MARINHA DO BRASIL
ESCOLA DE GUERRA NAVAL
PROGRAMA DE PÓS-GRADUAÇÃO EM ESTUDOS MARÍTIMOS

WALMOR CRISTINO LEITE JUNIOR

MEDIDAS DE SEGURANÇA CIBERNÉTICA PARA O AMBIENTE MARÍTIMO: UMA ANÁLISE HÍBRIDA DE PROPOSTAS E TENDÊNCIAS NO CONTEXTO BRASILEIRO

Rio de Janeiro
2021

WALMOR CRISTINO LEITE JUNIOR

MEDIDAS DE SEGURANÇA CIBERNÉTICA PARA O AMBIENTE MARÍTIMO: UMA ANÁLISE HÍBRIDA DE PROPOSTAS E TENDÊNCIAS NO CONTEXTO BRASILEIRO

Dissertação apresentada ao Curso de Mestrado Profissional em Estudos Marítimos da Escola de Guerra Naval, como requisito parcial à obtenção do grau de Mestre em Estudos Marítimos. Área de Concentração em Defesa, Governança e Segurança Marítimas.

Orientadores: Prof. Dr. Nival Nunes de Almeida
Prof. Dr. Alan Oliveira de Sá

Rio de Janeiro
2021

L533m Leite Junior, Walmor Cristino
Medidas de segurança cibernética para o ambiente marítimo: uma análise híbrida de propostas e tendências no contexto brasileiro**.** / Walmor Cristino Leite Junior **.-** Rio de Janeiro, 2021**.**
122 f : il.

Dissertação (Mestrado) - Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos (PPGEM), 2021.

Orientadores: Nival Nunes de Almeida
Alan Oliveira de Sá

Bibliografia: f. 83 – 87

1.Ambiente marítimo. 2. Segurança cibernética. 3. Políticas Públicas. I. Escola de Guerra Naval. II. Título.

CDD 001.53

Ficha catalográfica elaborada pela bibliotecária
Cremilda Santos – CRB7/3200
Biblioteca da Escola de Guerra Naval

WALMOR CRISTINO LEITE JUNIOR

MEDIDAS DE SEGURANÇA CIBERNÉTICA PARA O AMBIENTE MARÍTIMO: UMA ANÁLISE HÍBRIDA DE PROPOSTAS E TENDÊNCIAS NO CONTEXTO BRASILEIRO

Dissertação apresentada ao Curso de Mestrado Profissional em Estudos Marítimos da Escola de Guerra Naval, como requisito parcial à obtenção do grau de Mestre em Estudos Marítimos.
Área de Concentração em Segurança, Defesa e Estratégia Marítima.

Aprovada em ___ de _____ de 2021

Banca Examinadora:

_____

Prof. Dr Nival Nunes de Almeida
Doutor da Escola de Guerra Naval

_____

Prof. Dr. Alan Oliveira de Sá
Doutor da Universidade Federal do Rio de Janeiro

_____

Prof. Dr. Claudio Rodrigues Corrêa

Doutor da Escola de Guerra Naval

_____

Prof. Dr. Adriano Lauro

Doutor da Escola de Guerra Naval

_____

Prof. Dr. Raphael Carlos Santos Machado

Doutor da Universidade Federal Fluminense

Dedico este trabalho ao Aviso de Instrução Guarda-Marinha Jansen, e a todos aqueles que tiveram a honra de lá servir.

AGRADECIMENTOS

Após a árdua jornada acadêmica, que hora se encerra, faz-se necessário reconhecer aqueles que estiveram empenhados em contribuir para o bom andamento desta pesquisa. Ao meu Orientador, Prof. Dr. Nival Nunes de Almeida, agradeço o precioso tempo dispendido em conversas e reuniões que foram fundamentais para o meu desenvolvimento acadêmico. Ao meu coorientador, Prof. Dr. Alan Oliveira de Sá, agradeço por incutir o gosto pela ciência e por acreditar no meu potencial. Meus orientadores, saibam que os senhores representam uma etapa fundamental da minha formação pessoal e profissional, sempre serei grato pelo tempo compartilhado com os senhores. Aos demais membros da banca examinadora, agradeço pelas importantes contribuições, sempre construtivas e pertinentes, sem as quais o presente trabalho não seria possível.

Não poderia deixar de citar a importante contribuição daqueles que comigo dividem os conveses dos navios da Marinha do Brasil. Aos Oficiais e Praças que estiveram comigo na Fragata Liberal, meu primeiro navio, agradeço por me ensinarem a fazer correto e a me empenhar na busca constante pela excelência. A tripulação do Aviso de Instrução Guarda-Marinha Jansen, agradeço a lealdade e a cordialidade na convivência diária, os senhores fizeram parte dessa conquista.

Aos meus familiares e amigos, sou grato pelas palavras de incentivo, sempre oportunas e presentes, sem as quais nada teria sido possível. As particularidades da vida nos levam por caminhos diversos, por vezes diferentes dos que imaginávamos, mas as experiências vividas são as bases para a nossa construção. Agradeço por tudo que vivi nesse período, pois esses acontecimentos me conduziram até esse dia.

“Nem cora o livro de ombrear co'o sabre...
Nem cora o sabre de chamá-lo irmão...”

(Castro Alves)

MEDIDAS DE SEGURANÇA CIBERNÉTICA PARA O AMBIENTE MARÍTIMO: UMA ANÁLISE HÍBRIDA DE PROPOSTAS E TENDÊNCIAS NO CONTEXTO BRASILEIRO

RESUMO

O presente estudo apresenta a importância da segurança cibernética nas relações de poder no contexto das relações internacionais e em questões de segurança marítima, trazendo à tona a necessidade de se enfrentar essa problemática. São apresentados os riscos e medidas mitigatórias identificados a partir de 2017, através de uma revisão sistemática nas bases de dados SCOPUS, IEEE Explore, ACM Digital Library e Google Scholar. Analisam-se dados obtidos através da mineração de dados em texto em documentos de nível político brasileiros e americanos. Além disso, são apresentados os resultados de um questionário respondido pela sociedade civil, pesquisadores e militares brasileiros, com o objetivo de colher a percepção desses grupos sobre o assunto segurança cibernética no contexto brasileiro. Dessa forma, são obtidos os resultados que permitem concluir que há indícios de que uma maior presença do assunto em documentos oficiais de nível político se traduz em maiores índices de segurança cibernética. Também se percebe que a presença do tema em documentos brasileiros não se encontra em níveis satisfatórios, fato reforçado pelos resultados dos questionários. Nota-se que o assunto vem ganhando cada vez mais importância ao longo dos anos e que as medidas mitigatórias identificadas apresentam potencial para serem implementadas no Brasil, como políticas públicas.

Palavras-chave: Segurança cibernética. Políticas públicas. Ambiente marítimo.

CYBER SECURITY MEASURES FOR THE MARITIME ENVIRONMENT: A HYBRID ANALYSIS OF PROPOSALS AND TRENDS IN THE BRAZILIAN CONTEXT

ABSTRACT

This study presents the importance of cyber security in relations of power, in the context of international relations and in maritime security issues, bringing to light the need to face this problem. The risks and mitigation measures identified since 2017 are presented through a systematic review in SCOPUS, IEEE Explore, ACM Digital Library and Google Scholar databases. Data obtained through data mining in Brazilian and American political documents are analyzed. In addition, the results of a questionnaire answered by Brazilian civil society, researchers and the military are presented, with the aim of gathering the perception of these groups, on the subject of cybersecurity in the Brazilian context. Thus, the results obtained allow to conclude that there are signs that a greater presence of the subject in official documents at a political level translates into higher levels of cyber security. It is also noticed that the presence of the topic in Brazilian documents is not at a satisfactory level, a fact reinforced by the results of the questionnaires. It is noted that the subject has gained increasing importance over the years and that the identified mitigation measures have the potential to be implemented in Brazil as public policies.

Key words: Cyber security. Public policy. Maritime environment.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTAS DE SIGLAS E ABREVIATURAS

IMO	*International Maritime Organization*
EUA	Estados Unidos da América
CREDN	Comissão de Relações Exteriores e Defesa Nacional
ORCOM	Orientações do Comandante da Marinha
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
PRISMA	*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*
IEEE	*Institute of Electrical and Electronic Engineers*
ACM	*Association for Computing Machinery*
GPS	*Global Positioning System*
ECDIS	*Eletronic Chart Display and Information System*
MDA	*Maritime Domain Awareness*
OTAN	Organização do Tratado do Atlântico Norte
CNUDM	Convenções das Nações Unidas para o Direito do Mar
DICA	Direito Internacional dos Conflitos Armados
SOLAS	*Safety Of Live At Sea*
GMDSS	*Global Maritime Distress Safety System*
AIS	*automatic identification system*
BIMCO	*Baltic and International Maritime Council*
ISO	*International Organization for Standardization*
IEC	*International Electrotechnical Commission*
NIST	*National Institute of Standards and Technology*
NLTK	*Natural Language Toolkit*
CPEM	Curso de Política e Estratégia Marítima
CEMOS	Curso de Estado-Maior para Oficiais Superiores
LSC	Laboratório de Simulações e Cenários
EGN	Escola de Guerra Naval
PPGEM	Programa de Pós-Graduação em Estudos Marítimos
IMM	Instituto Meira Mattos
CoNavOpEsp	Comando Naval de Operações Especiais
SICCCIBER	Segurança da Informação, das Comunicações, dos Computadores e do Espaço Cibernético

UFF	Universidade Federal Fluminense
LIDAR	*Laser Imaging Detection and Ranging*
WTA	*Worldwide Threat Assessment*
NCSI	*National Cyber Security Index*

SUMÁRIO

INTRODUÇÃO

Vive-se em uma era de crescente dependência de sistemas computadorizados. A automação industrial e diversos sistemas de controle e sensoriamento tornam-se cada vez mais dependentes de complexos módulos eletrônicos, conectados em redes de computadores, que gerenciam grande parte dos processos de forma autônoma. Porém, as vulnerabilidades desses sistemas têm sido exploradas de diversas maneiras. A literatura (PARCHARIDIS, 2018; FERRARI *et al.*, 2020) identifica e realiza simulações de ataques cibernéticos maliciosos que foram desenvolvidos para prejudicar o funcionamento e, em casos recentes, afetar o mundo físico através da manipulação de atuadores controlados eletronicamente. Essas simulações fornecem informações técnicas fundamentais para o entendimento da dinâmica de ataques híbridos – *i.e.*, que não se restringem ao domínio cibernético (SÁ, MACHADO e ALMEIDA, 2019). Esses atos hostis, que exploram os domínios físico e cibernético, demonstraram grande capacidade de afetar instalações sensíveis, transformando-se em meios eficazes para alcançar objetivos estratégicos. Segundo Sanger (2018), uma usina nuclear iraniana, de Natanz, teve seu funcionamento prejudicado em virtude de um ataque cibernético envolvendo o vírus *Stuxnet* e o serviço de distribuição de energia elétrica ucraniano sofreu um mau funcionamento provocado por um vírus denominado *Killdisk*, ambos os ataques supostamente conduzidos por Estados.

O ambiente marítimo não está imune a esse tipo de ameaça (HAYES, 2016). Em 2011 a estatal iraniana responsável pelo controle portuário foi vítima de um ataque que embaralhou os registros de containers, corrompendo os controles de localização e conteúdo, causando um grande prejuízo logístico. Entre 2011 e 2013, O terminal portuário da Antuérpia, na Bélgica, foi alvo de um ataque patrocinado por traficantes de drogas. Esse ataque cibernético proporcionou acesso ao controle de inventário de containers, possibilitando que os traficantes liberassem containers para retirada sem que fossem devidamente inspecionados. Em 2013 uma plataforma de perfuração e prospecção de petróleo e gás, baseada no golfo do México, foi vítima de um ataque responsável por paralisar os sistemas de navegação. Assim, a plataforma perdeu a capacidade de manter a posição, causando a interrupção da extração.

Na área dos sensores de navegação que exploram o espectro eletromagnético, a conversão de sinais analógicos para digitais possibilitou a ampliação da capacidade operacional. Esse processo permite a representação de dados analógicos em binários e promove a integração dos radares com sistemas computacionais (FALLEIRO, 2015). Assim, o processamento de dados digitais torna-se cada vez mais presente em sistemas eletrônicos de sensoriamento. No entanto, ao mesmo tempo em que a interface desses sensores com o espectro eletromagnético

os torna vulneráveis a Guerra Eletrônica, a componente digital dos mesmos os torna susceptíveis a ataques cibernéticos (SÁ, MACHADO e ALMEIDA, 2019).

Isto significa que sistemas baseados na integração entre sensores eletromagnéticos e sistemas computacionais podem ser vulneráveis a ataques que atuem na interseção entre a guerra eletrônica e a guerra cibernética, também conhecidos como ataques ciber-eletrônicos. Os meios militares empregam extensivamente tecnologias desse tipo e ao analisar, por exemplo, uma plataforma naval moderna verifica-se que diversos sistemas podem ser alvo de ataques ciber-eletrônicos (SÁ, MACHADO e ALMEIDA, 2019).

