial da *internet* circula através dos CSs (Brown, 2016). Os alvos principais que permitem a escuta submarina são os repetidores submarinos, “Segundo os relatórios publicados, este parece ser um método ciber-cinético¹³ combinado que introduz um novo item de equipamento físico num sistema para recolher inteligência cibernética” (Brown, 2016, p. 630), onde são recolhidas enormes quantidades de informações, podendo-se considerar uma “mina de ouro de espionagem” (Brown, 2016, p. 630). Num ataque deste tipo são conseguidos todos os dados que passam pelo cabo, os quais incluem dados de segurança nacionais, como dados comerciais e uma enorme quantidade de informações pessoais. Contudo, no que toca a este tema, a competência está presente nas Forças de Segurança e nos Serviços de Informações, que têm o dever de atuar em conformidade para resolver o crime. No caso dos equipamentos físicos serem projetados para serem conectados a CSs, a capacidade de bloquear ou interferir com o tráfego eletrónico seria uma boa forma de negar comunicações durante um conflito, porque o sistema poderia ser restaurado essencialmente sem custos após o conflito (Brown, 2016). Por fim, a simples presença no sistema poderia desenvolver um caso de espionagem ou a preparação para conflitos, tendo, para isso, a capacidade de intervir, as FFAA e os Serviços de Informações. De modo a permitir uma vigilância e monitorização acústica submarina eficazes, nas primeiras dezenas de quilómetros do CS a partir da CLS, introduz-se, interligado com este tema, o projeto do *Fibersense*. Através deste projeto, seria possível a deteção acústica da presença de qualquer objeto submarino que fosse ruidoso e que circulasse perto de um CS o que, neste caso, permitiria detetar o caso de espionagem abordado como exemplo. De acordo com o seguinte “A penetração dos cabos submarinos que transportam cumulativamente 99% do tráfego mundial da *Internet* foi provavelmente conseguida através de uma variedade de meios físicos” (Brown, 2016, p. 630) e “Como o equipamento de espionagem foi fisicamente ligado aos cabos, continuou a manter a

¹³ Ciber-cinético- refere-se a uma classe de ataques cibernéticos, que através da exploração dos alvos (sistemas, processos e redes de informação vulneráveis), aproveitam para acionar ou controlar processos físicos, causando danos físicos diretos ou indiretos. Englobam ofensivas originadas no domínio cibernético, com o objetivo de causar impacto diretamente no domínio cinético (Applegate, 2013).

presença no sistema” (Brown, 2016, p. 630), seria possível evitar o caso através desta tecnologia de fibra ótica.

Através do quadro resumo da **Tabela 1**, pode-se observar os atores/ intervenientes, quem possui a capacidade de atuação no caso de crime e os vários tipos de crime associados (Cordey & Dewar, 2019; Nunes, 2012).

Quem possui a ação (atores)		Tipos de crime
Cibersegurança	Forças de Segurança	Cibercrime
		Hacktivismo
	Serviços de Informações	Ciberespionagem
		Ciberterrorismo
Ciberdefesa	Forças Armadas	Ciberguerra

Tabela 1 - Cibersegurança e Ciberdefesa relação com atores e tipos de crime, adaptado de Estruturas de Coordenação Nacional no Ciberespaço

(Adaptado de Nunes, 2013)

Contudo, existe a possibilidade dos dois domínios se interligarem, obrigando a colaboração de ambos os atores para a obtenção de uma resolução mais eficaz no ambiente conhecido como o ciberespaço vinculado aos CSs, como abordado no exemplo anterior. Realça-se assim a importância desta cooperação para a eficiência da proteção dos CSs, tornando-se necessário a perceção relativamente a normas e políticas de utilização destes domínios.

3.2. Políticas e Regulamentações no caso de ataques aos cabos submarinos

O mundo dos CSs está-se a tornar cada vez mais um isco de fácil acesso. Estando inserido na SI, surgem diariamente novos desafios e crimes reais, que os envolvem (Militão, 2014). Torna-se, agora necessário conhecer que tipo de instrumentos legais existem, em conjunto com os órgãos do Ministério da Defesa Nacional (MDN), do Estado Maior General das Forças Armadas (EMGFA), assim como outros organismos importantes, que contribuem para a segurança e defesa dos CSs a nível nacional (Despacho n.º 13687/2013 de 28 de outubro, 2013).

Quanto à questão da cibersegurança ao nível do panorama nacional, existem quatro pilares fundamentais, sendo eles, o Centro Nacional de Cibersegurança (CNCS), o Centro de Ciberdefesa (CCD), a Polícia Judiciária (PJ) e o Serviço de Informações de Segurança (SIS). O *Computer Emergency Response Team* (CERT) existe a nível internacional e nacional. Apenas a nível nacional, o CNCS foi estabelecido pelo Decreto-Lei n.º 69/2014 de 9 de maio, no mesmo ano do CCD criado pelo Decreto-Lei n.º 184/2014 de 29 de dezembro (Morais, 2022). O CERT é responsável pela resolução de incidentes de segurança informática com o fim de poder criar alterações a longo prazo nos sistemas de rede, no que toca ao tema da cibersegurança, assim como de possíveis vulnerabilidades de segurança informática (CERT, s.d.; Jõgi, 2015). O CNCS, é responsável pela “implementação das medidas e instrumentos necessários à antecipação, à deteção, reação e recuperação de situações que, face à iminência ou ocorrência de incidentes ou ciberataques, ponham em causa o funcionamento das infraestruturas críticas e os interesses nacionais” (Decreto-Lei n.º 69/2014 de 9 de maio, 2014, p. 2715) e ainda:

“apostar claramente numa estratégia de prevenção, sensibilizando e educando as organizações em particular e a sociedade civil em geral para as questões da cibersegurança, contribuindo desta forma para a criação de uma comunidade de conhecimento e de uma cultura nacional de cibersegurança” (Leite, 2016, p. 8).

O CCD “constitui o órgão responsável pela condução de operações no ciberespaço e pela resposta a incidentes informáticos e ciberataques, com responsabilidades de coordenação, operacionais e técnicas” (Despacho n.º 13692/2013 de 28 de outubro, 2013, p. 31978). Compete ainda a este órgão:

“A defesa contra as ameaças cibernéticas deve incluir o reforço da proteção das redes, a monitorização e análise dos padrões de tráfego, a deteção precoce de ataques e a resposta aos mesmos, envolvendo para esse efeito, sempre que necessário, a condução de operações no ciberespaço” (Despacho n.º 13692/2013 de 28 de outubro, 2013, p. 31978).

Ao se considerar algumas categorias, a nível nacional, como principais, no que concerne à abordagem dos CSs, segurança das informações e dos STI, no domínio da segurança interna e externa, existe o organismo, apelidado de Sistema de Informações da República Portuguesa (SIRP), sendo caracterizado como:

“(…) o organismo público que tem a responsabilidade de prestar apoio ao decisor político, antecipando e avaliando as diferentes ameaças que visem Portugal e os seus interesses: a segurança interna e externa, a independência, os seus interesses nacionais, a integridade da unidade do Estado” (SIRP, s.d.).

O SIRP engloba, numa vertente interna, o Serviço de Informações de Segurança (SIS) e numa vertente externa, o Serviço de Informações Estratégicas de Defesa (SIED), importante para a cibersegurança numa perspetiva externa (SIRP, s.d.). O SIS é responsável pelos serviços de informações e é o único, em território nacional, com competência legal para atuar no campo das informações. Os serviços de informações atuam numa perspetiva preventiva, de modo a apoiar o decisor político, procurando antecipar a investigação criminal para a defesa do Estado (SIS, s.d.). Os serviços de informações englobam o Serviço de Informações Militares (SIM), que em Portugal tem o nome de Centro de Informações e Segurança Militares (CISMIL), estando integrado na estrutura do EMGFA, considerado muito importante no que se refere à defesa (Melo, 2011). Caracteriza-se como sendo “o órgão de informações e de segurança militares das FFAA e tem por missão assegurar a produção de informações necessárias ao cumprimento das missões das FFAA e à garantia da segurança militar” (EMGFA, s.d.). O SIED é “a entidade com competência exclusiva para a produção de informações tendentes à salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português” (SIED, s.d.).

Contribuindo de igual modo para este ecossistema, a Polícia Judiciária (PJ), está sob a dependência do Ministério da Justiça, no âmbito da justiça criminal e investigação criminal, sendo o principal ator e possui como especialidade, a repressão ao crime organizado, terrorismo e ainda muitos outros tipos de criminalidade de competência reservada (Lei n.º 49/2008 de 27 de agosto, 2008).

Ao ter-se em conta os pilares fundamentais da atuação do Estado, nos domínios da cibersegurança e da ciberdefesa, importa saber como funcionam no combate a ameaças sabendo que em muitos casos os perfis das ameaças e os modelos de terrorismo são imprevisíveis. Esta imprevisibilidade torna o Estado vulnerável e vem obrigar quer o próprio Estado, quer as organizações internacionais, à necessidade de assumirem novos formatos de cooperação, mais reforçados e eficazes (Diogo, 2004).

As ameaças e os ataques aos CSs são frequentes e podem ser de diversos tipos, como por exemplo, originários de causas naturais, fatores externos ou humanos sendo que estes últimos, se podem dividir em acidentais (pesca, arrastamento do ferro (âncora) dos navios ou dragagem) ou ataques maliciosos (ciberataques, ciberameaças ou terrorismo, entre outros) (Bueger et al., 2022; Eleftherakis & Vicen-Bueno, 2020). Tendo em consideração os tipos de ataques referidos, em média, são danificados entre 100 a 200 CSs, todos os anos (Clare, 2021).

Tipos de ameaças	Natureza	
	Interna	Externa
Natural	Não aplicável	Causas naturais como sismos, tsunamis, tempestades tropicais que provoquem alterações nas correntes subaquáticas, deslizamento de terra, erosão, temperatura extrema, ataques de animais marinhos
Deliberada	Sabotagem ou roubo	Terrorismo, crime, sabotagem, ação hostil, ação militar, insurreição, espionagem estatal ou corporativa, ciberataques, ativismo político
Acidental	Uso indevido de objetos (ferros ou artefactos de pesca), manutenção imprópria	Corte propositado do cabo
Deterioração	Desgaste, negligência, envelhecimento precoce do equipamento ou material	Fadiga pelo tempo, ferrugem da proteção mecânica

Tabela 2 - Tipos de ameaças consoante a natureza

(Adaptado de Boone, 2013)

As ciberameaças ainda se podem distinguir por cibercrime, ciberespionagem, hacktivismo, ciberguerra e ciberterrorismo (Barbosa, 2016). A ciberespionagem, o hacktivismo e os conflitos digitais têm vindo a ser cada vez mais prejudiciais, mas o cibercrime é que tem sido o mais prejudicial para a *internet* e o principal “protagonista” para a cibersegurança (Stevens, 2023). Quanto aos CSs, os mais prejudiciais são os ataques

físicos, a sabotagem e a espionagem (Recomendação (UE) 2024/779 de 26 de fevereiro, 2024; IT SECURITY, 2023). “Em média, ocorrem mais de uma centena de falhas nos cabos submarinos todos os anos, dois terços devido a âncoras de navios ou à pesca” (Ganz et al., 2024, p. 11; TeleGeography, 2024) e ainda “O risco de sabotagem intencional para os cabos submarinos é provavelmente muito maior, uma vez que a localização da maioria dos cabos é de conhecimento público” (Ganz et al., 2024, pp. 11-12), no entanto, não é fácil determinar se um ataque classificado como sabotagem ao um CS, é intencional ou não (Ganz et al., 2024). Não descurando o forte potencial de um ataque coordenado, tendo como referência o “Relatório sobre a cibersegurança e a resiliência das infraestruturas e redes de comunicações da UE” (Comissão Europeia, 2024), publicado pelos Estados-Membros da UE com o apoio da Comissão Europeia e da ENISA, a 21 de fevereiro de 2024, em que este relatório apresenta vários aspetos, destacando neste caso os potenciais cenários de risco, que apresentam um elevado nível de risco, o seguinte “R6. Ataque físico coordenado/ sabotagem à infraestrutura digital” (NIS Cooperation Group, 2024, p. 15), no qual se refere que:

“Um ator estatal lança um ataque físico coordenado/ sabotagem a múltiplos cabos submarinos redundantes, mas geograficamente próximos, a uma estação de desembarque de cabos e a um grande centro de dados que contém um IXP ou funciona como um *hub* de hiperconectividade. Além disso, o ator estatal também realiza uma sabotagem/ataque físico a um navio de reparação. A intenção do atacante é causar interrupções de rede em larga escala, afetando a conectividade à *Internet* de toda uma região da UE que depende principalmente de cabos submarinos. O ataque ao cabo submarino ocorre em águas internacionais, onde não está claro quem tem jurisdição legal. O incidente dura vários dias porque o reparo é lento e há um número limitado de navios de reparação” (NIS Cooperation Group, 2024, pp. 15-16).

Ou seja, conclui-se que este cenário se caracteriza também como um dos piores, que poderia acontecer aos CSs, com um elevado risco para estas infraestruturas.

Apesar do poder destrutivo do potencial dos ciberataques, têm vindo a tornar-se uma preocupação estratégica para os Estados e comunidades internacionais (Nunes, 2012). No âmbito nacional e internacional, o avanço das ciberameaças tem trazido um grande impacto na sociedade, o que exige o fortalecimento das capacidades de proteção

e defesa (Santos et al., 2012). Contudo, estas capacidades não são conseguidas da melhor forma “há uma necessidade urgente de criar novos sistemas para o tratamento eficiente de incidentes e apoiar a compreensão completa e comum de situações de ataques cibernéticos em tempo útil” (CNCS, 2020) e atendendo ao facto de que:

“A perceção de que os processos e mecanismos de cibersegurança existentes dificilmente acompanham a dinâmica das vulnerabilidades, levanta a necessidade urgente de uma forte sensibilização nacional para a importância de prevenir e responder à ocorrência de disrupções e ataques, garantindo assim a proteção e defesa das infraestruturas críticas e recursos de informação nacionais” (Nunes, 2012, p. 125).

Por outro lado, “Apesar destas ameaças, muitos estados não tomaram medidas de proteção para aumentar a segurança destes cabos. Além disso, não são impostas penalidades aos infratores por negligência ou dano deliberado” (Eleftherakis & Vicen-Bueno, 2020, p. 3), comprovado e de acordo com o seguinte autor, ainda se enuncia que:

“os cabos submarinos acabam por não ser devidamente protegidos no direito internacional. De facto, embora o artigo 113.º da CNUDM estabeleça que os Estados devem adotar leis que punam «a ruptura ou danificação, por um navio arvorando a sua bandeira ou por uma pessoa submetida à sua jurisdição, de um cabo submarino no alto mar, causadas intencionalmente ou por negligência culposa», a realidade é que a maioria dos países (incluindo Portugal) não possui legislação específica sobre esta matéria” (Monteiro, 2019, p. 4).

No qual se pode deduzir e concluir que a proteção dos CSs, segundo o direito internacional, não ocorre devidamente, da forma como estas IC deveriam ser protegidas (Monteiro, 2019). Quanto às ameaças, estas podem ser conduzidas tanto por pessoas isoladas (amadores, *hackers* ou *crackers*), por grupos (criminosos, grupos de pressão social ou terroristas) e ainda por outros Estados (ciberguerra) (Eleftherakis & Vicen-Bueno, 2020; Nunes, 2012).

No âmbito do plano nacional, em 2003, foi iniciado o desenvolvimento do Projeto de Proteção de Infraestruturas Críticas (PIC) pelo Conselho Nacional de Planeamento Civil de Emergência (CNPCE) com o propósito das IC fundamentais serem identificadas e protegidas, em território nacional, tanto em períodos de crise como apenas de forma

preventiva, através da formulação de políticas com uma maior adequação para assegurar a proteção destas infraestruturas (Leite, 2016).

Devido à falta de proteção, em 2008, foi publicado no Relatório sobre a Execução da Estratégia Europeia de Segurança, a necessidade de existir “mais capacidade, mais coerência e mais acção” (União Europeia, 2009, p. 9). Somente em 2009 é que surgiu em Portugal, a Lei do Cibercrime, Lei n.º 109/2009 de 15 de setembro, relativa a ataques contra sistemas de informação (Lei n.º 109/2009 de 15 de setembro, 2009). Posto isto, em Portugal, no ano de 2015, foi publicada a primeira Estratégia Nacional de Segurança do Ciberespaço (ENSC) a fim de se estabelecer objetivos e linhas de ação para atingir uma eficaz gestão de crises, coordenação da resposta operacional a ciberataques e intensificação da cooperação nacional, europeia e internacional no domínio do ciberespaço (Nunes, 2012).

De acordo com o quadro legislativo que existe em Portugal, em matéria de terrorismo, é o SIS que tem a competência de identificar ameaças à segurança interna, sendo depois a informação conduzida a outras entidades responsáveis (Decreto-Lei n.º 226/2006 de 15 de novembro, 2006). A Lei n.º 53/2008 de 29 de agosto, aprovou a Lei de Segurança Interna, sendo que esta Lei se destina principalmente, segundo o artigo 1º, a:

“Proteger a vida e a integridade das pessoas, a paz pública e a ordem democrática, designadamente contra o terrorismo, a criminalidade violenta ou altamente organizada, a sabotagem e a espionagem, a prevenir e reagir a acidentes graves ou catástrofes, a defender o ambiente e a preservar a saúde pública” (Lei n.º 53/2008 de 29 de agosto, 2008, p. 6135).

Na medida em que, está relacionada com os atos de criminalidade, sabotagem e espionagem, sendo por este motivo relevante para este tema, assim como, considerando os CSs IC de comunicações, segundo o artigo 18º, uma das competências de controlo é: “Ataques a órgãos de soberania (...) infra-estruturas destinadas ao abastecimento e satisfação de necessidades vitais da população, meios e vias de comunicação (...) e infra-estruturas classificadas como infra-estruturas nacionais críticas” (Lei n.º 53/2008 de 29 de agosto, 2008, p. 6138).

Contudo, o Decreto-Lei n.º 62/2011 de 9 de maio trouxe a relevância da proteção das IC, nomeadamente, os procedimentos de identificação e proteção das IC, os quais

versam sob duas dimensões já abordadas neste capítulo, *safety* e *security*, “Seja em simultâneo ou individualmente, qualquer uma destas dimensões é fulcral para obter, em matéria de IC, quer uma identificação assertiva, quer medidas efetivas de proteção contra as ameaças e riscos” (Martinho, 2017, p. 6). Embora este Decreto seja direcionado para as infraestruturas críticas europeias, trouxe a obrigatoriedade de elaboração de planos de segurança por parte dos operadores dos cabos e determina a existência de planos de segurança externos, fazendo a aplicação dos mesmos para as infraestruturas críticas nacionais (Martinho, 2017).

Ainda relacionado com este tema, de acordo com a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que defende que, “Os ciberataques são de natureza transfronteiriça e um incidente significativo pode perturbar e danificar infraestruturas críticas de informação das quais depende o bom funcionamento do mercado interno” (Diretiva (UE) 2022/2555 de 14 de dezembro, 2022, p. 94), ou seja, meter em risco o país. Ao atender-se ao Regulamento (UE) 2019/796 do Conselho, de 17 de maio de 2019, este aborda e defende o seguinte, segundo o artigo 1.º, número 4., alínea a) “os ciberataques que constituem uma ameaça para os Estados-Membros incluem os que afetam os sistemas de informação relacionados, nomeadamente, com (...) infraestruturas críticas, incluindo cabos submarinos” (Regulamento (UE) 2019/796 de 17 de maio, 2019, p. 2). Ainda relacionado, de acordo com a Recomendação (UE) 2017/1584 de 13 de setembro de 2017 sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala, no n.º 4, tem-se o seguinte:

“Os incidentes de cibersegurança são imprevisíveis, ocorrem e evoluem, frequentemente, num curto espaço de tempo, pelo que as entidades afetadas e os responsáveis pela reação e atenuação dos efeitos do incidente devem coordenar rapidamente as suas ações de resposta. Além disso, muitas vezes os incidentes de cibersegurança não se confinam a uma área geográfica específica, podendo ocorrer em simultâneo ou propagar-se imediatamente por vários países” (Recomendação (UE) 2017/1584 de 13 de setembro, 2017, p. 36).

Conclui-se, desta forma, que os ciberataques assim como os incidentes de cibersegurança, constituem uma ameaça podendo vir a afetar os sistemas de informação, mais precisamente, as infraestruturas críticas de informação, no qual se incluem os CSs.

Assim como a Diretiva (UE) 2022/2555, enuncia, no artigo 7.º relativo à Estratégia nacional de cibersegurança, no ponto 2., alínea d), “os Estados-Membros devem adotar, em especial, políticas (...) sobre a manutenção da disponibilidade geral, da integridade e da confidencialidade do núcleo público da *Internet* aberta, incluindo, quando pertinente, a cibersegurança dos cabos submarinos de comunicações” (Diretiva (UE) 2022/2555 de 14 de dezembro, 2022, p. 115), o que conclui a ligação da cibersegurança com a rede dos CSs.

O Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, é relativo à Agência da União Europeia para a Cibersegurança (ENISA) e à certificação da cibersegurança das TIC, estando inserido neste tema e sendo um regulamento que visa alcançar um nível elevado de cibersegurança, segundo o número (29) deste Regulamento:

“Com vista a estimular a cooperação entre o setor público e privado e dentro do setor privado, nomeadamente para apoiar a defesa de infraestruturas críticas, a ENISA deverá apoiar a partilha de informações dentro dos diferentes setores e entre eles ... bem como prestando orientações sobre a forma de abordar questões regulamentares relativas à partilha de informações, designadamente facilitando a criação de centros de partilha e análise de informações a nível setorial” (Regulamento (UE) 2019/881 de 17 de abril, 2019, p. 19).

A ENISA é uma agência da União que foi criada pelo Regulamento (CE) n.º 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004 com o fim de atingir um elevado e eficaz nível comum de cibersegurança na União e “desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores, das empresas e das administrações públicas” (Regulamento (UE) 2019/881 de 17 de abril, 2019, p. 17), segundo o número (14) do presente Regulamento. Esta agência tende a reforçar a resiliência das infraestruturas da UE, apoiando, também, mas não só, o setor das TIC (ENISA, s.d.). Funciona como “centro de conhecimentos especializados em cibersegurança, recolhendo informação e disponibilizando assistência e aconselhamento técnico independente e de elevada qualidade aos Estados-Membros e organismos da UE em matéria de cibersegurança” (Regulamento (UE) 2019/881 de 17 de abril, 2019, p. 34) e ainda contribui para o fortalecimento das capacidades de preparação e na resposta da

Europa a ciberincidentes, contribuindo assim para a política cibernética da UE (ENISA, 2020; ENISA, s.d.).

No que se refere às infraestruturas críticas, segundo a Comunicação da Comissão Europeia ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, foi emitido este documento em 31 de março de 2011, relativo à Proteção das infraestruturas críticas da informação “Realizações e próximas etapas: para uma cibersegurança mundial” (Comissão Europeia, 2011, p. 1), contudo, em 2009 já existia essa preocupação:

“Em 30 de Março de 2009, a Comissão adoptou uma Comunicação relativa à protecção das infra-estruturas críticas da informação (PICI) - «Proteger a Europa contra os ciberataques e as perturbações em grande escala: melhorar a preparação, a segurança e a resiliência», que apresenta um plano (o «Plano de Acção PICI») destinado a reforçar a segurança e a resiliência das infra-estruturas TIC (tecnologias da informação e das comunicações) vitais” (Comissão Europeia, 2011, p. 2).

Salienta-se que a Comissão adotou a comunicação sobre a Proteção das Infraestruturas Críticas da Informação (PICI), a 30 de março de 2009, e que constam no documento, detalhes sobre os principais desafios das infraestruturas críticas de informação, é proposto um plano de ação, destinado a aumentar a proteção e ainda, se destaca que a política:

“visa reforçar a segurança e a resiliência das infraestruturas vitais para as TIC, estimulando e apoiando o desenvolvimento de um alto nível de preparação, a segurança e a capacidade de resiliência, tanto a nível nacional como a nível da UE” (ANETIE, s.d.).

Contudo, estando relacionado com o Documento acima mencionado, tem-se o Decreto-Lei n.º 20/2022 de 28 de janeiro de 2022, sobre a Resiliência das Infraestruturas Críticas Nacionais e Europeias, em que são estabelecidos, no artigo 1.º, alínea a), “os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias” (Decreto-Lei n.º 20/2022 de 28 de janeiro, 2022, p. 3).

Ainda se destaca o “Relatório sobre a cibersegurança e a resiliência das infraestruturas e redes de comunicações da UE” (Comissão Europeia, 2024), apresentado anteriormente, no qual foram identificadas muitas ameaças que metem em risco as redes e infraestruturas de comunicações. De modo a atenuarem estes riscos, apresentam-se no relatório, várias recomendações estratégicas, sendo a seguinte uma das mais relevantes relacionadas com o tema, a “SR2. Avaliar a criticidade, resiliência e redundância das infraestruturas essenciais da *Internet*, como os cabos submarinos” (NIS Cooperation Group, 2024, p. 18).

Por último, relativamente aos regulamentos com este assunto relacionados, tem-se, a Recomendação da UE 2024/779 da Comissão Europeia, sobre infraestruturas de cabos submarinos seguras e resilientes, elaborada a 26 de fevereiro de 2024 com vários objetivos, sendo:

- O aumento da segurança física e cibernética dos CSs;
- Propõe medidas para melhorar a resiliência dos próprios cabos contra interrupções causadas por causas naturais ou atividades humanas;
- Incentiva a cooperação e a coordenação internacionais entre os Estados-Membros da UE e outras partes interessadas, incluindo empresas de telecomunicações e operadores de cabos, para partilhar informações e melhores práticas sobre a segurança e a manutenção dos cabos submarinos;
- Recomenda o desenvolvimento de políticas e normas comuns a serem adotadas pelos Estados-Membros de forma a assegurar uma abordagem coordenada e harmonizada em relação à proteção das infraestruturas de cabos submarinos;
- Incentiva investimentos em tecnologias avançadas e pesquisa para desenvolver métodos mais eficazes de monitorização e proteção dos cabos submarinos;
- Estabelece a necessidade de revisões e atualizações regulares das práticas e políticas de segurança, levando em consideração o avanço tecnológico e as novas ameaças.

Embora os CSs pertençam ao Estado, Estado costeiro e a empresas privadas, impõem a obrigatoriedade da partilhada participação de diferentes poderes no que se refere à gestão da segurança destas IC, que transpõe uma grande questão geopolítica e geoestratégica. Mas, segundo o autor Sunak:

“embora os investimentos por parte das empresas privadas desonerem os gastos governamentais, e aumente a resiliência da infraestrutura, as empresas pouco refletem sobre a relevância dos cabos submarinos para a segurança dos países. Além disso, uma vez que a infraestrutura não configura uma propriedade formal dos Estados, não há uma proteção robusta estabelecida no que tange o direito internacional” (Sunak, 2017; Vichi, Pinto, & Sá, 2020, p. 332).

Contudo, tendo em conta que os “cabos submarinos também podem ser usados como ferramentas de ciberespionagem e recolha de informações” (Davenport, 2015, p. 59; Khazan, 2013), ou seja, podem ser utilizados para se obterem informações importantes sobre o país, através da sabotagem ou até mesmo de ataques físicos, importa intensificar o facto de que:

“A construção de um futuro digital para Portugal, seguro e sustentável, passa assim por um desafio coletivo e por uma partilha de responsabilidades que envolva, numa visão conjunta, o governo, a administração pública, forças armadas e de segurança, empresas e cidadãos” (Nunes, 2012, p. 125).

O facto dos CSs atravessarem várias jurisdições, sem uma entidade soberana “A segurança marítima é intrinsecamente geopolítica, posto que se trata de projetar o poder público além das suas fronteiras externas dentro do domínio global marítimo” (Germond, 2015, p. 141), deduz-se, portanto, que a segurança dos CSs, antes de ser um problema nacional, é considerada um problema global.

Posto isto, uma vez que são as empresas privadas que têm a responsabilidade pelos cabos, os Estados-Membros decidiram criar uma série de cenários de risco com importância estratégica, do ponto de vista da UE (Recomendação (UE) 2024/779 de 26 de fevereiro, 2024; O'Malley, 2019). De forma a comprovar o acima referido, a Recomendação da UE 2024/779 da Comissão Europeia, destaca o incentivo aos Estados-Membros, da elaboração de “testes de esforço com base em princípios comuns a nível da União e, em especial, nas avaliações consolidadas, à escala da União, dos riscos, vulnerabilidades e dependências das infraestruturas de cabos submarinos” (Recomendação (UE) 2024/779 de 26 de fevereiro, 2024, p. 9) pelos operadores dos CSs, coordenados a nível da União, com o objetivo de contribuírem para futuras avaliações de risco. Os testes “ajudarão a avaliar a resiliência das entidades em diferentes cenários”

(Recomendação (UE) 2024/779 de 26 de fevereiro, 2024, p. 4) a fim de garantir que os CSs permaneçam seguros.

3.3. Propostas de atuação que garantam a segurança dos cabos submarinos

Atualmente, os sistemas de comunicações não se encontram tão devidamente protegidos como deveriam. Estas IC fazem parte do património mundial de dados, o que implica que tanto a segurança a nível nacional como a nível internacional, se encontre claramente dependente e comprometida pela segurança dos CSs (Santos, 2011).

Neste subcapítulo, são apresentadas algumas propostas de atuação que visam garantir a proteção e segurança da operação contínua e confiável dos CSs, uma vez que se destaca a necessidade crítica de implementação de medidas robustas de proteção (Saraiva, 2022). Apresentam-se, de seguida, as seguintes propostas elaboradas:

- a. Reforçar as competências do Estado costeiro quanto ao lançamento e implantação de CSs na ZEE e na PLATCON.
- b. Assegurar uma proteção mais adequada e eficaz nos *Beach Manhole* (BMH), restringindo o acesso indesejado, utilizando perímetros de segurança ou sensores de movimento, uma vez que se encontram enterrados na costa/ praia e são facilmente alcançáveis.
- c. A nível da colocação dos CSs:
 - Evitar a colocação de CSs em zonas onde tenha sido reportado uma vasta quantidade de casos de incidentes com navios ou embarcações, zonas de atracação ou locais de fundeadoiro;
 - Evitar a montagem de CSs perto de locais que são muito utilizados para atividades Humanas, devido à exploração de recursos marinhos, como a pesca de arrasto ou a instalação de infraestruturas *offshore*.
- d. Implementação de sistemas e observação do fundo do mar:
 - Proceder à implementação de sistemas de deteção nos CSs, através da tecnologia SMART para fornecer informações sobre o fundo do mar, através do uso de sensores, para apoio da climatização, vigilância oceânica e o alerta precoce de causas naturais (como sismos e tsunamis);

- Melhorar as capacidades de mapeamento e monitorização avançados dos oceanos através do uso de aparelhos e veículos autónomos que o permitam como o caso dos *landers*¹⁴ e *gliders*¹⁵;
 - Detetar atividades suspeitas próximas aos CSs através de sistemas autónomos que possuam capacidade para efetuarem varredura lateral e que sejam protegidos com sistemas altamente capacitados de proteção de dados ou roubo (possuam ainda GPS e Sistemas de Identificação Automática (AIS) para identificar os navios que o atravessem);
 - Implementar tecnologias avançadas de deteção, como sistemas de deteção de intrusão acústica e câmaras subaquáticas de alta resolução, que permitam identificar e responder rapidamente a tentativas de danificar ou interferir nos CSs;
 - Investigação detalhada/ Estudo/ Implementação do uso da tecnologia de Deteção Acústica Distribuída (DAS) através da utilização de cabos de fibra ótica a fim de melhorar a monitorização e o conhecimento situacional marítimo através de sensores capazes de captação e deteção submarina no âmbito da segurança e proteção do domínio marítimo.
- e. Promover a cooperação internacional entre países para desenvolver padrões comuns de segurança e regulamentações para proteger os CSs em águas internacionais, garantindo a conformidade e a implementação eficaz de medidas de proteção. Pode-se justificar esta necessidade pela citação do Centro de Excelência para a Ciberdefesa Cooperativa da OTAN (CCDCOE), “No entanto, os cabos submarinos para ligarem vários países e continentes têm de passar em águas internacionais, não podendo ser protegidos pela legislação nacional de um país” (CCDCOE, 2019, p. 1).
- f. Melhorar a capacidade física dos CSs utilizando tecnologia avançada:
- Utilizar técnicas de engenharia avançadas para reforço das componentes físicas dos CSs e instalação de melhores proteções físicas;

¹⁴ *Landers* são sistemas submersíveis de posicionamento autónomo para monitorização sísmica e acústica, projetados para permanecer no mar por longos períodos. Têm a capacidade de ir até à profundidade dos 1000 metros. Permitem comunicações acústicas com a superfície, comunicações GPS e sem fios e têm um processamento e recolha de dados incorporado. Possuem ainda uma câmara com capacidade de “*time-lapse*” (ECOREST, 2023; Person et al., 2006).

¹⁵ *Gliders* são sistemas autónomos que se movimentam através das próprias alterações de flutuação, projetados para atingirem profundidades até 1500 metros e servem para monitorização dos oceanos (Eleftherakis & Vicen-Bueno, 2020; Lancker & Baeye, 2015).

- Desenvolvimento de técnicas avançadas com capacidade para reparações de emergência que possam ser rapidamente implementados em caso de danos aos CSs, incluindo o uso de Veículos Autónomos Subaquáticos (AUVs) para realizar reparações submarinas complexos de forma rápida;

- Promover o investimento contínuo em pesquisa e desenvolvimento tecnológico para identificar soluções inovadoras que melhorem a segurança e a eficiência dos CSs;

- Estabelecer programas de manutenção preventiva e inspeção regular aos CSs, incluindo o uso de Veículos subaquáticos Controlados Remotamente (ROVs) para realizar inspeções visuais, possuindo câmaras para avaliar, com regularidade, a integridade dos cabos;

- Integrar sistemas de monitoração ambiental para avaliar o impacto das operações de instalação e manutenção dos cabos submarinos no ecossistema marinho e implementar medidas para prevenir danos ecológicos através do uso de materiais eco-amigáveis e práticas de instalações sustentáveis.

g. Desenvolvimento de rotas alternativas no caso de incidente com uma rota submarina, ou seja, desenvolver redes de CSs com rotas diversificadas e implementar sistemas de redundância para garantir a continuidade do serviço em caso de interrupção numa determinada rota.

h. Incentivar e consciencializar a população sobre a importância dos CSs:

- Promover a consciencialização pública através do desenvolvimento de campanhas para dar a conhecer a importância dos CSs e a catastrófica potencialidade de acidentes que podem ocorrer com estas infraestruturas, fazendo obrigatoriamente parte do público alvo, os pescadores, operadores de embarcações e toda a população no geral;

- Colaborar com a indústria de pesca e navegação com o objetivo de estabelecer parcerias colaborativas através do desenvolvimento de diretrizes de segurança e melhores práticas que minimizem o risco de danos aos CSs durante atividades comerciais e recreativas em áreas submarinas.

i. Proposta de elaboração de um Protocolo/ Convenção Internacional a uma Convenção existente que permita tipificar, em sede internacional, o crime de disrupção dos CSs, na forma tentada ou consumada, a título doloso ou negligente, nos espaços marítimos para além da jurisdição dos Estados (isto é,

Área e Alto mar). Pretende-se, desta forma, legitimar a intervenção dos navios de guerra ou equipados (de um determinado Estado) para vigiarem, monitorizarem e fiscalizarem os CSs nos espaços marítimos internacionais e, poderem abordar um navio ou uma embarcação suspeito.

Explica-se melhor esta proposta de atuação (i.), fazendo um enquadramento da Convenção para a Supressão de Atos Ilícitos Contra a Segurança da Navegação Marítima (*SUA Convention*), que é um Tratado Internacional, adotado pela OMI em 1988 com o fim de reforçar a segurança da navegação marítima e combater atos ilegais (como o terrorismo e pirataria) que possam ameaçar a segurança de navios mercantes e plataformas marítimas. Esta Organização decidiu adotar a Convenção SUA, uma vez que houve um aumento das preocupações internacionais no que se refere à segurança marítima e, concretamente, contra atos ilícitos praticados a bordo e que não sejam classificados de atos de pirataria. O objetivo principal desta convenção é garantir que os atos ilícitos cometidos contra a segurança da navegação sejam considerados crimes em todos os países signatários, proporcionando uma base legal para a apreensão, julgamento e punição de indivíduos envolvidos nestes atos (UN General Assembly, 1992). Em 2005, a Convenção passou a incluir, após a criação de um novo Protocolo, embarcações que fossem utilizadas para fins terroristas, transporte de materiais perigosos, assim como outras atividades relacionadas com o terrorismo (IMO, s.d.), abrangendo as plataformas *offshore*.

Interligando o assunto abordado acima com o tema dos CSs, seria um grande reforço para a segurança destas infraestruturas, a criação deste novo Protocolo a esta Convenção com o objetivo de se estender à proteção dos CSs devido à importância que estes cabos possuem a nível global, podendo vir a serem classificados como infraestruturas críticas (Diretiva (UE) 2022/2555 de 14 de dezembro, 2022).

De forma a mitigar os ataques aos CSs, torna-se relevante enfatizar a utilização da IA, mais concretamente, o ML que é utilizado na cibersegurança. Como já foi mencionado anteriormente, realça-se a existência de uma ligação entre o ciberespaço e os CSs, devido, de uma forma geral, aos dados que circulam nestas infraestruturas, portanto, a utilização da IA vem enriquecer a segurança deste domínio (Dasgupta et al., 2022).

Tendo em conta que “o ciclo de vida da segurança abrange três processos: a prevenção, deteção e reação” (Apruzzese et al., 2023, p. 7), existem mecanismos de

segurança, baseados em ML, que se concentram na detecção de ameaças cibernéticas (Williams et al., 2018). Destacam-se, assim, a detecção de intrusões de rede, a detecção de *malware* e a detecção de *phishing*.

Contudo, através da implementação destas propostas de atuação, estando algumas prestes a serem implementadas e outras por implementar, em conjunto com as que já existem, poder-se-á encontrar infraestruturas mais protegidas e garantir a segurança das vias de comunicação oceânicas, a importância da utilização contínua da conectividade global e alcançar a soberania digital europeia.

4. Ciberespaço: Organização, Segurança e Defesa

O conceito Ciberespaço surgiu em 1984, por *William Gibson*, no romance revolucionário de ficção científica, intitulado por *Neuromancer*. A partir desse ano o mundo tecnológico tem vindo a evoluir, combinado com diversas alterações, devido à descoberta das Tecnologias da Informação e Comunicação (TIC) (Raboin, 2011; Singer & Friedman, 2014).

De acordo com muitos especialistas, o termo ciberespaço define-se como um ambiente tecnológico digital (um ambiente virtual/ artificial), não sendo somente governado por uma nação, ou seja, não está sujeito à soberania de um único Estado ou grupo de Estados. Este ambiente é formado por um conjunto de sistemas informáticos interligados capazes de armazenar, processar e utilizar a informação, permitindo a comunicação através de redes cooperativas e da *internet* no qual se agrupam e relacionam utilizadores humanos, linhas de comunicação, *sites* e serviços de *internet* (Clark, 2010; Ottis & Lorents, 2011; Santos, 2011). Sendo, no geral, mais do que “a *Internet*, incluindo não apenas *hardware*, *software* e sistemas de informação, mas também pessoas e interação social dentro destas redes” (Klimburg, 2012, p. 8). Torna-se num ambiente único, com regras, técnicas, métodos e políticas com um uso diferenciado (Ottis & Lorents, 2011; Singer & Friedman, 2014).

Este domínio pode ser assumido como um ambiente virtual onde todos os sistemas têm a capacidade de comunicar mutuamente, portanto, estão todos vulneráveis aos riscos e perigos que existem no mundo digital devido a esta partilha constante de comunicações (Neves, 2015). O ciberespaço não é uma exceção, uma vez que, as vulnerabilidades existem em todo o tipo de sistemas de informação (Singer & Friedman, 2014).

Atualmente o ciberespaço é reconhecido como um espaço vital e caracterizado de diferentes formas, conhecendo-se, principalmente, enquanto via de comunicação onde circulam as informações através de computadores ligados em rede ou pela realidade virtual (Maias & Bravo, 2010). Salienta-se a seguinte, que se encontra na publicação da OTAN, *Allied Joint Doctrine for Cyberspace Operations* (AJP-3.20) e apresenta o ciberespaço como:

“O ciberespaço não se limita, mas na sua essência consiste num ambiente informatizado, construído artificialmente e em constante desenvolvimento. A

infraestrutura do ciberespaço está em grande parte interconectada globalmente; no entanto, as fronteiras geográficas aplicam-se no contexto da jurisdição, com responsabilidades nacionais. É por isso que a atribuição de fronteiras operacionais clássicas no ciberespaço é particularmente difícil. O ciberespaço não está apenas em constante fluxo, mas ainda mais importante, pode ser usado por qualquer pessoa para quase todos os fins. O ciberespaço também se distingue pelo facto de os seus elementos físicos subjacentes serem inteiramente criados pelo homem, o que é diferente da terra, do ar, do espaço e do mar. Os riscos no ciberespaço podem ser geridos através da manipulação do próprio domínio” (NATO, 2020, p. 2).

O cenário atual, no âmbito do ciberespaço, obriga os vários Estados a definirem estratégias de forma a defenderem os ativos e interesses estratégicos (Santos, 2017). Uma vez que Portugal integra tanto a OTAN como a UE, importa destacar a envolvimento destas duas organizações neste tema. A fim de se lidar com as problemáticas de “segurança no ciberespaço, a Defesa cooperará com intervenientes internacionais, como a UE, a OTAN, o BENELUX, a ONU e outros parceiros, de acordo com os acordos celebrados” (ACOS STRAT, 2014, p. 9). Uma vez que o “ciberespaço requer uma abordagem estratégica específica e doutrinas específicas. A Defesa desenvolverá conceitos, processos e procedimentos especiais para recrutamento, sensibilização, educação e formação, aquisição de equipamento, capacidade de mobilização” (ACOS STRAT, 2014, p. 10). Posto isto, em 2013, a Comissão Europeia aprovou a “Estratégia da União Europeia para a Cibersegurança: Um ciberespaço aberto, seguro e protegido” (Comissão Europeia, 2013, p. 1). Portugal aprova a Estratégia Nacional de Segurança do Ciberespaço, a 12 de junho de 2015 (RCM n.º 36/2015 de 12 de junho, 2015), tendo sido esta a primeira versão da ENSC, embora esteja à data atual, revogada. À data da presente Dissertação, existe, em vigor, a ENSC para o período de 2019-2023, aprovada pela RCM n.º 92/2019, a 5 de junho de 2019 (RCM n.º 92/2019 de 5 de junho, 2019). A ENSC 2024 está na iminência de estar terminada. Em contacto com o CNCS e com o XI Curso de “Cibersegurança e Gestão de Crises no Ciberespaço”, conforme o **Anexo C- Certificado de participação no XI Curso de “Cibersegurança e Gestão de Crises no Ciberespaço”**, uma possível previsão para a publicação da mesma, será numa data antecedente ao mês de outubro.

Relativamente à responsabilidade pelo ciberespaço, uma das competências do Conselho Superior de Segurança do Ciberespaço (CSSC)¹⁶ é, segundo o artigo 4.º, alíneas b) e c), verificar a implementação, propor a revisão e elaborar a Estratégia Nacional de Segurança do Ciberespaço (ENSC) (Despacho n.º 1195/2018 de 2 de fevereiro, 2018).

Apesar das incumbências do CSSC, é difícil prever o futuro do ciberespaço, uma vez que surgem constantemente novas ameaças que põem em risco este domínio, tornando-se numa dificuldade acrescida a previsão do futuro deste. A Inteligência Artificial (IA) trouxe novas oportunidades para o mundo cibernético e com estas novas oportunidades, surgirão também novas ameaças. Quando ocorre um ataque no ciberespaço, existe uma dificuldade tremenda em estudar e perceber quem iniciou o ataque, quais foram os alvos (podendo ser múltiplos). Acrescenta-se o facto de que não existindo limites territoriais, ou melhor, fronteiras físicas, devido à vasta dimensão que possui, torna os riscos e perigos potencializados por atores muito divergentes, dificultando a identificação do indivíduo, grupo ou Estado (ACOS STRAT, 2014).

4.1. Operações militares no ciberespaço com ligação à OTAN e à Marinha Portuguesa

De uma forma crítica, não se deve desassociar o ciberespaço dos Cabos Submarinos (CSs), uma vez que, no que se refere à informação, ambos são vitais para a soberania de um Estado (Neves & Correia, 2016). Como prova da afirmação acima mencionada, no caso de um atacante querer interromper o acesso a um determinado Estado para evitar o contacto deste com os Aliados, o objetivo seria desenvolver um ataque coordenado em que os alvos seriam o ciberespaço e os CSs (Rose, 2017). De modo a garantir a segurança e qualidade da informação que circula neste domínio e nas IC, será necessário a defesa quer do ciberespaço, quer dos CSs por parte das FFAA, sabendo que a segurança da informação e a proteção das IC são da responsabilidade do Estado (Neves & Correia, 2016).

¹⁶ De acordo com o Despacho n.º 1195/2018, de 2 de fevereiro de 2018, sendo este o Regulamento Interno do Conselho Superior de Segurança do Ciberespaço, segundo o artigo 1.º, “O Conselho Superior de Segurança do Ciberespaço (CSSC) é o órgão específico de consulta do Primeiro-Ministro para os assuntos relativos à segurança do ciberespaço” (Despacho n.º 1195/2018 de 2 de fevereiro, 2018, p. 3949).

O facto do ciberespaço ser um domínio de livre acesso, permite ações providas de qualquer indivíduo o que afeta as FFAA e torna-se numa vulnerabilidade aplicada aos ataques cibernéticos (NATO, 2020), atendendo à citação seguinte, “Em cerca de 300 milissegundos, um toque numa tecla pode viajar duas vezes ao redor do mundo, mas a investigação forense necessária para identificar um atacante no ciberespaço pode levar semanas, meses ou até anos”, uma simples ação deste género, pode originar consequências devastadoras (ACOS STRAT, 2014, p. 6).

A capacidade de Comando e Controlo (C2) efetiva, torna a condução de uma operação militar eficaz, assim como a capacidade de segurança da informação que circula no ciberespaço, através das IC nacionais. Contribuem para a confidencialidade, integridade e disponibilidade dos STI, que devem ser altamente resilientes face às ameaças do ciberespaço, tanto em tempo de paz como em conflitos armados (NATO, 2020).

O facto da Marinha Portuguesa ser um dos três ramos pertencentes às FFAA, faz desta um organismo de defesa do ciberespaço. De modo a conseguir-se implementar capacidades operacionais¹⁷ de ciberdefesa na Marinha Portuguesa, apresenta-se a metodologia adotada pela OTAN, Doutrina, Organização, Treino, Material, Liderança, Pessoal, Infraestruturas e Interoperabilidade (DOTMLPI-I)¹⁸, sendo estes os componentes básicos para constituir uma capacidade operacional, ou seja, para a transformação de objetivos estratégicos em capacidades operacionais (Despacho n.º 11400/2014 de 11 de setembro, 2014).

Esta metodologia serve para identificar lacunas na operação das capacidades operacionais, tendo uma grande relevância no que concerne à perspetiva militar. Apresenta-se de seguida, o significado de cada um dos termos mencionados anteriormente, tendo em conta a resposta a incidentes no âmbito da cibersegurança.

¹⁷ Uma capacidade operacional, de acordo com a definição da OTAN é “a possibilidade de um comandante militar conseguir executar um conjunto específico de ações, identificando os efeitos necessários para atingir determinado objetivo” (NATO, 2009; Neves & Correia, 2016).

¹⁸ A metodologia DOTMLPI-I foi desenvolvida pelo Departamento da Defesa dos EUA, *Department of Defense* (DoD). Refere-se aos componentes básicos da edificação de uma capacidade operacional (Neves, 2015).

Ao se ter em conta que o domínio do ciberespaço está relacionado com a cibersegurança, em que se atinge, portanto, uma situação ótima, quando “a proteção do ciberespaço seja proporcional à ameaça cibernética e às possíveis consequências dos ataques cibernéticos” (ACOS STRAT, 2014, p. 18), de uma forma generalizada, a cibersegurança garante a proteção do sistema interno através de medidas de segurança que visam proteger tanto a comunicação, como a informação e ainda os sistemas eletrónicos que estão associados aos dados (NATO, 2020). Pode-se relacionar a Doutrina, uma vez que esta é essencial para a construção de uma capacidade de cibersegurança. Através da Doutrina são estabelecidas as normas a serem realizadas, os objetivos e desígnios de uma legislação, entre outros, dependendo de que documento se tratar, podendo-se chamar, de uma forma ambígua, documentos doutrinários, como o nome indica.

A nível prático, são utilizados diplomas legais, políticas e estratégias para evitar ambiguidades (Neves & Correia, 2016), a nível nacional e numa perspetiva jurídica, existe a Lei n.º 46/ 2018 de 13 de agosto de 2018, que estabelece o regime jurídico da segurança do ciberespaço. Esta Lei contém a estrutura de segurança do ciberespaço, aborda a segurança dos Sistemas de Informação e ainda define uma estratégia de ação relativa à dimensão da cibersegurança (Lei n.º 46/2018 de 13 de agosto, 2018). A ENSC 2019-2023 sendo a mais recente estratégia implementada neste âmbito, é considerada, para a segurança do ciberespaço, um instrumento essencial (Neves, 2015; RCM n.º 92/2019 de 5 de junho, 2019).

A Marinha Portuguesa, no que se refere à segurança da informação e dos Sistemas de Informação e Comunicações (SIC), a nível interno, rege-se pelas seguintes Publicações de Comunicações da Armada (PCA), PCA 2- Doutrina para os Sistemas de Informação e Comunicação Automatizados (SICA) na Marinha, PCA 3- Política de segurança para interligação de redes e sistemas de informação e comunicação automatizados, PCA 10- Conceito de implementação dos sistemas de informação e comunicação automatizados (SICA) no domínio do utilizados, PCA 15- Doutrina para a Intranet e *Internet* na Marinha e PCA 16- Conceito de Implementação da Capacidade de Resposta a Incidentes de Segurança da Informação na Marinha, conhecida como a publicação mais importante no que toca à ciberdefesa na Marinha.

Ao nível dos domínios dos três ramos das FFAA, em conjunto com o espacial, cibernético e de informações, tem-se o Comando Conjunto para as Operações Militares (CCOM). Este é “indispensável para a adaptação das Forças Armadas ao novo contexto global de segurança, que exige a edificação de capacidades numa lógica de maximização do produto operacional conjunto, bem como a integração da informação operacional dos diversos sistemas de comando e controlo do EMGFA” (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022, p. 3), “fazendo face ao aumento da competição geopolítica, às agressões com recurso a tecnologias disruptivas, às ameaças transnacionais e híbridas e às emergências civis” (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022, p. 3).

O CCOM detém a autoridade de coordenação no relacionamento do Comando de Operações de Ciberdefesa (COCiber) e do Centro de Informações e Segurança Militares (CISMIL) (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022). O COCiber está diretamente dependente do Chefe do Centro de Comunicações e Informação, Ciberespaço e Espaço (CCICE) (Decreto-Lei n.º 19/2022 de 24 de janeiro, 2022).

Atualmente, existe o Centro de Operações de Ciberdefesa (COCiber) que está na dependência do EMGFA, tendo a missão de “planear, dirigir, coordenar, controlar e executar operações no, e através do, ciberespaço, em apoio a objetivos militares, de modo a garantir a liberdade de ação das Forças Armadas neste domínio” (Decreto Regulamentar n.º 2/2023 de 6 de junho, 2023, p. 41), tem o objetivo de, tendo como referência a defesa nacional, “desenvolver as capacidades nacionais de prevenção, monitorização, deteção, reação, análise e correção de incidentes de cibersegurança e ciberataques” (Decreto Regulamentar n.º 2/2023 de 6 de junho, 2023, p. 42). Existe uma estrutura sólida constituída por trabalho conjunto entre vários organismos para garantir respostas no combate às ciberameaças. A nível internacional, o NCIRC, está relacionado com o CNCS e com o COCiber. Este, por sua vez, partilha informação com o CNCS, com *Computer Incident Response Capability* (CIRC) nacionais e *Computer Emergency Response Teams* (CERT) internacionais. O CERT partilha informações com o *North Atlantic Treaty Organization* (NATO) *Cyber Security Centre*.

A Organização é a estruturação da capacidade, no sentido em que é necessário uma hierarquização, coordenação e estrutura bem definidas com o fim do cumprimento de um objetivo/ tarefa/ missão (NATO, 2021). No caso da cibersegurança, existem vários

departamentos e organizações com um objetivo partilhado, garantir a segurança do ciberespaço.

Na Marinha, a segurança do ciberespaço e da informação são da responsabilidade de vários organismos. O EMA, sendo o órgão que apoia o CEMA, tem responsabilidade, a nível estratégico no que concerne à coordenação, engloba a Divisão de Operações e esta Divisão, o Núcleo de Ciberdefesa e Tecnologias de Informação e Comunicações (CEMA, 2018). Quanto ao nível operacional, o Comando Naval (COMNAV) é a entidade incumbente da coordenação. Existe ainda a Superintendência das Tecnologias da Informação (STI) regulada pelo DR n.º 10/2015, de 31 de julho. A STI é conhecida como o Órgão Central de Administração e Direção da Marinha (OCAD) sendo responsável por garantir a “segurança da informação e do ciberespaço, pela governação dos sistemas de informação, pelo controlo da configuração das redes e pela gestão do parque informático” (Decreto Regulamentar n.º 10/2015 de 31 de julho, 2015, p. 5200). Salienta-se ainda que a STI compreende a DITIC e esta tem o dever de:

“Gerir, operar e manter a estrutura de segurança e defesa do ciberespaço e da informação na Marinha, assegurando a capacidade de resposta a incidentes no ciberespaço e de segurança da informação (CIRC) na Marinha, através de equipas próprias de combate às ameaças em computadores e em infraestruturas de redes (CERT ou CSIRT), disponibilizando processos e tecnologias que assegurem o adequado nível de segurança num contexto de gestão de risco” (Decreto Regulamentar n.º 10/2015 de 31 de julho, 2015, p. 5213).

Relativamente ao Treino, este é crucial para garantir a segurança e eficácia das operações militares num ambiente cada vez mais digitalizado, uma vez que, o ciberespaço é conhecido como um espaço dinâmico e complexo, torna-se fundamental que os intervenientes, através do treino, adquiram diversas competências para reconhecer, mitigar, avaliar e combater possíveis ameaças cibernéticas que possam afetar as IC. A capacidade de defesa e resposta a ameaças emergentes nestes domínios depende de militares treinados para agir de forma eficiente e sempre prontos para que não ocorram incidentes nas redes e sistemas de informações da Marinha, CSs ou outras infraestruturas nacionais garantindo a segurança das comunicações e a eficácia das operações (Neves & Correia, 2016).

O Material “refere-se a tudo o que é necessário para suportar e equipar as unidades operacionais” (Neves, 2015, p. 59). Incluem-se assim “os equipamentos, à tecnologia e às infraestruturas de comunicações” para que se possa operar de forma eficaz (Neves, 2015, p. 59).

No que concerne à Liderança, esta está diretamente ligada à capacidade de preparação da chefia, de formação, de comando, desempenhando um papel crucial na postura proativa perante a missão. Os líderes militares têm de ser capacitados para a direção e motivação dos restantes militares, devem estabelecer diretrizes que promovam a consciencialização e o incentivo de uma abordagem colaborativa na proteção dos CSs.

Em relação ao Pessoal, este é o fator chave uma vez que:

“Numa capacidade de resposta a incidentes de segurança, mesmo existindo todo o material necessário para a sua operacionalização, o Pessoal ou fator humano é determinante, pois tem sempre de existir uma fase muito importante de análise e decisão das ações a seguir” (Neves & Correia, 2016, p. 18).

Assim sendo, para a seleção e atribuição de pessoas em conformidade com as habilidades e competências que cada um possua de modo a contribuir para o ambiente cibernético com equipas treinadas e preparadas para enfrentar as ameaças emergentes.

Ao nível das Infraestruturas, sendo estas o suporte das informações e estas possuírem “diferentes níveis de segurança” (Neves & Correia, 2016, p. 20), torna-se fundamental a segurança física das instalações (Neves & Correia, 2016). A capacidade nacional de ciberdefesa “deve, sempre que possível, aproveitar as infraestruturas existentes” (Nunes, 2018, p. 76) e “terá também de possuir comunicações redundantes, áreas de segurança para a operação dos sistemas, com os devidos mecanismos de controlo de acessos e de videovigilância” (Neves & Correia, 2016, p. 20).

Por último, a Interoperabilidade sendo garantida através da cooperação entre as forças militares nacionais e internacionais e pela partilha de informações, centra-se em gerar uma abordagem comum entre as várias entidades que fazem parte das operações através de um conjunto de conceitos partilhados entre as partes (Neves, 2015). Deve-se ter em conta ainda a adoção de procedimentos, mas também a utilização de regras, propósitos e doutrinas com capacidade para garantir a normalização de sistemas, serviços

e redes. Esta torna-se com elevada relevância uma vez que “Nos casos em que não for possível assegurar a interoperabilidade dos sistemas, podem surgir vulnerabilidades adicionais, suscetíveis de comprometer a segurança das infraestruturas de informação, criando eventuais ‘pontos de entrada’ passíveis de vir a ser explorados pelos ciberataques” (Nunes, 2018, p. 77).

Contudo, pode-se concluir que a metodologia abordada anteriormente fornece uma sólida estrutura no que toca ao estabelecimento de prioridades, o que vem facilitar o fortalecimento da capacidade nacional de ciberdefesa. Logo, quanto à segurança do ciberespaço, pode-se afirmar que a Marinha Portuguesa possui uma estrutura edificada, organizada e eficaz para assegurar a qualidade da informação que circula no ciberespaço (Neves, 2015).

4.2. Criptografia, autenticação e proteção dos dados

A capacidade de controlo dos dados que circulam num dado país, tanto em contexto civil ou militar, está em risco devido à vulnerabilidade dos CSs, quanto às escutas e vigilância submarinas, pois, circulam nestes cabos, tanto informações classificadas como não classificadas. Tomam-se como exemplos, a coordenação de operações militares, a recolha de informações e a execução de missões diplomáticas, que são feitas através dos mesmos (Ganz et al., 2024). Ou seja, deles resulta uma vasta acumulação de dados e informações sigilosas, tornando-os suscetíveis a escutas clandestinas, o que vem trazer cada vez mais ameaças à integridade das nações, em geral, por isso é que se torna de extrema importância a proteção destas infraestruturas (Clark, 2016).

A criptografia desempenha um papel fundamental na segurança dos dados e informações que circulam através dos CSs, comportando-se como um “escudo” dos dados que circulam nestas IC. Desde o controlo de acesso, às proteções legais de dados, onde a confidencialidade da informação é sempre garantida, mas mesmo assim “as violações à segurança dos dados são uma ocorrência quase diária” (Kramer, 2023, p. 21).

As preocupações com a espionagem no que se refere aos dados são constantes devido a dois principais fatores: a capacidade para a leitura de dados que não estão encriptados (como metadados e a maioria dos e-mails que são enviados) e a

descriptação de dados que se encontram encriptados. Ao se criptografar os dados que são transmitidos pelos CSs, as informações tornam-se ilegíveis para qualquer pessoa que tente interceptar a comunicação (hackers ou qualquer agência de espionagem), tornando este método eficaz contra a intercessão dos dados e contra os próprios ataques o que garante que apenas os destinatários autorizados possam ter acesso mas com as novas tecnologias, ou melhor, com a IA e novas técnicas de computação quântica, nas próximas duas décadas, poderá ser possível fazê-lo (Kramer, 2023), uma vez que a *internet* oferece às organizações terroristas, técnicas de pirataria informática com o objetivo de assumirem, de forma rápida, o controlo do ciberespaço (ACOS STRAT, 2014). A utilização da IA, mais concretamente, o uso do ML, aplicado ao caso da autenticação baseado na biometria, não é considerado uma má utilização, pois, nesta autenticação de utilizadores baseado neste método, esta utilização, enriquece a segurança deste domínio. O grande problema são a dimensão dos ataques que ocorrem e que tornam os algoritmos do ML, vulneráveis nas fases de testes experimentais, o que resultam em violações de segurança da informação (Dasgupta et al., 2022).

Com a era da globalização e o advento do ciberespaço, as ameaças transformaram-se de forma significativa, sendo possível realizar um ataque devastador, a nível mundial, através de um simples computador (Militão, 2014). Surge assim, a crescente necessidade de segurança dos dados e informações relativos à Humanidade. Segurança da informação define-se, segundo a norma internacional ISO/IEC 27002 (2005), como “a preservação da confidencialidade, integridade e disponibilidade da informação” (ISO/IEC 27002, 2005, p. 1; Solms & Niekerk, 2013). De modo a garantir a confidencialidade dos dados, estes têm de ser encriptados antes de serem enviados (Kharade et al., 2019). Existem, portanto, restrições relativas ao acesso, podendo apenas ser feito por pessoas autorizadas através de uma chave de descodificação apropriada, permitindo a interpretação das informações (Hanif et al., 2021). Além da confidencialidade, a criptografia também permite garantir a integridade dos dados, o que significa que qualquer alteração dos dados encriptados seria detetada, se os dados fossem modificados ou corrompidos durante a transmissão, promovendo a segurança e a autenticidade dos mesmos (Jiang, 2019).

Considerando, como já foi referido anteriormente, que circulam tanto dados civis como militares através dos CSs e a capacidade de um país controlar os dados que possui encontra-se, portanto, em risco devido à vulnerabilidade destes cabos às escutas telefónicas (Ganz et al., 2024). De modo a colmatar este facto, torna-se necessário

proceder à proteção dos dados de uma forma mais eficaz. Em 2018, foi implementado o Regulamento Geral sobre a Proteção de Dados (RGPD) da UE, este é um diploma europeu que tem como objetivo, reforçar a proteção de dados e coadunar a legislação seguida nos Estados-Membros. Este regulamento, segundo o artigo 1.º, “estabelece as regras relativas à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados” (Regulamento (UE) n.º 679/2016 de 27 de abril, 2016, p. 25) em todos os países membros da União Europeia. No entanto, os CSs possuem vulnerabilidades como o acesso aos dados através dos BMH (que se encontram nas praias), uma vez que, “Atualmente, tudo o que é necessário para conectar um cabo submarino é o acesso aos cabos de fibra ótica que estão no seu núcleo” (Ganz et al., 2024, pp. 9-10), mesmo que uma grande parte dos dados estejam criptografados, “é difícil determinar a percentagem do tráfego de *internet* que é criptografada, uma vez que grande parte é privada” (Ganz et al., 2024, p. 9).

De modo a ter em conta a importância dos dados que circulam nos CSs, estes devem ser encriptados de forma rápida e deve-se utilizar métodos ou esquemas de encriptação quântica seguros para os dados considerados mais sensíveis. Estes métodos têm como objetivo garantir a segurança dos dados a fim de os proteger e defender contra escutas telefónicas atuais e futuras (Ganz et al., 2024).

Em resumo, a criptografia é uma “camada” crucial de segurança que ajuda a manter a privacidade e a segurança das comunicações globais. De uma perspectiva evolucionista, torna-se complicado garantir o acesso apenas a certas entidades devido à natureza dos CSs e ao elevado custo da implementação de medidas de proteção que restrinjam o acesso não autorizado a qualquer indivíduo (Ganz et al., 2024). Logo, a proteção dos dados, dos dispositivos e a própria privacidade dos utilizadores no ciberespaço torna-se um desafio com uma preocupação extrema, uma vez que nos utilizadores estão incluídas as organizações empresariais e os governos nacionais (Dasgupta et al., 2022). Apesar da utilização dos cabos para fins civis e militares, os países dependem desta rede para garantir a segurança nacional e pode-se ainda acrescentar, como medidas de segurança futuras, o uso de *firewalls* avançados e sistemas de deteção com a finalidade de proteger as redes de informações contra ameaças cibernéticas.

5. Projeto *Fibersense*

O projeto *Fibersense* é um projeto europeu, que surgiu em 2021, fruto de um consórcio entre três países, a Grécia, Alemanha e Portugal. Este projeto é financiado pela *European Defense Fund* (EDF)¹⁹.

Ao nível de Portugal, o Centro de Investigação Naval (CINAV) da Escola Naval (EN), foi responsável pela coordenação dos primeiros testes experimentais que foram realizados no Centro de Experimentação Operacional da Marinha (CEOM), em Tróia, em ambiente real.

Com o fim de responder ao desejado com a investigação deste projeto, ou seja, estudar a viabilidade desta tecnologia, estando relacionado com o âmbito da presente Dissertação, foram realizados e analisados testes preliminares experimentais subaquáticos em ambiente controlado e isolado (no tanque de Arquitetura Naval da EN) e serão posteriormente realizados também novos testes experimentais em ambiente operacional real, no presente ano.

De forma a contextualizar o projeto no âmbito da presente Dissertação, salienta-se que esta tecnologia visa permitir a deteção de sinais acústicos (que se traduzem em ondas de pressão) nas proximidades do cabo, ao longo de grandes distâncias, de forma a possibilitar uma monitorização, vigilância, deteção e identificação futuras eficazes (Lindsey & Martin, 2021; Bueger et al., 2022).

5.1. Introdução à tecnologia DAS

Este projeto foi desenvolvido para a utilização da tecnologia emergente *Distributed Acoustic Sensing* (DAS), sendo este um método geofísico (Lindsey & Martin, 2021). A tecnologia DAS conhecida como a tecnologia de Deteção Acústica Distribuída, através da utilização de Cabos de Fibra Ótica (CFO), sendo estes os Cabos Submarinos (CSs) que existem atualmente, através desta tecnologia, este tipo de cabos pode ser utilizado para conhecimento situacional marítimo, estando assim associado ao domínio marítimo e às operações marítimas, no âmbito da segurança, proteção, economia e do

¹⁹ O Fundo Europeu de Defesa “apoia empresas de todos os Estados-Membros no desenvolvimento de projetos de defesa competitivos e colaborativos que proporcionarão tecnologias e equipamentos de defesa inovadores e interoperáveis. Oferece apoio e aconselhamento aos participantes ao longo de todo o ciclo de investigação e desenvolvimento” (European Commission, s.d.).

meio ambiente.

O cabo “atua” como um conjunto de sensores de deformação dinâmica. De uma forma simplificada, esta tecnologia utiliza o conjunto de toda a fibra ótica como elemento sensorial (Bueger et al., 2022; OFS Optics, s.d.). Conhecida por ter a capacidade de enviar, de forma regular e contínua pulsos de laser para o núcleo do CFO (onde se encontram as fibras óticas), medindo as mudanças de fase ótica da luz por *backscattering* de *Rayleigh* (Lindsey & Martin, 2021). Conclui-se, de forma simplista que serve para deteção acústica através da exploração do *backscattering* de *Rayleigh*, ao longo do próprio cabo.

Tem também como uma das finalidades, a deteção de causas naturais como “microterramotos, terremotos regionais, telessismos e sinais de infraestrutura” (Lindsey & Martin, 2021, p. 309). No que se refere à deteção acústica, toma-se como exemplo principal, a passagem de um navio na ZEE, uma vez que este provoca ruído submarino através da cavitação do hélice (ou dos hélices), no caso de possuir mais do que um, através de ondas de pressão mecânicas, ou seja, vibrações mecânicas das partículas que um CFO submarino tem capacidade para detetar.

Introduzindo, de forma simplificada a acústica submarina, neste âmbito, é conhecida como a ciência que estuda a propagação do som na água e o som como é uma onda mecânica, esta ciência estuda a interação das ondas mecânicas no ambiente aquático.

A água do mar é um bom meio para o som se propagar, mas também está limitado devido à atenuação do sinal por absorção da própria água, o que limita o alcance sonoro. O facto da não homogeneidade da água, intensifica a reflexão e os trajetos do sinal, contudo, pode-se concluir que contribui para a existência de ruído sonoro uma vez que existem muitos fatores que impõem limitações à propagação das ondas acústicas, como por exemplo, a agitação marítima e os animais marinhos, que retardam, de alguma forma, a receção do sinal sonoro.

Por último, este método pode vir a suportar a indústria na medida em que poderá contribuir para determinar “quando e onde ocorreram quebras ou danos” em infraestruturas críticas (Bueger et al., 2022), uma vez que esta tecnologia tem a capacidade de emitir um alarme quando há uma rutura no CFO. Esta vantagem, será muito útil no futuro, para a deteção de ameaças ou danos nos CSs acrescentando o facto de que esta tecnologia ainda contribuirá como prova de danos, de acordo com o autor, “os dados destes sistemas também são utilizados em processos judiciais sobre danos e

indenizações” (Bueger et al., 2022, p. 28).

5.2. Descrição e objetivos do projeto

O projeto consiste na realização de uma investigação detalhada e metódica a fim de verificar a viabilidade e sensibilidade dos CFO com o DAS integrado. No caso específico da presente Dissertação, tratam-se dos primeiros testes realizados num ambiente controlado e isolado, onde se pretende simular que o cabo está depositado no “fundo do mar” ou “enterrado”, relativamente à captação de sinais acústicos, incluindo o limite de deteção e o intervalo de frequências que permitam uma monitorização eficaz e analisar a integridade da transmissão de dados assim como a relação sinal-ruído dos CFO comparando com um conjunto de hidrofones e sonobóias tradicionais. No âmbito da presente Dissertação, esta última análise e comparação não será feita.

Será verificada a capacidade e configuração do equipamento DAS, utilizando, para o efeito, a fonte emissora escolhida para o estudo, mais concretamente, um projetor de som (o altifalante subaquático LL916C), o qual se encontra descrito no **Anexo B-Especificações do modelo do altifalante subaquático LL916C**, para consulta das especificações que possui.

Espera-se, contudo, que estes resultados preliminares indiquem que os CFO, tendo o DAS integrado, poderão ser uma solução viável e económica para a vigilância, monitorização e investigação acústica submarina, a nível operacional e científico. Acrescenta-se ainda a grande possibilidade, de poder criar um sistema de alerta relativo à deteção de navios na ZEE portuguesa contribuindo assim para a vigilância desta grande área marítima que Portugal possui.

5.3. Especificações do projeto

Relativamente às especificações do projeto, este será, como já foi referido anteriormente, realizado no tanque de Arquitetura Naval da EN, caracterizado por se realizar em ambiente controlado e isolado.

5.3.1. Tanque de Arquitetura Naval

O tanque possui 8 m de comprimento, mas apenas foram objeto de estudo, dos 0,850 m, onde se começou a colocar os sacos de areia a simular o fundo do mar, em linha reta, até aos 5,850 m, ou seja, apenas 5 m em estudo.

Foram escolhidas duas posições, a posição 1 (P1) e a posição 2 (P2), sendo que a P1 se situa nos 4,5 m e a P2 nos 3,3 m onde foi posicionada a fonte sonora (o altifalante subaquático), como se pode observar na **Figura 19** que se segue, uma ilustração do tanque com as referidas posições assim como o CFO, os sacos de areia representados pelos retângulos pretos e ainda a estrutura metálica representada na extremidade direita do tanque (gerador de ondas), sendo de melhor visualização a **Figura 20**, realçando ainda que a figura seguinte não se encontra representada à escala.

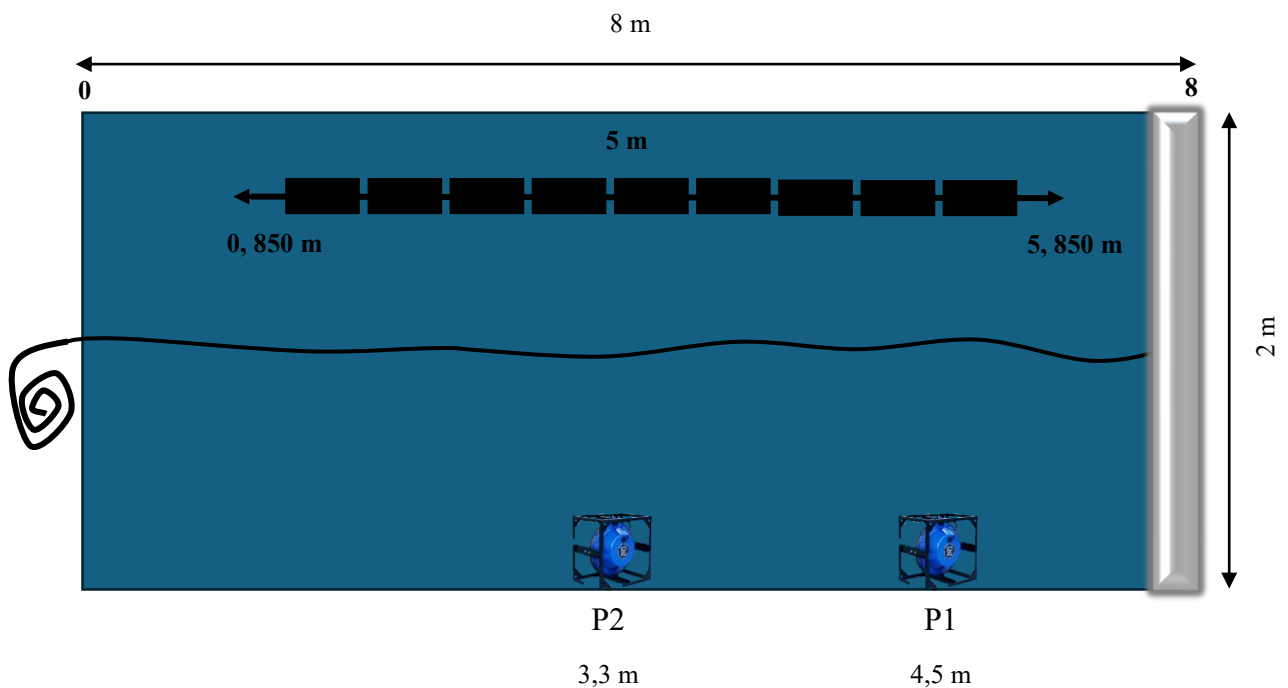


Figura 19 - Ilustração do tanque em estudo



Figura 20 - Gerador de ondas

Salienta-se ainda, em relação ao tanque que não existe qualquer isolamento sonoro nas paredes e no fundo do mesmo, o que pode conduzir a interferências construtivas ou destrutivas, ou seja, respetivamente, a amplificação ou atenuação das ondas sonoras.

5.3.2. Cabo de Fibra Ótica submarino

O CFO utilizado para o estudo foi um cabo que possui uma elevada resistência e segurança de transmissão, sendo monomodo e encontra-se no **Anexo A- Especificações do Cabo de Fibra Ótica utilizado no projeto**, as especificações do mesmo.

Em relação à zona em estudo, no tanque, são considerados quatro sensores incorporados, distanciados entre si de 1,25 m.

5.3.3. Altifalante subaquático

O projetor de som, mais conhecido como, o altifalante subaquático cujo modelo é da *Lubell Labs LL916C*, adequado para ser utilizado em tanques de teste, mas possui uma especificação que limitou o estudo, mais precisamente, possui um intervalo de resposta às frequências, dos 200Hz aos 21 kHz. No **Anexo B- Especificações do modelo do altifalante subaquático LL916C**, encontram-se as instruções de utilização deste tipo de altifalante subaquático, assim como as características do mesmo. Pode-se observar, de seguida, na **Figura 21**, o modelo do altifalante subaquático referido.



Figura 21 - Altifalante subaquático

(Adaptado de MarSensing, s.d.)

5.4. Funcionamento do projeto

Para efeitos de testar o funcionamento desta tecnologia juntamente com o CFO submarino, este encontrava-se ligado a um aparelho, o DAS da *AP Sensing*, que posteriormente, também liga este CFO e outro cabo ao computador para visualização e utilização do *software* da *AP Sensing*.