Dessa forma, percebe-se que o crescente emprego de sistemas computacionais a bordo de embarcações e instalações marítimas, como portos e plataformas, significa um maior espaço para a atuação de agentes maliciosos através do ambiente cibernético. A possibilidade de utilização de ataques híbridos agrava ainda mais esse quadro, pois ataques que antes só poderiam ser conduzidos através de computadores e redes podem ser executados por meio do espectro eletromagnético, e ter impactos físicos. Nesse contexto, a Organização Marítima Internacional (IMO, sigla em inglês) (2017) manifestou sua preocupação através de documento oficial, onde emite recomendações de alto nível para o gerenciamento de riscos cibernéticos em instalações marítimas. É importante comentar que esse movimento foi acompanhado por Estados como os Estados Unidos da América (EUA), através do *National Maritime Cybersecurity Plan* (EUA, 2020b), e pelo Reino Unido, através do *Code of Practice: Cyber Security for Ships* (REINO UNIDO, 2017).

Objetivos

Este trabalho tem como objetivo geral verificar se o Estado brasileiro trata o tema de forma satisfatória e identificar vulnerabilidades e medidas mitigatórias, concernentes ao gerenciamento de riscos cibernéticos em meios e instalações marítimas, analisadas pela comunidade acadêmica internacional após orientações da IMO, em 2017. Dessa forma, poderão ser fornecidos subsídios para que a MB possa elaborar novas ações e propostas de orientações para reforçar a segurança cibernética no mar.

Para obter o resultado esperado, busca-se a consecução dos seguintes objetivos específicos:

a) Compreender a importância da segurança cibernética marítima na dinâmica de poder internacional e em questões de segurança.

b) Revisar, de forma sistemática, a literatura, em bases de dados internacionais, sobre riscos cibernéticos no mar e ações para mitigá-los;
c) Analisar a incidência de termos relacionados à segurança cibernética, de maneira ampla (não apenas no escopo do setor marítimo), em documentos oficiais de nível político, para identificar tendências relacionadas a políticas para gestão de riscos cibernéticos;
d) Identificar a perspectiva de pesquisadores e especialistas sobre o assunto, a partir dos dados gerados nos objetivos “b” e “c”.

Tema

A pesquisa se enquadra no estudo de políticas públicas de segurança cibernética no ambiente marítimo, e sua discussão nos contextos nacional e internacional. Se colocando, dessa forma, nos campos da ciência política e das relações internacionais.

Delimitação do Tema

São analisadas propostas para o incremento da segurança cibernética no ambiente marítimo posteriores a orientação sobre risco cibernético da IMO (2017) até o presente. Também são estudados, através de técnica de mineração de dados em texto, o comportamento do Estado brasileiro no nível político, tendo como referência documentos oficiais como o relatório anual da Comissão de Relações Exteriores e Defesa Nacional (CREDN) da câmara dos deputados e os Orientações do Comandante da Marinha (ORCOM), de 2006 até 2020. É importante ressaltar que este estudo se dedica a análise de segurança cibernética em meios e instalações marítimas de maneira geral e que, dessa forma, não serão abordados temas exclusivamente militares.

Justificativa

O presente estudo contribui para o incremento da consciência situacional, nos campos das ciências políticas e das relações internacionais, em relação a medidas de aprimoramento da segurança cibernética no ambiente marítimo que vem sendo propostas desde a emissão de orientação específica pela IMO (2017). O trabalho serve como material para assessoria às autoridades navais em questões afetas ao assunto e embasará propostas de políticas públicas.

Vale ressaltar que a Estratégia Nacional de Defesa identifica a segurança cibernética como um dos pontos fundamentais para a garantia dos interesses nacionais brasileiros (BRASIL, 2020a). Por isso, um estudo que contribua para o assunto possui valor estratégico.

Objeto

A pesquisa está direcionada ao estudo de políticas de segurança cibernética no ambiente marítimo.

Problema

A IMO (2017) sugere que a segurança cibernética a bordo de embarcações seja discutida nos contextos nacional e internacional, e incentiva a participação dos Estados membros. De acordo com o entendimento da organização, essa discussão possibilitará o surgimento de requisitos e normas de segurança cibernética capazes de fortalecer o setor marítimo. Nesse contexto, entende-se que o Brasil, componente dessa organização, deve envidar esforços para pesquisa e desenvolvimento nessa área. A título de esclarecimento, a Doutrina Militar Naval (BRASIL, 2017) explana a separação dos níveis de decisão em político, estratégico, operacional e tático. De maneira geral, o nível político se refere a decisões da esfera do governo federal, o nível estratégico está relacionado com a dimensão ministerial, o nível operacional está ligado ao planejamento e condução de forças operativas em situação de conflito e o nível tático é o responsável pela execução das ações. Nesse contexto, as esferas inferiores têm o dever de traduzir as orientações e determinações das esferas superiores para o seu nível.

No Brasil, os setores cibernético, nuclear e espacial são considerados estratégicos e foram designados para o Exército, Marinha e Aeronáutica, respectivamente. No setor cibernético ainda se observa uma divisão entre *Segurança Cibernética*, no nível político, e *Defesa Cibernética,* nos níveis estratégico, operacional e tático. O Gabinete de Segurança Institucional da Presidência da República (GSI/PR) atua no campo da segurança cibernética, enquanto o Exército gerencia a defesa cibernética (BRASIL, 2019). É importante destacar que a Doutrina Militar Naval (BRASIL, 2017) afirma, conforme a Lei Complementar nº97 de 9 de junho de 1990 (BRASIL, 1999), que é papel da Autoridade Marítima, função da Marinha do Brasil, garantir a segurança marítima. Dessa forma, considerando as peculiaridades do meio naval, é conveniente que a Marinha contribua para a formulação de políticas em consonância

com as orientações da IMO, incluindo, portanto, questões afetas a segurança cibernética no ambiente marítimo.

Questão Básica

A pesquisa busca identificar se há medidas de segurança cibernéticas, específicas para o meio marítimo, propostas pela comunidade acadêmica internacional que apresentem potencial para serem implementadas no Brasil, como políticas públicas.

Questões Secundárias

Também são produzidas respostas para os seguintes questionamentos:

a) A presença do tema segurança cibernética nas ORCOM e nos relatórios da CREDN são compatíveis com as necessidades brasileiras?
b) A presença do tema segurança cibernética nas ORCOM acompanha a tendência dos relatórios da CREDN da câmara dos deputados?

Hipótese e Pressupostos

A hipótese central da pesquisa é a de que há medidas de segurança cibernética, focadas no meio marítimo, propostas pela comunidade acadêmica internacional que podem servir de base para a criação de políticas públicas no Brasil. Tem-se como pressuposto que o ritmo de estabelecimento de políticas de segurança cibernética deriva diretamente do grau de discussão do tema em documentos oficiais de nível político.

Metodologia

As discussões sobre os métodos mais apropriados para o desenvolvimento científico são especialmente polarizadas entre os acadêmicos que defendem os métodos de ciências humanas e os que defendem os métodos de ciências exatas. Nas ciências humanas percebe-se a predominância de métodos interpretativos e a exploração da sensibilidade do pesquisador, enquanto nas ciências exatas são evidenciados os métodos fortemente baseados no raciocínio lógico, que não admitem interpretações de seus resultados (BERLIN, 1980). Nesse contexto,

esse trabalho sugere a aplicação de um arranjo metodológico híbrido, empregando técnicas quantitativas e qualitativas para chegar ao resultado.

São empregadas técnicas de revisão sistemática de literatura e mineração de dados em texto. Os resultados da revisão sistemática são analisados e usados como subsídios para a construção de questionários. A pesquisa testa a hipótese e o pressuposto, ambos de caráter exploratório. Conforme Van Evera (1997), hipóteses exploratórias buscam, também, explicações sobre dinâmicas relacionais. Essas explicações podem inclusive levar à identificação de outras questões.

É utilizado o método indutivo para analisar os dados obtidos e transportá-los para um contexto mais abrangente. De maneira geral, "indução é um processo mental por intermédio do qual, partindo de dados particulares, suficientemente constatados, infere-se uma verdade geral ou universal, não contida nas partes examinadas" (MARCONI E LAKATOS, 2003).

Revisão Sistemática de Literatura

O procedimento de revisão sistemática de literatura está pautado em um roteiro para busca e análise de artigos, em bases de dados acadêmicas. O objetivo do método é potencializar a imparcialidade do estudo, fazer com que seja o mais completo possível e facilitar a reprodução das buscar por pares. É empregada uma adaptação do previsto no guia *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) (LIBERATI *et al*., 2009). O universo para a revisão de literatura será composto pelas bases de dados *Scopus*, *Institute of Electrical and Electronic Engineers* (IEEE*) Explore*, *Association for Computing Machinery* (ACM) *digital library*, *Open Grey* e *Google Scholar*.

Mineração de Dados em Texto

As tecnologias da ciência de dados são cada vez mais difundidas e fornecem ferramentas inestimáveis para a pesquisa científica (KATSURAI, 2017). Uma dessas técnicas é a *mineração de dados em texto*, onde informações quantitativas são extraídas de fontes qualitativas, como documentos e discursos. O método é implementado através de aplicações computacionais, com objetivos de análise definidos pelo programador. É importante comentar que a automatização do processo possibilita a análise de grandes massas de dados, em muito menos tempo do que seria necessário sem o emprego da técnica. vale ressaltar que esses dados também se tornam subprodutos muito interessantes. No presente trabalho, são analisados documentos ostensivos

de nível político e estratégico e refletem a postura do Estado brasileiro e da Autoridade Marítima acerca da segurança cibernética, de 2006 até 2020.

Questionário

A utilização de questionários objetiva formar uma representação quantitativa/qualitativa da percepção de um determinado assunto, a partir de informações dadas por uma parcela de indivíduos pertencentes a um determinado grupo de interesse (GERHARDT e SILVEIRA, 2009). As informações para a elaboração do questionário utilizado são originadas a partir dos produtos da revisão sistemática de literatura. Dessa forma, a presente pesquisa emprega essa técnica para colher a opinião de pesquisadores, de áreas relacionados à segurança cibernética e defesa, e da sociedade como um todo, sobre o tema em questão.

Embasamento Teórico

O desenvolvimento tecnológico forneceu uma série de equipamentos capazes de otimizar processos característicos de instalações marítimas moveis e estáticas. Dentre esses processos é possível citar o de geolocalização, para instalações móveis, e o de controle de estoques de carga, em instalações portuárias. Hoje a presença de sistemas cibernéticos a bordo é notável e, cada vez mais, essencial para a operação de tais instalações. Entretanto, essas mesmas ferramentas podem ser exploradas por indivíduos com intenções maliciosas.

Em (BHATTI e HUMPHREYS, 2017), os autores avaliam a hipótese de ataques eletro-cinéticos (SÁ, MACHADO e ALMEIDA, 2019) serem lançados contra sistemas de navegação *Global Positioning System* (GPS). É possível privar um alvo do acesso aos sinais de GPS. Além disso, é possível inserir informações de posição adulteradas no sistema alvo. Em navios modernos os sistemas de auxílio a navegação estão cada vez mais integrados. Os sistemas GPS, piloto automático, controle de velocidade e outros, se comunicam com um sistema integrado de navegação, *Eletronic Chart Display and Information System* (ECDIS). Nesse cenário, Hayes (2016) aponta casos em que plataformas marítimas foram alvos de ataques cibernéticos responsáveis por grandes prejuízos, a nível nacional.

No âmbito dos sistemas radar, a conversão analógico-digital possibilita a integração entre estes sensores eletromagnéticos e sistemas computacionais (FALLEIRO 2015). Esse fato promove um grande incremento na capacidade dos sistemas que utilizam essa tecnologia, pois as informações obtidas por eles podem ser processadas e apresentadas de forma otimizada.

Porém essa tecnologia abre as portas dos sistemas computacionais envolvidos para ataques deflagrados a partir do espectro eletromagnético e captados por sensores. Sá, Machado e Almeida (2019) apresentam como exemplo a operação *Orchard* – ação militar conduzida pelo Estado de Israel em 2007 contra alvos estratégicos sírios. Na referida operação, um conjunto de aeronaves israelenses realizaram um bombardeio em território sírio sem que fossem detectados pelos radares aéreos inimigos.

Esse fato levantou diversos questionamentos sobre as técnicas que poderiam ser utilizadas para atingir tamanho nível de furtividade. Neste caso, a literatura (ADEE, 2008) aponta para a possibilidade de uso de um sinal eletrônico em coordenação com um mecanismo cibernético previamente instalado nos sistemas sírios. Adee (2008) chama esse tipo de mecanismo de *Kill Switch*. O ataque eletrônico teria sido empregado para transmitir um sinal eletromagnético que após recepção, e conversão para linguagem de máquina, foi capaz de ativar o gatilho digital alojado no sistema a fim de adulterar a imagem apresentada na tela do radar (ADEE, 2008; SÁ, MACHADO e ALMEIDA, 2019). Assim os operadores não foram capazes de detectar as aeronaves antes da execução dos ataques.

Uma pesquisa recente, de autores brasileiros, demonstra a possibilidade de emprego de ataques híbridos, que atuam nas dimensões eletrônica e cibernética, empregando técnicas relativamente simples de processamento de dados para afetar sistemas radar (LEITE JUNIOR e SÁ, 2020). Esse mesmo estudo foi expandido, empregando a mesma lógica de ataque para outros sistemas de navegação, como o AIS (LEITE JUNIOR, *et al.*, 2021). A exploração desses conceitos sinaliza para os riscos da aplicação dessas técnicas com objetivos hostis. Esses estudos não foram incluídos na revisão pois foram indexados após a data de realização das buscas nas bases de dados utilizadas na revisão sistemática.

Essas técnicas despertam preocupações de autoridades, e devem ser levadas em consideração no ambiente marítimo. As orientações da IMO (2017) sobre gerenciamento de risco cibernético a bordo representam uma formalização dessa preocupação para a comunidade internacional e um incentivo para que esse assunto seja discutido. No contexto nacional, constata-se um esforço político na consolidação de marcos em relação a segurança cibernética (BRASIL, 2019). Porém, nota-se ainda uma carência em questões específicas do meio marítimo. Por isso, a produção de conhecimento nesse sentido é de grande valia para a administração pública nacional.

Estrutura

O Trabalho de Conclusão de Mestrado (TCM) é organizado conforme a estrutura descrita a seguir:

INTRODUÇÃO, expõe objetivo, justificativa, objeto e problema abordado no trabalho. Também promove uma breve contextualização sobre os assuntos tratados e apresenta a metodologia empregada.

O capítulo 1, REFERENCIAL TEÓRICO, promove a compreensão de assuntos fundamentais para o entendimento do trabalho. Comenta sobre conflitos nas sociedades humanas e como o processo político organiza as relações de disputa intraestatais. Introduz o pensamento de poder para o Estado e o papel do mar no desenvolvimento das estratégias nacionais. Também menciona questões contemporâneas de segurança no mar e as ameaças cibernéticas presentes na atualidade, com especial foco no ambiente marítimo. Por fim, expressa uma conclusão parcial.

O capítulo 2, FERRAMENTAS, apresenta as técnicas de revisão sistemática de literatura, mineração de dados em texto e elaboração de questionários, empregadas na obtenção dos resultados.

O capítulo 3, RESULTADOS E DISCUSSÃO, apresentará os resultados obtidos e uma discussão acerca deles.

Finalmente, o capítulo 4, CONCLUSÃO, completa o TCM, apresentando as conclusões e considerações finais referentes ao trabalho, assim como sugestões para trabalhos futuros.

1 REFERENCIAL TEÓRICO

Para a melhor compreensão dos objetivos e resultados do presente trabalho, este capítulo promove um breve panorama conceitual. São apresentados conceitos básicos sobre conflitos e poder nas relações humanas e entre Estados, a dinâmica política nas relações intraestatais, uma singela exposição da evolução do pensamento estratégico marítimo e questões de segurança relacionadas ao mar, com especial destaque para o campo da segurança cibernética, e uma conclusão parcial.

1.1 O Conflito nas Relações Humanas e no Desenvolvimento do Estado

O ponto de partida para esta breve contextualização é o *estado de natureza*. Esse estado seria o que os primeiros seres humanos viveram antes que as sociedades fossem formadas. O conceito possui diferentes interpretações, dentre as quais destacam-se as visões de Hobbes, Rousseau e Locke (FREUND, 1995). Para o primeiro, esse estado é caracterizado como naturalmente conflituoso, pois há uma liberdade irrestrita. Assim, o mais forte teria a prerrogativa de impor sua vontade aos mais fracos, sem qualquer restrição. Para o segundo, o estado de natureza era naturalmente pacífico, e todos os seres humanos viveriam em harmonia e compartilhariam os recursos disponíveis. O fato gerador da violência na segunda visão seria a propriedade privada, os conflitos teriam tido origem quando um indivíduo se considerou dono de algo que deveria proteger. O último defende que o homem nasce com direitos inalienáveis à vida, liberdade e propriedade.

Para solucionar os problemas relacionados aos conflitos foram criadas organizações que se caracterizam como: contrato social. Para a primeira visão, o contrato social está baseado na premissa de que o indivíduo deve renunciar a sua liberdade, característica do estado de natureza, para ganhar proteção contra a violência de seu ambiente. A ordem seria mantida através de uma entidade superior e soberana, o Estado, com o monopólio da violência e poder para impor regras sociais. Para a segunda visão, o contrato social foi criado como forma de impor a propriedade privada, invalidando a visão de que todos deveriam partilhar os recursos disponíveis. Locke apresenta uma interpretação próxima a de Hobbes, porém afirma que mesmo o Estado não poderia privar o homem de seus direitos inalienáveis. É importante destacar que essas visões estão avaliando sociedades e regramentos internos a elas, mas não estão levando em consideração conflitos entre sociedades.

Independentemente da linha de pensamento adotada, é possível entender que a interação entre seres humanos é um potencial fator de conflito (MALESEVIC, 2014). Sendo assim, pode-se pensar que em um mundo hipotético, onde indivíduos vivem isoladamente, não haveria conflito. Conforme Aristóteles (MARCONDES, 2007), esse mundo não seria possível pois o homem é um animal social. A necessidade de perpetuação da espécie é um exemplo de fator que faz com que a interação entre pares seja mandatória, a reprodução só é possível a partir do contato entre indivíduos de sexos opostos. Dessa forma, Aristóteles entende que o ser humano necessita de outros para realizar sua humanidade. Assim, a vida em sociedade seria inevitável para o homem. De forma análoga, pode-se expandir essa visão para o relacionamento entre Estados.

Entretanto, uma sociedade compreende indivíduos com diferentes antecedentes e opiniões. É natural que em situações em que uma escolha se faz necessária, diferentes posicionamentos sejam levantados em um determinado grupo social. Dessa forma, observa-se a fagulha que pode dar origem às disputas (CENTENO e ENRIQUEZ, 2016). É importante destacar que, mesmo quando há acordo sobre o que deve ser feito, a maneira de atingir um determinado objetivo também é uma possível fonte de conflitos. Assim, verifica-se que as sociedades não eliminam conflitos, apenas os organizam. Três tipos possíveis de conflitos no contexto do contrato social, conflitos internos a uma sociedade, entre sociedade e Estado e entre modelos de Estado. O contrato social só seria capaz de evitar o primeiro tipo.

Para Aristóteles, como comentado anteriormente, a sociedade é um fenômeno natural para os seres humanos, logo não haveria necessidade de contrato social. Essa visão ficou em evidência após a revolução francesa, que serviu como demonstração de que uma sociedade poderia quebrar o contrato com o regime dominante. A revolução industrial trouxe um novo contexto, a aceleração da produção gerou a expectativa de em algum momento haveria abundância de produtos para todos os indivíduos do mundo. Ao analisar a natureza dos conflitos, pode-se considerar que eles se devem à disputa por recursos limitados (MALESEVIC, 2014). Dessa forma, entende-se que a produção em larga escala poderia acabar com os conflitos. Assim, Saint-Simon chegou à conclusão de que os recursos produzidos seriam naturalmente divididos entre os seres humanos, trazendo a paz.

Marx e Engels (2005) foram os responsáveis por desenvolver o pensamento de que essa divisão não era tão simples assim. A abundância de recursos não seria igualmente distribuída, mas obedeceria a uma tendência histórica de acumulação pelas classes privilegiadas. Além da acumulação de recursos econômicos, esse contexto levaria a alienação humana, pois as classes menos favorecidas seriam privadas do desenvolvimento intelectual necessário para o

questionamento da ordem vigente. Porém, o conflito era inevitável, pois em algum momento as classes exploradas seriam levadas à luta por direitos. Essa luta terminaria na tomada do poder pelos menos favorecidos, o que levaria a distribuição igualitária dos recursos. Observa-se que o conflito estaria presente, mesmo com a abundância de recursos, e a paz só seria alcançada após o fim da luta entre classes.

A visão sociológica dos conflitos posterior a Marx, capitaneada por Max Weber, Simmel, Pareto e Durkheim, volta a analisar o conflito como inerente às sociedades (FREUND, 1995). Nesse contexto, a paz seria apenas um período excepcional. Isso ocorre, pois a unanimidade é praticamente impossível dentro de um grupo social e divergências de opiniões sempre levam a conflitos. Porém, interpreta-se que os resultados dos conflitos não são sempre necessariamente prejudiciais.

1.1.1 O Papel da Violência

Segundo Freund (1995), os estudos da violência e dos conflitos na organização dos Estados não são comumente abordados em estudos sociológicos. Entretanto, ao observar autores clássicos percebe-se que nem sempre foi assim. Houve um período em que o estudo da violência esteve intimamente relacionado ao entendimento sociológico de Estado. Porém, as grandes guerras fizeram com que esse pensamento fosse correlacionado com o comportamento de governos totalitários e militaristas, fazendo com que as abordagens dos pós Segunda Guerra se mantivessem afastadas do assunto (FREUND, 1995). Dessa forma, os principais autores da sociologia moderna, Marx, Weber e Durkheim, abordaram a violência de um ponto de vista mais distante. Para Durkheim, a violência seria uma condição patológica a ser superada pela humanidade. Porém esse mesmo autor identificou que em situações de guerra as taxas de suicídio apresentavam uma queda significativa. Para Marx, a violência seria um mecanismo de mudança de ordem social e uma ferramenta de coerção capitalista sobre o mundo. Weber, em sua discussão sobre a vida política do homem, reflete sobre o papel fundamental da disciplina militar no estabelecimento de ordens sociais. Esse autor também identifica a violência como um instrumento político de um Estado sobre sua população ou sobre outros Estados. Um terceiro ponto bordado por Weber é que a formação das elites possui raízes na história militar, pois trata-se de uma influência construída ao longo dos anos pelas elites responsáveis por atividades bélicas. Dessa forma, percebe-se que mesmo em um plano secundário, a violência possui um papel fundamental nas análises sociológicas.

O pensamento social no século 19 e do início do século 20 apresentam um foco muito maior no comportamento conflituoso, em especial na Alemanha (MALESEVIC, 2014). Para Heinrich von Treitschke, autor alemão, o poder estatal se resume a sua capacidade de impor a sua vontade, e a própria criação do Estado se dá através da imposição de sua existência a uma população. Dessa forma, a posse de uma força militar é essencial para a manutenção do Estado. Otto Hintze, estudante do autor anterior, afirma que a organização de um Estado é construída a partir de uma organização militar prévia. Carl Schmitt afirma que a vida social é baseada em relações de poder pautadas no princípio *nós contra eles*. Esses três autores concordam na ideia de que o poder coercitivo faz parte da estrutura das sociedades. Ludwig Gumplowicz vê o Estado como um produto de relações violentas entre grupos. Após a vitória de um grupo sobre outro, são estabelecidas normas sociais para a imposição da vontade dos vitoriosos. Gustav Ratzenhofer, de forma semelhante, percebe que apenas através da violência, ou da ameaça dela, é possível impor interesses aos demais componentes de uma sociedade. Lester Ward argumenta que situação de conflito são inerentes ao processo de socialização e de construção de suas estruturas. Franz Oppenheimer concorda com esse ponto de vista ao afirmar que o Estado é uma instituição criada para impor a vontade do vencedor aos vencidos. Esse autor identifica ações sociais políticas, tipicamente violentas, e ações econômicas, tipicamente pacíficas, e apresenta uma visão otimista ao afirmar que há uma tendência de que ações econômicas predominem no futuro. Vilfredo Pareto e Gaetano Mosca abordam a teoria das elites, que afirma a alternância de elites no poder de um Estado. Nesse contexto a violência funcionaria como um meio através do qual uma elite, minoria, exerceria sua vontade sobre a maioria. Além disso, a violência também se daria como um mecanismo de transição de poder entre elites. A teoria evolucionária, ilustrada pelos autores Herbert Spencer e William G. Sumner, apresenta uma abordagem biológica das relações sociais, recorrendo a teoria da evolução como ferramenta. Dessa forma, entende-se que o organismo mais adaptado prosperará. Em um mundo violento, a adaptação significa o desenvolvimento de capacidades militares para proteção e imposição de poder. Já Georges Sorel e Georg Simmel percebem a violência como uma necessidade social, pois sem ela não há mudanças nas relações.