Este *software* permite a análise de sons emitidos que são transmitidos para o cabo através do altifalante subaquático. Para o efeito, é utilizado o altifalante subaquático **Figura 21** que se encontra dentro do tanque para emissão de um som, com as duas posições diferentes estabelecidas anteriormente para este projetor de som, P1 e P2. Escolheram-se estas posições uma vez que a zona em estudo foi restringida entre os 0,850 m e os 5,850 m (medições do próprio tanque), perfazendo um total de 5 m para o estudo, para avaliar e detetar o som emitido num caso concreto de estudo, abrangendo a área do cabo que contém os sacos de areia.

De forma a testar esta tecnologia, foram realizados testes experimentais subaquáticos, os Testes A e os Testes B, com dois cenários em cada, incluindo, em cada teste, diferentes frequências e diferentes potências em intervalos de emissão específicos. Em cada teste, foram emitidos vários áudios específicos, com uma certa frequência e várias potências através do altifalante subaquático. De seguida, estará claro e detalhado, o que foi feito em cada um destes testes e como estava disposto o CFO submarino (cenários), em cada uma das posições em estudo.

Em relação ao som, ou melhor, aos áudios, foram transmitidos sete áudios (com o

amplificador a meia potência) com sete frequências diferentes para cada uma das posições, para cada Teste. Passa-se a explicar, com pormenor: para cada uma das duas posições foram emitidos e analisados sete áudios uma vez que se escolheram sete frequências para o estudo, sendo as seguintes, da mais baixa para a mais alta frequência, respetivamente: 25Hz, 50Hz, 100Hz, 200Hz, 400Hz, 800Hz e os 1600Hz²⁰. Mais pormenorizadamente, cada áudio possuía a duração de 4 minutos e 50 segundos, iniciando-se com 10 segundos de silêncio e 30 segundos de som e assim sucessivamente até terminar. Os 30 segundos de som emitido correspondiam a cada Amplitude de Potência (AP) e como existiam sete APs em estudo, sendo: 0,01; 0,02; 0,05; 0,1; 0,2; 0,5 e 1, foram reproduzidos sete sons diferentes (isto é, sete potências relativas²¹ diferentes). Conclui-se, de uma forma mais explícita, que cada áudio de som emitido correspondia a uma das sete frequências, com uma repetição contínua até completar os 4 minutos e 50 segundos, inicialmente com 10 segundos de silêncio, 30 segundos com um som a emitir uma potência relativa de 0,01, seguido de 10 segundos de silêncio, 30 segundos com um som a emitir uma potência relativa de 0,02 e assim sucessivamente até chegar ao fim, com um som emitido com uma potência relativa de 1 e assim que terminarem esses 30 segundos, o áudio termina.

5.4.1. Descrição dos Testes A e dos Testes B

No que se refere aos testes experimentais, estes foram executados durante o mês de março e abril do presente ano.

Os Testes A, para as duas posições, P1 e P2, são caracterizados pelo posicionamento dos sacos de areia usados para o efeito, se encontrarem no fundo do tanque situados ao longo dos 5 m em estudo, abordados anteriormente, com o CFO por cima dos sacos, ou seja, sobreposto, (a supor-se que o cabo está depositado no fundo do mar), considerando que este não se encontra totalmente esticado, ao longo do tanque.

Nas duas figuras seguintes, pode-se observar a disposição do altifalante subaquático, nos Testes A, sendo que na primeira, **Figura 22**, o altifalante subaquático encontra-se na primeira posição, P1, nos 4,5 m, como se pode ver na disposição que se

²⁰ Estas frequências foram definidas genericamente, isto é, para poderem ser emitidas por diversos altifalantes subaquáticos.

²¹ Para este estudo do projeto foram utilizadas sete APs conduzindo a sete potências relativas, contudo, de forma a não estar sempre a repetir o termo “potência relativa”, entenda-se que quando se refere ao nome “potência” significa potência relativa.

segue.



Figura 22 - Disposição dos Testes A com o altifalante subaquático na posição 1

Na **Figura 23**, pode-se observar o altifalante subaquático na segunda posição, P2, nos 3,3 m, de acordo com a disposição seguinte.



Figura 23 - Disposição dos Testes A com o altifalante subaquático na posição 2

Quanto aos Testes B, para as duas posições, P1 e P2, a disposição dos sacos de areia é diferente, sendo que o CFO está posicionado entre os sacos de areia, simulando

que o cabo está “enterrado” no fundo do mar, quase totalmente esticado, ao longo dos 5 m em estudo, no tanque.

À semelhança do que se abordou anteriormente acerca dos Testes A, nas duas figuras seguintes, pode-se observar a disposição do altifalante subaquático, nos Testes B, sendo que na primeira, **Figura 24**, o altifalante subaquático encontra-se na primeira posição, P1, nos 4,5 m, de acordo com a disposição que se segue.



Figura 24 - Disposição dos Testes B com o altifalante subaquático na posição 1

Na **Figura 25**, pode-se observar o altifalante subaquático na segunda posição, P2, nos 3,3 m, de acordo com a disposição seguinte.



Figura 25 - Disposição dos Testes B com o altifalante subaquático na posição 2

5.5. Processamento de dados

Relativamente à disposição e configuração dos procedimentos para a execução do projeto, criou-se sete áudios no computador foram criados sete áudios em que cada um destes possui sete AP diferentes a serem emitidas ao longo do tempo, como abordado anteriormente, sendo depois amplificados e emitidos pela fonte sonora, o altifalante subaquático acústico.

À medida que este sinal é emitido pela fonte sonora, o equipamento do DAS está ligado ao computador, onde se observa, em tempo real, o som que está a ser emitido e a disposição do mesmo através de um gráfico de *Frequency Band Energy* (FBE), pelo *software* do DAS *Configurator*. Este tipo de gráfico caracteriza-se por conseguir fazer a separação dos vários sons acústicos em diferentes bandas de frequências, ou seja, representa um *waterfall plot* depois da aplicação de um filtro de frequência no conteúdo dos dados de fase, ou seja, é realizada uma *Fast Fourier Transform* (FFT) nos dados de fase ao longo dos sensores do cabo apresentando, neste tipo de gráfico, apenas o conteúdo do sinal na banda de frequência específica pré-definida, podendo também apresentar em todas as bandas de frequência pré-definidas. Estas bandas de frequência pré-definidas são as seguintes: 4–8Hz, 8–20Hz, 20–48Hz, 48–100Hz e 100Hz–*Nyquist* mas para este caso de estudo, considerou-se as seguintes: FBE 1: 4–8Hz, FBE 2: 8–20Hz, FBE 3: 20–48Hz, FBE 4: 48–100Hz e FBE 5: 100Hz–5000Hz. Ou seja, os sinais *backscattered* detetados

ao longo dos sensores do cabo são processados e emitidos em diferentes bandas de frequência à escolha do utilizador, através da energia total por banda (AP Sensing, 2023).

Este *software* fornece um ficheiro com o formato HDF5 que posteriormente foi extraído e processado em linguagem de programação *python* para se obter os dados experimentais. Foram desenvolvidos vários *scripts* no *python* e utilizado o *Microsoft Excel* para análise dos dados. Estes *scripts* foram adaptados para a análise dos dados em bruto do estudo e para os dados reduzidos, para assim se extraírem os padrões acústicos significativos.

De forma a analisar estes dados, qualitativamente, analisou-se o desempenho do CFO submarino restringindo apenas o estudo para uma frequência, sendo esta os 800Hz devido às especificações do altifalante subaquático. Para este estudo, foram elaborados quatro gráficos no *python*, correspondentes, aos Testes A e Testes B, para cada uma das posições, ou seja, dois gráficos para cada um dos testes.

Os gráficos têm como título “FBE Data” e foram obtidos através do código em linguagem *python* que se encontra no **Apêndice B- Código em linguagem de programação *python* utilizado**, assim como toda a explicação de como se obtiveram os mesmos.

No *Excel*, obtiveram-se tabelas e gráficos correspondentes aos dados que se encontravam no *python* para uma análise mais concreta.

5.6. Interpretação dos resultados

De forma a analisar os sinais sonoros, com todas as especificidades abordadas anteriormente, foram obtidos através do *software* da *AP Sensing*, os ficheiros, que se encontram discriminados no **Apêndice A- Ficheiros transferidos do *software* DAS da *AP Sensing***.

Selecionou-se apenas uma frequência para o estudo, a frequência dos 800Hz pelo motivo abordado no subcapítulo 5.5, tendo assim obtido, através da análise dos ficheiros abordados acima, no *python*, um a um, no qual se obtiveram os seguintes *heatmaps*, para cada situação em estudo.

Relativamente à primeira análise, da frequência dos 800Hz, referente aos Testes A, posição 1 do altifalante, obteve-se o seguinte *heatmap* da posição (em metros) em função do tempo (em segundos), com uma escala representativa das cores correspondente ao gráfico. Quanto à posição, restringiu-se apenas os dados às posições 839 à 843, que correspondem aos 5 m em estudo, no tanque.

Assim, de forma a estudar a sensibilidade do CFO submarino em relação às várias AP em causa, obtém-se as seguintes análises dos gráficos, através de esquemas representativos para tornar os resultados mais explícitos, nas duas posições, P1 e P2, correspondentes apenas a uma frequência em estudo, os 800Hz, nos Testes A e nos Testes B.

O gráfico que se segue, representado pela **Figura 26**, correspondente aos Testes A, posição 1, possui sete “barras horizontais” que são as sete APs emitidas, com cores diferentes devido à capacidade de captação/ sensibilidade do CFO em relação a cada uma delas, na qual se pode afirmar que, das sete APs, as que o CFO deteta melhor, tem maior sensibilidade, são as três APs, de 0,2; 0,5 e 1. Em relação às zonas a azul, estas correspondem aos períodos de 10 segundos em que não foi emitido nenhum som.

Quanto à posição do altifalante subaquático, uma vez que este está na posição 1, ou seja, mais próximo dos 840, o CFO é mais sensível nas posições mais afastadas da fonte sonora e com maiores AP, como se pode observar pela análise da figura seguinte.

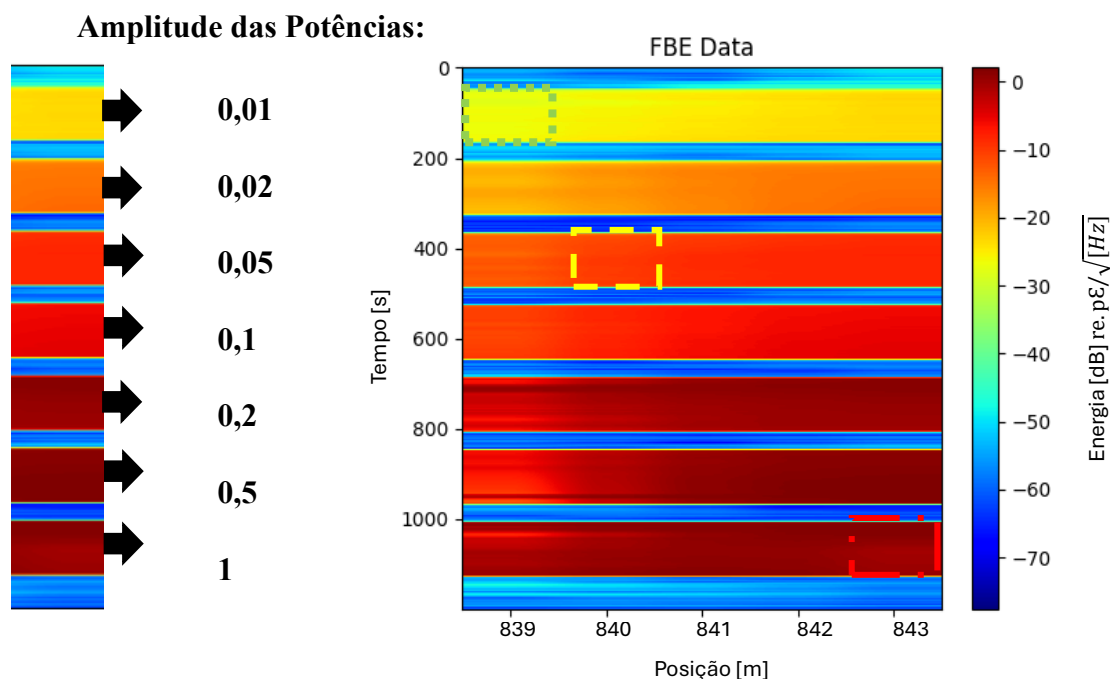


Figura 26 - FBE Data para os Testes A e posição 1

Conclui-se, pela análise da figura que, quanto maior for a AP e mais afastado da fonte sonora, ou seja, mais próximo dos 843, maior será o valor da energia do sinal.

Posto isto, de forma a relacionar e comprovar os resultados obtidos no *python* com os resultados obtidos no *Excel*, explica-se o seguinte: no *Excel*, selecionou-se as cinco colunas do *python* correspondentes às posições de estudo, 839, 840, 841, 842 e 843 e obteve-se a tabela que se encontra no **Apêndice C- Tabela do Excel relativa aos Testes A, posição 1**, com cinco colunas e mil e duzentas linhas.

De seguida, fez-se a média apenas dos valores correspondentes ao tempo de emissão do som (os 30 segundos de emissão), de cada coluna, ou seja, dos valores correspondentes a uma AP, de onde se reduziu significativamente os dados.

Para uma melhor compreensão do que foi explicado acima, através dos três retângulos representados a verde, amarelo e vermelho, respetivamente, que se encontram na **Figura 26 e Tabela 3**, explica-se o seguinte: iniciando-se com a explicação do retângulo com o tracejado verde que está presente na mesma figura, este representa o conjunto de dados dos quais se fez a média, correspondentes à posição 839 e à primeira AP, (0,01), obtendo-se o resultado -27,3115, que consta na **Tabela 3**. No retângulo com o tracejado amarelo presente **Figura 26**, está representado o conjunto de dados

correspondentes à posição 840 e à terceira AP, (0,05), no qual se fez a média daquele conjunto de dados e se obteve o valor -10,7806 (que consta na tabela), assim sucessivamente, para cada AP e para cada posição, até que se obteve o retângulo com o tracejado vermelho presente na **Tabela 3** com o resultado 0,4685. Os valores médios correspondentes por colunas, encontram-se presentes na tabela seguinte:

Tabela dos dados reduzidos					
AP	Valor médio por coluna				
	839	840	841	842	843
0,01	-27,3115	-26,2657	-25,4236	-24,6649	-24,0186
0,02	-20,8968	-18,7247	-17,0435	-15,9294	-15,3905
0,05	-13,1947	-10,7806	-9,4448	-8,8429	-8,6731
0,1	-10,8140	-8,3002	-6,6624	-5,7983	-5,4827
0,2	-3,9672	-1,1253	0,0408	0,4276	0,5694
0,5	-7,2100	-1,6957	0,7267	1,4583	1,6369
1	-1,7212	0,1757	0,9772	1,0485	0,4685

Tabela 3 - Dados reduzidos do Teste A na posição 1

De forma a compreender melhor o que foi abordado anteriormente, destacou-se, através do retângulo e de uma seta, representados a preto, a última coluna dos dados, correspondentes à posição 843. Estes sete valores presentes nesta coluna, são os valores médios de cada AP.

Através da análise desta tabela, pode-se confirmar o que foi referido anteriormente, no que respeita à **Figura 26**, uma vez que, segundo a **Tabela 3**, considerando as sete AP, o CFO deteta-as melhor (tem mais sensibilidade) nas posições 842 e 843 para AP superiores a 0,2, ou seja, é mais sensível nas posições mais afastadas da fonte sonora.

Posteriormente, para cada posição, obteve-se um gráfico da média das energias em função da AP. Este gráfico foi elaborado com o objetivo de se estudar a sensibilidade do CFO à AP, ou seja, avalia o comportamento do CFO na mesma posição para as várias APs.

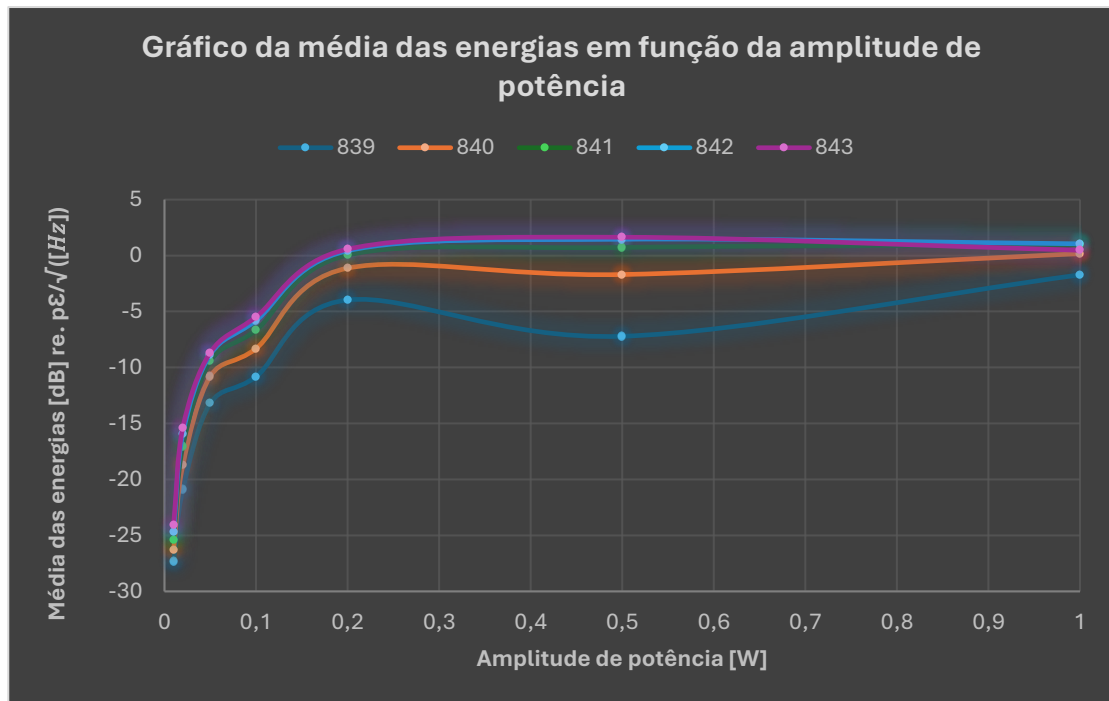


Gráfico 1 - Média das energias em função da amplitude de potência dos Testes A em P1 (escala linear)

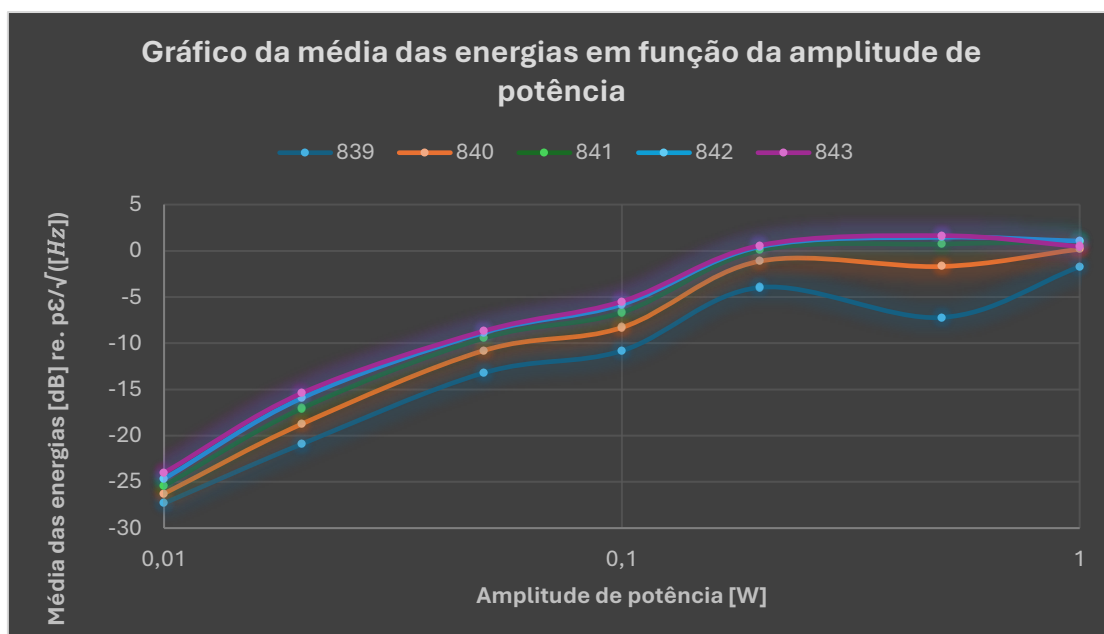


Gráfico 2 - Média das energias em função da amplitude de potência dos Testes A em P1 (escala logarítmica)

Analisando os gráficos, sendo iguais, exceto a escala, estando o **Gráfico 1** em escala linear e o **Gráfico 2** em escala logarítmica, observa-se que, para AP baixas, independentemente das posições (das curvas representadas com as cinco cores), obtém-se valores significativamente diferentes e há medida que a AP vai aumentando, as curvas vão-se aproximando, exceto a dos 839 e dos 840. Estas duas curvas apresentam os valores mais baixos da média das energias (valores mais negativos/ piores). Isto deve-se ao facto de, neste caso de estudo (com o cabo depositado nos sacos de areia), quanto mais próximo da fonte sonora, piores são os resultados.

Tendo em consideração apenas as curvas das posições 841, 842 e 843, através do **Gráfico 2**, somente para melhor visualização, pode-se concluir que, para casos futuros de estudo, seriam consideradas as AP a partir do valor 0,2 ou seja, (0,2; 0,5; 1) pois as curvas são muito similares, o que significa que o CFO é mais sensível a AP maiores (deteta melhor), sendo, assim, mais coerente em termos de resultados. Quanto às curvas dos 839 e 840, poderá haver diversos motivos que condicionam os valores e as curvas apresentadas anteriormente, podendo-se dever, por exemplo, à presença da estrutura metálica (gerador de ondas) que o tanque possui próximo da posição P1, que possa ter provocado interferências destrutivas, logo, atenuação do som, o que poderá ter impedido que o CFO detetasse o som emitido pela fonte nas proximidades. Contudo, carece de mais ensaios e análises para se poder avaliar esta situação de forma cuidada e precisa.

Em conclusão, relativamente a P1, para a frequência escolhida, no que se refere às cinco posições, o gráfico tem uma tendência para posições mais afastadas da fonte e com maiores AP, deduzindo-se que o CFO tem uma melhor resolução, maior sensibilidade ao sinal acústico, para AP superiores a 0,5 e que os resultados são mais coesos apenas mais próximo da AP de 1.

Por fim, de forma a complementar-se o estudo para esta posição, fez-se a média total correspondente, a cada coluna, para se obter uma ideia generalizada da captação feita pelo cabo ao longo da posição. Estes valores médios totais por coluna, permitem uma visão global do comportamento da intensidade sonora para cada coluna, resumindo assim a tendência geral que os resultados presentes no gráfico representam confirmando mais uma vez, a consistência verificada a partir da posição 841 até à 843, como se pode observar na **Tabela 4**.

	839	840	841	842	843
Valor médio total por coluna	-12,1593	-9,5309	-8,1185	-7,4716	-7,2700

Tabela 4 - Valor médio total por coluna

Relativamente ao valor da coluna 843, este corresponde ao valor mais elevado comparativamente aos restantes (mais próximo de zero), assim como se pode observar nos gráficos.

De forma a fazer uma comparação com os resultados anteriores, obteve-se, da mesma forma que se obteve o gráfico FBE *Data* para P1, o mesmo para os Testes A, para P2, com a mesma frequência.

Amplitude das Potências:

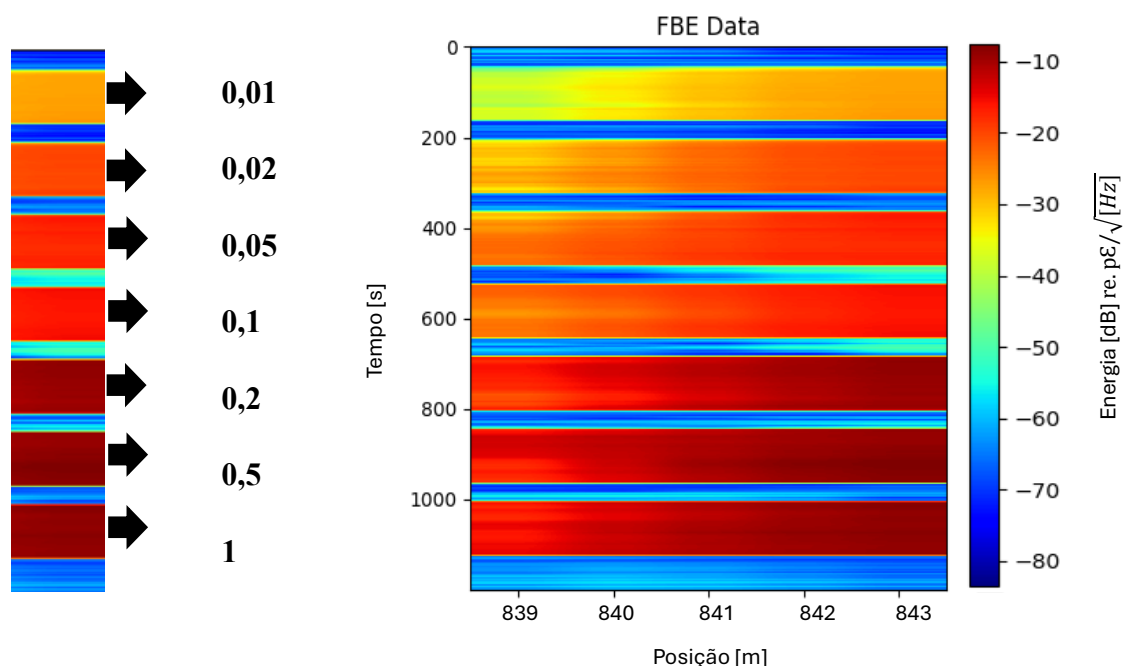


Figura 27 - FBE Data para os Testes A e posição 2

De acordo com a análise da **Figura 27**, das sete AP, as que o CFO tem maior sensibilidade, são as três AP superiores, 0,2; 0,5 e 1.

Quanto à posição do altifalante subaquático, uma vez que este está na posição 2, ou seja, mais próximo dos 843, conclui-se que o CFO possui uma detecção mais eficaz com AP mais elevadas mais próximo da fonte emissora, considerando-se assim, mais sensível, mais próximo da fonte, para esta posição.

Relativamente à **Tabela 5**, esta foi obtida no *Excel*, com o altifalante na posição 2.

Tabela dos dados reduzidos					
AP	Valor médio por coluna				
	839	840	841	842	843
0,01	-35,5894	-31,9431	-28,9286	-27,1115	-26,3694
0,02	-28,5367	-25,5834	-22,7824	-21,0491	-20,4035
0,05	-24,2827	-22,0510	-20,0406	-18,4891	-17,8833
0,1	-23,1667	-21,3922	-19,3789	-17,5943	-16,6570
0,2	-18,2667	-15,7118	-13,6614	-12,1434	-11,2424
0,5	-16,3744	-14,0664	-12,3346	-11,1470	-10,5752
1	-16,5916	-14,1526	-12,4415	-11,3451	-10,7565

Tabela 5 - Dados reduzidos do Teste A na posição 2

Pode-se afirmar que acontece o mesmo com a análise anterior, que com AP mais baixas torna-se mais difícil detetar o som e que o cabo possui maior sensibilidade nas três AP mais elevadas, mais próximo da fonte sonora, contudo, existe a necessidade de elaboração de mais casos de estudo e de um estudo mais pormenorizado. Embora, nesta posição (P2), os resultados serem mais coerentes, de acordo com a tabela.

Apresenta-se, de seguida, os gráficos da média das energias em função da AP, para P2, em escala linear e em escala logarítmica, respetivamente, para uma melhor visualização da variação das curvas de posição.

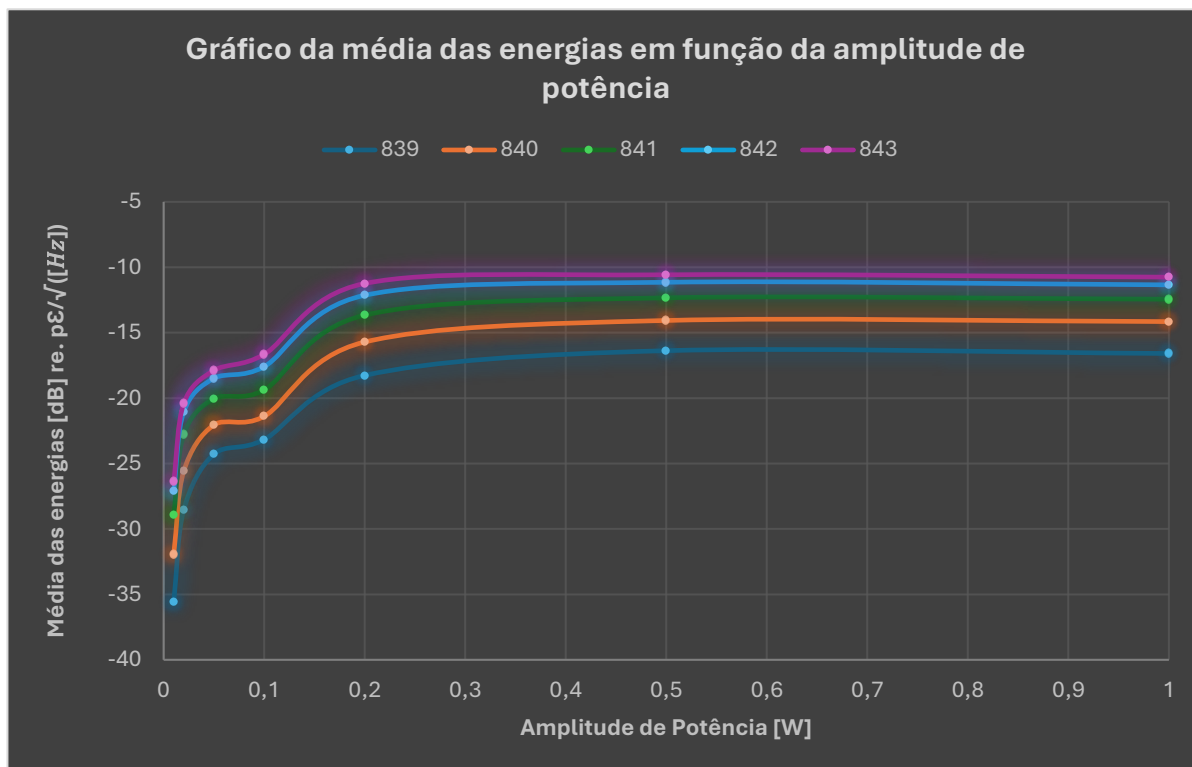


Gráfico 3 - Média das energias em função da amplitude de potência dos Testes A em P2 (escala linear)

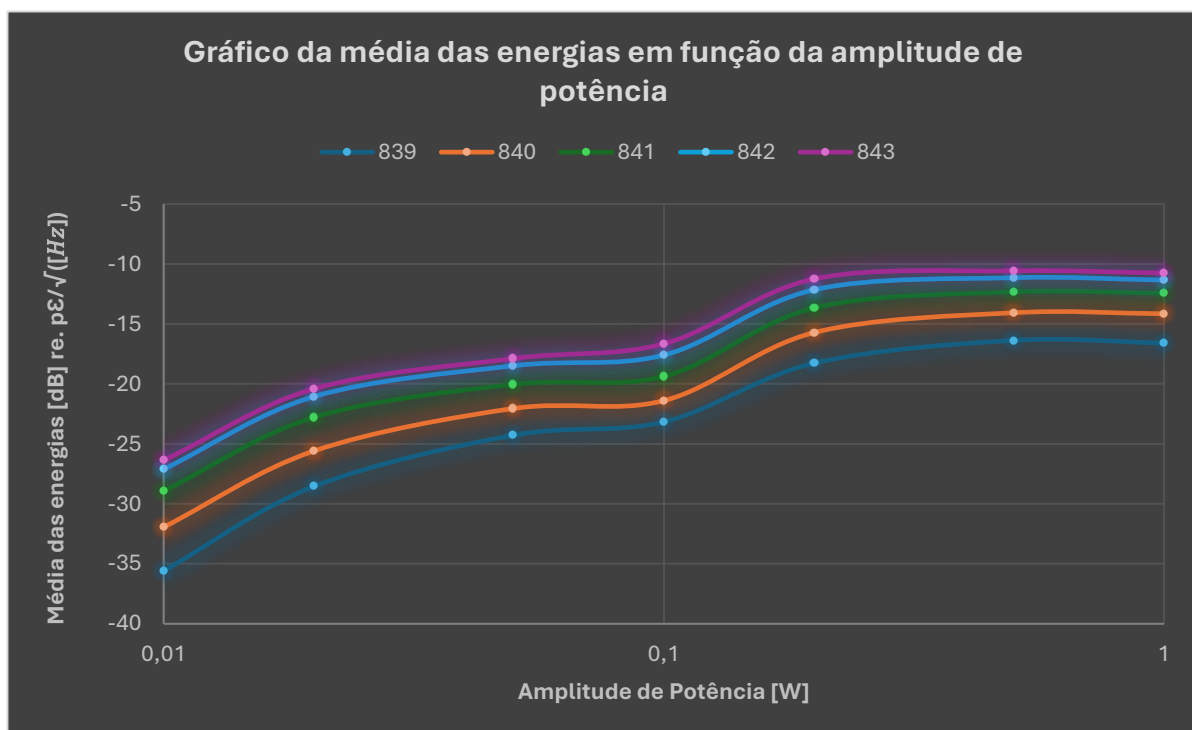


Gráfico 4 - Média das energias em função da amplitude de potência dos Testes A em P2 (escala logarítmica)

De acordo com uma análise qualitativa destes gráficos, uma vez que se refere a P2, conclui-se que, de uma forma generalizada, quanto mais próximo da fonte sonora e maior a AP, mais constantes/ lineares são as curvas, deixando de existir as não linearidades que se observam para AP mais baixas.

A partir da AP de 0,2 os dados são mais coerentes, mais propícios a serem estudados e avaliados, para posições mais próximas da fonte sonora, 841, 842 e 843.

A **Tabela 6**, ilustrada de seguida, refere-se à média total correspondente, a cada coluna:

	839	840	841	842	843
Valor médio total por coluna	-23,2583	-20,7001	-18,5097	-16,9828	-16,2696

Tabela 6 - Valor médio total por coluna

Depois de analisados os resultados obtidos para os Testes A, posições P1 e P2, obtém-se, de seguida, uma análise relativamente aos gráficos e tabelas referentes aos Testes B, para as mesmas posições P1 e P2 e para a mesma frequência.