Assim, nota-se que os estudos da violência e dos conflitos apresenta uma estreita relação com a sociologia intraestatal, e precisa ser tratado como tal (MALESEVIC, 2014). Ainda existe uma carência na abordagem do assunto pela corrente principal da sociologia, porém há um amplo campo para atuação no que se refere a pesquisa. Uma das abordagens contemporâneas faz referência ao Darwinismo, resgatando argumentos biológicos para explicar comportamentos violentos. Ao longo do processo evolutivo, os organismos que apresentaram

maior capacidade de resistir a aplicar a violência se perpetuaram, dessa forma seria natural que a violência estivesse no subconsciente humano. Os fundamentos culturais e sociais seriam uma consequência da herança genética. O principal problema com essa abordagem é o subdimensionamento das influências culturais e ideológicas no comportamento violento. Um outro problema é que, considerando que a violência é instintiva, esse ponto de vista ignora a burocratização das instituições militares. Uma outra visão seria a econômica. Dessa forma, a violência se daria na disputa por recursos econômicos entre povos. Entretanto, essa abordagem apresenta a limitação de subdimensionar impactos de outros fatores sobre os conflitos. Há duas correntes com maior relevo nessa visão, a *globalisation theory* e a *rational choice of social action*. Na primeira, a violência se intensificaria em decorrência dos processos globalizantes, pois a possibilidade de exploração de recursos de outros Estados motivaria comportamentos violentos. A segunda afirma que os conflitos seriam conduzidos a partir de uma relação de custo-benefício, sendo evitado em situações de possível prejuízo. Há também a vertente cultural, ilustrada pelo pensamento de Samuel P. Huntington, que afirma a relação direta entre os conflitos e as diferenças culturais entre civilizações. Entretanto, essa perspectiva não é capaz de explicar as origens ou a persistência de conflitos, os estudos de caso apresentados pelo autor são fortemente influenciados pela geopolítica e também desconsideram a possibilidade de as próprias culturas já serem o produto de conflitos. O materialismo organizacional é apresentado como uma teoria para o entendimento da formação dos Estados, e está fortemente baseada na violência. Essa teoria afirma que a primeira organização social teria se originado através de um conflito e essa organização teria passado por diversos outros conflitos até a formação do Estado moderno. Dessa forma, a estrutura do Estado nação seria um produto de diversas interações conflituosas que contribuíram para a formação das instituições de um determinado Estado, explicando assim todos os vieses presentes na estrutura social.

1.1.2 O Papel da Guerra

Ao observar a história, é possível perceber que a violência organizada é relativamente recente (FREUND, 1995). Isso não significa dizer que o ser humano é naturalmente pacífico, apenas que agressões isoladas não podem ser consideradas conflitos organizados. O advento da guerra enquanto instituição foi sendo construído ao longo do tempo, tendo como base uma série de características psicológicas e sociais. Estima-se que antes da consolidação da agricultura e da vida urbana houve poucos atos organizados de violência. Porém, a partir da adoção do sedentarismo, foi necessário que os agrupamentos humanos desenvolvessem mecanismos para

garantir a sua própria segurança. Para isso, foi necessário desenvolver sistemas burocráticos que permitissem a administração dos recursos, humanos e materiais, disponíveis. Nesse contexto, é possível notar a articulação de um aparelho burocrático rudimentar que deu origem a uma série de atividades, como registros públicos, estratificação social, identidade cultural e sistemas de crenças. Os conflitos entre agrupamentos, utilizados para a imposição da vontade de um grupo sobre outro, também são um fator importante para compreender o processo de estratificação social. Nesses casos, o grupo mais forte se estabelece como uma classe superior em relação aos derrotados. Esses conflitos estavam diretamente relacionados com a geopolítica local e com a disponibilidade de recursos de subsistência. De forma semelhante, a atividade de coerção interna contribui para a construção do aparelho burocrático, pois também exige organização.

Os atos organizados de violência na antiguidade foram, de maneira geral, fundamentados na obtenção de recursos de grupos mais fracos pelos que tinham maior capacidade bélica (MALESEVIC, 2014). O estabelecimento da supremacia de uma sociedade sobre outra gerou a estratificação social, com especial destaque para os guerreiros. Nesse contexto, as sociedades que empregavam camponeses como guerreiros em determinadas situações apresentavam maior tendência democrática pois precisavam da lealdade do povo. É importante destacar que a magnitude dos conflitos na antiguidade era muito reduzida quando comparados aos atuais. Com o passar do tempo, notou-se a necessidade de profissionalização da violência, ilustrada pela figura do militar profissional. Roma foi responsável por uma das primeiras implementações desse conceito e demonstrou um significativo avanço organizacional.

A queda do império romano causou muitas perdas em relação a organização do Estado. A adoção do regime feudal, baseado em relações de interdependência entre senhores e vassalos, fez com que a atividade militar ficasse restrita aos nobres, isso acentuou ainda mais a estratificação social e gerou retrocessos em relação aos direitos individuais. A religião cristã surgiu como principal fator de legitimação de poder. Apesar de ser retratada como uma época de violência extrema, os conflitos eram de baixa intensidade e a quantidade de mortos era muito reduzida. A maior parte dos óbitos ocorria durante fugas do campo de batalha. Além disso, a qualidade dos armamentos não favorecia a letalidade. Os avanços tecnológicos disponibilizaram novas ferramentas, como a pólvora, que foram responsáveis por alterar significativamente a dinâmica dos conflitos. As metodologias e práticas militares tiveram que ser revistas, e iniciou-se o processo que levaria aos grandes exércitos, baseados no recrutamento em massa. As reformas religiosas também causaram grande impacto nesse contexto, pois

reduziram a influência religiosa e introduziram a secularização ideológica. A organização e disciplina voltaram a ser cultivadas no meio militar, que passou a abordar diversas classes sociais. Os exércitos passaram a ser compostos por uma parcela de militares profissionais e uma grande massa de indivíduos recrutadas para esforços de guerra. Isso exigiu o desenvolvimento de novas regras de conduta, cada vez mais abrangentes, para possibilitar o controle dessas grandes massas. Academias militares foram criadas para pensar o melhor emprego das novas tecnologias no campo de batalha e aprimorar o nível de instrução dos oficiais. Para que tudo isso fosse possível, foi necessário implementar uma máquina pública capaz de recolher os tributos necessários para a manutenção de suas forças armadas e isso exigiu organização.

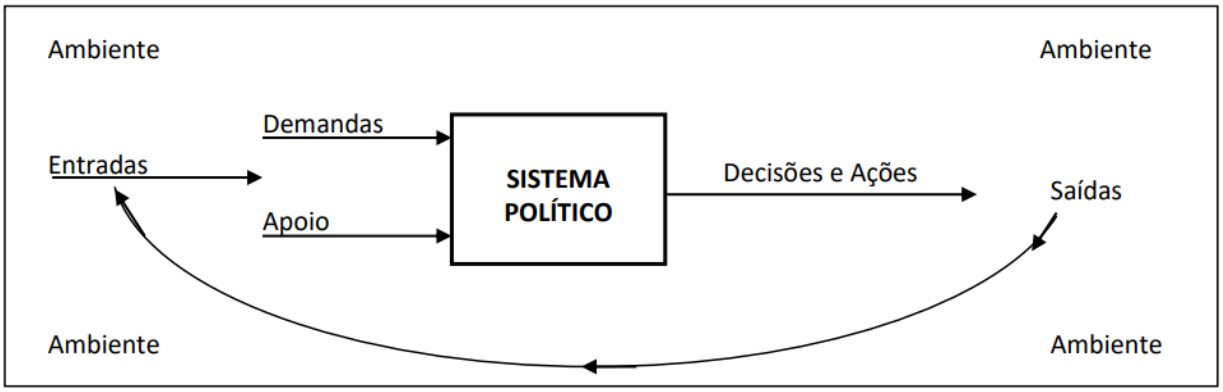
O sistema híbrido, baseado na profissionalização de uma parcela dos indivíduos e no recrutamento em massa por conscrição, gerou a necessidade de incentivar a população a lutar em defesa de seu Estado (MALESEVIC, 2014). Isso fez com que os governos se preocupassem em fornecer maiores direitos civis, para ganhar corações e mentes de seus cidadãos. Também foi necessário criar regulamentos e normas que possibilitassem uma padronização de comportamento pelas tropas. O serviço militar obrigatório por curtos períodos foi criado para apresentar as peculiaridades da vida militar para a população passível de recrutamento no futuro, servindo como um nivelamento profissional. A educação e a saúde públicas foram instituídas, entre outros motivos, para prover soldados mais preparados intelectualmente e mais saudáveis. Ao longo do tempo, os conceitos originados na necessidade de organização militar foram sendo expandidos para outras áreas da administração pública. Dessa forma, chegou-se a organização moderna dos Estados.

1.2 A Estrutura Política do Estado

Conforme apresentado anteriormente, a organização em sociedades não elimina os riscos de conflitos. Disputas ainda ocorrerão entre os grupos sociais que formam uma determinada sociedade. Entretanto, há uma organização formal sobre como as disputas serão solucionadas e isso se dá através da política. O termo política envolve um conjunto de fatores que podem ser representados por ação ou inação (HAM e HILL, 1993). O exercício político envolve conjuntos de decisões formais de governo tomadas de forma sistêmica em relação a um determinado objetivo, que pode mudar ao longo do tempo. A metodologia para essas decisões varia de acordo com a forma de governo em questão, mas, de forma geral, obedecem a ritos formais pré-estabelecidos. O modelo sistêmico de Easton (1965a, apud HAM e HILL,

1993), apresentado de forma gráfica na Figura 1, apresenta um modelo genérico do processo de tomada de decisões políticas.

Figura 1 - Modelo sistêmico de Easton



Fonte: HAM e HILL, 1993.

Observando a Figura 1 é possível notar que as demandas surgem a partir do ambiente, acompanhadas, ou não, pelo apoio de determinados atores. Essas entradas passam pelo devido processo político, de acordo com o rito local, e são traduzidas em decisões e ações que caracterizam uma política. Essas políticas geram resultados, que somados às condições preexistentes no ambiente, geram novas entradas no sistema, que está em perpétuo funcionamento.

1.2.1 Políticas Públicas

O estudo mais aprofundado das políticas públicas foi iniciado nos anos quarenta, para promover a compreensão de como determinadas decisões políticas são tomadas, entender seus efeitos e avaliar sua eficiência e eficácia (SOUZA, 2006). Assim, é possível entender que esse ramo do conhecimento busca fomentar ações governamentais, analisar seus efeitos e propor mudanças e adaptações nessas ações. O ponto de partida para a criação de uma política pública é a inserção do assunto na agenda política de um determinado governo. Essas questões podem ter origem quando a comunidade, como um todo, acredita que algo deve ser feito para solucionar um problema, quando um determinado grupo político-social levanta assuntos de seu interesse ou através da atuação de integrantes da sociedade como políticos, mídia, partidos e acadêmicos. Os mecanismos utilizados para levantar discussões são a divulgação de indicadores, eventos marcantes, como desastres, e os efeitos gerados pelo estabelecimento de políticas prévias.

1.3 O Poder e as Relações Internacionais

O surgimento do campo das relações internacionais no meio acadêmico se deu após a Primeira Guerra Mundial, como forma de entender esse fenômeno que apresentou horrores nunca observados na história humana (DUNNE, *et al*., 2016). Em um primeiro momento, duas grandes vertentes dominaram os debates sobre o tema, a corrente realista, pautada nas ideias de autores como Tucídides, Hobbes e Maquiavel, e a corrente liberal, fundamentada nos conceitos expostos por pensadores como Rousseau, Kant e Woodrow Wilson. Para a primeira vertente ficava claro que os Estados viviam em uma condição de alerta constante, sendo responsável por sua própria sobrevivência em um ambiente potencialmente hostil. Para garantir a sua existência era necessário manter uma substancial capacidade militar. Porém, sabendo que todos os demais Estados estariam em condições semelhantes de busca pela sobrevivência, não havia motivo para cessar o desenvolvimento bélico. Nesse contexto não há espaço para cooperação. Dessa forma, admite-se que, para o realismo clássico, a garantia de sobrevivência estatal no ambiente internacional seria a perpétua busca pela supremacia militar. Por outro lado, os liberais defendiam a ideia de que a humanidade estaria passando por um processo político evolutivo. Os regimes democráticos representavam um estado de evolução superior, pois ao observar a história era possível perceber a gradual redução da taxa de incidência de guerras. Assim, os liberais advogaram que com a proliferação de regimes democráticos as guerras terminariam.

O pós Segunda Guerra Mundial evidenciou falhas em ambas as linhas de pensamento e fez com que houvesse uma significativa revisão de conceitos (CASTRO, 2012). Os realistas passaram a adotar uma visão um pouco mais flexível. Mesmo estando em um ambiente extremamente hostil, era necessário manter apenas um nível de poder suficientemente grande para manter os adversários afastados. A cooperação seria possível, envolvendo Estados que não apresentassem concorrências mútua. Dessa forma, haveria a possibilidade de formação de alianças em relação a terceiros. Porém, o poder continuou a ser entendido como capacidades militares. Os liberais passaram a entender que o conflito de interesses não seria superado tão facilmente. Porém o advento da globalização, a intensificação do comércio internacional e o estabelecimento de métodos de comunicações e transportes eficientes para longas distâncias gerava uma intensificação na interdependência internacional. O desenvolvimento de laços comerciais e culturais cada vez mais intensos faria com que a ocorrência de conflitos se tornasse prejudicial a todos os envolvidos. Nesse contexto, os Estados ainda buscariam poder, mas esse

poder estaria mais relacionado a capacidades econômicas e culturais do que a capacidades bélicas.

Com o passar do tempo, novas interpretações foram se inserindo no arcabouço teórico das relações internacionais. Uma outra visão relevante é a visão construtivista, que afirma a relativização dos conceitos anteriores. O próprio conceito de poder seria uma construção que depende do contexto histórico (DUNNE, *et al.*, 2016). Em um determinado momento o poder poderia ser religioso, bélico, econômico ou outro, dependendo do momento do mundo e da situação em análise. Dessa forma, considera-se que o conceito de poder apresenta uma característica fluida, podendo se moldar de acordo com o contexto. Assim, é comum que se façam referências a parcelas de poder do Estado, como econômica e militar. Para esse trabalho é importante ressaltar os poderes Marítimo e Naval.

1.3.1 O Poder Marítimo e o Poder Naval

De acordo com o Plano Estratégico da Marinha, o Poder Marítimo pode ser entendido como o somatório de todas as capacidades das quais um determinado Estado dispõe para utilizar o mar, e águas interiores, nas dimensões política, econômica ou militar (BRASIL, 2020). Como exemplo de fatores componentes, é possível citar a Marinha Mercante, a Marinha de Guerra, infraestruturas portuária e hidroviária e instituições de ensino e pesquisa. O Poder Naval se refere à parcela militar desses fatores.

1.4 Estratégia Naval

Alfred Thayer Mahan, Oficial da marinha americana, organizou e apresentou de forma estruturada a influência do poder marítimo na história dos grandes Estados, com especial destaque para a Inglaterra. Mahan (1987) defende a ideia de que o domínio do mar, através de um poder marítimo sólido, é fundamental para a manutenção do desenvolvimento de um Estado, especialmente para aqueles que dependem em maior escala do comércio marítimo. Dessa forma, entende-se que o domínio dos mares é uma condição fundamental para o exercício do poder estatal no contexto internacional, pois garante a utilização do mar ao mesmo tempo em que pode negar aos rivais. Esse autor também defende que o papel do poder naval é ser empregado para garantir a supremacia nos mares através da guerra naval, e que o emprego de meios navais em atividades de suporte, como projeção de poder sobre terra, seria secundário.

Para o Almirante Phillip Colomb e para o teórico Julian Corbett (GOUGH, 1990), o poder naval deve ser utilizado de forma defensiva, enquanto para Mahan o poder naval deve ser utilizado de forma ofensiva para eliminar o poder dos inimigos. Entende-se que, para esses autores, atividades de suporte, como a defesa de comboios, não seriam atividades secundárias. Sendo assim, a estratégia naval de um Estado deve ser entendida como uma parte de uma estratégia maior de poder. O Almirante Herbert Richmond, outro grande nome entre os teóricos do poder marítimo, apresenta uma visão semelhante. Enfatiza a possibilidade de emprego do poder naval como garantia do controle de movimentos no mar, especialmente de natureza mercante.

Raoul Castex, Almirante francês, apresenta uma visão do poder naval a partir do ponto de vista de uma potência continental (GROVE, 2010). Ele afirma que batalhas no mar, em geral, não alcançam resultados definitivos e devem ser complementadas por ações terrestres. Bernard Brodie, teórico famoso por explorar questões relativas ao poder de fogo nuclear, apresenta uma visão materialista do poder marítimo, defendendo que a defesa dos interesses de um Estado no mar está diretamente relacionada ao seu poder de fogo nessa dimensão.

Stephen Roskill, oficial da marinha inglesa, afirma que o emprego do poder naval pela Inglaterra apresenta um padrão histórico em conflitos. Há um período defensivo, onde o poder naval é empregado em defesa, um período de equilíbrio, onde o inimigo tem seu poder reduzido, e um período ofensivo, onde, após a exaustão dos recursos do inimigo, o poder naval é empregado em ataque (TILL, 2009). Esse autor também afirma a importância de estabelecer zonas de controle, pois não é possível controlar completamente o mar. Nessas zonas, a utilização dos mares estaria garantida e a negação de sua utilização por Estados rivais seria possível. O Almirante Peter Gretton introduziu novas interpretações, e afirma que não é possível defender linhas de comunicação como espaço geográfico (GROVE, 2010). Essa defesa deve ter como objetivo navios e não uma área.

Com o passar dos anos novos vetores do poder naval foram incluídos no meio marítimo. A utilização de submarinos, aeronaves e mísseis inteligentes possibilitaram uma revolução na estratégia naval (TILL, 2009). Um único meio naval poderia ser capaz de demonstrar uma capacidade ofensiva nunca observada na história. Dessa forma, a simples presença de vetores navais já seria capaz de ser utilizada em benefício de um Estado. Assim, fortaleceu-se o conceito de diplomacia de navios de guerra, conforme James Cable, diplomata inglês, esse é um exemplo de como o poder naval passou a adotar novas possibilidades de emprego (GROVE, 2010). De acordo com o Almirante Stansfield Turner, admite-se que o poder naval pode ser utilizado como dissuasão, para o controle do mar, projeção de poder sobre terra e para ações de presença

(GROVE, 2010). Esse autor introduziu a ideia de que o controle de uma área marítima, considerando todos os novos equipamentos disponíveis em uma força naval, só poderia ser garantido em uma determinada janela de tempo. Assim, o cenário estratégico marítimo pode ser visto de uma maneira muito mais volátil do que antes. Outro ponto importante é a possibilidade de emprego da guerrilha marítima, onde uma determinada força, estatal ou não, poderia negar o uso do mar a uma força maior através de táticas não convencionais.

O Almirante Sergei G. Gorshkov, da antiga União Soviética, retoma o pensamento do poder naval como parte de uma estratégia estatal maior (GROVE, 2010). Um ponto especialmente destacado por esse autor é a possibilidade de emprego de meios navais como plataformas para a execução de ataques contra terra. Vale destacar que o elemento nuclear era fundamental nessa estratégia. Paul Kennedy argumenta que o poder marítimo é uma consequência das capacidades continentais de um Estado (GROVE, 2010). Interpreta-se que esse autor relaciona o poder naval aos recursos terrestres, como uma espécie de prolongamento. Ken Booth é responsável por uma análise que ressalta o papel do poder marítimo nas relações internacionais, apresentando uma grande capacidade de influenciar o ambiente internacional (GROVE, 2010). Essa capacidade diplomática é explorada novamente por Grove (2010), que apresenta atividades tipicamente diplomáticas desempenhadas pelo poder naval. Mostrar a bandeira e a diplomacia do navio de guerra são duas atividades destacadas pelo autor. A primeira se refere a ação de presença, já que um navio de guerra, como um navio mercante, possui uma grande mobilidade e pode ser empregado em ação de presença nos lugares mais remotos. De forma semelhante, a diplomacia do navio de guerra pode ser entendida como uma demonstração da capacidade de um Estado manter uma força naval longe de seu território. Por fim, Geoffrey Till (2009) se empenha em desenvolver uma análise mais moderna do poder naval. Esse autor foca na questão de novas e velhas marinhas, e da evolução de sua utilização ao longo da história

Observa-se que Mahan entende o poder de um ponto de vista realista, afirmando que o poder naval de um Estado deve ser maior que o dos demais para garantir seus interesses no mar. O poder deveria ser buscado até a obtenção da hegemonia, garantindo assim o desenvolvimento. Os autores seguintes apresentam visões táticas distintas, mas estrategicamente estão voltadas para o mesmo fim. Percebe-se que falam recorrentemente sobre capacidades navais superiores, seja como atividade fim ou como suporte para outras. Roskill apresenta uma visão que pode ser entendida de maneira mais flexível, a ideia da manutenção de zonas de segurança traz a ideia de uma superioridade relativa (GROVE, 2010). Não seria necessária uma hegemonia global,

apenas nas áreas necessárias para garantir o interesse nacional. Posteriormente, Gretton apresenta uma visão semelhante que foca nos meios navais e não em áreas geográficas.

A inclusão de novas tecnologias nos meios navais e a ampliação das capacidades de utilização dos submarinos e aeronaves revolucionaram o poder naval. Dessa forma pode-se perceber que esse poder passou a ter diferentes manifestações. O que antes podia ser quantificado em unidades de navio, agora passou a ser relativo, dependendo do emprego e do cenário. Um único meio naval passou a apresentar o potencial para superar toda uma força. A hegemonia mundial foi gradativamente sendo deixada de lado, entendeu-se que o controle de um determinado cenário se tornava cada vez mais fluido. O aprimoramento dos mísseis balísticos, especialmente daqueles dotados de tecnologia nuclear, apresentaram uma nova capacidade dos meios navais enquanto plataformas de lançamento. Nota-se a construção de uma nova característica, uma nova interpretação, que se pode relacionar com o construtivismo.

A construção das novas capacidades do poder naval criou uma gama de empregos possíveis. O simples impacto cultural gerado pela presença de uma embarcação em um porto estrangeiro pode gerar benefícios. A presença de ameaças comuns, como a guerrilha marítima, é um ponto capaz de gerar cooperação entre Estados para a sua repressão. Um exemplo desse caso é a postura de cooperação no golfo de Áden, onde há uma coalizão internacional voltada ao combate à pirataria e em defesa do fluxo mercante. Nesse caso pode-se observar a influência direta da interdependência internacional (TILL, 2009).

Dessa forma, é possível entender que um primeiro momento de qualquer análise é adotar um referencial para o conceito de poder. Dependendo do momento histórico e da situação em questão deve-se levar em consideração a visão mais adequada para que se tenha um entendimento mais próximo da realidade. Com o poder naval não é diferente, para um dado contexto, é possível avaliar esse poder através de uma das interpretações de poder citadas anteriormente. É importante ressaltar que alguns casos podem apresentar características que remetem a mais de uma interpretação de poder, ponto que torna as análises ainda mais complexas.

1.5 Segurança no Mar

Buerger (2015) discorre sobre o que seria *maritime security*. Esse termo é considerado como um conceito moderno nas relações internacionais, que ganha cada vez mais importância à medida em que novas iniciativas internacionais tomam forma. Estados como Inglaterra, Estados Unidos, e mesmo organizações internacionais como OTAN e União Africana, têm se

empenhado cada vez mais na organização de uma governança relativa à segurança no mar. Isso se deve, em grande medida, ao terror disseminado pelo atentado às torres gêmeas nos Estados Unidos, que causou reflexões sobre a possibilidade de utilização do meio marítimo para ataques semelhantes. Além disso, ações de pirataria ganharam força e chegaram a representar uma grande ameaça ao tráfego mercante internacional. É importante mencionar que se vive em um contexto de grande desenvolvimento do poder naval de Estados em desenvolvimento como China e Índia que se apresentam, cada vez mais, como potências navais significativas em sua região.

Maritime security apresenta novos desafios que devem ser enfrentados pela comunidade internacional. Disputas interestatais, terrorismo marítimo, pirataria, tráfico de narcóticos e pessoas, contrabando e descaminho, proliferação e armamentos, pesca ilegal, crimes ambientais e desastres naturais são alguns dos pontos que compõe a agenda de discussões relacionadas ao tema. É comum o entendimento de que *maritime security* representa a ausência dos pontos citados anteriormente, fato que geraria uma ordem estável no mar. Mas há uma série de questões envolvendo o entendimento dos diversos atores do sistema internacional sobre como essa ordem deve ser buscada. Percebe-se que qualquer forma de governança marítima abrange diversas esferas de interesse, é claro que cada parte interessada busca o entendimento mais coerente com suas necessidades particulares (BEIRÃO, 2014).

Entretanto, como se pode observar com os termos *peacebuilding* e *human security*, que também não estão consensualmente definidos, a utilização do conceito *maritime security* possibilita ações coordenadas, mesmo na ausência de consenso. É comum atribuir significado a conceitos por correlação, dessa forma é importante refletir sobre os conceitos que estariam relacionados a *maritime security*. Destacam-se quatro conceitos em especial: *seapower*, *marine safety*, *blue economy* e *human resilience* (BUERGER, 2015). O primeiro conceito se refere ao poder naval, parcela militar do poder marítimo de um Estado, responsável por garantir os interesses estatais no mar. Dessa forma, considera-se que a segurança militar/policial está dentro dos fatores que devem ser levados em consideração. O termo *marine safety* está relacionado à segurança da navegação, trata-se de normas e procedimentos para garantir a segurança dos meios marítimos e instalações terrestres de apoio aos mesmos. *Blue economy* diz respeito a parcela econômica afetada pelo poder marítimo de um Estado, e da economia internacional, como transporte marítimo, atividade pesquisa e exploração de recursos minerais. Por fim, *human resilience* se refere a capacidade que a exploração dos recursos do mar tem de fornecer recursos para a sobrevivência humana, como fonte de proteína animal e fonte renda para população costeira, por exemplo.