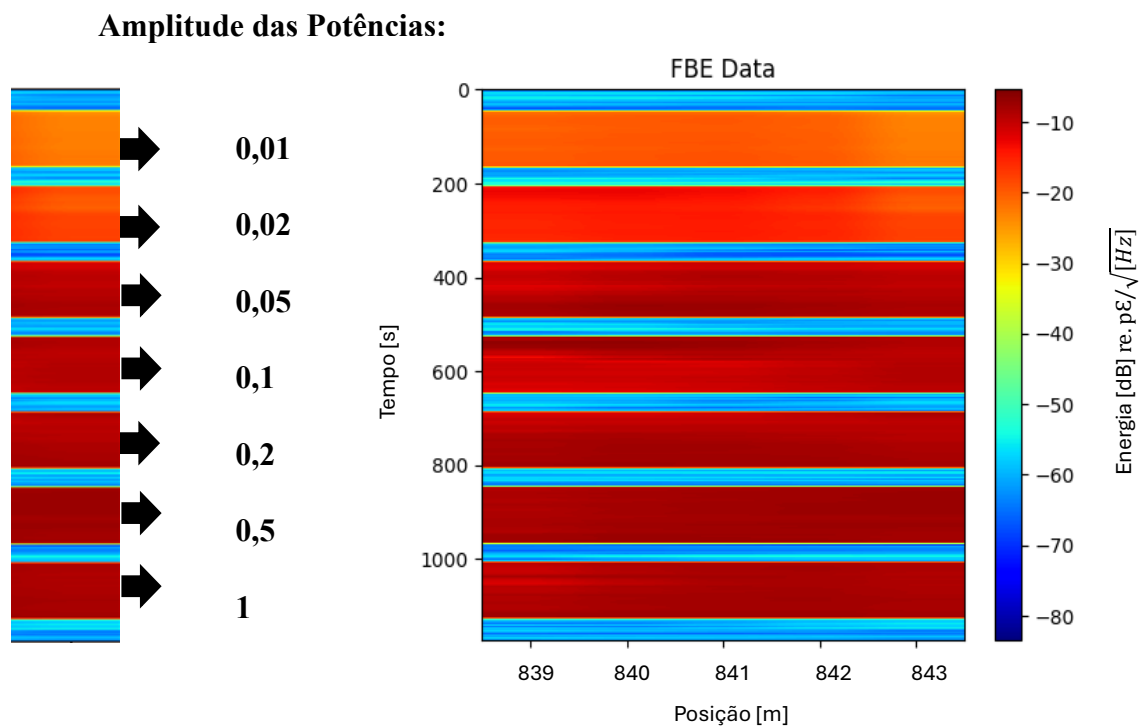


Figura 28 - FBE Data para os Testes B e posição 1

Tabela dos dados reduzidos					
AP	Média por coluna				
	839	840	841	842	843
0,01	-20,2733	-19,8224	-19,6763	-20,3340	-23,1338
0,02	-14,8947	-14,4236	-14,5314	-15,7194	-18,8850
0,05	-10,2067	-9,2606	-8,8587	-9,0548	-9,5716
0,1	-10,2344	-9,8396	-9,6588	-9,3516	-9,1046
0,2	-9,0247	-8,7396	-8,6842	-8,6744	-8,7764
0,5	-8,4567	-7,9442	-7,7103	-7,5981	-7,5879
1	-9,3235	-8,4432	-8,0432	-8,0229	-8,4375

Tabela 7 - Dados reduzidos do Teste B na posição 1

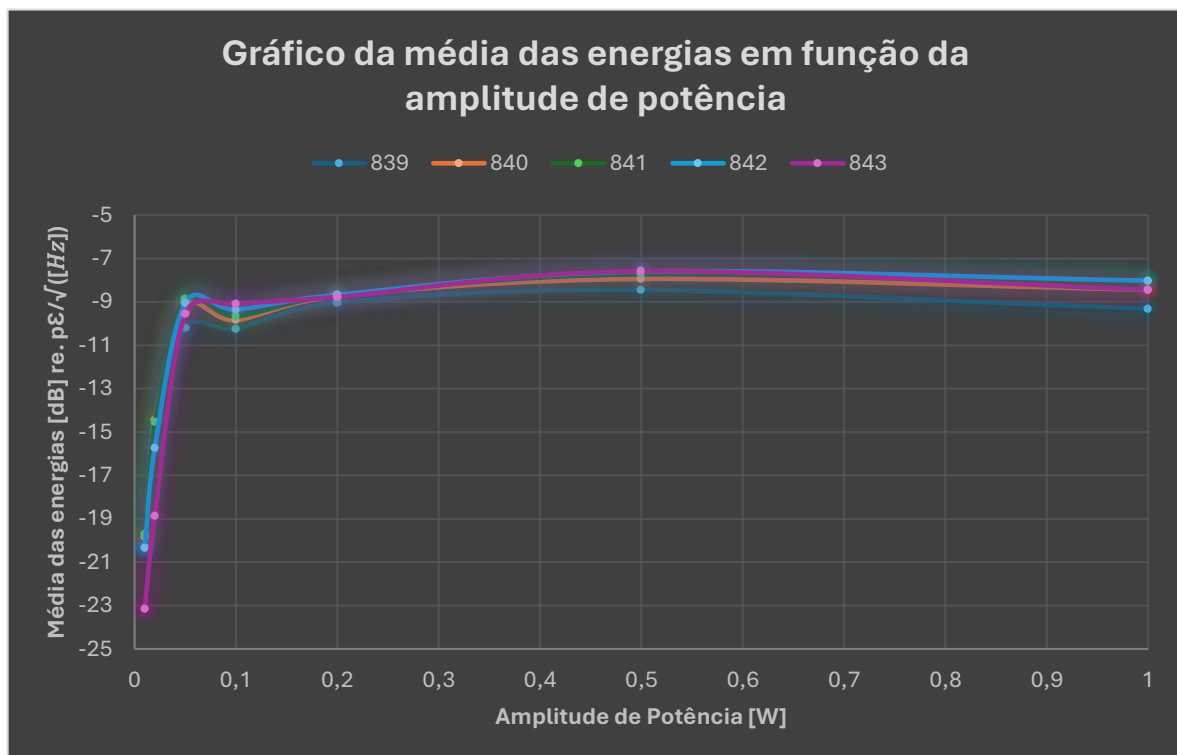


Gráfico 5 - Média das energias em função da amplitude de potência dos Testes B em P1 (escala linear)

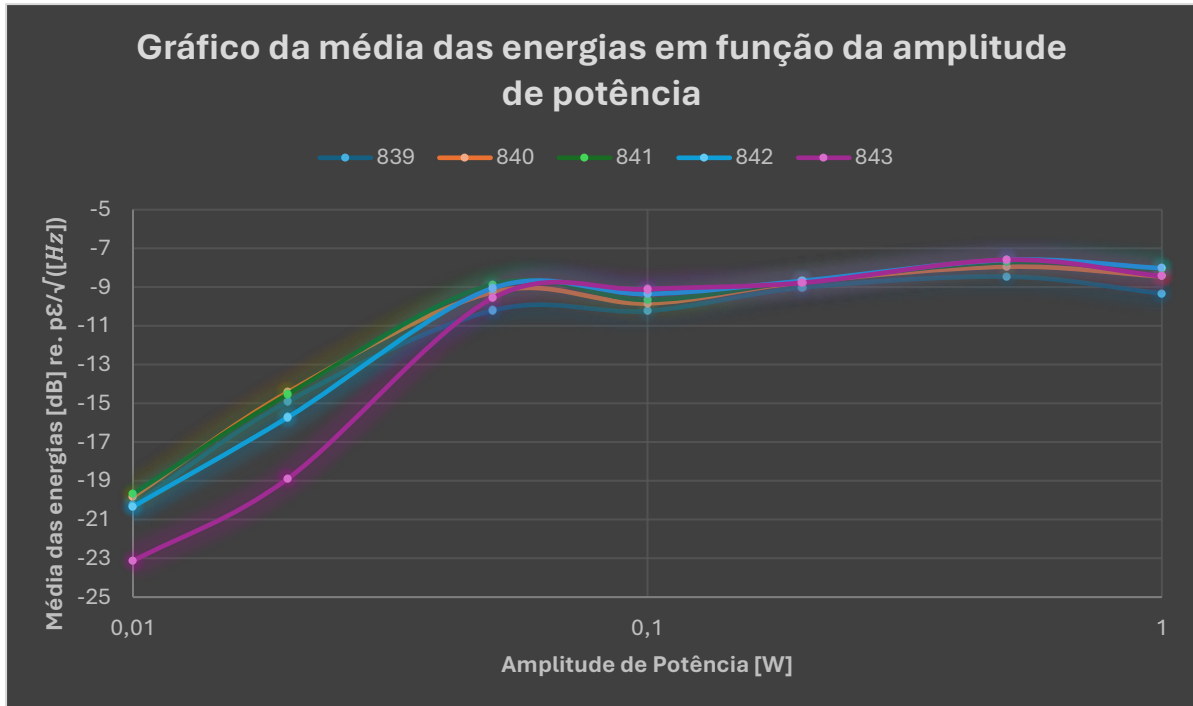


Gráfico 6 - Média das energias em função da amplitude de potência dos Testes B em P1 (escala logarítmica)

	839	840	841	842	843
Valor médio total por coluna	-11,7734	-11,2104	-11,0233	-11,2507	-12,2138

Tabela 8 - Valor médio por coluna

Após se ter obtido a **Figura 28**, **Tabela 7**, **Gráfico 5**, **Gráfico 6** e a **Tabela 8**, pode-se retirar as seguintes conclusões: o facto destes testes terem sido realizados com o cabo entre os sacos de areia torna, para esta posição, P1, o cabo mais sensível à captação do som para as duas AP mais baixas, 0,01 e 0,02 uma vez que os valores a vermelho na **Tabela 7** correspondem à posição onde o altifalante se encontrava. Também pode dever-se à influência do gerador de ondas por interferências construtivas, onde o som possa ter sido amplificado. A partir dessas duas AP, os resultados não são transparentes ao estudo, carecendo de mais ensaios para um estudo mais aprofundado assim como de mudança das condições de fronteira (alteração da posição do altifalante subaquático, por exemplo) para possíveis resultados melhorados.

A **Tabela 8** realça a posição 841, com o valor mais baixo, estando relacionada com o que fora abordado relativamente à **Tabela 7**.

Em relação aos **Gráfico 5** e **Gráfico 6**, pode-se determinar que, a partir da AP de 0,2, as curvas são mais coesas, destacando a posição dos 841 (sabendo que a fonte se encontra próximo dessa posição), até à AP de 1. As curvas 842 e 843, visto estarem mais afastadas da fonte, teriam de ser feitos mais testes para poder afirmar e estudar a causa dos resultados, havendo, contudo, uma explicação que poderá estar relacionada com o facto do CFO estar “enterrado” nos sacos de areia e o sinal ser “homogêneo” ao longo do cabo.

Em conclusão, para esta posição do altifalante subaquático, o CFO, na generalidade, possui uma eficaz deteção ao longo do cabo para AP superiores a 0,2, especialmente para as posições, 840, 841 e 842.

No último caso de estudo, para os Testes B, posição P2, obteve-se, a **Figura 29**, a **Tabela 9**, o **Gráfico 7**, o **Gráfico 8** e a **Tabela 10**, respetivamente.

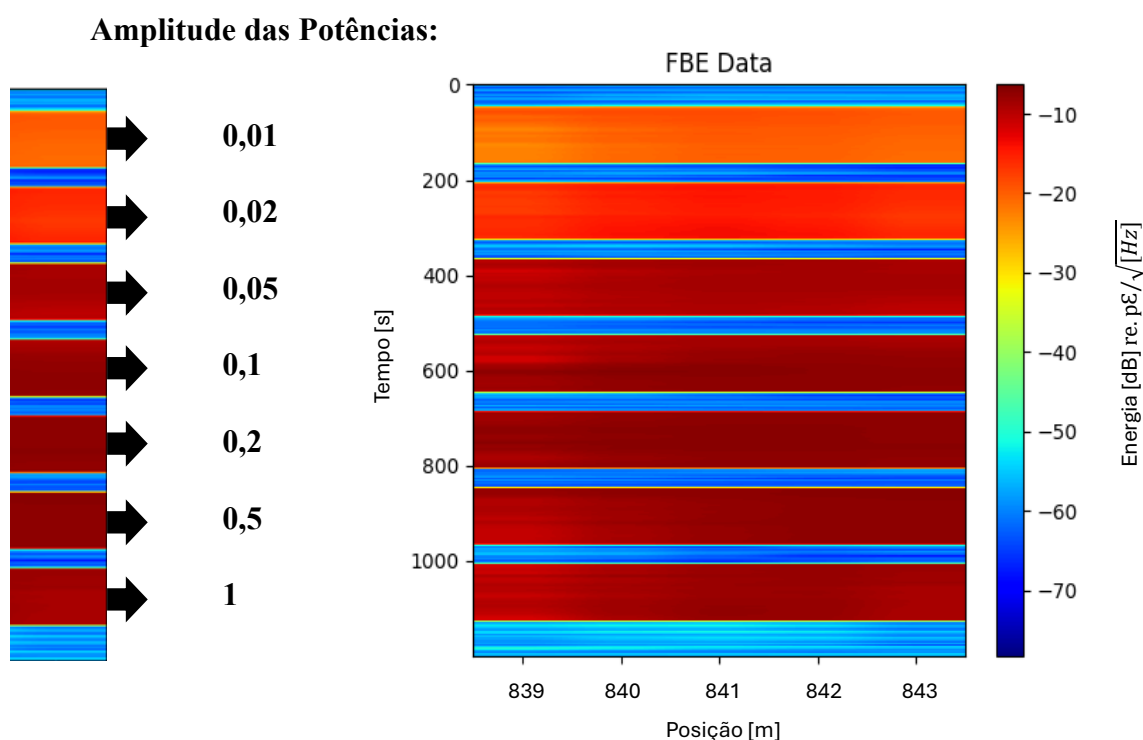


Figura 29 - FBE Data para os Testes B e posição 2

Deduz-se desta figura que a energia contida no CFO é muito mais uniforme quando o cabo está “enterrado” e ainda se pode observar claramente que é mais sensível para as AP superiores a 0,1, especialmente, a partir da posição 841 até à posição 843.

Tabela dos dados reduzidos					
AP	Média por coluna				
	839	840	841	842	843
0,01	-21,9049	-20,3308	-19,7844	-19,9746	-20,6601
0,02	-16,7464	-15,0925	-14,4995	-14,9636	-16,4415
0,05	-10,2761	-9,2536	-8,8848	-8,9471	-9,2885
0,1	-9,4425	-8,1553	-7,7019	-7,7159	-7,8776
0,2	-8,0757	-7,3798	-7,1704	-7,1838	-7,2845
0,5	-9,6647	-8,3092	-7,6074	-7,2838	-7,1996
1	-10,4173	-8,7912	-7,9440	-7,8664	-8,7075

Tabela 9 - Dados reduzidos do Teste B na posição 2

No que concerne à análise da **Tabela 9**, tendo em conta que o altifalante subaquático se encontra posicionado entre as posições 841 e 842, pode-se concluir que pelos valores que se obteve (estando destacados a vermelho), que estes testes foram os que resultaram melhor relativamente a todos os testes efetuados. Destacando ainda a sensibilidade do cabo a AP acima dos 0,1 nestas posições.

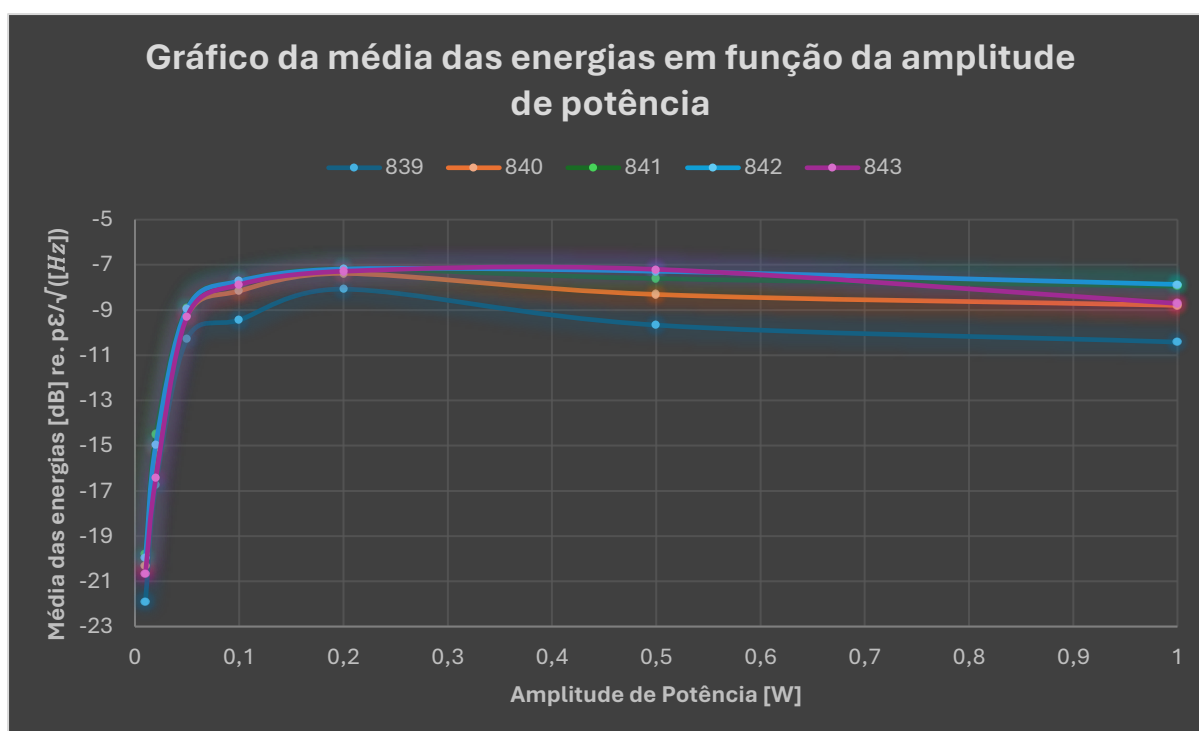


Gráfico 7 - Média das energias em função da amplitude de potência dos Testes B em P2 (escala linear)

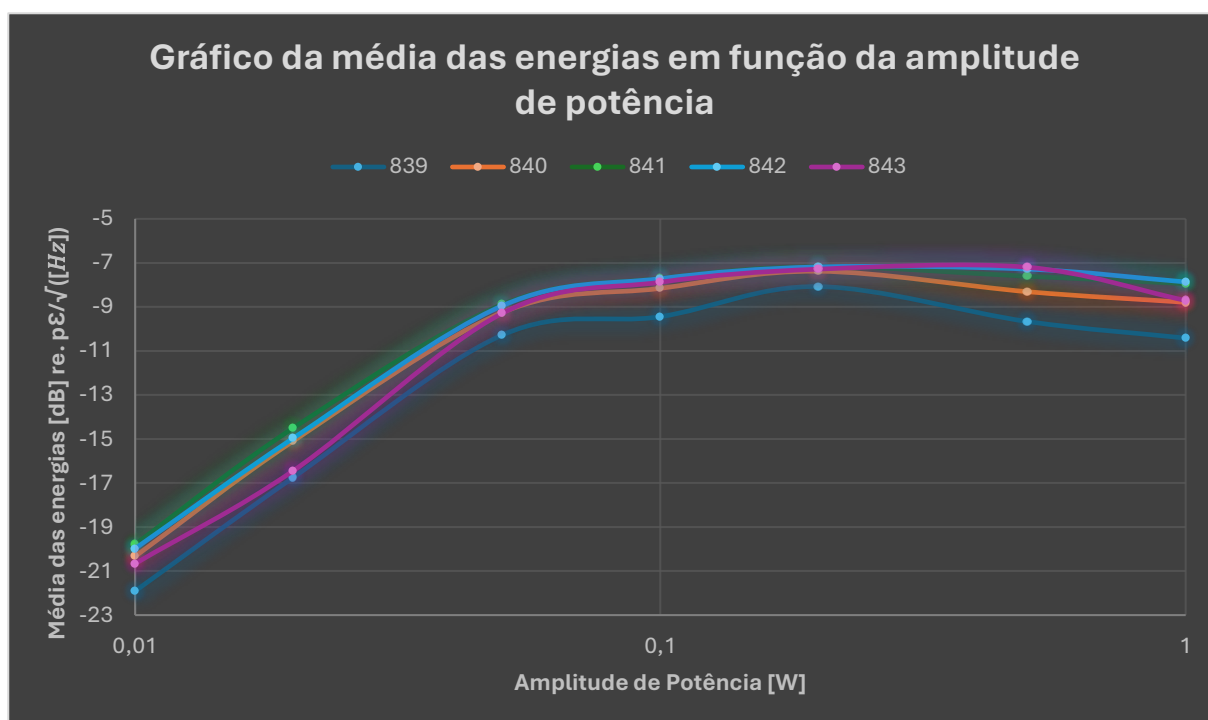


Gráfico 8 - Média das energias em função da amplitude de potência dos Testes B em P2 (escala logarítmica)

Após a análise dos dois gráficos (**Gráfico 7** e **Gráfico 8**), pode-se concluir que o CFO é mais sensível nas posições próximas da fonte, como verificado anteriormente, em 841 e 842, logo, pode-se verificar que para estes testes, nesta posição, existe sensibilidade do cabo perante o som emitido, nestas condições. Na tabela seguinte, confirma-se que os valores mais negativos, das referidas posições, vão ao encontro do que foi mencionado e provado.

	839	840	841	842	843
Valor médio total por coluna	-12,3611	-11,0446	-10,5132	-10,5622	-11,0656

Tabela 10 - Valor médio por coluna

Em conclusão, pode-se afirmar que, dos testes executados e analisados, onde se obtiveram melhores resultados, comprovando a sensibilidade do CFO para este estudo, foram os Testes B, especialmente em P2.

Acrescenta-se a importância da realização de mais ensaios futuros para se conseguir validar o estudo com uma base sólida e estatisticamente válida, tendo em consideração as seguintes sugestões:

- Efetuar alterações nas condições de fronteira (como referido anteriormente);

- Executar testes em que o altifalante subaquático esteja posicionado (em três posições diferentes ou ambas em simultâneo), cujo absorvedor acústico se encontre na parte superior, na parte inferior e nas laterais do altifalante subaquático para isolamento acústico a fim de direcionar o som e diminuir possíveis interferências construtivas ou destrutivas;
- Retirar a estrutura metálica (**Figura 20**) para a execução de novos testes;
- Evitar a influência de fatores externos na realização dos testes.

5.7. Análise final dos resultados

Apresentar-se-á, de seguida, uma análise referente ao objeto em estudo, neste caso, que será a forma como varia a AP ao longo da posição tendo em conta a média das energias, ou seja, os valores obtidos durante a execução dos testes, a fim de se obter uma melhor perceção da sensibilidade do CFO tendo como referência a influência da AP. Apresenta-se, assim, os quatro gráficos obtidos através da linguagem de programação *python*, cujo código se encontra no **Apêndice D- Código em linguagem de programação *python* utilizado, relativo aos Testes A, posição 1.**

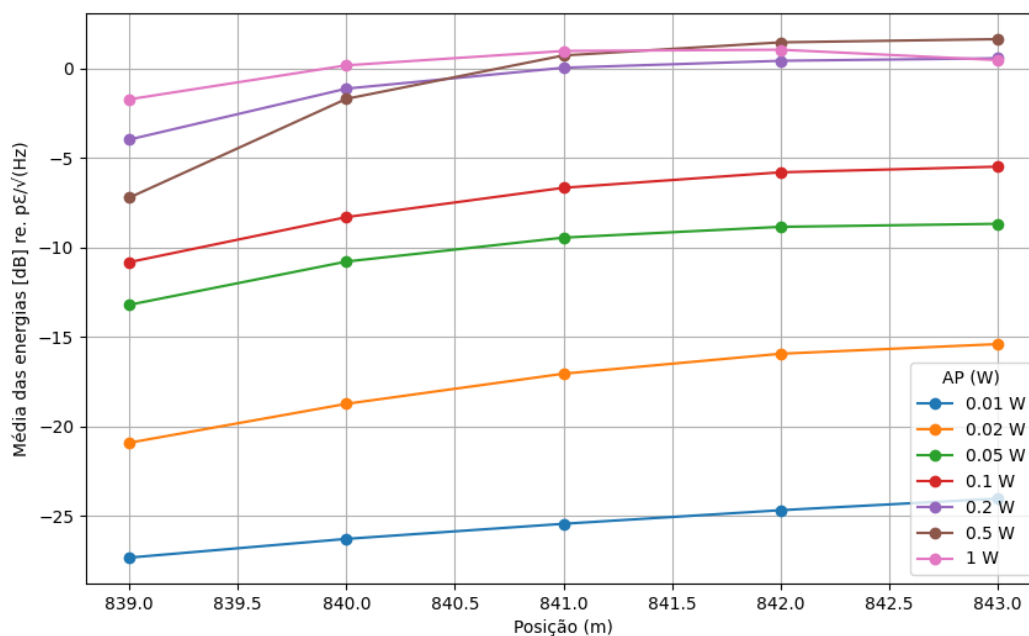


Gráfico 9 - Média das energias em função da posição dos Testes A em P1

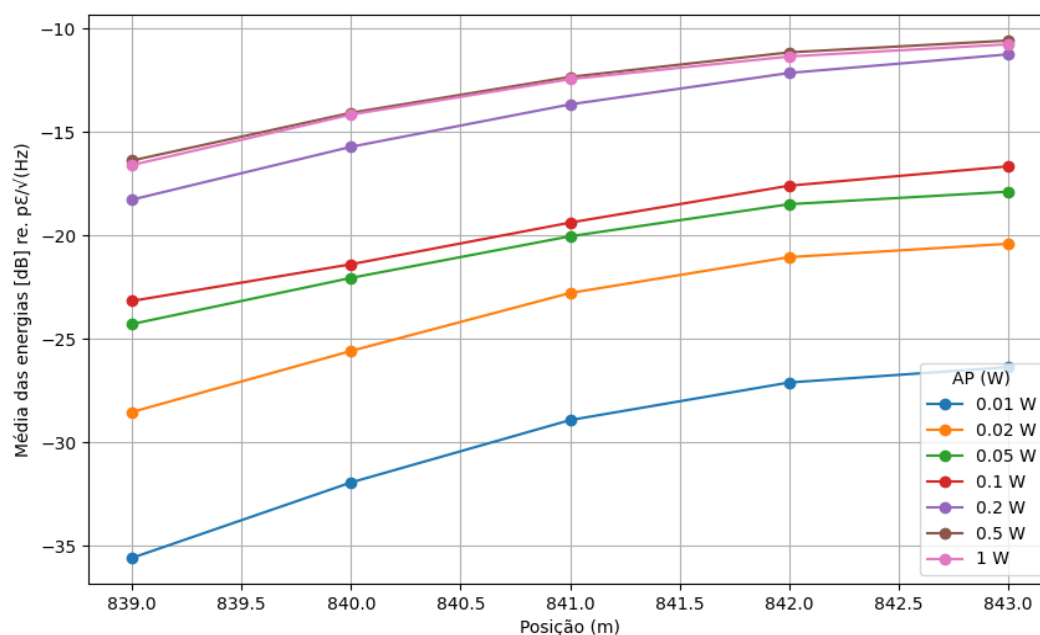


Gráfico 10 - Média das energias em função da posição dos Testes A em P2

Em conclusão, no que se refere aos **Gráfico 9** e **Gráfico 10**, conclui-se que o CFO é muito sensível às AP de 0,2; 0,5 e 1, confirmando-se que reage melhor, no caso do primeiro, para as posições mais afastadas da fonte sonora e no caso do **Gráfico 10**, é sensível para esta posição do altifalante.

No caso de existirem mais ensaios de estudo, conclui-se para este caso que as melhores AP para análise futuras, para os Testes A, são acima de 0,2.

Pode-se concluir ainda que a posição da fonte sonora (destes testes em P1) possui uma relação inversa com a AP emitida, ou seja, a média da energia é mais elevada, mais longe do altifalante subaquático. Mas também se observa que, para as três AP mais elevadas, a partir da posição dos 840, a média da energia vai aumentando e as três curvas correspondentes às AP 0,2; 0,5 e 1 aproximam-se.

Entre estas duas posições, P1 e P2, a que mais se adequa para este tipo de cabo e análise em estudo é a P2, devido não só à linearidade dos resultados do **Gráfico 10** para as três AP mais elevadas como também devido a todos os outros argumentos abordados anteriormente. A posição P2 é onde o cabo reage melhor, mais próximo da fonte sonora.

Relativamente aos Testes B, para as duas posições, apresentam-se de seguida os dois gráficos.

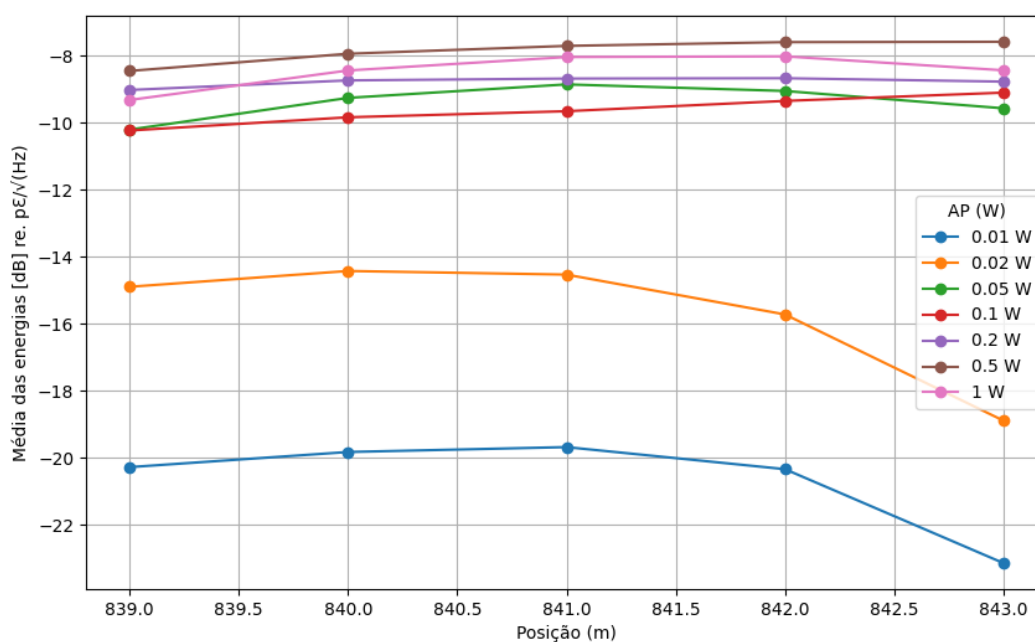


Gráfico 11 - Média das energias em função da posição dos Testes B em P1

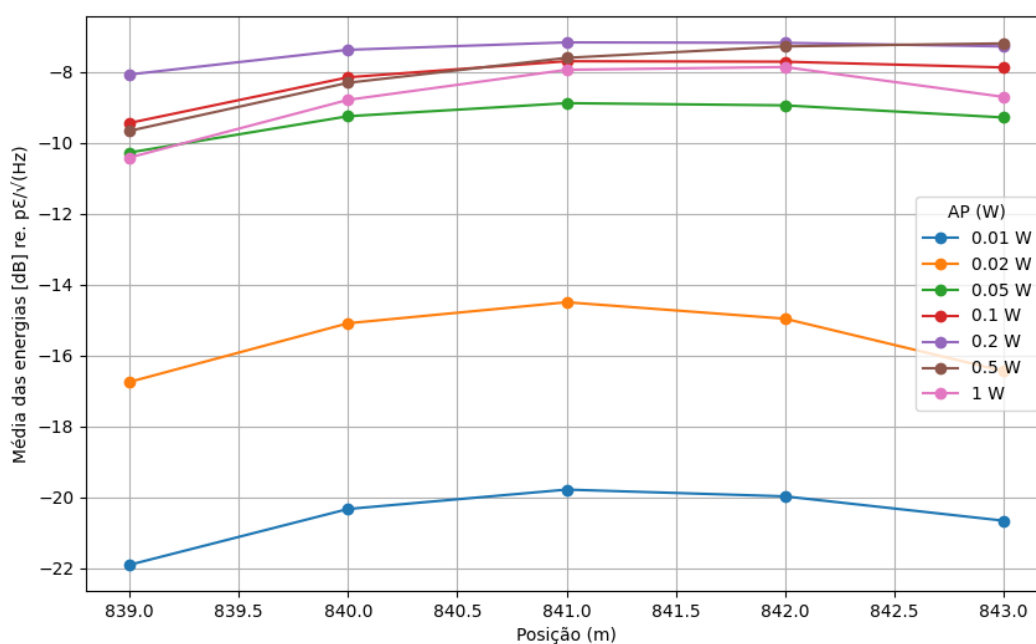


Gráfico 12 - Média das energias em função da posição dos Testes B em P2

Após uma análise efetuada em relação aos **Gráfico 11** e **Gráfico 12**, os quais correspondem ao CFO estar “enterrado”, deduz-se que se obtiveram os melhores resultados de todos os testes efetuados para a posição P2, uma vez que, analisando cada um dos gráficos, se deduziram as conclusões seguintes.

No que se refere ao **Gráfico 11**, na posição P1, destacam-se as AP 0,01 e 0,02 devido aos valores que se obtiveram, tendo-se destacado para a posição onde o altifalante se encontrava comparativamente com as restantes posições e com os restantes resultados, não conseguindo concluir-se mais nada relativamente a esta posição, sendo necessários mais casos de estudo para comparar os resultados. Acrescenta-se ainda o facto de existir também, neste gráfico, para as mesmas AP referidas, fenómenos anómalos, uma vez que a AP aumenta ligeiramente, de forma gradual e parcialmente linear e depois a AP diminui abruptamente. Uma possível justificação para este acontecimento é o facto do som se dissipar ao longo da distância ou ainda devido às reflexões sentidas no tanque, para a posição P1.

Quanto ao **Gráfico 12**, destacam-se estes resultados, relativos a P2, tanto para 841 como para a posição de 842, acima da AP de 0,05 onde se sente a diferença da média das energias, mas em 0,1 realçam-se os valores, sendo estes muito lineares e constantes até sensivelmente à AP de 1.

Conclui-se assim que apesar das medições não serem consistentes ao longo das diferentes posições, relativas às AP mencionadas, o CFO destaca a sensibilidade que possui para determinados sons emitidos (com uma frequência de 800Hz), simulando que está enterrado, na posição P2, ou seja, mais afastado da estrutura metálica, podendo esta ter influência nos resultados apresentados.

Em suma, após uma análise robusta dos resultados obtidos, é possível concluir que existe uma relação significativa entre a média das energias e AP sentida ao longo das diferentes posições. No geral, conclui-se que o CFO é mais sensível para AP mais elevadas. Contudo, para os Testes A, lembrando que o CFO se encontra depositado sobre os sacos de areia, para ambas as posições, determinando-se que, quando a fonte está a emitir tanto em P1, como P2, o CFO é mais sensível para posições maiores, ou seja, a partir dos 841, 842 e 843 e também para as AP mais elevadas. Para os Testes B, lembrando que o CFO se encontra entre os sacos de areia, para as posições P1 e P2, conclui-se que, reage de forma positiva também para APs mais elevadas, sendo que, para P2, o cabo é mais fiável para AP também mais elevadas, mas mais próximo do altifalante subaquático.

Em conclusão, obteve-se uma análise preliminar pormenorizada acerca da sensibilidade e fiabilidade do CFO aos vários sons emitidos (para a mesma frequência

mas dependentes da AP) e ainda se acrescenta que, caso se executassem mais testes experimentais a este tipo de CFO, aconselha-se o uso de AP mais elevadas e todas as alterações mencionadas anteriormente a fim de se obterem melhorias.

Por fim, conclui-se que num futuro próximo, dependendo dos resultados de novos ensaios e testes, poder-se-á implementar a utilização deste tipo de CFO para uma possível utilização como um avanço na tecnologia marinha para monitorização acústica submarina e sensibilização do ambiente marítimo. Apesar da intensa análise do estudo efetuado, uma vez que o CFO não demonstra a sensibilidade esperada para todos os casos, apenas quando está “enterrado” e próximo da fonte, serão imprescindíveis mais testes e ensaios a fim de comprovar a sensibilidade do mesmo, tendo como referência todas as propostas de melhoria já apresentadas. Posto isto, esta tecnologia será um grande feito com impacto na melhoria das respetivas capacidades das operações navais.

Conclusão

A segurança dos Cabos Submarinos (CSs) é um assunto bastante complexo e o facto de estar inserido no mundo do ciberespaço, ainda torna este tema mais relevante, atual e promissor. Por este motivo, foi feita uma análise detalhada acerca do tema, como se pode observar ao longo da Dissertação, no qual se optou por fazer uma divisão em cinco capítulos:

O primeiro capítulo é referente a aspetos mais direccionados para a história, constituição, funcionamento e instalação destes onde se fornece um entendimento mais robusto sobre a evolução histórica e o papel crucial dos CSs.

No segundo capítulo, é destacada a localização geográfica, a parte jurídica relacionados com os CSs e destaca-se ainda a localização geoestratégica de Portugal que facilita não só a conectividade como coloca o país no centro da dinâmica atlântica de cooperação internacional e das tensões geopolíticas atuais. A competição estratégica global e a presente conflitualidade reforçam a necessidade de uma abordagem assertada para proteger estas IC.

No terceiro capítulo, refere-se à segurança dos CSs, sendo este um assunto central, onde se enfatiza a cibersegurança e a segurança marítima, as políticas e regulamentações relacionadas com estes cabos, pois, apesar de existirem novos diplomas legais que incidam sobre a resiliência destes cabos, estes ainda continuam a ser um assunto crítico nos dias que correm, por todos os motivos abordados anteriormente. As propostas de atuação que garantam a segurança destas infraestruturas, visam assegurar a integridade, funcionalidade e mitigar os riscos a fim de responder eficazmente a potenciais ataques, protegendo assim estas infraestruturas.

No quarto capítulo, relaciona-se a organização, segurança e defesa do ciberespaço assim como as operações militares no contexto da OTAN e da Marinha Portuguesa, sublinhando a crescente importância da defesa cibernética. Termina-se com a criptografia, autenticação e proteção dos dados como componentes críticos para a segurança da informação transmitida por estes cabos.

No quinto capítulo, foi estudado o projeto *Fibersense*, sintetizando este trabalho científico, numa descrição teórica, foi explicado o projeto em si, assim como o âmbito e interligação deste com a Dissertação e a tecnologia associada. Por último, foram

processados os dados e interpretados os resultados através do programa DAS *Configurator* do *AP Sensing*, do *software python* e do *Excel*.

Atendendo à necessidade de uma maior proteção destas infraestruturas, ainda se destacaram as seguintes citações consideradas imprescindíveis no âmbito do presente tema e servindo como um “reforço” em destaque para a gravidade da situação. Segundo o relatório de “*Cyber Defense Across the Ocean Floor*” os CSs são considerados a “principal infraestrutura física que suporta o ciberespaço” (Carvalho, 2023a), tornando-se imperativa a proteção tanto a nível físico como através do cumprimento das regulamentações impostas com o objetivo de garantir a segurança dos dados através da transmissão pelos CSs.

Considerando ainda a falta de “responsabilidade” única e não conjunta pela existência destes cabos, dificultando assim a governação dos mesmos, de acordo com, “A natureza multinacional dos cabos submarinos, combinada com a sua existência conjunta em diferentes jurisdições legais e a propriedade conjunta público-privada dos cabos submarinos, dificulta a governação” (Ganz et al., 2024, p. 21).

Com a elaboração deste trabalho científico, pretendeu-se estudar a segurança dos CSs, concluindo-se assim que ainda não é suficiente. Apesar dos estudos já desenvolvidos e os que ainda estão em desenvolvimento, ainda se considera um tema muito sensível. Serão necessárias e urgentes mais medidas para a proteção destes cabos a fim de mitigar possíveis danos e intervir em causas futuras, agindo no que se refere à resiliência.