O ímpeto para a promoção da securitização do mar veio, em sua forma mais explícita, após o fim da guerra fria. Antes disso, grande parte das discussões referentes ao assunto foram colocadas de lado em decorrência do regime bipolar que paralisava qualquer negociação nesse sentido. A Organização das Nações Unidas define sete grandes ameaças no mar: Pirataria e roubo armado, atos terroristas, tráfico de armas, e artefatos de destruição em massa, tráfico de narcóticos, tráfico de pessoas, pesca ilegal e danos ao meio ambiente marítimo (BEIRÃO, 2014). A securitização promove um aumento nas ações de repressão a essas atividades, porém também pressupõe ações mais assertivas, incluindo o emprego de meios militares, por exemplo.

Na prática, a securitização vem sendo implementada através de diversas medidas, tanto normativas como práticas. O conceito *maritime domain awareness* (MDA) representa um conjunto de medidas, como o emprego de sistemas satélite, radar e de comunicações responsáveis por acompanhar todo o tráfego marítimo em determinadas áreas (TILL, 2009). Isso possibilita que Estados, ou mesmo outros atores como o setor privado, possam obter informações precisas sobre a situação do tráfego marítimo. As atividades de patrulha e inspeção também são uma importante ferramenta para a dissuasão de atos criminosos. Atividades de imposição da lei, como ações policiais no mar, também são empregadas como meio de afirmação Estatal no mar. Todas essas ações demandam uma atuação cada vez mais integrada entre setores de segurança, jurídicos e privados para garantir a adequabilidade das medidas adotadas. Finalmente, as atividades típicas do poder naval, como projeção de poder, não podem ser desconsideradas nesse contexto.

Tendo em vista o caráter internacional do ambiente marítimo, é importante comentar que, além de todas as medidas comentadas acima, a cooperação interestatal é fundamental. Não é possível que apenas um Estado seja responsável por garantir a segurança no mar, dessa forma é importante promover um engajamento internacional (BEIRÃO, 2014). Diversas iniciativas têm tomado forma ao longo do tempo, como iniciativas de segurança coletiva pela União Europeia e pela Organização do Tratado do Atlântico Norte (OTAN). Também se deve levar em consideração os interesses de atores transnacionais como organizações internacionais e setores civis, pois a insegurança marítima pode afetar a todos. Sendo assim, observa-se a necessidade de desenvolvimento de uma mentalidade de uma comunidade internacional voltada para a segurança marítima.

O término da guerra fria representou um aparente alinhamento em direção a ações de securitização em diversos campos, inclusive sobre o ambiente marítimo. Todo o arcabouço legal criado até então, com especial destaque para Convenções das Nações Unidas para o Direito do Mar (CNUDM), focou-se em questões relacionadas à regulação do uso do mar e não

especificamente para sua securitização (BUERGER, 2015). Nesse contexto é importante comentar que a tradução do termo *maritime security*, segurança marítima em português, promove uma ambiguidade. Na língua inglesa os termos *safety* e *security* apresentam sentidos diferentes, mas ambos são traduzidos como segurança. *Safety* se refere a segurança da navegação, das embarcações, das instalações e do pessoal envolvido em atividades marítimas. Já o termo *security* se refere a defesa contra ameaças propriamente ditas, como pirataria e outros crimes.

Dessa forma, verifica-se que grande parte dos pontos abordados internacionalmente a respeito do ambiente marítimo, até o fim da guerra fria, estiveram voltados para o *safety* pois representavam interesses comuns independentes no cenário bipolar. Já os assuntos voltados para *security* ficavam minimamente regulados pelo Direito Internacional dos Conflitos Armados (DICA) e convenções correlatas. Assim, é sempre importante pensar sobre que segurança está sendo abordada em cada contexto, tendo em vista que convenções internacionais são, usualmente, escritas em língua inglesa. Na grande maioria das vezes em que o termo segurança é citado na CNUDM é observado o sentido de *safety*. Sendo assim, pode-se perceber uma grande lacuna referente a *security* na governança internacional.

Para contornar essas lacunas, é necessário estabelecer normas adicionais, sejam internas a um Estado específico, seja entre Estados. Dessa forma, é necessário que os Estados estabeleçam um arcabouço legal responsável por criminalizar atos que não encontram definição universal, como pirataria (BEIRÃO, 2014). Acordos entre Estados, especialmente no que se refere a critérios para visita e inspeção de embarcações, se mostram uma ferramenta útil para evitar conflitos decorrentes de abordagens contestadas pelo Estado de bandeira do navio abordado. Acordos comunitários têm se tornado cada vez mais comuns, em virtude da criação de forças multinacionais voltadas para o combate à pirataria, e envolvem a normatização das ações obedecendo ao entendimento do grupo.

Com relação ao *safety*, pode-se perceber que desde o naufrágio do Titanic, em 1914, houve uma tentativa de levar o assunto ao nível internacional (BEIRÃO, 2014). Esse ímpeto obteve grande adesão e originou a convenção internacional *Safety Of Live At Sea* (SOLAS), voltada para a salvaguarda da vida humana no mar. Entende-se que, nesse caso, o termo *safety* foi traduzido como salvaguarda. Essa área tem, historicamente, como foco a normatização de procedimentos e critérios de segurança que devem ser observados pelos navegantes em todo o mundo. Requisitos mínimos de equipamentos de segurança, bem como sua padronização, são definidos por convenções como essa. O *Global Maritime Distress Safety System* (GMDSS), baseado em uma combinação de tecnologias de comunicações, também surgiu nesse contexto.

Esse sistema tem como objetivo aumentar a MDA para proporcionar apoio a embarcações que apresentem emergências a bordo.

Assim, pode-se entender que as bases legais e procedimentos relacionados ao *safety* encontram-se melhor consolidados no contexto internacional. Porém, nem todas as questões foram abordadas, novos temas têm sido apresentados nesse contexto como questões relacionadas à poluição marinha. Nesses casos ainda não há consenso sobre os métodos utilizados para mensurar impactos e para responsabilização dos autores. Em relação a *security*, nota-se que os Estados estão se empenhando em discutir e definir as melhores estratégias para a securitização dos mares em seus respectivos contextos, particulares e regionais, porém ainda não há consenso internacional. Mesmo com todas as tentativas de prover normatização, mesmo que regional, novas questões ainda são apresentadas. A utilização de veículos marítimos não tripulados e os riscos cibernéticos no ambiente marítimo são exemplos que representam novos desafios que ainda não foram devidamente discutidos.

1.6 A Ameaça Cibernética

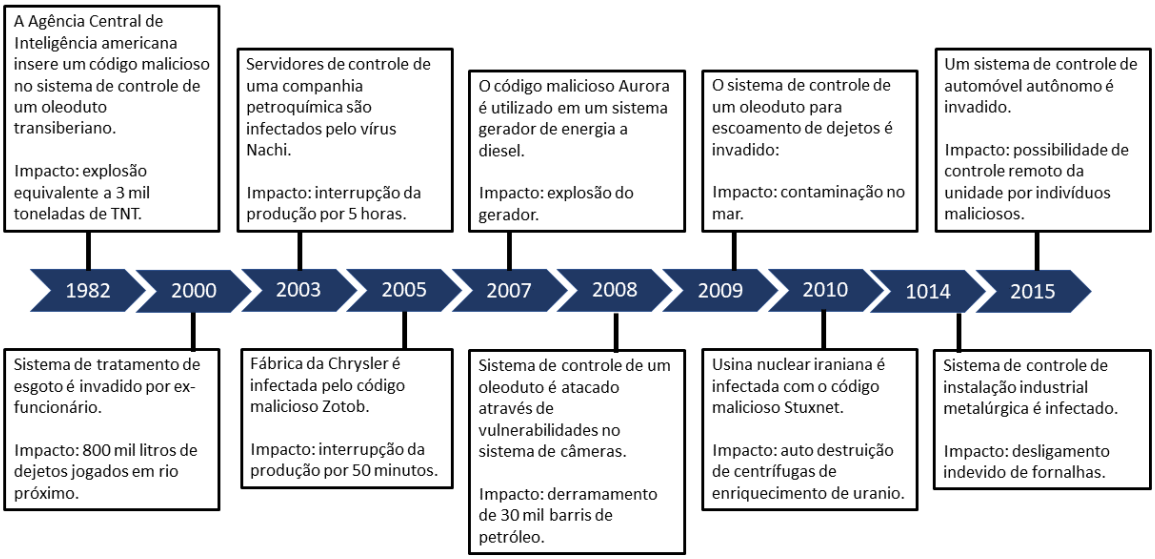
A utilização da dimensão cibernética como meio para a realização de ataques em busca de objetivos estratégicos não é uma novidade. Conforme a Figura 2, ataques de grande vulto tem ocorrido desde a década de 80. Com o passar do tempo a complexidade dessas ações foi incrementada e atualmente possui alto nível de sofisticação. Vale ressaltar que cada um desses eventos está relacionado a um impacto relevante e com tremendo potencial estratégico. Assim, é importante realizar uma breve revisão de alguns pontos nessa linha do tempo (MCLAUGHLIN *et al*., 2016).

Um *malware* é um *software,* ou parte dele, que tem como objetivo explorar vulnerabilidades dos sistemas de informação para alcançar determinados objetivos. O *malware* Aurora, testado em 2007 pelo Laboratório Nacional de Idaho, é um exemplo de como um código malicioso pode causar impactos na dimensão física. O alvo desse código foi uma planta elétrica baseada em um gerador a diesel controlado eletronicamente. Após obter acesso a rede de controle, o atacante implantou o malware. Os atuadores eletrônicos passaram a receber comandos maliciosos fazendo com que o sistema entrasse em colapso, chegando a causar a explosão do gerador (MCLAUGHLIN *et al*., 2016).

Em 2008 vulnerabilidades de *softwares* de controle de câmeras sem fio foram exploradas para que atacantes conseguissem acesso a rede de controle de um oleoduto turco. Após a obtenção do acesso necessário, comandos maliciosos foram emitidos para os elementos

responsáveis pelo controle de pressão dos dutos, fazendo com que o funcionamento ocorresse fora dos limites de segurança. Como consequência houve uma explosão responsável pelo derramamento de trinta mil barris de petróleo (MCLAUGHLIN *et al*., 2016).

Figura 2 - Linha do Tempo dos Grandes Ataques Cibernéticos



Fonte: MCLAUGHLIN et al., 2016, tradução nossa.

O advento do *malware* Stuxnet, em 2010, merece especial destaque nesse contexto. Segundo Zetter (2015), o malware alcança um nível de complexidade surpreendente. Verificou-se que o código estava baseado em várias vulnerabilidades *zero day*, falhas em programas em computadores que nem mesmo os seus fabricantes têm conhecimento. Seu refinamento levanta questões sobre o seu desenvolvimento, não seria possível desenvolver uma arma tão elaborada sem um amplo suporte técnico associado a um material humano com elevada capacitação. Sanger (2018) afirma que ele teria sido criado por instituições Estatais para alcançar objetivos estratégicos no ambiente internacional. A vítima de maior vulto do Stuxnet foi uma usina nuclear iraniana que teve seu funcionamento prejudicado, atrasando o programa nuclear desse país em alguns anos.

Nota-se uma notável evolução na complexidade dos ataques cibernéticos com o passar do tempo. O Stuxnet apresentou um novo nível de sofisticação, onde toda a ação é automatizada. Ele também apresenta uma modularidade em relação a suas funções. Hoje diversas análises estão disponíveis para todos aqueles que desejarem estudá-lo, inclusive para indivíduos com intenções maliciosas. Os mesmos conceitos podem ser explorados para atingir outras plataformas, inclusive sistemas utilizados em meios navais que empregam sistemas com

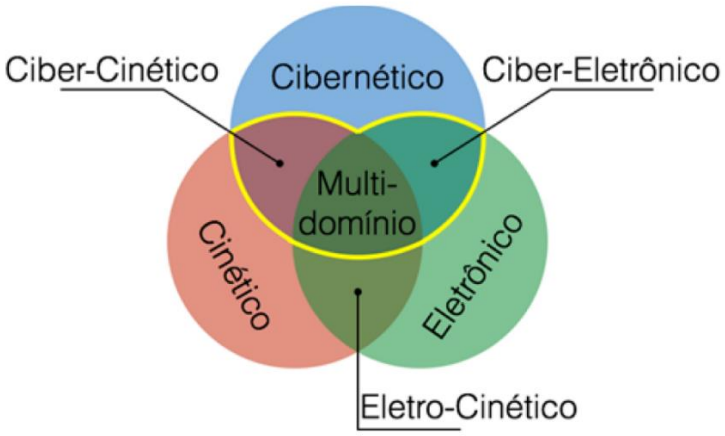
as mesmas vulnerabilidades. A proliferação de armas cibernéticas patrocinados por Estados, organizações ou indivíduos, não pode ser ignorada. Aqueles que não estiverem preparados para enfrentar essa nova tendência serão inevitavelmente vitimados em algum momento.