Salientam-se como resultados deste estudo, as seguintes necessidades urgentes a serem praticadas:

- Adotar a expressão de “Infraestrutura Crítica” aos cabos submarinos de forma explícita em instrumentos/ diplomas legais. Apesar de existir implicitamente, não é abordada de forma explícita;
- Reforçar as competências do Estado costeiro quanto ao lançamento e implantação de CSs na ZEE e na PLATCON;
- A necessidade de uma proteção mais eficaz nos *Beach Manhole*;
- Ter mais atenção às zonas onde são colocados os CSs, evitando zonas onde tenham sido reportados muitos casos de incidentes marítimos;
- Divulgar a localização exata dos CSs apenas a entidades autorizadas;

- Melhorar e aumentar a vigilância, monitorização e observação marítimas através de aparelhos e veículos autónomos, como os *landers* ou os *gliders* que possuem uma elevada autonomia;
- Implementar um maior uso de sistemas de deteção e observação do fundo do mar que incluam a tecnologia SMART a fim de se integrar sistemas de monitoração ambiental para avaliar o impacto das operações de instalação ou aviso prévio acerca de potenciais causas naturais;
- Melhorar os sistemas de deteção dos CSs, através da tecnologia do DAS para suspeitas de proximidade aos CSs que existam na ZEE portuguesa;
- Implementar tecnologias avançadas de deteção que possuam câmaras subaquáticas de alta resolução, incorporadas nos repetidores submarinos;
- Melhorar a cooperação internacional entre países a fim de desenvolver padrões comuns de segurança e regulamentações para a proteção dos CSs, em águas internacionais, garantindo a conformidade e a implementação eficaz de medidas de proteção ou o simples facto de reparação de um Cabo Submarino ser feito de forma rápida e adequada;
- Utilizar técnicas de engenharia avançadas para reforço das componentes físicas dos CSs e instalação de melhores proteções físicas;
- Utilizar AUVs para realizar reparações submarinas complexas de forma rápida;
- Estabelecer programas de manutenção preventiva e inspeção regular aos CSs, incluindo a utilização de ROVs para realizar inspeções visuais, possuindo câmaras para avaliar, com regularidade, a integridade dos cabos;
- Implementar medidas para prevenir danos ecológicos através do uso de materiais eco-amigáveis e práticas de instalações sustentáveis;
- Incentivar e consciencializar a população sobre a importância dos CSs de forma a promover a consciencialização pública através do desenvolvimento de campanhas ou a catastrófica potencialidade de acidentes que podem ocorrer com estas infraestruturas, fazendo obrigatoriamente parte do público alvo, os pescadores, operadores de embarcações e de toda a população no geral;
- Propor a elaboração de um Protocolo/ Convenção Internacional a uma Convenção existente que permita tipificar, em sede internacional, o crime de

disrupção dos CSs, na forma tentada ou consumada, a título doloso ou negligente, nos espaços marítimos para além da jurisdição dos Estados (isto é, Área e Alto mar). Pretendendo-se, desta forma, legitimar a intervenção dos navios de guerra ou equiparados (de um determinado Estado) para vigiarem, monitorizarem e fiscalizarem os CSs nos espaços marítimos internacionais e, poderem abordar um navio ou uma embarcação suspeito.

Em suma, existe uma relação entre a interseção da tecnologia, geopolítica e da segurança relativamente aos CSs. A análise robusta e as propostas apresentadas visam reforçar a necessidade de uma maior garantia das políticas e normas de segurança uma vez que a segurança dos CSs é essencial para a estabilidade das redes de comunicação globais. Reforçando a necessidade da continuidade dos esforços de pesquisa e desenvolvimento nesta área, sendo crucial para assegurar a resiliência dessas infraestruturas vitais.

Em relação ao projeto *Fibersense*, pode-se concluir dos ensaios preliminares realizados que, o CFO possui mais sensibilidade para AP superiores a 0,2 (na generalidade dos testes executados) e que reage de uma forma mais significativa para as posições mais próximas da fonte sonora quando esta se encontra a emitir o som. Desta conclusão pode-se retirar uma relação positiva quanto ao âmbito da presente Dissertação de Mestrado, embora careça de mais ensaios e testes, mas como foi referido anteriormente, poderá servir para a possível deteção e vigilância submarinas assim como para um grande feito, visto que Portugal possui uma ZEE de grande dimensão, tendo esta tecnologia muito potencial para a monitorização de parte desta área de jurisdição.

Limitações do Estudo

Quanto às limitações do estudo, destaca-se como uma grande limitação, o facto dos testes experimentais em ambiente operacional real serem realizados depois da data de entrega da presente Dissertação, o que fez com que este estudo acerca do projeto apenas se restringisse a dados experimentais preliminares obtidos através de ensaios realizados em ambiente controlado e isolado, no tanque de Arquitetura Naval da EN, contendo, por isso, apenas conclusões acerca deste ambiente em questão.

No que se refere aos testes efetuados neste ambiente, a fim de comprovar a viabilidade da tecnologia do DAS para todos os casos de estudo, seriam necessários mais ensaios e testes experimentais.

Destaca-se ainda a quantidade de dados que são gerados, os quais rondam o 1GB/minuto, por cada ensaio o que requiere um considerável esforço computacional para o pós-processamento.

Sugestões de Estudos Futuros

Para além do que foi já mencionado relativamente aos ensaios experimentais, salientam-se como sugestões de estudos futuros, o desenvolvimento do tema da Criptografia Quântica no apoio à proteção dos dados que circulam pelos cabos submarinos, o desenvolvimento da Inteligência Artificial no que se refere à necessidade urgente de legislação e o estudo das possíveis vulnerabilidades da ENSC 2024, mesmo que ainda não se encontre publicada, à data da presente Dissertação.

Referências Bibliográficas

- ACOS STRAT. (2014). *Cyber Security Strategy for Defence*. Defence Strategy Department, ACST- Strategy-CyberSecurity-001 Ed 001/ Rev 000.
- Adhitama, M. (2019). Geopolitics of Portugal in Atlantic Sea. *IPTEK Journal of Proceedings Series*(6), 48. doi:10.12962/j23546026.y2019i6337
- Agência dos Direitos Fundamentais da União Europeia. (2014). *Manual da Legislação Europeia sobre Proteção de Dados*. Luxemburgo: Serviço das Publicações da União Europeia. doi:10.2811/73790
- Albuquerque, M., Abreu, M., Coelho, P., Lourenço, N., Campos, A., Conceição, P., . . . EMEPC, E. (2012). Extensão da Plataforma Continental, Um Projecto de Portugal - Seis anos de missão (2004-2010).
- Altantic Cable Maintenance & Repair Agreement [ACMA]. (s.d.). *Submarine Cable Services*. Obtido em 3 de março de 2024, de acma: acma2017.com/services/submarine-cable-services/
- ANACOM [Autoridade Nacional de Comunicações]. (2021). Surveillance and Protection of Submarine Cables in the Portuguese EEZ. *Int'l Connectivity / EU Atlantic Data-Gateway Platform, Session 4, Safe and Secure Connectivity: Linking up Data services*, 1-15. Sines.
- ANACOM. (2020). *portal5G*. Obtido em 20 de abril de 2024, de UIT – União Internacional das Telecomunicações: <https://portal5g.pt/organizacoes-5g/uit-uniao-internacional-das-telecomunicacoes/>
- ANETIE. (s.d.). *Segurança Electrónica*. Obtido em 21 de maio de 2024, de TIC.UE: <https://ue-tie.anetie.pt/pt-pt/electronic-security>
- AP Sensing. (2023). User's Guide. *AP Sensing DAS Configurator Client , 6th Edition*.
- Applegate, S. (2013). The Dawn of Kinetic Cyber. *2013 5th International Conference on Cyber Conflict*.
- Apruzzese, G., Laskov, P., Oca, E., Mallouli, W., Rapa, L., Grammatopoulos, A., & Franco, F. (2023). The Role of Machine Learning in Cybersecurity. *Digit. Threat.: Res. Pract.* 4.1, Article 8, p. 38.
- Barbosa, M. (2016). *As Ameaças ao Ciberespaço e a Estratégia de Segurança da UE e Portugal*. [Trabalho Individual, Faculdade de Direito da Universidade Nova de Lisboa]. Obtido de https://www.academia.edu/37494690/AS_AMEA%C3%87AS_AO_CIBERESP_A%C3%87O_E_A_ESTRAT%C3%89GIA_DE_SEGURAN%C3%87A_DA_U_E_E_PORTUGAL
- Barros, J. (2017). Conectividade Internacional- Enquadramento à escala global. *Workshop- Conectividade Internacional: Desafios e Oportunidades*, 1-5.
- Barros, J. (2021). Cabos Submarinos num Mar de Conectividades. pp. 1-30.

- Barros, J. (2024). Cabos Submarinos: Uma agenda emergente. *Instituto Universitário de Lisboa- ISCTE*, 1-42. Lisboa.
- Barros, J., & Bernardino, L. (2024). Conferências do Círculo do Mar: "Geoestratégia dos Cabos Submarinos e Impacto na Segurança Nacional". *Sociedade Histórica da Independência de Portugal*. Obtido em 25 de fevereiro de 2024, de <https://www.youtube.com/watch?v=pa3DZm4WpeY>
- Beaufils, J. (2000). How Do Submarine Networks Web the World? *Optical Fiber Technology*, 6(Nº 1), 15-32.
- Bischof, Zachary; Fontugne, Romain; Bustamante, Fabián. (2018). Untangling the world-wide mesh of undersea cables. 78-84. Redmond, Washington, USA, Washington, USA: HotNets. doi:<https://doi.org/10.1145/3286062.3286074>
- Bogdandy, A., Wolfrum, R., Bernstorff, J., Goldmann, M., & Dann, P. (2009). The Exercise of Public Authority by International Institutions: Advancing International Institutional Law. pp. 777-806. Obtido de https://www.researchgate.net/publication/41935532_The_Exercise_of_Public_Authority_by_International_Institutions_Advancing_International_Institutional_Law
- Bohan, M. (2018). *NOAA- Ocean Exploration*. Obtido de NOAA's Participation in the U.S. Extended Continental Shelf Project: <https://oceanexplorer.noaa.gov/oceanos/explorations/ex1810/ecs/welcome.html>
- Boone, W. (2013). Risk Management. R. Radvanovsky & J. Brodsky, eds. *Handbook of SCADA/ Control Systems Security*, 69-111.
- Brake, D. (2019). Submarine Cables: Critical Infrastructure for Global Communications. *Information Technology & Innovation Foundation*, 11. Obtido de <https://www2.itif.org/2019-submarine-cables.pdf>
- Brown, G. (2016). Spying and Fighting in Cyberspace: What is Which? *Journal of National Security Law & Policy*, 8, 621-635. Obtido de https://jnsplp.com/wp-content/uploads/2017/10/Spying-and-Fighting-in-Cyberspace_2.pdf
- Bueger, C., Franken, J., & Liebetrau, T. (2022). Security threats to undersea communications cables and infrastructure- consequences for the EU. *Report for SEDE Committee of the European Parliament, PE702.557*, pp. 11-56. Obtido de [https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA\(2022\)702557_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/702557/EXPO_IDA(2022)702557_EN.pdf)
- Burnett, D. (2011). The 1884 International Convention for Protection of Submarine Cables Provisions Not in UNCLOS Deserve Attention Now. In *Workshop on Submarine Cables and Law of the Sea, Singapore*, pp. 1-12.
- Burns, B. (2009). *History of the Atlantic Cable & Undersea Communications from the first submarine cable of 1850 to the worldwide fiber optic network*, Originally published in the early 1970s in the IEEE Communications Society Newsletter. Obtido de Atlantic Cable: <https://atlantic-cable.com/Article/Easton/index.htm>

- Cabral, M. C. (2022). *A segurança dos cabos submarinos*.
- Calderon, R. (2019). *The Benefits of Artificial Intelligence in Cybersecurity [Thesis: Master of Science]*. La Salle University Digital Commons, Computer Science. Obtido de https://digitalcommons.lasalle.edu/ecf_capstones/36
- Campos, A. (2013). *A extensão da plataforma continental na perspectiva da ONU*. Instituto Superior de Ciências Sociais e Políticas, Seminário do Mar, Lisboa.
- Carter, L., Burnett, D., Drew, S., Marle, G., Hagadorn, L., Bartlett-McNeil, D., & Irvine, N. (2009). *Submarine Cables and the Oceans - Connecting the World*(31), pp. 8-54. Obtido de https://www.iscpc.org/publications/icpc-uneep_report.pdf
- Carvalho, A. R. (2023). Cabos Submarinos: Portugal (Novamente) no Epicentro da Globalização. *Revista da Armada*(Nº 583), pp. 22-24. Obtido de https://www.marinha.pt/conteudos_externos/Revista_Armada/PDF/2023/RA_583.pdf
- Castells, M. (1999). *A Era da Informação: economia, sociedade e cultura*. 3.
- CCDCOE. (2019). Strategic importance of, and dependence on, undersea cables. Obtido de <https://www.ccdcoe.org/uploads/2019/11/Undersea-cables-Final-NOV-2019.pdf>
- CEMA. (2018). Despacho do Almirante Chefe do Estado-Maior da Armada, n.º 59/18 de 11 de dezembro. *Ordem da Armada, n.º 56, 12 de dezembro de 2018*.
- Centre for the Protection of National Infrastructure [CPNI]. (2006). *An Overview of the Use of Submarine Cable Technology by UK PLC*.
- CERT. (s.d.). *The CERT Division*. Obtido em 17 de maio de 2024, de Software Engineering Institute: <https://www.sei.cmu.edu/about/divisions/cert/>
- Choo, F.-K., Smith, R., & McCusker, R. (2007). *The future of technology-enabled crime in Australia*. Trends & Issues in crime and criminal justice. Nº 341, Australian Government - Australian Institute of Criminology.
- Clare, M. (2021). Submarine Cable Protection and the Environment. *International Cable Protection Committee*(Issue #2). Obtido de https://www.iscpc.org/publications/submarine-cable-protection-and-the-environment/ICPC_Public_EU_March%202021.pdf
- Clark, B. (2016). Undersea cables and the future of submarine competition. *Bulletin of the Atomic Scientists*, 72(Nº 4), 234-237. doi:10.1080/00963402.2016.1195636
- Clark, D. (2010). Characterizing cyberspace: past, present and future. *ECIR Working Paper, Massachusetts Institute of Technology*.
- CNCS. (2020). *Quadro Nacional de Referência para a Cibersegurança*. Obtido de <https://www.cncs.gov.pt/docs/cnccs-qnrccs-2019.pdf>

- CNCS. (2024). *Relatório Cibersegurança em Portugal*. Riscos e Conflitos, 5ª Edição. Obtido de <https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obciberencns.pdf>
- Comissão Europeia. (2011). COM(2011) 163 final. Protecção das infra-estruturas críticas da informação «Realizações e próximas etapas: para uma cibersegurança mundial». Bruxelas. Obtido de <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:PT:PDF>
- Comissão Europeia. (2013). JOIN(2013) 1 final. *Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido*. Bruxelas. Obtido de <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52013JC0001>
- Comissão Europeia. (2021). COM(2021) 206 final. *Proposta de Regulamento do Parlamento Europeu e do Conselho que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da União*. Bruxelas. Obtido de eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206
- Comissão Europeia. (2024). Obtido em 27 de maio de 2024, de Relatório sobre a cibersegurança e a resiliência das infraestruturas e redes de comunicações da UE: <https://digital-strategy.ec.europa.eu/pt/library/report-cybersecurity-and-resiliency-eu-communications-infrastructures-and-networks>
- Communications Security, Reliability and Interoperability Council [CSRIC]. (2016). *Final Report - Clustering of Cables and Cable Landings*. Working Group 4A Submarine Cable Resiliency.
- Conselho da UE e Conselho Europeu. (2024). *Conselho da União Europeia e Conselho Europeu*. Obtido em 3 de maio de 2024, de Inteligência Artificial: <https://www.consilium.europa.eu/pt/policies/artificial-intelligence/>
- Conselho da UE e Conselho Europeu. (2024). *Conselho da União Europeia e do Conselho Europeu*. Obtido em 3 de maio de 2024, de Cronologia - Inteligência Artificial: <https://www.consilium.europa.eu/pt/policies/artificial-intelligence/timeline-artificial-intelligence/>
- Cordey, S., & Dewar, R. (Edits.). (2019). National Cybersecurity and Cyberdefense Policy Snapshots: Updated Collection 2. *Center for Security Studies - Cyber Defense Project*.
- Correia, P. (2002). Análise Geoestratégica de Portugal. *Nação e Defesa*(1 - 2.ª Série), 79-98.
- Crawford, S. (1983). The Origin and Development of a Concept: The Information Society. 380-385. Obtido de <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC227258/pdf/mlab00068-0030.pdf>
- Dasgupta, D., Akhtar, Z., & Sen, S. (2022). Machine learning in cybersecurity: a comprehensive survey. *Journal of Defense Modeling and Simulation*:

Applications, Methodology, Technology, 19(1), 57-106.
doi:10.1177/1548512920951275

- Davenport, T. (2012). Submarine Communications Cables and Law of the Sea: Problems in Law and Practice. *Ocean Development & International Law*, 43(Nº3), 201-242. doi:<https://doi.org/10.1080/00908320.2012.698922>
- Davenport, T. (2015). Submarine Cables, Cybersecurity and International Law: An Intersectional Analysis. *Catholic University Journal of Law and Tchnology*, 24(1), 57-109. Obtido de <https://scholarship.law.edu/jlt/vol24/iss1/4>
- De Mauro, A., Greco, M., & Grimaldi, M. (2016). A formal definition of Big Data based on its essential features. *Library Review*, 65, 122-135. doi:10.1108/LR-06-2015-0061
- Deloitte Technology. (2021). Moving towards an hyper secure world. Em P. Tavares (Ed.), *SESSION 4 - Safe and secure connectivity: linking up data services, Conference on International Connectivity and the EU-Atlantic Data Gateway Platform, May 2021*. TelecomEngineeringExcellence. Obtido em 20 de fevereiro de 2024, de https://www.anacom.pt/streaming/Pedro_Tavares.pdf?contentId=1642783&field=ATTACHED_FILE
- Diogo, L. d. (2004). Ameaças Difusas nos Espaços Marítimos sob Jurisdição Nacional. A Autoridade Marítima no Quadro Constitucional da Intervenção dos Órgãos de Estado. Em IDN, *Nação e Defesa- Portugal e o Mar* (Vols. Nº 108, 2ª Série). Lisboa.
- Diogo, L., & Gouveia, J. (2005). A Security em Ambiente Marítimo, O Código ISPS. *Cadernos Navais*, 15.
- Dutton, H. J. (1998). Understanding Optical Communications. *International Business Machines [IBM] Corporation, International Technical Support Organization*, 613.
- ECOREST. (2023). *Landers, innovative tools to study the seabed*. Obtido em 25 de maio de 2024, de Ecorest: <https://www.life-ecorest.eu/landers-innovative-tools-to-study-the-seabed/>
- Eleftherakis, D., & Vicen-Bueno, R. (2020). Sensors to Increase the Security of Underwater Communication Cables: A Review of Underwater Monitoring Sensors. *Sensors. Research Department, NATO STO Center for Maritime Research and Experimentation (CMRE)*, 1-39.
- EMGFA. (s.d.). *CISMIL | Centro de Informações e Segurança Militares*. Obtido em 23 de maio de 2024, de Forças Armadas | Portugal: emgfa.pt/pt/unidades/CISMIL
- EMSA. (s.d.). *Safety & Security*. Obtido em 5 de maio de 2024, de European Maritime Safety Agency [EMSA]: <https://www.emsa.europa.eu/we-do/safety.html>
- English, T. (2020). *Connecting the World: How the First Transatlantic Cable was Laid*. Obtido em 18 de fevereiro de 2024, de Interesting Engineering:

<https://interestingengineering.com/innovation/connecting-the-world-how-the-frist-transatlantic-cable-was-laid>

ENISA. (2020). *Uma Europa de Confiança e com Cibersegurança- Estratégia da ENISA*. Obtido de <https://www.enisa.europa.eu/publications/enisa-strategy-leaflet-translations/enisa-strategy-leaflet-pt.pdf>

ENISA. (s.d.). *About ENISA - The European Union Agency for Cybersecurity*. Obtido em 19 de maio de 2024, de enisa| EUROPEAN UNION AGENCY FOR CYBERSECURITY: <https://www.enisa.europa.eu/about-enisa>

European Commission. (s.d.). *Defence Industry and Space*. Obtido em 19 de maio de 2024, de European Defence Fund (EDF): https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

European Liberal Forum. (2023). *Towards a New European Security Architecture*. (F. Cappelletti, Ed.) Obtido de <https://doi.org/10.53121/ELFS6>

Evans, G. (2009). Overview of Submarine Cable Route Planning & Cable Route Survey Activities. pp. 1-37. Obtido de <https://cil.nus.edu.sg/wp-content/uploads/2009/10/CIL-Survey-Background-Presentation-Graham-Evans.pdf>

Finn, B., & Yang, D. (Edits.). (2009). *Communications Under the Seas: The Envolving Cable Network and Its Implications*. The MIT Press. doi:<https://doi.org/10.7551/mitpress/9780262012867.001.0001>

FPC. (2017). *Fundação Portuguesa das Comunicações | Museu das Comunicações*. Obtido em 20 de fevereiro de 2024, de Cabos Submarinos: 1988: fpc.pt/timeline_slider_post/tat-8/

FPC. (2022). *Fundação Portuguesa das Comunicações | Museu das Comunicações*. Obtido em 20 de fevereiro de 2024, de A travessia do oceano Atlântico pelos cabos submarinos: fpc.pt/pta-travessia-do-oceano-atlantico-pelos-cabos-submarinos/

Frasca, D., & Galantini, L. (2023). The Issue of Submarine Cable Security. (F. Cappelletti, Ed.) *Towards a New European Security Architecture*, 51-62. doi:<https://doi.org/10.53121/ELFS6>

Fundação Calouste Gulbenkian. (2023). *Fundação Calouste Gulbenkian*. Obtido em 3 de maio de 2024, de Inteligência Artificial: Que Humanidade? [Vídeo/ Conferência]: <https://gulbenkian.pt/read-watch-listen/inteligencia-artificial-que-humanidade/>

Galinec, D., Guberina, B., & Možnik, D. (2017). Cybersecurity and cyber defence: national level strategic approach. *Automatika - Journal for Control, Measurement, Electronics, Computing and Communications*, 58, 273-286. doi:10.1080/00051144.2017.11407022

Gallagher, J. C. (2022). *Undersea Telecommunication Cables: Technology Overview and Issues for Congress*. Congressional Research Service. Obtido de <https://crsreports.congress.gov/product/pdf/R/R47237>

- Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine Cables and the Risks to Digital Sovereignty. *SSRN Electronic Journal*. doi:10.2139/ssrn.4693206
- Germond, B. (2015). The geopolitical dimension of maritime security. *Maritime Policy*, 54, 137-142. doi:10.1016/j.marpol.2014.12.013
- Global Marine. (2018). *International Fibre Optic Cable Landing*. Scottish Futures Trust.
- Gotschalg, R. V. (2009). União Internacional das Telecomunicações - Um Desafio na Gestão da Internet. *Revista Eletrónica de Direito Internacional*, 5, 447-498.
- Governo dos Açores. (2022). *Governo dos Açores*. Obtido em 25 de fevereiro de 2024, de Nota à imprensa- Cabos Submarinos dos Açores: <https://portal.azores.gov.pt/web/comunicacao/news-detail?id=9223322>
- Gregor, K., & LeCun, Y. (2010). Learning Fast Approximations of Sparse Coding. *n ICML 2010 - Proceedings, 27th International Conference on Machine Learning*, pp. 399-406.
- Hanif, F., Waheed, U., Masood, S., Shams, R., & Inayatullah, S. (2021). An Energy Efficient Crypto Suit for Secure Underwater Sensor Communication using Genetic Algorithm. *Sukkur IBA Journal of Emerging Technologies - SJET*, 4(2).
- Hayes, J., & Schwartz, M. (2008). A History of Transatlantic Cables. *IEEE Communications Magazine*, 46(9), 42-48. doi:10.1109/MCOM.2008.4623705
- Hopper, A. G., & Drew, S. C. (2009). Fishing and Submarine Cables: Working Together. *International Cable Protection Committee*, pp. 1-54.
- Howe, B. M., Arbic, B. K., Aucan, J., Barnes, C. R., Bayliff, N., Becker, N., . . . Weinstein, S. (2019). SMART Cables for Observing the Global Ocean: Science and Implementation. *Frontiers in Marine Science*, 6, 1-27. doi:10.3389/fmars.2019.00424
- ICPC. (2024). International Cable Protection Committee. *Member List*. Obtido de Member List: <https://www.iscpc.org/documents/?id=1773>
- ICPC. (s.d.). International Cable Protection Committee Ltd. *Formal Invitation Letter*. Portsmouth. Obtido de [iscpc.org/join-the-icpc/](https://www.iscpc.org/join-the-icpc/)
- IMO. (s.d.). *IMO*. Obtido em 27 de julho de 2024, de Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf: <https://www.imo.org/en/About/Conventions/Pages/SUA-Treaties.aspx>
- Instituto Hidrográfico. (2015). *SNIMar - Sistema Nacional de Informação do Mar*. Obtido em 29 de abril de 2024, de Zona Económica Exclusiva: geoportal.snimar.pt/metadados.html?id=209cf0fe-ffb1-4db1-abad-2ee0299d53f4

- ISO/IEC 27002. (2005). Information technology - Security techniques - Code of practice for information security management. *International Standard ISO/IEC 27002:2005(E)*.
- IT SECURITY. (2023). *Sabotagem e espionagem: Os riscos para os cabos submarinos num mundo cada vez mais conectado*. Obtido em 24 de maio de 2024, de IT SECURITY: <https://www.itsecurity.pt/news/analysis/sabotagem-e-espionagem-os-riscos-para-os-cabos-submarinos-num-mundo-cada-vez-mais-conectado>
- Jakhar, D., & Kaur, I. (2019). Artificial Intelligence, machine learning and deep learnig: definitions and differences. *Clinical and Experimental Dermatology*, 45. doi:10.1111/ced.14029
- Jamadar, R., Ingale, S., Panhalkar, A., Kakade, A., & Shinde, M. (2019). Survey of Deep Learning Based Intrusion Detection Systems for Cyber Security. 6(Issue 2), 257-261.
- Jesus, H. F. (2020). *A aplicabilidade do conceito "Proteção, Segurança e Defesa" para a ciber-resiliência no contexto do Atlântico português*. Instituto Universitário Militar (IUM).
- Jiang, S. (2019). On Securing Underwater Acoustic Networks: A Survey. *IEEE Communications Surveys & Tutorials*, 21(1), 729-752.
- Jõgi, K. (2015). *ENISA - CERT Inventory*. Version 2.17. doi:10.2788/14231
- Jordan, M., & Mitchell, T. (2015). Machine Learning: Trends, perspectives, and prospects. *American Association for the Advancement of Science* , 349(Issue 6245), 255-260.
- Kettani, H., & Wainwright, P. (2019). On the Top Threats to Cyber Systems. *IEEE 2nd International Conference on Information and Computer Technologies*.
- Keupp, M. (Ed.). (2020). *The Security of Critical Infrastructures: Risk, Resilience and Defense* (Vol. 288). Springer. doi:doi.org/10.1007/978-3-030-41826-7
- Khanna, S. (2019). Machine Learning v/s Deep Learning. *International Research Journal of Engineering and Technology* , 6(Issue 2).
- Kharade, K., Kharade, S., & Katkar, S. (2019). Cyber Security - A Method of Generic Authentication of Data with Ip Security. *International Journal of Information Systems*, 9(Issue II), 63-65. Obtido de https://www.researchgate.net/publication/350603619_Cyber_Security_-_A_Method_of_Generic_Authentication_of_Data_with_Ip_Security
- Khazan, O. (2013). The Creepy, Long-Standing Practice of Undersea Cable Tapping. *The Atlantic*. Obtido de <https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cabletapping/277855/>
- Klimburg, A. (Ed.). (2012). National Cyber Security Framework Manual. *NATO Cooperative Cyber Defence Centre of Excellence Publication*.

- Kontis, G. (2022). *Technical and Organizational Challenges on Enhancing Cybersecurity with Artificial Intelligence [Master's Thesis]*. Tallin University of Technology-School of Information Technologies. Obtido de <https://digikogu.taltech.ee/en/Download/079f2596-2ea8-4589-b36d-59b44ded6aeb>
- Kramer, D. (2023). The future has arrived for securing confidential data. *Physics Today*, 76(Issue 11), 21-24. doi:10.1063/PT.3.5340
- Kulick, A. (2012). Global Public Interest in International Investment Law. *Cambridge Studies in International and Comparative Law*.
- Kumar, R., & Nagpal, B. (2018). Analysis and prediction of crime patterns using big data. *International Journal of Information Technology*, 11. doi:10.1007/s41870-018-0260-7
- Lancker, V., & Baeye, M. (2015). Wave glider monitoring of sediment transport and dredge plumes in a shallow marine sandbank environment. *PLOS ONE*, 10(6). doi:10.1371/journal.pone.0128948
- LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521, 436-444. doi:10.1038/nature14539
- Lee, K. (2019). *As Superpotências da Inteligência Artificial: a China, Silicon Valley e a nova ordem mundial*. (M. Cardoso, Ed.) Lisboa: Relógio d'Água.
- Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., . . . Wolff, S. (1997). Brief History of the Internet. *Internet Society*.
- Leite, A. (2016). A problemática da cibersegurança e os seus desafios - Cybersecurity and its challenges.
- Li, J.-h. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, 19, 1462-1474.
- Lindsey, N., & Martin, E. (2021). Fiber-Optic Seismology. *Annual Review of Earth and Planetary Sciences*, 49, 309-336. doi:10.1146/annurev-earth-072420-065213
- Lopes, T. (2018). Responsabilidade e governação das empresas no âmbito do novo Regulamento sobre a Proteção de Dados. *Anuário da Proteção de Dados*, 45-69.
- Maias, A., & Bravo, R. (2010). *Geopolítica, geoestratégia e ciberespaço: Notas introdutórias*. Lisboa. Obtido de https://www.academia.edu/5543845/Geopolitica_geoestrategia_e_ciberespaco_Notas_introdutórias
- MarSensing. (s.d.). *MarSensing Lda - Marine Sensing and Underwater Acoustic Technologies*. Obtido em 3 de junho de 2024, de Underwater Speakers: <https://www.marsensing.com/>
- Martinho, J. (2017). *As infraestruturas críticas em Portugal: um modelo de abordagem*. [Trabalho de Investigação Individual, IUM]. Obtido de

https://comum.rcaap.pt/bitstream/10400.26/21379/1/TI_Infraestruturas%20Criticas_v13Jun2017.pdf

- Matis, M. S. (2012). *The Protection of Undersea Cables: A Global Security Threat*. U.S. Army War College, Carlisle, Philadelphia. Obtido de <https://apps.dtic.mil/sti/citations/ADA561426>
- Matos, J. C. (2020). CTT 150 ANOS. *150 ANOS DO CABO SUBMARINO EM PORTUGAL*, p. 2. Obtido em 24 de fevereiro de 2024, de <https://www.ctt.pt/contentAsset/raw-data/4e896394-baa4-4c3d-abcb-3c12e7a92f85/ficheiro/0df5b436-1295-4614-a247-6403c0de5063/export/Pagela-diptica-cabos-submarino-nova-versao-2020.pdf>
- MDN. (2006). Estratégia Nacional para o Mar. *Estrutura de Missão para os Assuntos do Mar*. Obtido de <https://www.mdn.gov.pt>
- Medeiros, S., & Pinto, D. (2022). Cabos submarinos e segurança cibernética no Atlântico. *Atlantic Centre Policy Brief*(Nº 11). Obtido de https://www.defesa.gov.pt/pdefesa/ac/pub/acpubs/Documentos/Atlantic-Centre_PB_11.pdf
- Melo, H. (2011). *As informações nas Forças Armadas Portuguesas - o passado, o presente e um modelo para o futuro*. [Trabalho de Investigação Individual do CPOG 2011/12, Instituto de Estudos Superiores Militares]. Obtido de <https://comum.rcaap.pt/bitstream/10400.26/10050/1/CMG%20Henrique%20Melo.pdf>
- Mendes, F. A. (2020). *Público*. Obtido em 25 de fevereiro de 2024, de Portugal na linha da frente dos cabos submarinos que detectam sismos: <https://www.publico.pt/2020/02/24/ciencia/noticia/portugal-linha-frente-cabos-submarinos-detectam-sismos-1905117>
- Militão, O. (2014). Guerra da Informação: a cibersegurança, a ciberdefesa e os novos desafios colocados ao sistema internacional. [Tese de Mestrado, Faculdade de Ciências Sociais e Humanas da Universidade Nova de Lisboa]. Obtido de https://run.unl.pt/bitstream/10362/14300/1/Dissertacao_OMilitao_35664.pdf
- Monteiro, N. S. (2019). Cabos Submarinos: As artérias da Sociedade Contemporânea. *Revista da Armada*(Nº 538), pp. 4-5. Obtido de https://www.marinha.pt/conteudos_externos/Revista_Armada/2019/538/index.html#p=1
- Morais, V. (2022). O Ecossistema de Cibersegurança em Portugal. [Tese de Mestrado, Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Leiria]. Obtido de https://iconline.ipleiria.pt/bitstream/10400.8/8077/1/O_Ecossistema_Ciberseguranca_em_Portugal.pdf
- Msongaleli, D. L. (2015). *Survivable and Disaster-Resilient Submarine Optical-Fiber Cable Deployment*. Sakarya University- Institute of Science and Technology.

- NATO. (2009). NATO Military Committee MC 0583 Policy for NATO Concept Development and Experimentation.
- NATO. (2014). *NATO| OTAN*. Obtido em 8 de maio de 2024, de O que é a NATO?: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20180212_171208-What_is_NATO_POR_v1.pdf
- NATO. (2020). Allied Joint Doctrine for Cyberspace Operations. *Allied Joint Publication-3.20 (AJP-3.20), Edition A, Version 1*.
- NATO. (2021). AAP-06 NATO Glossary of Terms and Definitions (English and French) (2021th ed.). *NATO STANDARDIZATION OFFICE (NSO)*.
- Neves, P. (2015). Capacidade de resposta a incidentes de segurança da informação no ciberespaço - Uma abordagem DOTMLPI-I. [Tese de Mestrado, Instituto Superior Técnico]. Obtido de [https://fenix.tecnico.ulisboa.pt/downloadFile/1126295043834849/MestradoSIDC\(PNeves\).pdf](https://fenix.tecnico.ulisboa.pt/downloadFile/1126295043834849/MestradoSIDC(PNeves).pdf)
- Neves, P., & Correia, F. (2016). Resposta a incidentes de segurança da informação: uma abordagem DOTMLPI-I. *CyberLaw*(1). Obtido de <https://comum.rcaap.pt/handle/10400.26/18023>
- NIS Cooperation Group. (2024). *Cybersecurity and resiliency of Europe's communications infrastructures and networks*. Obtido de <https://ec.europa.eu/newsroom/dac/redirection/document/102529>
- Nunes, I. F. (2022). Segurança no Espaço Marítimo Euro-Atlântico. *IDN brief- Oceanos e Segurança dos Espaços Marítimos*, pp. 1-8. Obtido de https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN_Brief_setembro_2022.pdf
- Nunes, P. (2012). A Definição de uma Estratégia Nacional de Cibersegurança. *Cibersegurança. Nação e Defesa*.
- Nunes, P. (2013). Cibersegurança e Estratégia Nacional de Informação: Estruturas de Coordenação Nacional no Ciberespaço. *Conferência, Beja, IV SimSIC*.
- Nunes, P. (2018). Estratégia Nacional de Ciberdefesa. Em *Contributos para uma Estratégia Nacional de Ciberdefesa*. Lisboa: N° 28, IDN.
- OFS Optics. (s.d.). *What is Distributed Acoustic Sensing (DAS)?* Obtido em 23 de maio de 2024, de ofs: <https://www.pfsoptics.com/what-is-distributed-acoustic-sensing-das/>
- Oliveira, V. (2021). *Cibersegurança e Inteligência Artificial*. Nova Information Management School, Instituto Superior de Estatística e Gestão de Informação.
- O'Malley, S. (2019). Assessing Threats to South Korea's Undersea Communications Cable Infrastructure. *The Korean Journal of International Studies*, 17(3), 385-414. doi:10.14731/kjis.2019.12.17.3.385

- Ordem dos Psicólogos Portugueses. (2023). *O Factor Humano na Inteligência Artificial - Recomendações Estratégicas para a Sustentabilidade*. Lisboa.
- Ottis, R., & Lorents, P. (2011). Cyberspace: Definition and implications . *5th European Conference on Information Management and Evaluation (ECIME) 2011*, pp. 267-270.
- Pacheco, M. (2014). A Dimensão dos Espaços Marítimos de Portugal. *Anais do Clube Militar Naval, CXLIV*, 105-121.
- Palanivinayagam, A., Gopal, S., Bhattacharya, S., Anumbe, N., Ibeke, E., & Biamba, C. (2021). An Optimized Machine Learning and Big Data Approach to Crime Detection. *Wireless Communications and Mobile Computing*, 2021. doi:10.1155/2021/5291528
- Person, R., Aoustin, Y., Blandin, J., Marvaldi, J., & Rolin, J.-F. (2006). From bottom landers to observatory networks. *ANNALS OF GEOPHYSICS*, 49(2/3), 581-593.
- Raboin, B. (2011). Corresponding Evolution: International Law and the Emergence of Cyber Warfare. *Journal of the National Association of Administrative Law Judiciary*, 31(Issue 2), 603-668. Obtido de <https://digitalcommons.pepperdine.edu/naalj/vol31/iss2/5>
- Rego, P. (2017). *Terrorismo lone wolf: Uma revisao da literatura*. Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.
- REPÚBLICA PORTUGUESA, MINISTÉRIO DAS FINANÇAS E DA DEFESA NACIONAL - GABINETES DA MINISTRA DE ESTADO E DAS FINANÇAS E DO MINISTRO DA DEFESA NACIONAL. (2013). Despacho n.º 13687/2013, Extinção da Comissão de Coordenação da Execução das Operações à Rentabilização dos Imóveis (LPIM). *Diário da República, II Série n.º 208, 28 de outubro de 2013*, 31976.
- REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA. (1997). Resolução da Assembleia da República n.º 60-B/97 de 14 de outubro, Convenção das Nações Unidas sobre o Direito do Mar e o Acordo Relativo à Aplicação da Parte XI da mesma Convenção. *Diário da República, 1º Suplemento, I-A Série n.º 238, 14 de outubro de 1997*, 5486-(3)-5486-(192).
- REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA. (2008). Lei n.º 49/2008, Aprova a Lei de Organização da Investigação Criminal. *Diário da República, I Série n.º 165, 27 de agosto de 2008*, 6038-6042.
- REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA. (2008). Lei n.º 53/2008, Aprova a Lei de Segurança Interna. *Diário da República, I Série n.º 167, 29 de agosto de 2008*, 6135-6141.
- REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA. (2009). Lei n.º 109/2009, Aprova a Lei do Cibercrime, transpondo para a ordem jurídica interna a Decisão Quadro n.º 2005/222/JAI, relativa a ataques contra sistemas de informação, e adapta o direito interno à Convenção sobre Cibercrime do Conselho

da Europa. *Diário da República, I Série n.º 179, 15 de setembro de 2009*, 6319-6325.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA. (2018). Lei n.º 46/2018 de 13 de agosto, Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016. *Diário da República, I Série n.º 155, 13 de agosto de 2018*, 4031-4037.

REPÚBLICA PORTUGUESA, ASSEMBLEIA DA REPÚBLICA. (2018). Lei n.º 46/2018, Estabelece o regime jurídico da segurança do ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação. *Diário da República n.º 155, I Série de 13 de agosto de 2018*, 4031-4037.

REPÚBLICA PORTUGUESA, MINISTÉRIO DA DEFESA NACIONAL - GABINETE DO MINISTRO. (2013). Despacho n.º 13692/2013, Orientação para a política de Ciberdefesa. *Diário da República, II Série n.º 208, 28 de outubro de 2013*, 31976-31979.

REPÚBLICA PORTUGUESA, MINISTÉRIO DA DEFESA NACIONAL - GABINETE DO MINISTRO. (2013). Despacho n.º 13692/2013, Orientação para a política de Ciberdefesa. *Diário da República, II Série n.º 208, 28 de outubro de 2013*, 31976-31979.

REPÚBLICA PORTUGUESA, MINISTÉRIO DA DEFESA NACIONAL - GABINETE DO MINISTRO. (2014). Despacho n.º 11400/2014, Diretiva Ministerial de Planeamento de Defesa Militar. *Diário da República, II Série n.º 175, 11 de setembro de 2014*, 23656-23657.

REPÚBLICA PORTUGUESA, MINISTÉRIO DA DEFESA NACIONAL. (2015). Decreto Regulamentar n.º 10/2015, Aprova a orgânica da Marinha. *Diário da República, I Série n.º 148, 31 de julho de 2015*, 5200-5237.

REPÚBLICA PORTUGUESA, MINISTÉRIO DAS OBRAS PÚBLICAS, TRANSPORTES E COMUNICAÇÕES. (2006). Decreto-Lei n.º 226/2006, Objeto, conceitos e estrutura orgânica. *Diário da República, I Série n.º 220, 15 de novembro de 2006*, 7874-7890.

REPÚBLICA PORTUGUESA, MINISTÉRIO DOS NEGÓCIOS ESTRANGEIROS. (1987). Decreto do Governo n.º 25/87, Aprova para adesão o Protocolo de 1987 relativo à Convenção Internacional para a Prevenção da Poluição por Navios, 1973, feito em Londres em 17 de Fevereiro de 1978. *Diário da República, 1º Suplemento, I Série n.º 156/1987 de 10 de julho de 1987*, 2740-(2)-2740-(115).

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2013). RCM n.º 19/2013 de 5 de abril, Conceito Estratégico de Defesa Nacional. *Diário da República, I Série n.º 67, 05 de abril de 2013*, 1981-1995.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2013). RCM n.º 26/2013 de 19 de abril, Aprova as linhas de orientação para a

execução da reforma estrutural da defesa nacional e das Forças Armadas, designada por Reforma «Defesa 2020». *Diário da República, I Série n.º 77, 19 de abril de 2013*, 2285-2289.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2014). Decreto-Lei n.º 69/2014, Procede à segunda alteração ao Decreto-Lei n.º 3/2012, de 16 de janeiro, que aprova a orgânica do Gabinete Nacional de Segurança, estabelecendo os termos do funcionamento do Centro Nacional de Cibersegurança. *Diário da República, I Série n.º 89, 09 de maio de 2014*, 2712-2719.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2014). RCM n.º 12/2014 de 12 de fevereiro, Adota a Estratégia Nacional para o Mar 2013-2020. *Diário da República, I Série n.º 30, 12 de fevereiro de 2014*, 1310-1336.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2015). RCM n.º 36/2015 de 12 de junho, Aprova a Estratégia Nacional de Segurança do Ciberespaço. *Diário da República, I Série n.º 113, 12 de junho de 2015*, 3738-3742.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2018). Despacho n.º 1195/2018, Regulamento Interno do Conselho Superior de Segurança do Ciberespaço. *Diário da República, II Série, Parte C n.º 24, 2 de fevereiro de 2018*, 3949-3950.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2019). RCM n.º 203-A/2019 de 30 de dezembro, Aprova o Plano de Situação de Ordenamento do Espaço Marítimo Nacional para as subdivisões Continente, Madeira e Plataforma Continental Estendida. *Diário da República, 1º Suplemento, I Série n.º 250, 30 de dezembro de 2019*, 2-391.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2019). RCM n.º 92/2019 de 5 de junho, Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023. *Diário da República, I Série n.º 108, 05 de junho de 2019*, 2888-2895.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2021). RCM n.º 68/2021 de 4 de junho, Aprova a Estratégia Nacional para o Mar 2021-2030. *Diário da República, I Série n.º 108, 04 de junho de 2021*, 23-62.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2022). Decreto-Lei n.º 19/2022, Estabelece a Lei Orgânica do Estado-Maior-General das Forças Armadas e altera as Leis Orgânicas dos três ramos das Forças Armadas. *Diário da República, I Série n.º 16, 24 de janeiro de 2022*, 3-97.

REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2022). Decreto-Lei n.º 20/2022, Aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias. *Diário da República, I Série n.º 20, 28 de janeiro de 2022*, 2-14.

- REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2022). RCM n.º 104/2022 de 2 de novembro, Autoriza a Infraestruturas de Portugal, S. A., a lançar procedimentos pré-contratuais e contratuais necessários à implementação do sistema de cabos submarinos que integram o Atlantic CAM. *Diário da República, I Série n.º 211, 02 de novembro de 2022*, 8-10.
- REPÚBLICA PORTUGUESA, PRESIDÊNCIA DO CONSELHO DE MINISTROS. (2023). Decreto Regulamentar n.º 2/2023, Aprova a estrutura orgânica do Estado-Maior-General das Forças Armadas e altera as estruturas orgânicas da Marinha, do Exército e da Força Aérea. *Diário da República, I Série n.º 109/2023, 06 de junho de 2023*, 3-268.
- Roach, J. A. (2014). Military Cables. Em T. Davenport, T. M. Davenport, & R. C. Beckman (Edits.), *Submarine Cables: The Handbook of Law and Policy* (Vols. Part V- Special Purpose Submarine Cables, pp. 339-350). Leiden (Netherlands): Brill.
- Roh, Y., Heo, G., & Whang, S. (2018). A Survey on Data Collection for Machine Learning: a Big Data - AI Integration Perspective. *IEEE*.
- Rollo, M. F. (2013). Mar de Cabos- Portugal na rede mundial de cabos submarinos. *Ingenium, Revista da Ordem dos Engenheiros*(134), II Série, 92-94. (N. Tomás, Ed.) Lisboa: Ingenium Edições, Lda. Obtido de https://www.academia.edu/49355583/_As_redes_hist%C3%B3ricas_do_cabo_submarino_Um_tempo_pioneiro_na_hist%C3%B3ria_da_comunica%C3%A7%C3%B5es_um_patrim%C3%B3nio_transnacional_a_preservar_in_O_Tempo_dos_Cabos_Submarinos_na_Ilha_do_Faial_valor_universal_do_pa
- Rose, F. (2017). REMARKS - Emerging Threats: Outer Space, Cyberspace, and Undersea Cables. *Arms Control Association*, 52. Obtido de <https://www.armscontrol.org/act/2017-01/news/remarks-emerging-threats-outer-space-cyberspace-and-undersea-cables>
- Sampford, C., Zifcak, S., & Okur, D. (Edits.). (2015). Rethinking International Law and Justice. *Law, Ethics and Governance Series*, 359.
- Santos, J. (2011). Contributos para uma melhor governação da cibersegurança em Portugal . [Tese de Mestrado, Faculdade de Direito da Universidade Nova de Lisboa]. Obtido de https://run.unl.pt/bitstream/10362/7341/1/Santos_2011.PDF
- Santos, J. (2017). *Cibersegurança - Políticas da União Europeia no geral e em Portugal no particular*. Obtido de https://www.academia.edu/46904475/CIBERSEGURAN%C3%87A_POL%C3%8DTICAS_DA_UNI%C3%83O_EUROPEIA_NO_GERAL_E_EM_PORTUGAL_NO_PARTICULAR
- Santos, L., Bravo, R., & Nunes, P. (2012). Protecção do Ciberespaço: Visão Analítica. Em C. Soares, A. Teixeira, & C. Jacinto (Edits.), *Riscos, Segurança e Sustentabilidade* (pp. 163-176). Edições Salamandra. Obtido de https://comum.rcaap.pt/bitstream/10400.26/3578/1/Artigo_ENRSF_Revisto.pdf

- Santuraki, S. U. (2019). *Armed Non-State Actors and State Failure: Failing International Law or Failure of International Law*. Faculty of Law- University of Maiduguri, Department of Public Law, Nigeria.
- Saraiva, M. (2022). Governação dos Oceanos e Defesa Nacional . *IDN brief- Oceanos e Segurança dos Espaços Marítimos*, 2-3. Obtido de https://www.idn.gov.pt/pt/publicacoes/idnbrief/Documents/2022/IDN_Brief_sete_mbro_2022.pdf
- Sechrist, M. (2010). *Cyberspace in Deep Water: Protecting Undersea Communication Cables*. Harvard Kennedy School of Government.
- Shvets, D. (2017). The experience of the Russian Federation in the legal regulation of submarine cables. *Central and Eastern European Legal Studies*, 1, 163-199.
- Shvets, D. (2020). The International Legal Regime of Submarine Cables: a Global Public Interest Regime. *PhD thesis*.
- SIED. (s.d.). *Quem somos*. Obtido em 24 de maio de 2024, de SIED | Serviço de Informações Estratégicas de Defesa: <https://www.sied.pt/quem-somos/o-sied>
- Silva, J. (2020). *A função do mar no desenvolvimento de Portugal: uma análise estratégica*. Universidade de Lisboa, Instituto Superior de Ciências Sociais e Políticas , Lisboa.
- Singer, P., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. doi:10.1093/wentk/9780199918096.001.0001
- SIRP. (s.d.). *Quem somos*. Obtido em 23 de maio de 2024, de SIRP | Sistema de Informações da República Portuguesa: <https://www.sirp.pt/quem-somos/o-sirp>
- SIS. (s.d.). *Quem somos*. Obtido em 23 de maio de 2024, de SIS | Serviço de Informações de Segurança: <https://www.sis.pt/quem-somos/o-sis>
- Solms, R. v., & Niekerk, J. v. (2013). From information security to cyber security. *Computers & Security*, 38, 97-102. Obtido de <https://www.sciencedirect.com/science/article/pii/S0167404813000801>
- Starosielski, N. (2015). *The Undersea Network*. Duke University Press. doi:<https://doi.org/10.2307/j.ctv11smhj2>
- Stevens, T. (2023). *What is Cybersecurity for?* Bristol University Press.
- Strohmeier, M., Martinovic, I., & Lenders, V. (2020). Securing the Air-Ground Link in Aviation. Em M. Keupp (Ed.), *The Security of Critical Infrastructures: Risk, Resilience and Defense* (pp. 131-154). Springer. doi:doi.org/10.1007/978-3-030-41826-7
- Sunak, R. (2017). Undersea Cables: Indispensable, insecure. *Policy Exchange*. Obtido de <https://policyexchange.org.uk/wp-content/uploads/2017/11/Undersea-Cables.pdf>

- Szyrowski, T., Sharma, S., Kennedy, G., & Sutton, R. (2013). Developments in subsea power and telecommunication cables detection: Part 2 - Electromagnetic detection. *International Journal of the Society for Underwater Technology*, 31(3), 133-143. doi:10.3723/ut.31.133
- TeleGeography. (2023). *TeleGeography*. Obtido de <https://submarine-cable-map-2023.telegeography.com/>
- TeleGeography. (2024). *Submarine Cable Frequently Asked Questions*. Obtido em 3 de julho de 2024, de TeleGeography: <https://www2.telegeography.com/submarine-cable-faqs-frequently-asked-questions>
- TeleGeography. (2024). *Submarine Cable Map 2024*. Obtido em 5 de março de 2024, de TeleGeography: <https://submarine-cable-map-2024.telegeography.com/>
- Thomas, R., Rapp, R., Spalding, M., Stix, R., Kordahi, M., & Bergano, N. (2015). Technology in Undersea Cable Systems: 50 Years of Progress. *Marine Technology Society Journal*, 49(6), 88-109. doi:<https://doi.org/10.4031/MTSJ.49.6.4>
- UN General Assembly. (1992). Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation. 1678(29004), pp. 222-234. Obtido em 27 de julho de 2024, de <https://www.refworld.org/legal/agreements/unga/1988/en/28361>
- União Europeia. (2009). *Relatório sobre a Execução da Estratégia Europeia de Segurança*. Bruxelas: Conselho da União Europeia. Obtido de <https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf>
- UNIÃO EUROPEIA, COMISSÃO EUROPEIA. (2017). Recomendação (UE) 2017/1584, sobre a resposta coordenada a incidentes e crises de cibersegurança em grande escala. *Jornal Oficial da União Europeia*, n.º L 239, 13 de setembro de 2017, 36-58.
- UNIÃO EUROPEIA, COMISSÃO EUROPEIA. (2024). Recomendação (UE) 2024/779 da Comissão de 26 de fevereiro de 2024 sobre infraestruturas de cabos submarinos seguras e resilientes. *Recomendação (UE)*, JO L, 2024/779, 08 de março de 2024. Obtido de <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32024H0779>
- UNIÃO EUROPEIA, CONSELHO DA UNIÃO EUROPEIA. (2024). Recomendação do Conselho de 25 de junho sobre um plano de ação para a coordenação da resposta a nível da União a perturbações em infraestruturas críticas com importante relevância transfronteiriça. *Recomendação do Conselho*, JO C, C/2024/4371, 05 de julho de 2024. Obtido de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=OJ:C_202404371
- UNIÃO EUROPEIA, CONSELHO DA UNIÃO EUROPEIA. (2019). Regulamento (UE) 2019/796, relativo a medidas restritivas contra os ciberataques que constituem uma ameaça para União ou os seus Estados-Membros. *Jornal Oficial da União Europeia*, n.º L 129, 17 de maio de 2019, 1-12.

- UNIÃO EUROPEIA, PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. (2004). Regulamento (CE) n.º 725/2004, Relativo ao reforço da protecção dos navios e das instalações portuárias. *Jornal Oficial da União Europeia*, n.º L 129, 31 de março de 2004, 6-91.
- UNIÃO EUROPEIA, PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. (2016). Regulamento (UE) n.º 679/2016, Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, n.º L 119, 27 de abril de 2016, 1-88.
- UNIÃO EUROPEIA, PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. (2019). Regulamento (UE) 2019/881, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança). *Jornal Oficial da União Europeia*, n.º L 151, 17 de abril de 2019, 15-69.
- UNIÃO EUROPEIA, PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. (2022). DIRETIVA (UE) 2022/2555, Relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2). *Jornal Oficial da União Europeia*, n.º L 333, 14 de dezembro de 2022, 80-152.
- Vichi, L., Pinto, D., & Sá, A. (2020). A Defesa da Infraestrutura de Cabos Submarinos: por uma interface entre a defesa cibernética e a segurança marítima no Brasil. *Revista da Escola de Guerra Naval*, 26, 326-346. doi:10.21544/1809-3191.v26n2.p326-346
- Vilela, J. (2015). O Cabo Submarino num Mar de Conectividades | The Submarine Cable in a Sea of Connectivity. DNA Solutions.
- Vilela, J. (2016). *Datas e Factos do Cabo Submarino em Portugal (1855-2015)*. FPC. Obtido de <https://www.fpc.pt/wp-content/uploads/2017/03/Datas-e-Factos-do-Cabo-Sub-em-Portugal.pdf>
- Weiss, M., & Jankauskas, V. (2019). Securing cyberspace: How states design governance arrangements. (C. Wescott, Ed.) *Governance- An International Journal of Policy, Administration, and Institutions*, 32(2), 259-275. doi:10.1111/gove.12368
- Williams, L., McGraw, G., & Migueis, S. (2018). Engineering Security Vulnerability Prevention, Detection, and Response. *IEEE Software*, 35(5), pp. 76-80. doi:10.1109/MS.2018.290110854
- Wolff, J. (2021). How Is Technology Changing the World, and How Should the World Change Technology? *Global Perspectives*, 2, Issue 1.
- Wopschall, R. (2017). The Outer Side of Communication: Guardians of Global Connectivity. *The Fletcher Forum of World Affairs*, 41(Issue 1), 49-58.

Ye, Y.-C., Jiang, X., Pan, G., & Jiang, W. (2018). Installation of the Submarine Optical Cable. (Y.-C. Ye, X. Jiang, G. Pan, & W. Jiang, Edits.) *Submarine Optical Cable Engineering*, 161-193.

Apêndices

Apêndice A- Ficheiros transferidos do *software* DAS da *AP Sensing*

Relativamente à frequência escolhida para o estudo, os 800Hz, foram obtidos em formato .HDF5, os seguintes ficheiros através do *software* da *AP Sensing*, discriminados pelos Testes A e B.

Testes A: para a posição 1: “0000006408_2024-04-16_11.11.28.83808.hdf5”

Testes A: para a posição 2: “0000006450_2024-04-16_12.18.02.15034.hdf5”

Testes B: para a posição 1: “0000006527_2024-04-30_12.12.13.31888.hdf5”

Testes B: para a posição 2: “0000006553_2024-04-30_13.25.50.24653.hdf5”

Estes ficheiros foram fundamentais para o estudo do projeto, uma vez que foi através destes que se conseguiu obter os objetos de estudo apresentados ao longo do capítulo 5, através da linguagem de programação *python*.

Apêndice B- Código em linguagem de programação *python* utilizado

Os gráficos que têm como título “FBE Data”, foram obtidos através do código em linguagem *python*. Mais precisamente, uma vez que apenas se restringiu às posições em estudo, já abordadas, a distância que corresponde ao DAS, pois, os dados analisados no *python*, vieram do DAS, como referido no Apêndice anterior), foram as posições 839, 840, 841, 842 e 843, ou seja, corresponde aos 5 m do estudo no tanque. Estas posições correspondem no código a uma matriz que tem como título “Data_2T_Red”, sendo uma matriz (1200, 5) que corresponde aos dados reduzidos obtidos nestas cinco posições, para as mil e duzentas linhas de dados, que corresponde ao tempo.

Segue-se o código que foi utilizado, obtido no *python*, devidamente comentado.

```
# Para se obter o FBE Data

# Importação de Bibliotecas

import matplotlib.pyplot as plt # Biblioteca usada para criar gráficos e visualizá-los
import numpy as np # Biblioteca usada para as operações numéricas e manipular arrays
from apensing_dasfiles import Loader, DataRequest, index, meter #Específico para trabalhar com arquivos DAS
from scipy.io.wavfile import write, read # Bibliotecas que trabalha arquivos .WAV e operações científicas
from scipy import io

# Definição da diretoria e para carregar os arquivos
DirFicheiros = "C:\\FIBERSENSE\\"
file_path = DirFicheiros + "0000006408_2024-04-16_11.11.28.83808.hdf5"
das_loader = Loader.from_file( file_path )

# Usa a Transformada e serve para carregar e processar os dados
Data = das_loader.data.T #Define Array com os dados em bruto

#Seleção e transposição dos dados
Index = 5 #define a camada de dados que será selecionada (FBE1=0; FBE2=1; FBE3=2; FBE4=3; FBE5=4; FBE6=5)

Data_2 = Data[Index,:,:] # Obtenho o tipo relacionado com a camada de dados
Data_2T = np.transpose(Data_2) # Função transposta do Data_2T para reorganizar os dados

# Função usada para criar um heatmap para um array de 2D
def heatmap2d(arr: np.ndarray):
    plt.imshow(arr, cmap='jet', aspect="auto") # Faz o plot do array como uma imagem com o colormap "jet"
    plt.colorbar() # Adiciona uma barra de cores ao gráfico
    plt.xlabel("Position [m]") # Dá o nome ao eixo x
    plt.ylabel("Time [s]") # Dá o nome ao eixo y
    plt.title("FBE Data") # Dá o título do gráfico
    plt.show() # Mostra o gráfico

heatmap2d(Data_2T) # all scope # Chama a função "heatmap2d" para fazer o plot do heatmap 'Data_2T'

# Reduz os dados pretendidos
SP = 839 # Ponto inicial
EP = 844 # Ponto final
Data_2T_Red = Data_2T[:,SP:EP] # Seleciona um array reduzido entre os dados SP e EP
heatmap2d(Data_2T_Red) # Obtém-se o gráfico
```

O ficheiro que está presente no “file_path” é correspondente ao Teste A para a posição 1, como se pode observar no Apêndice A.

Apêndice C- Tabela do *Excel* relativa aos Testes A, posição 1

Esta tabela foi obtida do *python* e copiada para o *Excel*. No *Excel* procedeu a algumas alterações de cor para uma melhor percepção. Possui cinco colunas correspondente às cinco posições e mil e duzentos linhas correspondentes ao tempo.

Devido ao elevado número de páginas que ocupa, será apresentada apenas esta como exemplo.

839	840	841	842	843
-53,5967	-54,0072	-55,2406	-56,7156	-57,2626
-52,2687	-47,6669	-45,5275	-44,4159	-44,5764
-57,4825	-57,2138	-51,1982	-47,5184	-45,5161
-58,3879	-52,6493	-49,3419	-47,0589	-45,8998
-51,986	-59,2706	-63,4723	-53,2727	-49,408
-55,6378	-58,8406	-56,4669	-52,1306	-49,2294
-49,4932	-51,8613	-54,3062	-52,2412	-48,5757
-50,6097	-52,7172	-57,0807	-56,1385	-50,6241
-58,0738	-55,3806	-53,4206	-51,2665	-49,1834
-55,6897	-62,8587	-58,9835	-54,1264	-52,365
-51,6088	-59,7742	-57,6557	-50,9031	-48,3187
-54,1195	-53,0618	-49,9405	-46,7287	-44,7213
-54,154	-58,3762	-64,3313	-60,8308	-56,8899
-48,9164	-53,4397	-59,5522	-54,8866	-50,2749
-59,3808	-66,5024	-61,5484	-53,2125	-49,2668
-62,5493	-66,6698	-60,4675	-54,1881	-51,0833
-50,4761	-56,0089	-59,9522	-50,7049	-46,731
-58,7416	-58,5758	-58,8129	-57,6654	-55,1813
-57,0625	-55,6115	-53,4675	-51,1147	-49,7811
-60,3077	-62,4838	-68,7032	-65,7392	-58,4255
-53,4149	-55,3854	-59,7451	-57,7838	-52,6001
-51,6826	-52,5982	-53,5116	-51,9497	-49,8653
-51,5246	-52,6382	-53,6598	-53,1236	-52,0144
-60,114	-58,9058	-54,843	-50,0391	-47,1717
-55,8104	-62,0261	-62,3361	-51,5069	-48,0213
-54,972	-59,595	-56,6809	-48,9223	-45,8747
-51,6412	-53,629	-57,9483	-59,6987	-58,2161
-49,7344	-53,6855	-69,4023	-54,087	-50,2167
-50,4908	-52,7341	-55,8782	-54,5938	-53,1117
-47,2309	-52,5877	-60,1881	-49,9198	-47,6732
-50,1549	-59,1564	-57,2969	-51,2747	-51,5117
-52,1046	-55,2224	-51,7873	-46,2078	-43,6245

-64,6734	-55,6495	-49,0747	-46,3551	-46,1301
-54,5227	-50,3603	-47,0704	-45,9295	-46,7993
-59,7494	-54,2908	-51,1038	-50,6731	-53,0315
-59,0538	-51,4616	-47,5007	-45,6648	-45,4896
-57,5661	-60,1366	-57,0921	-54,4048	-54,2043
-57,5403	-55,348	-52,9195	-51,5644	-52,0403
-48,3625	-44,8658	-42,8022	-41,3792	-40,8176
-59,6927	-54,6096	-51,0943	-49,5789	-50,7415
-55,4634	-48,5591	-44,7269	-42,4175	-41,7224
-56,0638	-50,1279	-46,2003	-44,0439	-43,6674
-59,5262	-53,3661	-49,6543	-48,1617	-48,8978
-55,8625	-50,9005	-47,2303	-45,7135	-46,7188
-55,5788	-60,6408	-49,945	-46,3924	-46,0228
-60,1043	-56,0162	-48,883	-46,0913	-45,5689
-46,3632	-45,3177	-44,2107	-43,2453	-42,6128
-38,2006	-39,8176	-42,0033	-43,003	-40,4018
-35,0728	-34,4589	-33,8433	-33,1094	-32,2938
-33,0818	-32,1164	-31,3952	-30,7341	-29,9733
-31,1498	-30,6627	-30,0855	-29,1504	-27,9835
-30,0032	-29,2349	-28,6823	-28,0333	-27,1086
-29,2279	-28,4329	-27,8777	-27,208	-26,2622
-28,3974	-27,6045	-26,8425	-25,9054	-24,9181
-27,9245	-27,1522	-26,5697	-25,8487	-24,9371
-27,3208	-26,1592	-25,3235	-24,603	-23,952
-27,1464	-25,9526	-25,1013	-24,3853	-23,7225
-27,1763	-26,1129	-25,3058	-24,5509	-23,7902
-27,2527	-26,2325	-25,4014	-24,5779	-23,7543
-27,3295	-26,1979	-25,3092	-24,4961	-23,7092
-26,911	-25,7385	-24,8145	-23,9896	-23,2159
-26,9485	-25,86	-25,007	-24,2438	-23,5106
-26,899	-25,7232	-24,734	-23,8932	-23,1696
-27,0437	-25,8724	-24,8944	-24,0618	-23,2961
-26,8806	-25,436	-24,4242	-23,7058	-23,1387
-27,0326	-25,6915	-24,7601	-24,0494	-23,3815
-27,2306	-25,7862	-24,6255	-23,7843	-23,1767
-27,1302	-26,0055	-25,1115	-24,3176	-23,5545
-27,1278	-26,0746	-25,2674	-24,4935	-23,6779
-27,2633	-25,5047	-24,1892	-23,3551	-22,8289
-27,4328	-25,702	-24,3816	-23,5116	-22,9481
-28,1608	-26,5498	-25,2071	-24,1632	-23,3398
-27,7577	-26,2687	-24,9306	-23,8466	-23,0555
-28,0061	-26,6986	-25,4769	-24,3434	-23,372
-28,1669	-26,8183	-25,5433	-24,3883	-23,4652
-28,0939	-26,9331	-25,7278	-24,5212	-23,4643
-27,8073	-26,7275	-25,5355	-24,3039	-23,2988
-28,2536	-27,1561	-25,9883	-24,7565	-23,5861

-27,9011	-26,8579	-25,7709	-24,6573	-23,6133
-27,7056	-26,8074	-25,7702	-24,5716	-23,4792
-28,1779	-27,0011	-25,84	-24,6769	-23,5768
-28,1588	-27,0124	-25,7295	-24,3802	-23,2245
-27,4834	-26,6219	-25,6861	-24,6163	-23,5281
-27,6124	-26,699	-25,6707	-24,4653	-23,2716
-27,6997	-26,6413	-25,585	-24,4369	-23,3642
-27,3001	-26,4295	-25,465	-24,3019	-23,1709
-27,2773	-26,282	-25,2831	-24,1833	-23,1541
-27,0335	-26,1709	-25,3208	-24,3587	-23,3523
-26,8704	-26,0909	-25,3618	-24,496	-23,5553
-26,7184	-25,9899	-25,253	-24,306	-23,3181
-26,7305	-25,994	-25,3299	-24,5668	-23,78
-26,558	-25,9059	-25,2454	-24,3445	-23,3428
-26,6226	-25,9314	-25,2849	-24,4974	-23,634
-26,4298	-25,7678	-25,1089	-24,2462	-23,3434
-26,4756	-25,8002	-25,1663	-24,3854	-23,5382
-26,5222	-25,8159	-25,1401	-24,3483	-23,5416
-26,6183	-25,9368	-25,2536	-24,4148	-23,5295
-26,4655	-25,7758	-25,0603	-24,1609	-23,2612
-26,5245	-25,9404	-25,3197	-24,4872	-23,6289
-26,3475	-25,7008	-25,0246	-24,1597	-23,3058
-26,5592	-25,9284	-25,3495	-24,67	-23,9235
-26,6207	-25,892	-25,141	-24,1831	-23,1735
-26,536	-25,7996	-25,1017	-24,3482	-23,6605
-26,5707	-25,8029	-25,0295	-24,1093	-23,2041
-26,7361	-25,9746	-25,2543	-24,4786	-23,7143
-26,7022	-25,9159	-25,152	-24,3247	-23,5319
-26,5587	-25,8358	-25,1204	-24,2872	-23,4325
-26,4412	-25,6418	-24,8637	-24,0396	-23,3029
-26,6317	-25,8095	-24,9984	-24,1361	-23,3621
-26,488	-25,6568	-24,8405	-23,9832	-23,2127
-26,5862	-25,7631	-24,9667	-24,1257	-23,3687
-26,3112	-25,5461	-24,8518	-24,1654	-23,5347
-26,3852	-25,5176	-24,6914	-23,8808	-23,228
-26,311	-25,4715	-24,7402	-24,108	-23,653
-26,3475	-25,4977	-24,7134	-23,9315	-23,2334
-26,7053	-25,714	-24,7911	-23,9072	-23,2422
-26,4179	-25,5257	-24,724	-23,9683	-23,3444
-26,0453	-25,2462	-24,5703	-24,001	-23,5687
-25,9579	-25,1384	-24,4496	-23,8721	-23,4523
-26,5314	-25,5282	-24,6587	-23,9079	-23,4103
-26,2035	-25,3354	-24,6167	-24,0499	-23,6881
-26,6709	-25,6327	-24,7294	-23,9308	-23,3814
-27,2004	-26,0351	-24,9961	-24,0475	-23,307
-26,7194	-25,6844	-24,7734	-23,9832	-23,4088

-26,9803	-25,8594	-24,8851	-24,0524	-23,4696
-26,4795	-25,4225	-24,5243	-23,8077	-23,4086
-26,769	-25,7888	-24,9712	-24,3577	-24,0069
-26,4466	-25,3697	-24,4348	-23,6393	-23,1698
-26,7926	-25,7211	-24,8054	-24,0623	-23,609
-26,8874	-25,7692	-24,7653	-23,8658	-23,21
-26,439	-25,5037	-24,7445	-24,1921	-23,908
-26,3566	-25,3791	-24,5808	-23,9862	-23,7026
-26,5916	-25,6442	-24,8509	-24,2175	-23,797
-26,7727	-25,7617	-24,9215	-24,2332	-23,7116
-26,5884	-25,4352	-24,4831	-23,7088	-23,2887
-26,6915	-25,6025	-24,7311	-24,0903	-23,7572
-26,5549	-25,4799	-24,6282	-23,9772	-23,5569
-26,6343	-25,4955	-24,5781	-23,8765	-23,5159
-26,7703	-25,616	-24,7129	-24,0403	-23,6572
-26,7231	-25,507	-24,5225	-23,7384	-23,2731
-26,8923	-25,6011	-24,5748	-23,7756	-23,3276
-26,631	-25,3881	-24,4212	-23,71	-23,3779
-26,6484	-25,3975	-24,4549	-23,7923	-23,4882
-26,5478	-25,3751	-24,5315	-23,9653	-23,6898
-26,5347	-25,3494	-24,4801	-23,8619	-23,5001
-26,4938	-25,2811	-24,4112	-23,7996	-23,5249
-26,923	-25,6434	-24,7156	-24,0672	-23,7656
-26,5919	-25,3703	-24,5555	-24,0658	-23,8871
-26,8395	-25,5477	-24,6698	-24,1332	-23,9809
-26,6871	-25,4109	-24,5197	-23,8806	-23,5115
-26,3851	-25,0684	-24,1691	-23,5313	-23,1886
-26,5399	-25,2084	-24,3292	-23,7318	-23,4144
-26,6527	-25,2759	-24,412	-23,8878	-23,6789
-26,7124	-25,2913	-24,4102	-23,8831	-23,6425
-26,2263	-24,8076	-23,9564	-23,4688	-23,3124
-26,4062	-24,9008	-23,9976	-23,4302	-23,179
-26,5842	-25,0747	-24,2045	-23,727	-23,58
-26,2174	-24,7808	-23,9758	-23,532	-23,3662
-26,3396	-24,8162	-23,9934	-23,5252	-23,3474
-26,3496	-24,8558	-24,0849	-23,7213	-23,6544
-26,2485	-24,7486	-24,0069	-23,6636	-23,6263
-26,247	-24,7941	-24,0771	-23,7569	-23,733
-26,2266	-24,7004	-23,9727	-23,6363	-23,5782
-26,6893	-25,0345	-24,2276	-23,8645	-23,7942
-26,4937	-24,8517	-24,0581	-23,6884	-23,6181
-26,5353	-24,8883	-24,113	-23,7567	-23,6728
-36,4423	-34,9874	-34,4876	-34,2287	-34,1037
-51,9267	-50,4934	-50,083	-49,7609	-49,3257
-58,6927	-60,4676	-62,9255	-67,6284	-73,4476
-51,418	-53,1539	-55,4976	-57,4789	-58,1033

-58,76	-60,4828	-63,3899	-65,1888	-64,0733
-58,9323	-62,4455	-58,563	-56,5681	-56,6449
-57,6931	-58,2389	-59,3624	-60,3991	-61,478
-49,9744	-52,0697	-55,867	-59,8329	-62,1638
-52,2093	-52,1709	-53,0444	-53,8596	-54,1613
-49,2622	-50,0481	-51,1903	-51,9521	-52,2019
-52,114	-52,0821	-51,5141	-50,64	-50,3068
-48,7656	-50,8805	-54,2173	-56,0707	-55,83
-52,7354	-55,0223	-55,7628	-54,8314	-53,9839
-48,2297	-49,5495	-51,2461	-52,5469	-53,5037
-50,0371	-51,7019	-54,174	-53,9455	-52,1593
-49,1637	-50,1027	-51,0036	-50,4124	-49,6475
-55,1609	-57,7261	-64,3741	-60,9826	-55,8478
-48,0409	-48,4165	-48,9003	-48,2809	-47,5646
-56,3923	-55,7196	-55,3851	-55,2828	-55,5836
-52,1404	-52,737	-53,1764	-51,8899	-50,4327
-51,5672	-52,1418	-53,5276	-54,8305	-56,2847
-48,8251	-49,0633	-49,815	-50,4606	-51,4721
-60,7088	-60,0754	-57,2105	-54,0101	-52,6148
-56,0045	-55,8288	-54,6855	-53,1309	-52,4081
-50,5074	-54,5921	-60,778	-54,6073	-50,6851
-45,5042	-48,1753	-52,6713	-55,5578	-52,7162
-53,5068	-56,3568	-58,4744	-57,842	-56,2071
-54,504	-57,0263	-58,7352	-55,9156	-53,7996
-47,7592	-51,614	-59,2175	-54,5067	-49,7016
-55,2665	-55,8595	-56,0157	-55,9324	-56,6776
-57,8824	-61,7139	-62,5255	-57,281	-53,9372
-55,1089	-56,1651	-55,7	-54,3838	-53,9164
-50,5426	-51,822	-51,6204	-49,5635	-48,2185
-60,8901	-63,1559	-62,7874	-60,0596	-59,0666
-44,0776	-46,7437	-51,5452	-54,1679	-50,4558
-59,1233	-59,8781	-58,4722	-57,1841	-57,786
-53,6781	-57,5981	-61,7673	-57,705	-54,5992
-46,7583	-49,3947	-55,1467	-67,4538	-54,8381
-49,5756	-50,5467	-52,6638	-56,2951	-62,7005
-56,7491	-57,15	-57,2404	-57,6748	-60,2773
-40,8244	-38,1599	-36,4134	-35,4882	-35,3108
-33,972	-32,0462	-30,6778	-29,7416	-29,0567
-31,0526	-28,9732	-27,5086	-26,4926	-25,7465
-28,2851	-26,3072	-24,9046	-23,9534	-23,2773
-26,34	-24,2683	-22,7901	-21,8064	-21,1702
-25,1117	-22,9889	-21,4778	-20,5026	-19,9003
-23,9701	-21,9316	-20,5011	-19,5628	-18,9473
-23,1556	-21,076	-19,6575	-18,7541	-18,1815
-22,5597	-20,3606	-18,8542	-17,9209	-17,3768
-21,864	-19,7149	-18,2941	-17,4206	-16,904