Além dos ataques citados na Figura 2, é importante comentar ataques recentes que causaram grandes impactos no ambiente marítimo. Desde 2017 quatro grandes nomes da indústria marítima internacional foram vítimas de crimes cibernéticos. As empresas Maersk, MSC, COSCO *shipping* e CMA CGM foram vítimas de *ransonware* (SADEK, 2021). Esse tipo ataque é baseado no sequestro de bancos de dados, através de técnicas de criptografia, com posterior pedido de resgate desses dados. Tendo em vista o alcance global dessas empresas nota-se que os valores envolvidos nesses resgates não poderiam ser modestos. Além desses ataques, em 2020 os sistemas de gerenciamento do porto iraniano Shahid Rajaee foram vítimas de um ataque que causou a interrupção do funcionamento (WARRICK e NAKASHIMA, 2020). Nota-se que a indústria marítima precisa estar pronta para enfrentar as ameaças provenientes da dimensão cibernética.

1.6.1 O Encontro das guerras cibernética, eletrônica e cinética

Sá, Machado e Almeida (2019), dissertam sobre o fenômeno da integração entre as dimensões cibernética, eletrônica e cinética em operações de guerra. A aplicação desses conceitos separadamente tem sido usual em ações militares modernas, entretanto percebe-se que existe uma tendência de que esses ambientes sejam integrados de forma que ações em um deles cause efeitos nos demais.

Figura 3 - Domínios de influência/impacto em ações militares



Fonte: SÁ, MACHADO e ALMEIDA, 2019.

A Figura 3 apresenta os conceitos de campos ciber-cinéticos, ciber-eletrônico, eletro-cinético de multidomínio. Os autores descrevem a classificação ciber-cinética como ações que objetivam causar efeitos no mundo físico através de ataques à sistemas computacionais. O campo ciber-eletrônico é aquele onde ações de guerra eletrônica buscam atingir sistemas computacionais, corresponderia a uma nova etapa evolutiva de ataques eletrônicos. “Nesse caso, o espectro eletromagnético é utilizado pelo atacante para enviar um fluxo de dados ao processador do sistema alvo de forma a manipular seu processo computacional, comprometendo assim o seu funcionamento.” (SÁ, MACHADO e ALMEIDA, 2019). Já o campo eletro-cinético estabelece uma relação entre o mundo físico e o espectro eletromagnético, de acordo com os autores, um exemplo de aplicação seria a utilização de minas magnéticas. Nessas minas, a detonação, efeito físico, é realizada através da detecção do campo eletromagnético gerado por estruturas metálicas. Como se observa-nessa figura, o campo multidomínio se refere a ações que apresentam características de todos os campos.

É importante destacar que a integração dessas dimensões pode ser explorada em ataques à meios navais e instalações marítimas. Em navios modernos os sistemas de auxílio a navegação estão cada vez mais integrados. Os sistemas GPS, piloto automático, controle de velocidade e outros, se comunicam com um sistema integrado de navegação, ECDIS. Bhatti e Humphreys (2017) avaliam a hipótese de ataque ciber-eletrônicos a sistemas de navegação GPS. Através do ataque correto é possível privar um alvo do acesso à informação GPS, além disso, com o é possível inserir informações de posição adulteradas no sistema alvo. O sistema *automatic identification system* (AIS), utilizado para identificação e localização e acompanhamento de embarcações é fundamental para a segurança no mar. Há ataques capazes de fazer com que uma embarcação desaparece do sistema, impossibilitando sua localização, ou mesmo que uma falsa localização seja inserida, fazendo com que os tripulantes acreditem estar em uma posição diferente da real (HAYES, 2016). Assim, um ataque na dimensão cibernética teria o potencial de afetar toda a estrutura da embarcação. A mesma lógica, por indução, pode ser empregada em ações maliciosas contra plataformas e instalações portuárias.

1.7 Infraestruturas Críticas e Gerenciamento de Riscos Cibernéticos

Os atentados terroristas ocorridos em 2001 nos Estados Unidos da América levantaram um alerta para o país em questão, e para toda a comunidade internacional. Percebeu-se que

sistemas de infraestrutura, como o sistema de transporte aéreo, poderiam ser empregados como meios capazes de causar danos significativos. Além disso, a simples interrupção de um sistema desse tipo por si só já significa um grande prejuízo para uma cadeia logística. Assim, o entendimento do conceito de infraestrutura crítica é fundamental para que se perceba a importância da segurança cibernética na preservação de funções essenciais ao funcionamento interno de um Estado. Esse tipo de infraestrutura é definido como sistemas ou meios, físicos ou virtuais, tão vitais ao Estado que sua destruição ou interrupção de seu funcionamento poderiam causar graves impactos a segurança, economia, saúde e defesa civil, ou a qualquer combinação entre essas áreas (EUA, 2001). O governo americano definiu 16 setores que compreendem instalações sensíveis, conforme segue: químico, comercial, comunicações, manufatura, sistemas de represas, base industrial de defesa, serviços de emergência, energia, finanças, alimentação e agricultura, sistemas governamentais, saúde pública, tecnologia da informação, nuclear, transportes e de gerenciamento e abastecimento de água (EUA, 2020a).

O Brasil trata desse assunto na Estratégia Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2020c). Esse documento dá diretrizes gerais para garantir a salvaguarda do funcionamento apropriado dessas instalações. Dentre essas diretrizes, é possível observar a análise de riscos continuada. Conforme o documento, os riscos devem ser "identificados caracterizados e, em seguida, analisados quanto à necessidade e viabilidade de aplicação de controles, de maneira a reduzir a probabilidade de ocorrência dos eventos relacionados a tais riscos" (BRASIL, 2020c). A identificação dos riscos deve ser feita levando em consideração ameaças reais ou potenciais, probabilidade de ocorrência e grau de periculosidade. Tendo em vista o que foi comentado na seção 411.6, percebe-se que a ameaça cibernética não pode ser ignorada nesse contexto. Assim, entre os objetivos definidos no decreto, destaca-se o objetivo 4.3, que estabelece o incentivo a adoção de recursos e de procedimentos voltados para a segurança cibernética.

1.7.1 Infraestruturas Críticas Marítimas e o Gerenciamento de Riscos Cibernéticos

Tendo em vista o grande vulto de instalações marítimas como navios de grande porte, plataformas e portos, e seu papel estratégico, é perceptível seu enquadramento como infraestruturas críticas. Dessa forma, é necessário que haja um devido gerenciamento de risco cibernético também no ambiente marítimo. Como exemplo recente do grande impacto que um ataque cibernético pode causar a uma cadeia de suprimentos pode-se citar o caso do terminal portuário Shahid Rajaee no Irã. Em maio de 2020 os sistemas de gerenciamento do porto em

questão foram vítimas de um ataque que causou a interrupção do funcionamento. Essa interrupção foi responsável por grandes prejuízos a economia local (WARRICK e NAKASHIMA, 2020). A utilização intensiva de tecnologias cibernéticas, presentes inclusive em navios, otimiza diversos processos, porém tornam os usuários vulneráveis a esse tipo de ataque. Esse risco chamou a atenção da IMO que, através da circular nº3 de 2017, emitiu orientações gerais sobre o estabelecimento de gerenciamento de riscos cibernéticos no mar e encorajou o desenvolvimento e implementação de medidas adicionais pelos Estados membros.

Nessa circular, a IMO faz referência a *The Guidelines on Cyber Security Onboard Ships*, de autoria do *Baltic and International Maritime Council* (BIMCO) (2020), *standard on Information technology*, fruto de parceria entre a *International Organization for Standardization* (ISO) (2018) e a *International Electrotechnical Commission* (IEC), e o *Framework for Improving Critical Infrastructure Cybersecurity, do United States National Institute of Standards and Technology* (NIST) (BARRETT, 2018). Os efeitos dessa circular já podem ser sentidos, pois há diversas iniciativas no sentido de fortalecimento da governança relacionada ao assunto tratado como é possível observar nos *National Maritime Cybersecurity Plan* (EUA, 2020b) e no *Code of Practice: Cyber Security for Ships* (REINO UNIDO, 2017).

1.8 Considerações Parciais

Após essa breve revisão, é possível compreender que o conflito e a violência são constantes nas relações humanas. Essa mesma lógica pode ser expandida para o contexto internacional. Por isso, os Estados estão sempre preocupados em manter um poder significativo, a fim de garantir sua sobrevivência. O ambiente marítimo é uma dimensão fundamental para o planejamento estratégico de uma nação, pois, além se uma fonte de riquezas minerais e biológicas, serve como via de transporte e de comunicações. Uma das formas de expressão do poder estatal é o poder marítimo, do qual o poder naval é a parcela militar componente. Para garantir a defesa dos interesses estatais no mar, além das ameaças provenientes de outros Estados, uma nação deve estar atenta a questões de segurança marítimas. Diversos atores, estatais ou não, estão presentes no ambiente marítimo, muitos com interesses maliciosos que tornam esse ambiente hostil à atividades econômicas, científicas e de lazer. A pirataria é um exemplo clássico de como atores independentes podem representar riscos para a estabilidade de um determinado ambiente. Hoje, a dimensão cibernética possibilita atuação de novas ameaças, desde organizações até indivíduos, por vezes chamados de lobos solitários.

As ameaças cibernéticas vêm se mostrando cada vez mais perigosas, apresentando capacidades de afetar instalações cada vez mais complexas e de alto valor estratégico. A utilização desse tipo de ataque pode ter origem em indivíduos, organizações isoladas ou, em alguns casos, Estados interessados em expandir suas capacidades. Percebe-se que, com o emprego de sistemas computacionais cada vez mais desenvolvidos a bordo de embarcações e infraestruturas marítimas, o mar está cada vez mais vulnerável a dimensão cibernética. Essa vulnerabilidade vem se traduzindo em ataques reais, responsáveis por grandes impactos econômicos e com grande potencial militar. A possibilidade de emprego de ataques multidomínio torna esse contexto ainda mais ameaçador, pois sistemas característicos de instalações marítimas, como radar, tornam-se vulneráveis, mesmo desconectados da internet. Sendo assim, é necessário implementar medidas de controle de ameaças de maneira afirmativa, através de normas e regulações de gerenciamento de riscos cibernéticos no ambiente marítimo.

O emprego de políticas públicas, instrumentos que operacionalizam os interesses deliberados no nível político de um Estado, torna-se fundamental para enfrentar essas ameaças. Assim, percebe-se que é preciso que os Estados interfiram para manter a estabilidade no ambiente marítimo. É importante destacar que por estabilidade entende-se não apenas a garantia da utilização do mar perante os demais Estados do sistema internacional, mas também contra ameaças assimétricas e não convencionais como as que operam na dimensão cibernética. Essa atuação pode se dar através de políticas regulatórias, associadas a fiscalização, que estabeleçam normas e regulamentos que imponham a segurança cibernética no mar. Essas políticas devem ter origem no devido processo legal local, quando se trata de políticas de um único Estado, ou internacional, através de fóruns específicos. Para elaborar essas políticas, a participação da comunidade acadêmica é fundamental, como fonte de críticas e sugestões para políticas públicas.

2 MÉTODOS E TÉCNICAS

O presente capítulo objetiva introduzir as técnicas e métodos utilizados para obter os dados apresentados nesse trabalho para responder as questões propostas. Segundo Marconi e Lakatos (2003), um método científico é um procedimento planejado e organizado com o objetivo de produzir um conhecimento e uma técnica é um conjunto de processos para se alcançar um determinado resultado. São abordados assuntos sobre revisão sistemática de literatura, ciência de dados, com foco em mineração de dados em texto, e questionários.