-21,5296	-19,3344	-17,8984	-17,0377	-16,553
-21,3335	-19,1223	-17,6568	-16,7926	-16,3335
-21,1582	-18,8777	-17,3915	-16,5407	-16,1104
-21,1138	-18,7702	-17,239	-16,3735	-15,9535
-21,0555	-18,7031	-17,1772	-16,3135	-15,8805
-20,5978	-18,3132	-16,8484	-16,0156	-15,5994
-20,6318	-18,3023	-16,8404	-16,0473	-15,6738
-20,2615	-18,0097	-16,625	-15,879	-15,5351
-20,1349	-17,9204	-16,5838	-15,8748	-15,5371
-20,1456	-17,8736	-16,5318	-15,8421	-15,5241
-19,8132	-17,5675	-16,3306	-15,7293	-15,4442
-19,6532	-17,3723	-16,161	-15,6116	-15,3765
-19,768	-17,3326	-16,0539	-15,471	-15,2018
-19,807	-17,4166	-16,1904	-15,6718	-15,4618
-19,8622	-17,4164	-16,1327	-15,5755	-15,3446
-19,8197	-17,3943	-16,1123	-15,5549	-15,3284
-19,8161	-17,3658	-16,0322	-15,4395	-15,216
-19,9368	-17,4687	-16,1092	-15,5131	-15,3165
-20,0393	-17,4564	-16,022	-15,3672	-15,104
-19,9214	-17,3481	-15,9265	-15,2752	-15,0193
-19,9947	-17,4706	-16,0686	-15,4369	-15,2061
-20,1894	-17,5356	-16,0336	-15,3399	-15,0809
-20,2421	-17,597	-16,0739	-15,3677	-15,1093
-20,2531	-17,5469	-15,9973	-15,2762	-15,0077
-20,4448	-17,6519	-16,0472	-15,3054	-15,0433
-20,4071	-17,6818	-16,1022	-15,3727	-15,1195
-20,6841	-17,8541	-16,199	-15,426	-15,1523
-20,526	-17,7714	-16,1129	-15,3175	-15,0355
-20,603	-17,8445	-16,1576	-15,3362	-15,0631
-20,5822	-17,9159	-16,2269	-15,3625	-15,0436
-20,8146	-18,0408	-16,2765	-15,3746	-15,0592
-20,6314	-17,957	-16,2397	-15,3562	-15,0639
-20,8359	-18,1237	-16,3163	-15,3648	-15,038
-20,6832	-18,0104	-16,2193	-15,2622	-14,9425
-20,8326	-18,1554	-16,3155	-15,308	-14,9579
-20,8804	-18,2401	-16,3661	-15,3319	-14,9921
-20,9102	-18,2192	-16,3057	-15,2498	-14,9136
-20,9183	-18,195	-16,2723	-15,2081	-14,8579
-20,9063	-18,3056	-16,4075	-15,3354	-14,9831
-21,0847	-18,3152	-16,3008	-15,1725	-14,8084
-20,8447	-18,2388	-16,3249	-15,2419	-14,8903
-20,7711	-18,2331	-16,3382	-15,2378	-14,8597
-20,6338	-18,2071	-16,3729	-15,2884	-14,903
-20,6862	-18,1281	-16,2278	-15,1318	-14,7697
-20,6997	-18,1772	-16,3063	-15,2198	-14,8546
-20,5325	-18,1325	-16,3199	-15,2453	-14,8722

-20,4646	-18,1455	-16,3771	-15,3064	-14,9206
-20,4555	-18,1084	-16,2926	-15,1946	-14,8171
-20,1758	-18,0287	-16,3237	-15,2439	-14,842
-20,2287	-18,0602	-16,337	-15,2519	-14,8607
-20,011	-17,8902	-16,2002	-15,1238	-14,7333
-19,72	-17,8036	-16,2487	-15,2183	-14,8273
-19,755	-17,8041	-16,2063	-15,143	-14,7447
-19,5189	-17,7592	-16,2717	-15,2374	-14,8334
-19,4453	-17,6955	-16,2095	-15,1703	-14,7651
-19,2889	-17,6017	-16,1632	-15,1347	-14,7094
-19,1259	-17,5424	-16,1603	-15,144	-14,7122
-19,0986	-17,5578	-16,1908	-15,1595	-14,7005
-19,1143	-17,5877	-16,2224	-15,1732	-14,6901
-19,185	-17,6563	-16,2721	-15,1961	-14,6998
-19,0557	-17,5546	-16,1992	-15,1409	-14,6387
-19,0838	-17,5876	-16,2304	-15,1569	-14,6303
-18,9739	-17,5083	-16,1688	-15,0945	-14,5541
-19,2249	-17,6997	-16,2916	-15,1631	-14,5995
-19,2071	-17,6763	-16,2605	-15,126	-14,5594
-19,1862	-17,6935	-16,2955	-15,156	-14,5693
-19,2533	-17,7496	-16,3449	-15,1962	-14,5831
-19,1721	-17,6732	-16,2709	-15,1255	-14,5228
-19,1657	-17,6713	-16,261	-15,1002	-14,486
-19,2029	-17,7247	-16,3285	-15,1685	-14,5272
-19,3772	-17,8322	-16,3634	-15,158	-14,5283
-19,4038	-17,8595	-16,3855	-15,16	-14,473
-19,631	-17,9784	-16,424	-15,1764	-14,5288
-19,555	-17,9294	-16,3907	-15,1464	-14,4785
-19,6395	-17,9498	-16,3519	-15,0764	-14,4084
-19,7466	-18,012	-16,3718	-15,0681	-14,3719
-19,9199	-18,1568	-16,4728	-15,124	-14,3796
-19,8638	-18,0801	-16,3883	-15,0588	-14,37
-20,0509	-18,2186	-16,4756	-15,102	-14,3695
-20,2192	-18,3487	-16,5592	-15,1447	-14,3685
-20,1974	-18,3491	-16,5676	-15,1473	-14,3542
-20,2354	-18,357	-16,5484	-15,1169	-14,3325
-20,324	-18,3987	-16,5399	-15,0706	-14,2544
-20,3245	-18,4154	-16,5746	-15,1139	-14,294
-20,4246	-18,4413	-16,5255	-15,0211	-14,1971
-20,2371	-18,3081	-16,4569	-15,0131	-14,2434
-20,5427	-18,4813	-16,4983	-14,959	-14,1339
-20,5728	-18,5429	-16,5875	-15,056	-14,2043
-20,5854	-18,5545	-16,5888	-15,0599	-14,2262
-20,5678	-18,5409	-16,576	-15,045	-14,2112
-20,8151	-18,6759	-16,6116	-15,0137	-14,1343
-20,7134	-18,6157	-16,5817	-15,016	-14,1778

-20,8008	-18,6766	-16,6098	-15,0066	-14,1213
-20,7398	-18,6303	-16,5816	-15,0029	-14,1453
-20,8777	-18,6865	-16,5684	-14,9499	-14,0788
-20,9617	-18,7531	-16,6163	-14,9872	-14,1092
-20,9846	-18,7542	-16,5993	-14,9651	-14,0891
-21,1506	-18,8388	-16,6136	-14,9334	-14,0229
-21,0874	-18,7812	-16,5739	-14,9128	-14,0167
-20,948	-18,6994	-16,538	-14,909	-14,0346
-21,2515	-18,8605	-16,589	-14,8978	-13,9867
-21,0035	-18,7262	-16,5582	-14,9294	-14,0443
-21,0585	-18,7087	-16,4899	-14,8396	-13,9466
-20,8896	-18,6095	-16,4702	-14,8762	-14,0171
-21,0033	-18,6541	-16,4393	-14,7959	-13,9011
-20,8346	-18,5363	-16,3827	-14,7944	-13,9464
-21,0482	-18,6711	-16,4585	-14,829	-13,9435
-20,9163	-18,6058	-16,449	-14,8496	-13,9755
-20,8918	-18,5877	-16,4297	-14,8306	-13,9524
-20,9825	-18,616	-16,4142	-14,8075	-13,9448
-29,8388	-28,0686	-26,3394	-25,0043	-24,2357
-45,8797	-45,8808	-46,4194	-47,473	-48,963
-57,5512	-58,1264	-58,008	-57,2642	-57,1674
-60,4736	-62,1724	-62,3185	-61,3579	-62,0635
-52,7296	-56,2226	-64,0403	-70,0905	-65,1208
-67,1881	-68,7892	-71,5013	-74,733	-68,8595
-64,2793	-65,8866	-63,4677	-61,9622	-62,1817
-52,9191	-54,9986	-59,1907	-66,0606	-69,5326
-58,8456	-60,3483	-62,5566	-63,6653	-61,8236
-62,6288	-67,252	-66,508	-62,6394	-60,7416
-70,7901	-75,9259	-67,1299	-63,3063	-60,7358
-57,8462	-61,888	-69,648	-66,9113	-61,111
-64,5526	-66,2691	-65,4811	-63,3854	-61,6104
-59,6895	-61,6155	-64,9182	-72,5933	-68,4712
-70,593	-68,9907	-62,6488	-59,7654	-58,9355
-61,4324	-61,6348	-61,243	-61,0907	-61,7166
-71,1624	-66,1417	-60,3508	-57,3105	-55,9478
-65,5143	-72,5607	-68,681	-62,0284	-58,6126
-61,0404	-58,483	-55,9539	-54,7908	-54,9551
-63,0144	-63,7727	-62,5557	-60,3966	-58,6201
-58,7781	-59,7675	-58,7109	-56,463	-54,3532
-67,0189	-64,3707	-61,0519	-59,071	-58,0187
-56,8402	-58,3564	-58,5134	-56,2694	-53,8776
-70,6115	-66,8259	-59,9704	-56,7067	-55,2118
-67,8988	-71,6015	-64,2296	-61,26	-60,2576
-59,524	-65,1018	-67,2378	-59,4865	-55,7915
-60,9362	-60,8661	-59,4789	-57,9617	-56,8852
-63,6606	-66,0135	-60,4829	-56,3012	-53,9256

-56,3958	-58,5109	-62,2418	-66,1101	-65,8538
-65,4129	-59,7793	-55,4243	-52,7069	-51,2027
-67,4155	-65,6725	-62,8312	-59,9143	-57,9587
-68,1519	-64,9823	-60,6208	-57,5033	-55,5448
-58,5458	-59,2695	-59,7236	-59,496	-59,1241
-68,8184	-69,403	-65,5376	-61,8308	-59,7361
-59,7165	-60,6026	-61,8326	-62,3842	-63,1405
-57,7594	-62,3998	-63,2427	-58,4239	-55,5776
-63,831	-68,7617	-65,5622	-61,3343	-59,538
-72,0263	-63,7667	-58,1978	-55,168	-53,6146
-58,6789	-65,2464	-60,9134	-55,5279	-53,2955
-64,9897	-64,3816	-63,4042	-62,8075	-63,2155
-28,4166	-25,7341	-23,6698	-22,308	-21,5704
-21,3736	-18,9608	-17,0359	-15,7211	-14,9723
-18,7418	-16,4969	-14,7477	-13,564	-12,9005
-17,0161	-14,844	-13,1811	-12,0665	-11,4488
-15,9341	-13,8354	-12,2639	-11,2167	-10,6405
-15,0349	-12,9558	-11,4426	-10,4538	-9,92104
-14,4944	-12,3469	-10,8196	-9,8464	-9,33235
-14,1465	-12,0293	-10,5448	-9,60368	-9,11264
-13,744	-11,741	-10,3796	-9,5071	-9,04398
-13,295	-11,4398	-10,2241	-9,41359	-8,96077
-13,0124	-11,264	-10,1357	-9,3663	-8,92896
-13,055	-11,2834	-10,1115	-9,32501	-8,88011
-13,2429	-11,4179	-10,1694	-9,34787	-8,8895
-13,3061	-11,4479	-10,1609	-9,31473	-8,84209
-13,3153	-11,4253	-10,1253	-9,28337	-8,81737
-13,2669	-11,3641	-10,0726	-9,24616	-8,79909
-13,1123	-11,2506	-10,0149	-9,21604	-8,77152
-12,9249	-11,1024	-9,91558	-9,14698	-8,71776
-12,9944	-11,1355	-9,93265	-9,15822	-8,72057
-13,0407	-11,1519	-9,92449	-9,14245	-8,70919
-12,9849	-11,084	-9,8623	-9,09235	-8,67164
-13,1118	-11,1593	-9,90256	-9,11709	-8,69045
-13,0156	-11,0497	-9,78777	-9,0097	-8,59455
-12,9791	-11,0165	-9,76217	-8,99254	-8,58429
-12,9676	-11,0158	-9,78783	-9,03607	-8,63144
-12,9373	-10,9595	-9,73525	-8,99283	-8,59609
-12,8542	-10,8884	-9,68215	-8,95608	-8,57146
-12,8075	-10,8138	-9,61032	-8,89805	-8,52628
-12,8034	-10,7941	-9,57751	-8,86417	-8,49595
-12,872	-10,8206	-9,59127	-8,8798	-8,51734
-12,7999	-10,748	-9,53008	-8,83797	-8,49057
-12,8268	-10,729	-9,49091	-8,79354	-8,44876
-12,7829	-10,671	-9,43107	-8,74133	-8,4055
-12,8333	-10,6738	-9,40632	-8,71285	-8,3797

-12,8901	-10,6974	-9,41451	-8,72701	-8,41004
-13,0485	-10,7631	-9,42094	-8,70985	-8,3821
-13,1026	-10,7618	-9,4028	-8,69963	-8,38532
-13,1177	-10,727	-9,35284	-8,6565	-8,35795
-13,1537	-10,6978	-9,30134	-8,60677	-8,31278
-13,2205	-10,7119	-9,3021	-8,62402	-8,35043
-13,2869	-10,6539	-9,20908	-8,54436	-8,29305
-13,4175	-10,6736	-9,1749	-8,49543	-8,24447
-13,4511	-10,6178	-9,10538	-8,45247	-8,23462
-13,5693	-10,5901	-9,04057	-8,40824	-8,22304
-13,8244	-10,6324	-9,0092	-8,3927	-8,24418
-13,9685	-10,5964	-8,92115	-8,32292	-8,20773
-14,1556	-10,6637	-8,94297	-8,33939	-8,22272
-14,0774	-10,554	-8,84981	-8,28423	-8,20198
-14,1354	-10,5599	-8,84228	-8,27776	-8,20289
-13,8981	-10,4088	-8,75818	-8,23142	-8,17809
-13,836	-10,3613	-8,74194	-8,24332	-8,2068
-13,6921	-10,2897	-8,71364	-8,23098	-8,19338
-13,5823	-10,2628	-8,71713	-8,22816	-8,17686
-13,3454	-10,175	-8,71178	-8,25525	-8,21234
-13,2475	-10,1409	-8,70605	-8,25843	-8,22169
-13,0521	-10,0945	-8,73385	-8,30476	-8,26179
-12,7608	-9,99744	-8,71893	-8,30422	-8,26059
-12,6339	-9,97402	-8,74532	-8,34278	-8,29895
-12,5314	-9,96608	-8,77671	-8,3765	-8,32438
-12,3801	-9,92321	-8,78015	-8,38878	-8,33732
-12,3401	-9,9269	-8,77773	-8,35616	-8,28242
-12,3231	-9,91142	-8,76628	-8,34769	-8,27772
-12,2226	-9,89787	-8,79117	-8,38626	-8,3319
-12,2443	-9,92627	-8,81851	-8,4045	-8,3483
-12,349	-9,94441	-8,79271	-8,36313	-8,30935
-12,3402	-9,92201	-8,76463	-8,33727	-8,2963
-12,3526	-9,92343	-8,77464	-8,36744	-8,34666
-12,1482	-9,80761	-8,71238	-8,34116	-8,33978
-12,1963	-9,81961	-8,69583	-8,31731	-8,31989
-12,2521	-9,86851	-8,72256	-8,34149	-8,35425
-12,3797	-9,94211	-8,76078	-8,37576	-8,39892
-12,3607	-9,90459	-8,68024	-8,25529	-8,25702
-12,4089	-9,93231	-8,69393	-8,27753	-8,2993
-12,5103	-9,96431	-8,66029	-8,21104	-8,22334
-12,7292	-10,0525	-8,68714	-8,22601	-8,24525
-12,8454	-10,1059	-8,72345	-8,28256	-8,33336
-13,0503	-10,1613	-8,71741	-8,26246	-8,31568
-13,1559	-10,228	-8,76694	-8,31475	-8,3772
-13,1763	-10,2248	-8,73598	-8,25508	-8,28608
-13,0059	-10,1996	-8,76981	-8,30727	-8,34553

-12,9006	-10,2151	-8,83656	-8,3854	-8,42251
-12,798	-10,1626	-8,78839	-8,32786	-8,35861
-12,7849	-10,2007	-8,83125	-8,35579	-8,37114
-12,6092	-10,1774	-8,86023	-8,38622	-8,39565
-12,453	-10,19	-8,91164	-8,4219	-8,41394
-12,2908	-10,1831	-8,96336	-8,47497	-8,45609
-12,0749	-10,104	-8,90984	-8,40165	-8,36446
-12,0122	-10,1363	-8,9697	-8,44635	-8,38637
-11,9647	-10,1102	-8,95915	-8,43668	-8,37206
-12,0309	-10,1513	-9,00675	-8,48934	-8,42353
-12,0829	-10,1611	-9,02596	-8,52341	-8,46301
-12,1699	-10,1315	-8,96411	-8,46187	-8,40788
-12,289	-10,163	-8,98346	-8,50212	-8,4686
-12,2971	-10,0613	-8,87086	-8,40461	-8,37504
-12,4019	-10,0431	-8,84061	-8,39935	-8,38256
-12,4091	-9,99973	-8,80585	-8,38987	-8,38778
-12,5365	-10,1009	-8,85314	-8,39808	-8,38542
-12,6024	-10,1784	-8,90704	-8,43549	-8,42641
-12,6399	-10,1993	-8,87543	-8,36377	-8,34252
-12,9003	-10,3995	-9,01171	-8,45454	-8,41128
-12,8887	-10,415	-9,00714	-8,42054	-8,36029
-12,8733	-10,4165	-9,00527	-8,41155	-8,35238
-12,8794	-10,4323	-9,03625	-8,45142	-8,39446
-12,8855	-10,3942	-8,9817	-8,3958	-8,34584
-12,8889	-10,3813	-8,99083	-8,43044	-8,38995
-12,8068	-10,2823	-8,90944	-8,37411	-8,35129
-12,8281	-10,2462	-8,8685	-8,33487	-8,30869
-12,5976	-10,0773	-8,78326	-8,32489	-8,35225
-12,6523	-10,0595	-8,77182	-8,32661	-8,34234
-12,5979	-9,95594	-8,6796	-8,26013	-8,29231
-12,4161	-9,82672	-8,62424	-8,25557	-8,30232
-12,4241	-9,85178	-8,63946	-8,2572	-8,29743
-12,4435	-9,90531	-8,65148	-8,21653	-8,22475
-12,5009	-9,99541	-8,72441	-8,26705	-8,26822
-12,5598	-10,1036	-8,7718	-8,25169	-8,22186
-12,7242	-10,2627	-8,85788	-8,27738	-8,22267
-12,7753	-10,3466	-8,91155	-8,2994	-8,23295
-12,8257	-10,4044	-8,93802	-8,29578	-8,21343
-12,5528	-10,3033	-8,93973	-8,33733	-8,26904
-12,1763	-10,1301	-8,87802	-8,29248	-8,20261
-20,6136	-19,1257	-18,305	-17,9168	-17,8477
-42,6383	-42,4054	-42,3877	-42,6293	-43,3549
-59,5315	-56,9284	-53,586	-51,4417	-50,7118
-54,5382	-58,0802	-67,7232	-61,2984	-56,9725
-61,4099	-61,3727	-61,4562	-61,8586	-63,9461
-61,2105	-63,0869	-61,9902	-57,9153	-54,9161

-62,9502	-66,3678	-61,1239	-56,0259	-53,0622
-62,304	-62,0387	-62,9319	-63,0625	-61,5276
-54,9388	-56,169	-60,1969	-66,8505	-65,3388
-58,1209	-59,9506	-61,6302	-57,0969	-53,334
-59,9965	-58,6306	-57,7316	-57,1611	-56,9773
-64,4533	-62,1649	-58,2126	-55,029	-53,1675
-60,5787	-63,2436	-62,8128	-59,5492	-57,5658
-58,6858	-63,9838	-63,7564	-57,9294	-55,5972
-58,7415	-62,6968	-63,4871	-57,612	-55,4619
-54,8052	-58,3378	-72,5723	-59,3131	-55,8933
-55,351	-57,9496	-59,0965	-53,9034	-51,6461
-54,1487	-54,5473	-56,2747	-56,6728	-56,6454
-61,2613	-61,662	-59,2323	-56,8922	-56,2601
-58,0759	-57,0624	-52,7096	-49,938	-49,3425
-65,273	-71,7799	-69,5855	-66,0168	-64,8701
-69,323	-71,703	-64,2134	-61,8669	-60,3456
-56,9885	-62,1444	-67,2302	-61,0475	-58,9293
-51,714	-54,5768	-58,6083	-59,4218	-58,3977
-49,887	-51,5286	-55,101	-60,9333	-66,4647
-61,6208	-66,1026	-66,0272	-62,8764	-62,0137
-68,2363	-66,4883	-62,0129	-58,6294	-57,4528
-57,8973	-54,7727	-53,6656	-53,4795	-53,9369
-67,4778	-66,3808	-61,4595	-59,4436	-59,365
-64,3134	-60,5457	-57,4138	-57,062	-58,2707
-64,188	-65,1284	-62,2855	-58,9505	-58,4284
-56,1262	-54,6472	-54,7054	-56,4793	-59,3058
-60,514	-66,488	-67,1924	-60,6415	-58,8651
-65,8003	-58,3213	-53,5058	-51,5354	-51,8901
-64,5233	-57,4737	-53,8631	-52,7158	-53,6089
-58,7355	-55,643	-53,5158	-52,6674	-52,9465
-69,8236	-62,5118	-57,2667	-55,227	-55,0714
-55,4247	-54,3448	-54,9162	-57,2431	-61,4726
-67,8347	-59,2535	-54,9385	-53,1187	-52,9844
-55,2111	-50,1337	-47,607	-47,1518	-48,307
-20,613	-17,9191	-16,2073	-15,2762	-14,8917
-13,3755	-10,8306	-9,23577	-8,37522	-8,02645
-11,8447	-9,39595	-7,91092	-7,13144	-6,82902
-11,5687	-9,18568	-7,76919	-7,03638	-6,76095
-11,3113	-8,9317	-7,51052	-6,7629	-6,47549
-10,9338	-8,56245	-7,1723	-6,45407	-6,18431
-10,7631	-8,39234	-7,01321	-6,30841	-6,05056
-10,6664	-8,32169	-6,95362	-6,25031	-5,99298
-10,7766	-8,39543	-6,99877	-6,27955	-6,01466
-10,7501	-8,39953	-7,01553	-6,3002	-6,03764
-10,7351	-8,34684	-6,94924	-6,23295	-5,97381
-10,6657	-8,27229	-6,88051	-6,17352	-5,92029

-10,6222	-8,24739	-6,86916	-6,16933	-5,92204
-10,5884	-8,20952	-6,836	-6,14435	-5,89996
-10,6173	-8,227	-6,83792	-6,12961	-5,87171
-10,5951	-8,25082	-6,87538	-6,16592	-5,90876
-10,5616	-8,21816	-6,83806	-6,12322	-5,86426
-10,596	-8,22182	-6,81539	-6,08309	-5,81212
-10,5744	-8,22719	-6,83076	-6,10284	-5,83653
-10,5887	-8,23078	-6,82306	-6,0976	-5,8411
-10,6166	-8,23902	-6,81131	-6,06279	-5,78769
-10,5403	-8,19481	-6,77821	-6,02667	-5,74776
-10,6416	-8,27763	-6,83225	-6,05921	-5,76976
-10,6335	-8,27129	-6,83128	-6,06861	-5,78965
-10,5987	-8,25089	-6,81566	-6,0457	-5,75587
-10,6707	-8,30841	-6,84865	-6,06562	-5,77358
-10,6465	-8,27198	-6,78953	-5,99154	-5,69538
-10,5359	-8,2166	-6,76538	-5,97779	-5,68642
-10,567	-8,24985	-6,8076	-6,02302	-5,72655
-10,5908	-8,28024	-6,82716	-6,02645	-5,72045
-10,4825	-8,21859	-6,79881	-6,01133	-5,70758
-10,4422	-8,21261	-6,81946	-6,04174	-5,73907
-10,3174	-8,10908	-6,72836	-5,94829	-5,63894
-10,2728	-8,09374	-6,73338	-5,9594	-5,64947
-10,2349	-8,07295	-6,70895	-5,9319	-5,62251
-10,4196	-8,19267	-6,75376	-5,93772	-5,6161
-10,5313	-8,25823	-6,76298	-5,91909	-5,58965
-10,727	-8,38518	-6,80674	-5,92337	-5,58701
-10,8768	-8,47847	-6,82254	-5,89551	-5,54471
-11,1068	-8,62049	-6,8787	-5,90572	-5,53946
-11,1701	-8,66529	-6,89149	-5,90726	-5,54547
-11,2426	-8,69301	-6,8716	-5,86366	-5,49459
-11,3746	-8,77628	-6,90719	-5,87361	-5,49415
-11,5461	-8,8912	-6,97772	-5,93015	-5,55085
-11,4985	-8,83685	-6,90375	-5,8485	-5,46976
-11,4307	-8,77569	-6,84909	-5,80802	-5,44634
-11,1965	-8,7146	-6,86663	-5,84099	-5,46838
-11,0228	-8,60879	-6,8033	-5,79706	-5,43211
-10,7558	-8,48393	-6,72926	-5,73105	-5,36956
-10,5175	-8,42448	-6,75514	-5,7767	-5,41001
-10,3802	-8,3826	-6,74783	-5,77607	-5,41214
-10,361	-8,43441	-6,8072	-5,82295	-5,44844
-10,2732	-8,38871	-6,77187	-5,78603	-5,40867
-10,3112	-8,39777	-6,77473	-5,78856	-5,40989
-10,5416	-8,47794	-6,78693	-5,77905	-5,39149
-10,7034	-8,51612	-6,76752	-5,74247	-5,35074
-10,8819	-8,62068	-6,83572	-5,79965	-5,40345
-11,0399	-8,66435	-6,82262	-5,77008	-5,37074

-10,9781	-8,59694	-6,76963	-5,73352	-5,34473
-11,1188	-8,61809	-6,75401	-5,71688	-5,32954
-11,1658	-8,59041	-6,71836	-5,69687	-5,32527
-11,2299	-8,65177	-6,7639	-5,72327	-5,33332
-11,1967	-8,55697	-6,66614	-5,64537	-5,27415
-11,1589	-8,46656	-6,60659	-5,62891	-5,28149
-11,1395	-8,40901	-6,5774	-5,63275	-5,29879
-11,1066	-8,33111	-6,52032	-5,59622	-5,26184
-10,9757	-8,23761	-6,50029	-5,62551	-5,30536
-10,9272	-8,14001	-6,41168	-5,55751	-5,24684
-11,0312	-8,17912	-6,40783	-5,53562	-5,22087
-11,0523	-8,14602	-6,37872	-5,5295	-5,2295
-11,0577	-8,14853	-6,36446	-5,50431	-5,20326
-11,0486	-8,16407	-6,37446	-5,50763	-5,20745
-11,2005	-8,30243	-6,47746	-5,57317	-5,24337
-11,1091	-8,25168	-6,45265	-5,5625	-5,24034
-11,1173	-8,22764	-6,42923	-5,54865	-5,23239
-11,0313	-8,14087	-6,35414	-5,49372	-5,19659
-10,924	-8,07151	-6,31204	-5,46241	-5,16708
-10,9758	-8,06398	-6,29504	-5,45539	-5,17037
-10,9578	-8,04844	-6,28065	-5,43855	-5,15023
-10,9011	-7,99726	-6,24543	-5,41759	-5,13744
-10,9395	-7,972	-6,19602	-5,3688	-5,09706
-10,8236	-7,97535	-6,22917	-5,39271	-5,1054
-10,7956	-7,94609	-6,2083	-5,38024	-5,09838
-10,7658	-7,9677	-6,23284	-5,3919	-5,10072
-10,9093	-8,06676	-6,24572	-5,34783	-5,04355
-10,9722	-8,15183	-6,29668	-5,36966	-5,05612
-10,9467	-8,2144	-6,37332	-5,42873	-5,09529
-10,7773	-8,08366	-6,28015	-5,35912	-5,03693
-10,6224	-7,99159	-6,23018	-5,3298	-5,01483
-10,5671	-7,97333	-6,22612	-5,32649	-5,0123
-10,6276	-8,05171	-6,28694	-5,36264	-5,03559
-10,6609	-8,0778	-6,28274	-5,32949	-4,9861
-10,5999	-8,05798	-6,28121	-5,3247	-4,97248
-10,673	-8,07539	-6,28294	-5,32543	-4,97733
-10,6324	-8,08655	-6,34711	-5,42063	-5,08406
-10,5078	-7,95787	-6,24317	-5,33611	-5,0046
-10,541	-7,99023	-6,27079	-5,3625	-5,03097
-10,3593	-7,84752	-6,17626	-5,30221	-4,99017
-10,4543	-7,81831	-6,10973	-5,23737	-4,93072
-10,2819	-7,68896	-6,07363	-5,26351	-4,97594
-10,3353	-7,67454	-6,03836	-5,23148	-4,94992
-10,4332	-7,70618	-6,01349	-5,1743	-4,88672
-10,3272	-7,68098	-6,02789	-5,1867	-4,88441
-10,4883	-7,8548	-6,16586	-5,2783	-4,94402

-10,3955	-7,82664	-6,1704	-5,29489	-4,96928
-10,3191	-7,72696	-6,08497	-5,23	-4,92064
-10,5328	-7,89024	-6,19216	-5,29838	-4,96899
-10,2007	-7,62922	-5,97266	-5,10513	-4,79703
-10,3698	-7,78645	-6,10124	-5,2088	-4,88586
-10,5084	-7,90549	-6,19188	-5,27809	-4,94535
-10,3628	-7,8463	-6,19836	-5,31178	-4,98231
-10,1423	-7,6613	-6,0907	-5,2627	-4,96236
-10,1292	-7,61323	-6,058	-5,24715	-4,95264
-10,013	-7,50223	-5,96946	-5,17871	-4,89568
-10,0167	-7,50169	-5,98241	-5,20126	-4,92164
-10,0603	-7,48686	-5,93969	-5,15397	-4,87803
-10,1041	-7,50183	-5,95307	-5,16991	-4,89443
-10,0394	-7,47065	-5,9438	-5,16485	-4,88596
-9,80341	-7,3423	-5,86645	-5,10128	-4,8252
-9,79095	-7,33931	-5,86369	-5,10736	-4,84603
-18,1811	-16,0496	-14,7553	-14,117	-13,9249
-38,5739	-37,9621	-38,0229	-38,6124	-39,5308
-55,4995	-54,9086	-54,1389	-53,8974	-54,2247
-65,4215	-57,6409	-53,5273	-52,6809	-53,2198
-58,3791	-70,0387	-59,116	-54,7449	-53,2095
-63,1089	-62,9776	-61,0127	-60,1465	-59,1728
-59,4401	-71,56	-59,834	-55,8762	-54,4204
-65,2163	-61,8622	-59,4286	-59,709	-60,7933
-57,4108	-64,5458	-68,7253	-61,4881	-59,1533
-63,551	-63,3714	-62,857	-62,4298	-62,5862
-57,3368	-64,9602	-59,1473	-57,3599	-57,8769
-50,5733	-58,4137	-61,3032	-55,9678	-54,7316
-50,8395	-51,8456	-54,5211	-58,689	-62,8823
-59,7285	-65,7301	-61,1652	-58,8707	-58,5472
-54,9041	-56,4146	-55,8789	-54,2656	-53,1243
-69,964	-61,8143	-56,7427	-55,7052	-56,0379
-60,2636	-62,7962	-60,432	-58,9217	-58,4908
-58,4523	-58,1437	-59,6227	-58,8892	-57,5617
-58,5393	-57,9589	-57,8808	-57,1028	-55,8808
-57,807	-59,2538	-57,234	-54,8394	-53,4648
-54,2012	-54,3369	-59,3866	-66,92	-64,0421
-58,4433	-61,1139	-64,9894	-60,1718	-57,7685
-62,4867	-67,4663	-67,955	-61,4863	-58,6162
-60,1707	-70,4519	-65,0765	-60,9996	-58,4854
-58,5485	-61,0582	-65,523	-66,1743	-62,9502
-58,112	-58,2097	-57,1219	-56,4418	-56,0558
-54,4622	-56,0923	-60,2847	-64,13	-63,3627
-54,179	-56,7375	-62,8536	-77,5644	-68,2828
-56,7377	-60,2848	-60,3142	-58,4163	-56,952
-52,0965	-55,7432	-62,4408	-59,5528	-55,8146

-60,6667	-63,444	-60,0334	-57,4751	-55,6082
-58,9225	-59,0421	-60,6948	-60,8512	-59,4739
-54,1326	-58,1265	-60,1855	-57,9271	-55,484
-55,5059	-57,3589	-61,3422	-66,6609	-69,6966
-47,6029	-52,4292	-62,0079	-60,7745	-55,374
-48,0288	-51,7419	-55,5259	-55,9629	-54,3278
-56,5584	-66,5989	-61,7741	-57,4178	-55,2702
-52,5325	-54,9907	-58,4786	-61,0937	-61,9966
-51,1323	-55,5459	-61,6619	-61,0742	-58,0147
-48,8338	-50,3914	-53,2225	-55,6957	-57,0975
-12,3129	-9,52687	-7,94129	-7,15658	-6,89806
-4,64803	-1,64771	-0,40639	0,041348	0,259983
-3,6682	-0,56944	0,579643	0,946616	1,14803
-3,8771	-0,68813	0,498267	0,869082	1,06655
-4,17898	-0,80781	0,45665	0,841391	1,03496
-6,50263	-1,73539	0,264295	0,873473	1,09131
-7,6864	-2,19012	0,199998	0,919336	1,14601
-6,73787	-1,77209	0,308363	0,936297	1,15279
-5,37352	-1,24709	0,450331	0,971898	1,17531
-5,62041	-1,27454	0,494657	1,02239	1,22161
-5,70371	-1,30805	0,490275	1,02761	1,22955
-7,38975	-1,90077	0,372688	1,03784	1,25167
-7,84107	-2,03036	0,375837	1,08102	1,30329
-7,42378	-1,88197	0,418334	1,09318	1,31024
-4,76269	-0,82218	0,665587	1,09298	1,28332
-2,58169	0,254486	1,00473	1,17441	1,33966
-2,74602	0,194708	0,994454	1,18059	1,35032
-2,89432	0,153916	0,993643	1,18801	1,35651
-2,38652	0,258381	1,00433	1,19672	1,3699
-0,79123	0,63049	1,02939	1,19556	1,37331
-0,40813	0,733165	1,03123	1,18332	1,35869
-0,02141	0,842864	1,04825	1,19017	1,36507
0,476332	0,915581	1,02767	1,17141	1,35024
0,649116	0,909851	1,0125	1,16492	1,34736
0,530838	0,80722	0,939775	1,11097	1,30535
0,55049	0,780357	0,912685	1,08714	1,28063
0,553051	0,766259	0,89588	1,06905	1,26371
0,558473	0,758274	0,883947	1,05792	1,25329
0,554272	0,746422	0,86315	1,03595	1,2335
0,517725	0,717125	0,820759	0,99212	1,19513
0,281793	0,647869	0,785966	0,957895	1,16125
-0,24246	0,54784	0,785174	0,960472	1,16349
-0,57517	0,458002	0,745364	0,918736	1,12072
-1,18432	0,311778	0,72907	0,912445	1,11647
-2,46876	-0,02572	0,664424	0,868354	1,07031
-2,55357	-0,08953	0,603131	0,807179	1,00984

-3,65869	-0,34689	0,566647	0,791968	0,997179
-3,77973	-0,38367	0,551431	0,781398	0,987954
-3,80526	-0,45127	0,492583	0,732772	0,943278
-3,76173	-0,48736	0,445042	0,689633	0,900751
-3,60262	-0,4532	0,449274	0,694733	0,909453
-3,39668	-0,42739	0,441797	0,693101	0,910624
-3,32982	-0,46553	0,387547	0,640202	0,8576
-3,23396	-0,46506	0,373541	0,637895	0,86267
-3,19873	-0,48385	0,339854	0,597959	0,819199
-3,19306	-0,52873	0,289996	0,554968	0,778611
-3,13116	-0,52439	0,281327	0,545018	0,76888
-3,00845	-0,52258	0,260751	0,526807	0,750911
-2,96969	-0,50537	0,281533	0,560793	0,792221
-3,00464	-0,57321	0,214945	0,497708	0,729806
-3,04037	-0,64947	0,138826	0,426108	0,65671
-3,06916	-0,65723	0,142172	0,437897	0,674829
-2,9831	-0,6877	0,080493	0,370734	0,602782
-2,9206	-0,65692	0,108747	0,402265	0,6352
-2,90782	-0,6918	0,06989	0,365039	0,594703
-2,92246	-0,73727	0,027159	0,328552	0,558893
-2,8907	-0,74777	0,019235	0,328044	0,561762
-2,93467	-0,77871	-0,00744	0,296149	0,522442
-3,07161	-0,81151	-0,00368	0,308586	0,535383
-3,39235	-0,91266	-0,02998	0,290269	0,512663
-3,76423	-1,10761	-0,10312	0,25711	0,479027
-4,07408	-1,27117	-0,15425	0,245453	0,469104
-4,42154	-1,46102	-0,22368	0,216336	0,439831
-4,65781	-1,58354	-0,26421	0,214228	0,445899
-4,14699	-1,40029	-0,24435	0,185628	0,401566
-3,66461	-1,14437	-0,15988	0,214907	0,421431
-3,52596	-1,03729	-0,11299	0,232149	0,423112
-4,11089	-1,2569	-0,14684	0,235306	0,409555
-5,64837	-1,91455	-0,28205	0,24763	0,419395
-5,68632	-1,94438	-0,29423	0,240521	0,405928
-4,07012	-1,22982	-0,12983	0,235246	0,383931
-3,32219	-0,94847	-0,10589	0,19123	0,338141
-3,151	-0,92429	-0,13504	0,157138	0,307253
-3,46528	-1,10295	-0,19179	0,150807	0,304621
-4,16307	-1,47181	-0,31511	0,111322	0,268219
-4,63086	-1,69589	-0,36065	0,127978	0,289865
-4,56369	-1,69194	-0,38206	0,099641	0,25507
-4,18468	-1,49389	-0,32625	0,10217	0,243518
-3,66151	-1,20963	-0,21778	0,145224	0,271762
-3,30182	-1,04271	-0,18821	0,123235	0,234002
-3,12896	-0,95933	-0,16929	0,11993	0,224421
-3,39936	-1,09146	-0,20558	0,106508	0,199828

-3,93441	-1,35107	-0,26843	0,10488	0,195063
-4,52642	-1,62675	-0,33378	0,101958	0,189816
-5,11767	-1,91544	-0,41966	0,078717	0,165539
-5,41683	-2,06743	-0,46584	0,062017	0,143558
-5,6358	-2,14786	-0,473	0,070721	0,146585
-5,62293	-2,15992	-0,48504	0,057959	0,129093
-5,6959	-2,17765	-0,46977	0,083026	0,155227
-5,80585	-2,2357	-0,49785	0,060157	0,126612
-6,21558	-2,36966	-0,51032	0,063745	0,111819
-6,53906	-2,414	-0,45932	0,118402	0,15183
-7,00364	-2,59355	-0,50664	0,093803	0,110261
-7,20299	-2,63	-0,48045	0,130635	0,14169
-7,18434	-2,65472	-0,52432	0,076731	0,076666
-7,0795	-2,57083	-0,46253	0,130177	0,127722
-6,39156	-2,32988	-0,42527	0,115902	0,107413
-6,07365	-2,25241	-0,43942	0,091237	0,089307
-5,6274	-2,0854	-0,40701	0,0887	0,082951
-5,05111	-1,86648	-0,37765	0,063472	0,050955
-5,02668	-1,90615	-0,423	0,023167	0,011391
-4,83933	-1,82249	-0,39837	0,031825	0,019001
-4,72883	-1,76437	-0,39187	0,021098	0,007438
-4,62981	-1,74001	-0,39972	0,00938	-0,00166
-4,35007	-1,62985	-0,37942	0,001884	-0,01606
-4,35164	-1,62503	-0,36811	0,01276	-0,00709
-4,25528	-1,58605	-0,37102	-0,00404	-0,02345
-3,83422	-1,38185	-0,33883	-0,03762	-0,07218
-3,14769	-0,99361	-0,21114	-0,00511	-0,04762
-3,65246	-1,30034	-0,35488	-0,09058	-0,12666
-5,14315	-2,10659	-0,5987	-0,12752	-0,12831
-5,38668	-2,30459	-0,70057	-0,1748	-0,15687
-5,76871	-2,55311	-0,8189	-0,22326	-0,17683
-5,76463	-2,62263	-0,88471	-0,26291	-0,20253
-6,07109	-2,78676	-0,95103	-0,28214	-0,20724
-6,16179	-2,79663	-0,9289	-0,26065	-0,19364
-6,49027	-2,8878	-0,92327	-0,24235	-0,18097
-6,79967	-2,96419	-0,90564	-0,22578	-0,18652
-7,1495	-3,12237	-0,95078	-0,24169	-0,20489
-6,87209	-3,07569	-0,98719	-0,27028	-0,20616
-14,3624	-11,27	-9,55465	-8,99708	-8,99155
-34,2154	-33,9043	-34,5271	-35,4189	-36,1912
-57,0244	-54,8518	-53,3568	-53,1178	-53,954
-57,6323	-62,4886	-66,6984	-59,4948	-55,9944
-60,8412	-58,1222	-56,1961	-55,4579	-55,1027
-63,86	-64,747	-66,6202	-68,136	-67,7914
-60,9925	-65,5494	-63,0439	-58,1618	-55,0799
-70,4374	-65,4521	-63,2033	-62,5493	-61,5418

-61,317	-60,9966	-60,1328	-58,6205	-56,6722
-56,3538	-60,0183	-64,7904	-66,815	-68,6108
-56,6182	-63,0747	-73,4222	-69,2048	-66,8693
-59,7446	-60,263	-59,698	-57,7984	-56,2541
-57,0319	-57,7951	-57,9002	-58,142	-56,576
-64,657	-59,5044	-56,8816	-55,1865	-53,0197
-55,4884	-53,7072	-52,5675	-51,4368	-50,3625
-53,7266	-55,4975	-59,0651	-61,9964	-64,1322
-63,2497	-65,3763	-66,0961	-63,6316	-60,9599
-58,7621	-58,5356	-57,2784	-55,6714	-54,1966
-64,4818	-64,9075	-65,7385	-67,1276	-66,0383
-54,3868	-56,2349	-58,5994	-59,5518	-59,7863
-58,0494	-61,6828	-63,9455	-62,5487	-60,1234
-55,0947	-57,8523	-57,4938	-55,5012	-54,7323
-53,031	-57,9424	-69,8709	-60,583	-56,0095
-57,1848	-60,068	-61,96	-58,151	-55,5679
-68,1258	-70,4886	-69,5545	-68,465	-67,064
-53,5505	-58,512	-72,7215	-59,7134	-55,4954
-57,3315	-62,1369	-67,5197	-61,8255	-58,2249
-63,7937	-61,749	-60,4883	-59,4527	-58,0012
-56,4589	-56,839	-58,2408	-58,4923	-57,1417
-71,9512	-67,5839	-65,1998	-62,2958	-58,1335
-50,7981	-49,8761	-49,9127	-49,6496	-48,7429
-58,2121	-56,8576	-54,9269	-53,3841	-52,2591
-55,16	-56,555	-56,6426	-54,7029	-53,3168
-58,5416	-61,3052	-58,6011	-55,195	-53,4764
-55,3198	-62,331	-58,8933	-53,9956	-52,2134
-59,8971	-61,3326	-55,4745	-52,0131	-50,5426
-69,5474	-63,9874	-59,9573	-58,119	-56,7921
-61,8714	-61,4063	-56,7619	-54,1762	-53,0209
-67,9854	-63,6976	-61,6905	-60,8112	-60,6001
-65,6559	-61,4433	-58,5092	-56,859	-55,0261
-10,8817	-6,47044	-3,83425	-2,75765	-2,51039
-6,92632	-2,71649	-0,24574	0,715386	0,907809
-6,63246	-2,48045	-0,06136	0,866931	1,04407
-6,4861	-2,38343	-0,0066	0,899086	1,06959
-6,43675	-2,32628	0,035519	0,925186	1,08785
-6,3999	-2,30961	0,035371	0,919892	1,0835
-6,32633	-2,24935	0,06309	0,930203	1,09457
-6,19946	-2,14796	0,125976	0,972498	1,13578
-6,08773	-2,11523	0,11661	0,954212	1,12326
-6,05318	-2,0159	0,198867	1,0022	1,15294
-6,06616	-1,99825	0,216049	1,00853	1,15013
-6,02971	-1,92615	0,274951	1,0449	1,17575
-5,96667	-1,91047	0,259029	1,0168	1,14737
-5,89458	-1,78018	0,375757	1,10434	1,21921

-5,90273	-1,74506	0,419826	1,1424	1,25221
-5,74998	-1,62131	0,486616	1,1721	1,27238
-5,61155	-1,50442	0,517733	1,13856	1,21586
-5,53828	-1,42164	0,579371	1,18214	1,25721
-5,64133	-1,48102	0,552523	1,17408	1,2592
-5,64995	-1,52138	0,527984	1,17816	1,28353
-5,70199	-1,60798	0,457361	1,13213	1,25247
-5,75616	-1,65019	0,443402	1,14521	1,28149
-5,85118	-1,71318	0,413349	1,12932	1,26743
-5,99622	-1,7579	0,43197	1,17297	1,31571
-6,06999	-1,83142	0,378392	1,13739	1,28941
-6,07578	-1,82422	0,395408	1,15996	1,31468
-6,14914	-1,88226	0,354582	1,13432	1,29926
-6,19238	-1,88918	0,357787	1,13516	1,30097
-6,33264	-1,93282	0,364099	1,16006	1,33053
-6,39935	-1,93557	0,378619	1,1728	1,34177
-6,41765	-1,90369	0,422977	1,21326	1,38039
-6,37202	-1,87772	0,430862	1,21345	1,38181
-6,30079	-1,83748	0,448951	1,22901	1,4075
-6,18432	-1,76778	0,473634	1,23212	1,41015
-5,97421	-1,64249	0,528988	1,2551	1,42955
-5,87588	-1,59544	0,539702	1,25853	1,4418
-5,62277	-1,4737	0,57321	1,25807	1,43705
-5,57683	-1,4138	0,630691	1,3124	1,49558
-5,5994	-1,393	0,655193	1,33209	1,51509
-5,46473	-1,34086	0,652447	1,31026	1,49466
-5,28057	-1,23601	0,704539	1,3415	1,51982
-5,30761	-1,22763	0,722008	1,35586	1,53581
-5,46228	-1,27087	0,734767	1,38075	1,5587
-5,61257	-1,3092	0,748902	1,40658	1,58906
-5,80408	-1,35234	0,768695	1,44119	1,6234
-6,02	-1,43889	0,755253	1,4554	1,64946
-6,10698	-1,48791	0,721563	1,42673	1,62455
-6,2016	-1,53288	0,701998	1,41765	1,62478
-6,32735	-1,56493	0,710567	1,4366	1,64191
-6,38413	-1,56149	0,739958	1,47359	1,68138
-6,58662	-1,61761	0,748542	1,49468	1,70081
-6,68608	-1,6742	0,712902	1,47368	1,69228
-6,857	-1,72057	0,710168	1,47692	1,69906
-6,94224	-1,72759	0,720608	1,48745	1,70854
-6,9688	-1,7071	0,746913	1,50769	1,72357
-7,0971	-1,72761	0,749768	1,50785	1,72415
-7,13976	-1,69648	0,790646	1,54366	1,75549
-7,26271	-1,71354	0,8001	1,55571	1,77054
-7,27804	-1,66697	0,845778	1,58709	1,79402
-7,34493	-1,63648	0,892484	1,63041	1,8366

-7,43332	-1,64657	0,898027	1,63364	1,84018
-7,53291	-1,68136	0,885222	1,63023	1,84092
-7,59344	-1,64204	0,943228	1,68446	1,8922
-7,66377	-1,67018	0,927103	1,66988	1,87877
-7,76852	-1,67967	0,946087	1,69566	1,90691
-7,82819	-1,66545	0,980069	1,73075	1,93592
-7,9504	-1,7046	0,958716	1,70785	1,90928
-7,99991	-1,68144	1,00698	1,76299	1,96536
-8,08839	-1,70579	1,00475	1,76385	1,96128
-8,17804	-1,75653	0,982784	1,7556	1,95503
-8,25302	-1,77137	0,982925	1,75709	1,95499
-8,28388	-1,75881	1,00933	1,78764	1,98632
-8,32503	-1,76492	1,02111	1,80692	2,0091
-8,39635	-1,80776	0,982125	1,76847	1,97258
-8,48048	-1,81531	0,99042	1,77949	1,98447
-8,49056	-1,79086	1,0231	1,81664	2,02677
-8,58204	-1,83492	0,990864	1,7914	2,008
-8,69827	-1,88417	0,957661	1,76463	1,98612
-8,74681	-1,86262	0,994524	1,80116	2,02084
-8,90446	-1,92837	0,965172	1,79142	2,02083
-8,91	-1,9108	0,974269	1,78801	2,01282
-8,936	-1,9067	0,992993	1,8155	2,04214
-9,07492	-1,98256	0,94312	1,77508	2,0049
-9,09845	-1,94592	0,994738	1,82987	2,05867
-9,03358	-1,90871	1,0143	1,83707	2,05948
-9,12106	-1,96483	0,975428	1,80702	2,03022
-9,14103	-1,94943	0,997051	1,82913	2,05345
-9,17771	-1,96485	0,983928	1,81282	2,03365
-9,2926	-1,99425	0,984124	1,82115	2,04169
-9,42687	-2,04728	0,95369	1,79521	2,01385
-9,55051	-2,09966	0,91915	1,76027	1,97416
-9,69104	-2,12185	0,941817	1,79746	2,01198
-9,77408	-2,14295	0,945693	1,8071	2,01854
-9,93443	-2,20812	0,912865	1,77886	1,98561
-10,2428	-2,31188	0,873378	1,76049	1,974
-10,244	-2,28153	0,90635	1,78246	1,98243
-10,2739	-2,26442	0,933222	1,8084	2,0035
-10,7596	-2,39351	0,912526	1,82159	2,02626
-11,4232	-2,61563	0,812647	1,75292	1,95948
-4,77303	-0,42759	1,28074	1,74726	1,90175
-1,57332	1,06287	1,68177	1,77914	1,89535
-1,67173	1,03136	1,6873	1,79397	1,90684
-1,69935	0,999178	1,67746	1,79735	1,91125
-1,70011	0,977641	1,65241	1,76675	1,87349
-1,7579	0,971042	1,66768	1,78691	1,89252
-1,87548	0,916701	1,63147	1,74967	1,85039

-1,79857	0,972002	1,66238	1,76262	1,85212
-1,55899	1,11066	1,71129	1,77408	1,85368
-1,87259	0,941041	1,66358	1,77027	1,85055
-9,45943	-2,06562	0,900522	1,69868	1,8523
-11,6806	-2,70927	0,740565	1,66255	1,83068
-11,8225	-2,77443	0,706145	1,64341	1,82144
-11,7081	-2,71394	0,734667	1,65902	1,83389
-11,7224	-2,72535	0,728492	1,6569	1,83535
-12,1607	-2,80513	0,723993	1,66786	1,84875
-12,295	-2,8227	0,705841	1,64514	1,82804
-12,5539	-2,85321	0,696802	1,63562	1,82123
-12,9353	-2,91809	0,652254	1,5906	1,78118
-10,7003	-2,34497	0,766278	1,58735	1,77018
-6,50778	-0,97607	1,11362	1,65217	1,8071
-16,0953	-10,1566	-7,6933	-7,0679	-6,97979
-33,8114	-33,0942	-33,1325	-33,6095	-34,3003
-46,0749	-46,3412	-48,0259	-50,6568	-53,943
-60,918	-60,6509	-62,4678	-68,6293	-73,4121
-50,6482	-52,5841	-57,3732	-66,8721	-67,8434
-57,3002	-59,3391	-66,3847	-70,1005	-62,6334
-54,9949	-55,2113	-58,4939	-62,787	-58,9053
-57,5452	-59,2365	-62,8647	-69,698	-74,5355
-59,4605	-61,7452	-63,8396	-64,0765	-62,1153
-58,9	-60,7351	-65,7365	-71,5096	-61,3733
-51,8873	-53,2646	-56,8567	-63,0452	-66,314
-52,2238	-56,0558	-62,3617	-67,1451	-66,7533
-53,2674	-54,5124	-56,6845	-59,3749	-61,8539
-59,5692	-63,552	-64,8697	-68,252	-68,7454
-51,6335	-53,7564	-59,0074	-63,7896	-60,5287
-50,8351	-49,2856	-50,9974	-55,8336	-65,1508
-57,1533	-56,5387	-58,1855	-61,8155	-65,9304
-55,823	-56,4331	-58,1778	-59,5729	-60,0118
-57,3593	-58,683	-60,0463	-61,254	-61,7799
-67,3692	-64,724	-63,4252	-62,5698	-62,2641
-51,0739	-51,4078	-53,3984	-55,8248	-57,7917
-60,4319	-57,3326	-57,4719	-58,4502	-59,0706
-55,6428	-57,4788	-63,2826	-71,0516	-66,3009
-52,4039	-52,2082	-54,32	-57,8166	-61,3845
-60,4261	-65,09	-66,5626	-66,6942	-65,3371
-75,6342	-59,9046	-56,1061	-55,514	-55,1904
-63,0616	-60,6944	-60,1786	-61,8159	-63,7727
-53,1672	-53,1861	-54,4027	-56,2681	-57,7524
-62,9367	-60,0711	-59,717	-60,5378	-60,5483
-58,9453	-58,7564	-61,7934	-67,9013	-69,3311
-59,3175	-59,5475	-61,5913	-62,9456	-60,8372
-60,7246	-62,0178	-62,0082	-62,243	-63,8287

-60,1918	-65,0607	-65,623	-62,8404	-62,0865
-57,4846	-61,8339	-65,8658	-64,313	-62,0662
-55,8194	-57,8595	-60,1762	-61,7965	-64,2076
-54,3286	-56,9869	-58,0857	-58,2532	-59,1655
-53,0349	-54,3034	-56,6202	-59,1576	-61,9731
-62,8713	-64,0739	-60,5769	-57,7785	-56,2929
-53,6281	-54,7684	-56,6149	-58,24	-59,7895
-59,8822	-67,3812	-68,7181	-61,2723	-57,391
-6,59248	-3,77928	-2,91131	-2,68108	-2,58229
-0,57604	0,813667	1,12343	1,24476	1,37165
0,392757	1,22975	1,32954	1,4132	1,52944
0,826217	1,37724	1,38597	1,46919	1,59568
0,917144	1,41507	1,40585	1,48961	1,61797
0,837837	1,35198	1,35779	1,45006	1,58558
0,809414	1,32987	1,35364	1,46355	1,60987
0,726644	1,27583	1,31935	1,43648	1,59126
0,7094	1,2799	1,33423	1,44509	1,58606
0,612579	1,22402	1,31601	1,44972	1,60167
0,437009	1,16293	1,3127	1,46321	1,6238
-0,93227	0,82078	1,31402	1,48954	1,63992
-1,85241	0,577525	1,28851	1,50334	1,66303
-1,18392	0,70941	1,27042	1,4662	1,62258
0,428232	1,17484	1,3395	1,4809	1,62936
0,356462	1,13416	1,32233	1,47222	1,62929
0,366416	1,11946	1,31605	1,47694	1,64174
0,377087	1,0966	1,29053	1,45226	1,61235
-0,3241	0,883718	1,2651	1,44449	1,60364
-2,83383	0,276777	1,20459	1,44321	1,60596
-2,84663	0,301152	1,24106	1,48138	1,6416
-2,85581	0,287763	1,23416	1,48395	1,65191
-2,63384	0,336442	1,22894	1,4528	1,59956
-2,37191	0,453328	1,27707	1,48183	1,62418
-8,16059	-2,10417	0,619504	1,42633	1,62761
-8,62199	-2,14843	0,649379	1,45097	1,62775
-8,35202	-2,06264	0,680148	1,47011	1,64295
-8,21824	-2,01522	0,702377	1,48344	1,64913
-7,9573	-1,96521	0,680825	1,43404	1,57954
-7,98003	-1,98803	0,677715	1,44663	1,58862
-7,78654	-1,97223	0,640462	1,40112	1,53543
-7,4407	-1,9206	0,599931	1,33863	1,45017
-6,95863	-1,79164	0,597593	1,30343	1,39179
-6,27346	-1,57137	0,640682	1,30522	1,37363
-4,4891	-0,85684	0,789118	1,28168	1,28174
-3,03796	-0,1749	0,966033	1,29395	1,24104
-2,99689	-0,19257	0,947325	1,27695	1,16597
-3,12952	-0,26498	0,931764	1,27532	1,11577

-3,1781	-0,3707	0,836863	1,17478	0,948336
-3,09795	-0,33017	0,867857	1,20112	0,946452
-2,94033	-0,29735	0,855907	1,17697	0,912389
-2,97585	-0,32807	0,849694	1,18044	0,896442
-2,99437	-0,37433	0,802185	1,12457	0,812703
-3,16461	-0,46455	0,771018	1,09918	0,763019
-3,21555	-0,49363	0,770005	1,10018	0,73704
-3,0456	-0,41112	0,82224	1,13452	0,747142
-3,16326	-0,48088	0,790673	1,11188	0,709654
-3,11328	-0,46537	0,801263	1,11105	0,686995
-2,84488	-0,37796	0,811709	1,09338	0,641639
-2,77137	-0,41016	0,748622	1,01179	0,514159
-2,6441	-0,31915	0,820477	1,07212	0,557209
-2,53542	-0,3129	0,786823	1,00622	0,434715
-2,51839	-0,29753	0,800407	1,00101	0,383202
-2,60784	-0,36868	0,74583	0,919637	0,213159
-2,48085	-0,35007	0,709224	0,854357	0,114305
-2,27897	-0,26867	0,73264	0,830432	-0,00786
-2,24078	-0,24161	0,745702	0,815888	-0,0724
-2,39629	-0,23791	0,796086	0,831686	-0,15905
-2,41845	-0,24495	0,789804	0,816619	-0,19996
-2,01205	-0,09576	0,811945	0,775996	-0,3082
-1,93457	-0,07065	0,804382	0,76252	-0,31244
-1,66055	-0,00554	0,776961	0,717107	-0,35587
-1,35862	0,121176	0,805274	0,704087	-0,40195
-1,15429	0,184793	0,800039	0,673967	-0,4456
-0,94923	0,258417	0,814513	0,682015	-0,42901
-0,87857	0,272945	0,797328	0,64026	-0,50065
-0,79671	0,275543	0,770353	0,621312	-0,49282
-0,57907	0,351724	0,790089	0,628268	-0,48681
-0,52437	0,365381	0,797471	0,644552	-0,45942
-0,60442	0,305258	0,761704	0,629178	-0,45102
-0,65798	0,287815	0,768102	0,640329	-0,44284
-0,74352	0,221004	0,720348	0,600926	-0,47936
-0,76321	0,254715	0,781435	0,67473	-0,39153
-0,76861	0,262789	0,788183	0,673535	-0,40196
-0,7522	0,278756	0,797743	0,684832	-0,37309
-0,78531	0,271203	0,795342	0,676336	-0,3851
-0,79186	0,293768	0,829175	0,713224	-0,34012
-0,80229	0,325228	0,854668	0,717295	-0,34481
-0,82537	0,338917	0,857827	0,695016	-0,38063
-0,77008	0,436802	0,94713	0,769378	-0,30462
-0,69175	0,529116	1,00577	0,792446	-0,29164
-0,63881	0,612433	1,06167	0,811601	-0,2855
-0,68764	0,613179	1,08162	0,830431	-0,26892
-0,79657	0,56191	1,07805	0,849043	-0,24283

-0,85727	0,514116	1,06037	0,855589	-0,22537
-0,91421	0,450635	1,02131	0,842002	-0,2252
-0,91309	0,428056	1,01056	0,847537	-0,2075
-0,99408	0,382252	0,980668	0,832735	-0,19609
-0,96891	0,393614	1,00506	0,87125	-0,15773
-0,98336	0,344359	0,9728	0,862359	-0,15422
-1,02827	0,278855	0,916075	0,824442	-0,16714
-1,08566	0,224628	0,889224	0,822269	-0,15782
-1,09203	0,183452	0,854457	0,810948	-0,14037
-1,06104	0,207232	0,889559	0,855691	-0,09736
-1,05624	0,181446	0,851331	0,81527	-0,13514
-1,0244	0,228233	0,899163	0,861899	-0,08619
-0,945	0,283484	0,929557	0,878517	-0,07328
-0,83781	0,366446	0,982905	0,90537	-0,06252
-0,77235	0,424158	1,0191	0,921774	-0,05253
-0,66907	0,503567	1,07505	0,960006	-0,02982
-0,62952	0,537946	1,09181	0,966455	-0,00753
-0,53729	0,599618	1,11489	0,961078	-0,02589
-0,24629	0,83101	1,27647	1,07247	0,05496
-0,11583	0,908356	1,3062	1,07461	0,054269
-0,19951	0,863514	1,2899	1,07547	0,065069
-0,13884	0,897059	1,30536	1,0769	0,060468
-0,1451	0,912511	1,33547	1,11395	0,101344
-0,13684	0,926074	1,33958	1,10681	0,088123
-0,03938	1,00632	1,41893	1,18911	0,154903
-0,10492	0,973893	1,4015	1,17976	0,162943
-0,01696	1,02393	1,42369	1,18568	0,165647
-0,07724	0,978619	1,38891	1,15975	0,148993
-0,08153	0,948591	1,35035	1,12413	0,123358
0,114732	1,06467	1,42733	1,19184	0,178463
0,171392	1,0981	1,43745	1,19587	0,201814
0,267196	1,15782	1,47901	1,2305	0,221471
0,195129	1,0981	1,43071	1,2005	0,222944
0,228155	1,12359	1,4668	1,25489	0,288442
0,184935	1,06311	1,41368	1,21844	0,266496
0,129499	1,04198	1,41528	1,2333	0,287367
-7,76923	-6,86756	-6,57193	-6,8791	-7,88284
-30,2567	-29,7064	-30,0292	-31,4897	-34,1154
-46,9447	-46,3756	-46,7248	-48,4335	-51,8447
-54,9992	-59,3929	-65,9696	-63,0407	-60,4868
-57,8273	-62,2544	-64,8708	-58,5624	-56,0555
-51,3107	-53,6937	-58,8603	-60,4831	-55,6647
-53,4075	-55,2739	-59,4102	-66,9859	-62,9027
-59,5928	-58,0237	-58,4744	-60,5961	-61,5435
-52,2281	-52,6145	-54,6242	-58,564	-56,9982
-50,9969	-50,9722	-52,0423	-54,6448	-57,4719

-59,1332	-58,3859	-59,1535	-58,3672	-56,8965
-52,5043	-56,9333	-60,5607	-62,376	-63,4224
-49,6882	-53,6996	-58,2275	-59,998	-59,9885
-50,5609	-57,0328	-66,138	-58,2998	-56,0152
-52,5824	-60,1918	-54,4673	-51,2162	-51,0783
-53,4143	-54,6981	-54,2707	-53,417	-53,3196
-42,3016	-45,5477	-49,4002	-52,3076	-53,2156
-54,9758	-59,7294	-59,3542	-57,5627	-58,5312
-46,2339	-48,5558	-51,8441	-55,6167	-59,4157
-43,3526	-45,1095	-47,1255	-48,9566	-50,6402
-50,1075	-53,4675	-58,285	-62,5801	-62,785
-45,6771	-47,0271	-48,8775	-50,8413	-52,919
-46,9549	-48,7276	-51,2713	-54,2688	-58,3453
-54,8637	-54,9921	-55,6059	-56,4967	-58,4103
-44,3612	-46,2596	-48,9024	-51,8607	-55,4034
-50,9197	-51,6531	-52,7784	-54,8277	-58,3383
-52,1965	-52,4708	-53,768	-56,5189	-59,9134
-56,1598	-57,6009	-59,3195	-59,9348	-60,3212
-57,5866	-56,764	-56,373	-56,8163	-57,7807
-47,4507	-48,4866	-49,9792	-52,1796	-55,9741
-54,2585	-53,6187	-55,1461	-61,1019	-62,6583
-47,4357	-47,6053	-48,992	-51,1679	-53,6899
-53,6834	-54,5604	-56,4862	-56,9782	-58,0016
-53,1427	-53,3969	-53,2235	-52,8706	-55,1292
-64,5128	-67,0468	-66,5134	-64,7582	-66,012
-56,5056	-54,3007	-52,1003	-50,6704	-50,9599
-52,4523	-52,4959	-52,5337	-52,7121	-54,5856
-57,6316	-65,5349	-59,2752	-56,3215	-57,4872
-47,6634	-47,767	-49,0429	-50,7133	-53,0171
-44,5474	-45,4178	-47,6474	-50,1301	-53,1158
-48,2108	-49,2592	-51,89	-55,4082	-60,8801
-49,4438	-49,6837	-51,0141	-52,5245	-53,7048
-52,235	-51,186	-51,5427	-52,6185	-53,7411
-49,9889	-50,0573	-51,8902	-54,6407	-58,4868
-52,5882	-52,5772	-53,7557	-55,4694	-57,4132
-57,2401	-56,1251	-56,6648	-58,0029	-59,9546
-55,3198	-53,9465	-53,4383	-54,2707	-55,9435
-58,4025	-56,2271	-56,2737	-57,9368	-61,1326
-67,5531	-61,2411	-57,6995	-56,6418	-57,4352
-56,6278	-52,5391	-51,2996	-52,3166	-55,6965
-62,6175	-60,543	-60,2089	-61,7094	-64,3969
-56,2055	-57,1677	-58,1332	-58,7951	-59,7324
-59,0661	-60,7674	-62,452	-63,2218	-64,6326
-51,3986	-49,2799	-49,3395	-49,9829	-52,0104
-60,9463	-58,3787	-57,8137	-58,0882	-60,0333
-56,702	-57,2618	-57,602	-57,2478	-57,2185

-53,0617	-53,8958	-55,9249	-56,9235	-59,7533
-62,4544	-59,5155	-59,0872	-59,138	-61,4229
-54,8396	-55,2167	-56,9316	-58,6358	-60,3382
-53,7846	-56,0947	-59,9757	-61,2647	-62,6328
-54,68	-53,2683	-52,7412	-52,2966	-52,9969
-63,8464	-63,0593	-63,28	-63,4075	-63,9094
-58,8708	-59,1398	-60,2146	-61,837	-62,7209
-53,0682	-54,9867	-57,604	-59,6594	-64,1371
-53,5535	-53,5524	-54,5499	-56,3924	-59,0008
-53,5536	-52,5937	-51,9693	-51,6704	-52,0565
-50,1597	-50,7641	-51,6805	-52,6088	-54,6192
-62,3785	-60,7836	-59,5025	-58,758	-58,1362
-57,0556	-56,1168	-55,7424	-56,784	-59,0018
-64,3735	-62,4436	-59,4185	-59,4307	-60,7805
-65,8121	-66,629	-66,8945	-67,7376	-67,4839
-66,9705	-67,5094	-68,9917	-70,0927	-69,4219
-59,9158	-58,2133	-57,3198	-57,3093	-57,9849
-56,7762	-55,8695	-55,6706	-56,523	-58,0113

Apêndice D- Código em linguagem de programação *python* utilizado, relativo aos Testes A, posição 1

```
# Para os Testes A, posição P1
# Obtém-se o gráfico da média das energias em função da posição

import matplotlib.pyplot as plt

# Dados da tabela dos dados reduzidos
potencias = [0.01, 0.02, 0.05, 0.1, 0.2, 0.5, 1]
posicoes = [839, 840, 841, 842, 843]

# Valores médios para cada posição
valores = [
    [-27.3115, -26.2657, -25.4236, -24.6649, -24.0186],
    [-20.8968, -18.7247, -17.0435, -15.9294, -15.3905],
    [-13.1947, -10.7806, -9.4448, -8.8429, -8.6731],
    [-10.8140, -8.3002, -6.6624, -5.7983, -5.4827],
    [-3.9672, -1.1253, 0.0408, 0.4276, 0.5694],
    [-7.2100, -1.6957, 0.7267, 1.4583, 1.6369],
    [-1.7212, 0.1757, 0.9772, 1.0485, 0.4685],
]

# Plot dos dados
plt.figure(figsize=(10, 6))

for i, potencia in enumerate(potencias):
    plt.plot(posicoes, valores[i], marker='o', label=f'{potencia} W')

# Adicionar títulos e legendas
plt.title('Média das energias em função da posição dos Testes A em P1')
# plt.ylabel('PSD [dB/Hz]')
plt.xlabel('Posição (m)')
plt.ylabel('Média das energias [dB] re. pE/√(Hz)')
plt.legend(title='AP (W)')
plt.grid(True)
plt.show()
```

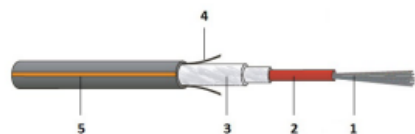

Anexos

Anexo A- Especificações do Cabo de Fibra Ótica utilizado no projeto



FO Outdoor ZGGT HP / A-DQ(ZN)B2Y

HighP Euroclass Fca
central tube design, metal-free,
longitudinally watertight, rodent protection



- 1 ≤ 24 fibres
- 2 Loose tube
- 3 Glass armour
- 4 Ripcord
- 5 HDPE sheath



Description

Robust, metal-free fibre optic outdoor cable with one central loose tube and up to 24 fibres.
High tensile strength and high radial load strength for the highest transmission security.
Lightweight and installation friendly cable construction.
Non-metallic rodent protection.
The two coloured ripcords are easy to identify and enable the safe opening of the cable sheath.
HDPE cable sheath, easy to lay.

Application

For pulling in or blowing through thermoplastic duct systems.
Suitable for laying in cable platforms, cable shafts
and even in very complex cable trays.
Direct burial.

Construction

Armouring (rodent protection)	rodent proof
Outer sheath material	PE

General Properties

Imprint	DATWYLER «cable type» «Datwyler designation» «DIN designation» «no. of fibres» «fibre type» «add. text» «batch no.» «meter marks»
Installation temperature	-10 °C - +50 °C
Operating temperature	-40 °C - +70 °C
Storage temperature	-40 °C - +70 °C

Standards

Tensile performance	IEC 60794-1-21 E1
Crush resistance	IEC 60794-1-21 E3
Impact	IEC 60794-1-21 E4
Repeated bending	IEC 60794-1-21 E6
Torsion	IEC 60794-1-21 E7
Bend	IEC 60794-1-21 E11
Water penetration	IEC 60794-1-22 F5
Reaction to fire (Euroclasses)	EN 13501-6
Zero halogen no corrosive gases	IEC 60754-1/-2, EN 60754-1/-2, VDE 0482-754-1/-2

Versions

Material number	Product	Reaction To Fire	Outer sheath colour	Fibre type	Outer sheath diameter (mm)	Bending radius (mm)	Weight (kg/km)	Tensile load (N)	Crush resistance short term (N)	Crush resistance continuous (N)	Fire load (kWh/m)	Packing unit
19016600FZ	FO Outdoor HP 1x4	Fca	black	E9/125 G.652.D OS2	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19212100FZ	FO Outdoor HP 1x4	Fca	black	G50/125 OM3	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19608900FZ	FO Outdoor HP 1x4	Fca	black	G50/125 OM4	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19016700FZ	FO Outdoor HP 1x6	Fca	black	E9/125 G.652.D OS2	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19074700FZ	FO Outdoor HP 1x6	Fca	black	G50/125 OM3	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19016800FZ	FO Outdoor HP 1x8	Fca	black	E9/125 G.652.D OS2	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19609000FZ	FO Outdoor HP 1x8	Fca	black	G50/125 OM4	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19016900FZ	FO Outdoor HP 1x12	Fca	black	E9/125 G.652.D OS2	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
18636100FZ	FO Outdoor HP 1x12	Fca	black	G50/125 OM3	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19361000FZ	FO Outdoor HP 1x12	Fca	black	G50/125 OM4	8.2	130	75	2,500	10,000	6,000	0.558	by the metre
19014900FZ	FO Outdoor HP 1x24	Fca	black	E9/125 G.652.D OS2	8.6	135	80	2,500	10,000	6,000	0.589	by the metre
19264300FZ	FO Outdoor HP 1x24	Fca	black	G50/125 OM3	8.6	135	80	2,500	10,000	6,000	0.589	by the metre
19216700FZ	FO Outdoor HP 1x24	Fca	black	G50/125 OM4	8.6	135	80	2,500	10,000	6,000	0.589	by the metre

Subject to technical modification

As of 2020-11-06 13:44:41

Anexo B- Especificações do modelo do altifalante subaquático LL916C

MARSENSING LDA
UNDERWATER ACOUSTICS & MARINE TECHNOLOGIES



UNDERWATER SPEAKERS

HIGH PERFORMANCE SPEAKERS FOR POWERFUL UNDERWATER SOUND
Lubell Labs, the world leader in portable and in-wall underwater speakers

Synchronized swimming
Hotels & private pools
SCUBA Diving

Sound Level
Up to 150 dB with only 20 V rms input voltage

Frequency band
Wide band coverage spanning an interval from 200 Hz to 20 kHz

Durability
Its extremely rugged construction promises long durability
(up to 5 years warranty!)



Portable and in-wall speakers





DESCRIPTION

The LL916 is an economical yet powerful piezoelectric underwater speaker developed, patented, and manufactured by Lubell Labs, Inc. (Columbus, Ohio). The LL916 series continue to set the world record for having the widest frequency response and output level of any commercial underwater speaker made, at a price that is reasonable and affordable. Because of its rugged PVC construction and cage-mounting system, the LL916C is nearly immune to damage, and may be used in test tanks, swimming pools, rivers, lakes, and oceans. The LL916 is provided with choice of audio isolation transformer box with cord, allowing phone jack connection to popular commercial sound amplifiers of various power and impedance ratings.

APPLICATIONS

Lubell underwater loudspeakers and systems find application in a range of areas including synchronized swimming, hotel and SPAs, home pools, SCUBA instruction and diver rescue. One single LL916 speaker is capable of filling a municipal pool or an Olympic pool. These underwater speakers are very popular for its exceptional performance, easy applicability, and durability.

SPECIFICATIONS

Frequency Response

200 Hz - 21 kHz

Sound level

150 dB re 1 µPa @ 1 m for 1 inch

Maximum Cable Voltage/Current

30 Vrms / 3A (100% duty cycle)

Maximum power rating

38 W

Maximum operating depth

15 m

Finish

Blue PVC

Cable

8 m length 18/3 PVC for customized

Cable Termination

3-pin proprietary (Creswell T350-3P5-52W) mates with transformer box

Weight

7 kg in air, 14 kg in water

Dimensions

Speaker: 23 cm diameter, 19 cm axis length

Cage: 27 cm x 27 cm x 20 cm

Transformers

AC150 150 W, 32 Ω, 40 V rms; AC250 250 W, 2 Ω, 10 V rms;

AC350 350 W, 8 Ω, 20 V rms; AC25C 120 W, 16 Ω, 25 V rms;

AC350E 180 W, 8 Ω, 25 V rms or 8 Ω or output and attenuator;

AC351 1200 W, 16 Ω, 40 V rms; 8 Ω or output and attenuator.

Warranty

5 years

THE LL916H UNDERWATER SPEAKER

The LL916H (hardest underwater speaker) is the economical version of the LL916C model for flexible usage in pools and at sea.



THE LL9484 UNDERWATER SPEAKER (IN-WALL)

The Lubell 9484 is a growth-in-wall underwater speaker system for municipal pools, pools in hotels and private homes.



MARSSENSING LDA

Centro Empresarial Pav. A5, Campus de Gambelas

8005-131 Faro - PORTUGAL

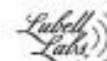
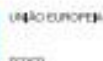
web: www.marsensing.com

e-mail: contact@marsensing.com

phone +351 963729660



Official dealer for:



Anexo C- Certificado de participação no XI Curso de “Cibersegurança e Gestão de Crises no Ciberespaço”

Certificado

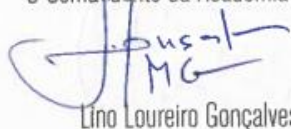
Daniela Filipa Miranda da Silva completou o

XI Curso de “Cibersegurança e Gestão de Crises no Ciberespaço”

Para que conste, é emitido o presente certificado que vai assinado e firmado com o selo branco.

Lisboa, 06 de junho de 2024

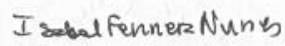
O Comandante da Academia Militar



Lino Loureiro Gonçalves

Major-General

Diretora do IDN


Isabel Ferreira Nunes

Prof. Doutora

academia
militar



idn Instituto
da Defesa Nacional