2.1 Revisão Sistemática de Literatura

Antes da implementação de sistemas informatizados de buscas acadêmicas, as revisões de literatura eram bastante dificultadas (ECO, 2012). Para encontrar uma determinada informação era preciso dispender uma grande quantidade de tempo em bibliotecas e acervos técnicos, que por vezes não possuíam o item que o pesquisador buscava. Além disso, determinados exemplares estavam indisponíveis em determinada localização geográfica ou, mesmo estando disponíveis, eram encontrados em idiomas desconhecidos ao leitor. A revolução informacional, especialmente com o advento da internet, possibilitou a popularização do acesso à acervos acadêmicos virtualizados, reduzindo essas dificuldades. Mesmo as barreiras linguísticas foram minimizadas com o desenvolvimento de sistemas de tradução automatizada de textos. Entretanto, a dificuldade de controlar a integridade da informação e sua validade científica, pode levar um pesquisador desavisado a informações falsas ou com falta de rigor científico. Para mitigar esse risco, surgiram as bases de dados científicas, patrocinadas por entidades acadêmicas. Essas bases servem como bancos de dados, onde as informações foram checadas por pares e se enquadram em critérios científicos preestabelecidos. Os mecanismos de busca em bases de dados operam através de palavras, ou conjunto de palavras, e operadores lógicos. Assim, é possível construir sintaxes de busca que retornam o mesmo resultado, independentemente do usuário que a inseriu. É importante ressaltar que a utilização de sintaxes distintas, mesmo que sobre o mesmo assunto, poderá gerar resultados distintos.

Caso o pesquisador não seja cuidadoso, sua pesquisa pode acabar sendo enviesada por uma série de fatores. Um exemplo é o fator geográfico, em uma determinada região uma informação poder ter um acesso dificultado. Esse fator era mais evidente antes da popularização de bases de dados acadêmicas internacionais, mas ainda pode ocorrer. A utilização de bases de dados nacionais, ou regionais, pode gerar viés. De forma análoga, o idioma ainda é um fator de

viés. Buscas em bases de dados utilizando idiomas específicos podem acabar deixando informações importantes de fora de uma pesquisa por estarem em outros idiomas. Um outro exemplo de fator gerador de viés é a construção das sintaxes de busca. Dois pesquisadores, pesquisando o mesmo assunto, terão resultados diferentes se utilizarem sintaxes de busca distintas. Esse fator pode levar dois estudos, sobre um mesmo assunto, a resultados incompletos, ou até mesmo conflitantes.

Quadro 1 - Itens a serem incluídos no relato de revisão sistemática ou meta-análise

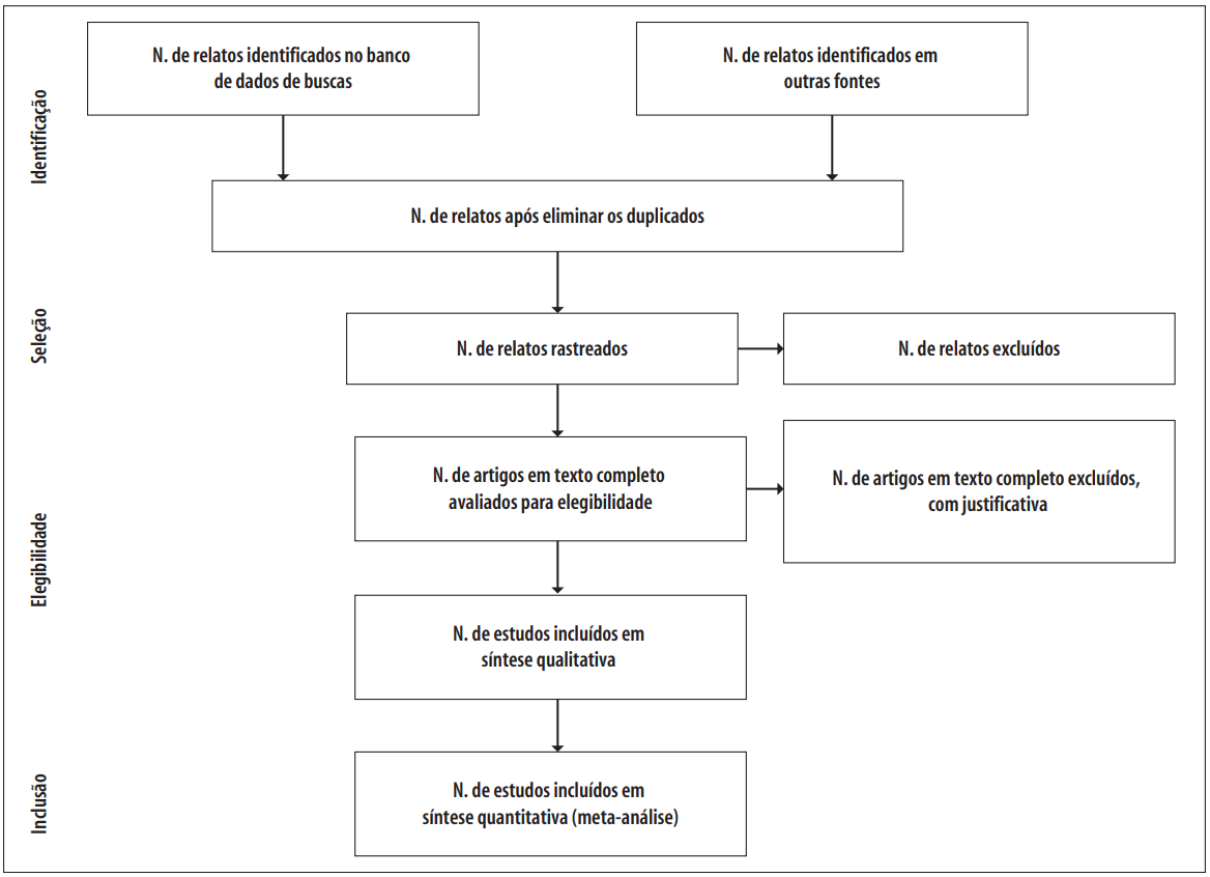
Nº	Seção/tópico	Item do checklist
	TÍTULO	
1	Título	Identifique o artigo como uma revisão sistemática, meta-análise ou ambos.
	RESUMO	
2	Resumo estruturado	Apresente um resumo estruturado incluindo, se aplicável: referencial teórico; objetivos; fonte de dados; critérios de elegibilidade; participantes e intervenções; avaliação do estudo e síntese dos métodos; resultados; limitações; conclusões e implicações dos achados principais; número de registro da revisão sistemática.
	INTRODUÇÃO	
3	Justificativa	Descreva a justificativa da revisão no contexto do que já é conhecido.
4	Objetivos	Apresente uma afirmação explícita sobre as questões abordadas com referência a participantes, intervenções, comparações, resultados e delineamento dos estudos.
	MÉTODOS	
5	Protocolo e registo	Indique se existe um protocolo de revisão, se e onde pode ser acessado (ex. endereço eletrônico), e, se disponível, forneça informações sobre o registro da revisão, incluindo o número de registro.
6	Critérios de elegibilidade	Especifique características do estudo e características dos relatos usadas como critérios de elegibilidade, apresentando justificativa.
7	Fontes de informação	Descreva todas as fontes de informação na busca (ex.: base de dados com datas de cobertura, contato com autores para identificação de estudos adicionais) e data da última busca.
8	Busca	Apresente a estratégia completa de busca eletrônica para pelo menos uma base de dados, incluindo os limites utilizados, de forma que possa ser repetida.
9	Seleção dos estudos	Apresente o processo de seleção dos estudos (isto é, rastreados, elegíveis, incluídos na revisão sistemática, e, se aplicável, incluídos na meta-análise).
10	Processo de coleta de dados	Descreva o método de extração de dados dos artigos e todos os processos para obtenção e confirmação de dados dos pesquisadores.
11	Lista dos dados	Liste e defina todas as variáveis obtidas dos dados e quaisquer suposições ou simplificações realizadas.

12	Risco de viés em cada estudo	Descreva os métodos usados para avaliar o risco de viés em cada estudo (incluindo a especificação se foi feito no nível dos estudos ou dos resultados), e como esta informação foi usada na análise de dados.
13	Medidas de sumarização	Defina as principais medidas de sumarização dos resultados (ex.: risco relativo, diferença média).
14	Síntese dos resultados	Descreva os métodos de análise dos dados e combinação de resultados dos estudos, se realizados, incluindo medidas de consistência para cada meta-análise.
15	Risco de viés entre estudos	Especifique qualquer avaliação do risco de viés que possa influenciar a evidência cumulativa.
16	Análises adicionais	Descreva métodos de análise adicional, se realizados, indicando quais foram pré-especificados.
	RESULTADOS	
17	Seleção de estudos	Apresente números dos estudos rastreados, avaliados para elegibilidade e incluídos na revisão, razões para exclusão em cada estágio, preferencialmente por meio de gráfico de fluxo.
18	Características dos estudos	Para cada estudo, apresente características para extração dos dados e apresente as citações.
19	Risco de viés em cada estudo	Apresente dados sobre o risco de viés em cada estudo e, se disponível, alguma avaliação em resultados (ver item 12).
20	Resultados de estudos individuais	Para todos os desfechos considerados (benefícios ou riscos), apresente para cada estudo: (a) sumário simples de dados para cada grupo de intervenção e (b) efeitos estimados e intervalos de confiança, preferencialmente por meio de gráficos de floresta.
21	Síntese dos resultados	Apresente resultados para cada meta-análise feita, incluindo intervalos de confiança e medidas de consistência.
22	Risco de viés entre estudos	Apresente resultados da avaliação de risco de viés entre os estudos (ver item 15).
23	Análises adicionais	Apresente resultados de análises adicionais, se realizadas (ver item 16).
	DISCUSSÃO	
24	Sumário da evidência	Sumarize os resultados principais, incluindo a força de evidência para cada resultado; considere sua relevância para grupos-chave (ex.: profissionais da saúde, usuários e formuladores de políticas).
25	Limitações	Discuta limitações no nível dos estudos e dos desfechos (ex.: risco de viés) e no nível da revisão (ex.: obtenção incompleta de pesquisas identificadas, viés de relato).
26	Conclusões	Apresente a interpretação geral dos resultados no contexto de outras evidências e implicações para futuras pesquisas.
	FINANCIAMENTO	
27	Financiamento	Descreva fontes de financiamento para a revisão sistemática e outros suportes; papel dos financiadores na revisão sistemática.

Fonte: LIBERATI et al., 2009, tradução de David Harrad, adaptação nossa.

A revisão sistemática de literatura propõe uma metodologia que busca minimizar os riscos de enviesamento dos resultados das buscas, facilitar a reprodução da pesquisa e maximizar a abrangência (LIBERATI *et al.*, 2009). Para isso, são propostos procedimentos padronizados que devem ser seguidos pelos pesquisadores que produzem esse tipo de revisão, de acordo com Liberati *et al*. (2009), um relato de revisão sistemática deve incluir os elementos apresentados no Quadro 1. Essa metodologia é mais comum na área da medicina, mas apresenta características que podem que podem ser adaptadas para outras áreas do conhecimento.

Figura 4 - Fluxograma genérico de uma revisão sistemática



Fonte: LIBERATI et al., 2009, tradução de David Harrad.

De maneira geral, uma revisão sistemática estabelece previamente um conjunto de bases de dados que serão utilizadas, preferencialmente acadêmicas, mas também se recomenda a utilização de ao menos uma base de dados mais geral. As referências científicas encontradas são chamadas de literatura branca, enquanto as demais são chamadas de literatura cinza. Após a definição das bases de dados que serão consultadas, o pesquisador deve definir uma sintaxe de busca única, que deverá ser utilizada em todas as bases escolhidas. Essa sintaxe deve ser

direcionada a pergunta que o pesquisador deseja responder. Os resultados obtidos passam então por um processo de filtragem que compreende a eliminação de referências em duplicidade e em avaliações criteriosas de critérios de inclusão. Esses critérios devem ser objetivos e previamente definidos pelo pesquisador. É importante ressaltar que se sugere a avaliação de todas as referências encontradas por mais de um analista, de modo a minimizar falhas no processo. Após esse procedimento, outras referências relevantes podem ser incluídas, a critério do pesquisador e com a devida justificativa. Por fim, os resultados são extraídos das referências que atenderam os critérios de elegibilidade através de análise qualitativa e, caso aplicável, quantitativa, através de meta-análises. A Figura 4 apresenta o fluxograma genérico de uma revisão sistemática.

Nesta pesquisa, foram consideradas referências, em língua inglesa, publicadas a partir de 5 de julho de 2017, data de emissão do documento *Guidelines on Maritime Cyber Risk Management* (IMO, 2017), e que fazem referência a organização emissora. As buscas foram realizadas nas bases de dados *Scopus*, IEEE Explore, ACM *digital library*, Open Grey e Google *Scholar*. Conforme Farias *et al.* (2016), os termos utilizados para a construção da sintaxe de busca foram reunidos em grupos, que contém sinônimos ou termos com valor semelhante no campo de estudo analisado, e apresentados na Tabela 1.

Tabela 1 – Termos utilizados nas buscas

	Grupo 1 (G1)	Grupo 2 (G2)	Grupo 3 (G3)
Termo 1 (T1)	cyber security	maritime	International maritime organization
Termo 2 (T2)	cybersecurity	naval	IMO
Termo 3 (T3)		ship	
Termo 4 (T4)		port	

Fonte: O autor, 2021.

A sintaxe de busca utilizada foi: ("cyber security" OR "cybersecurity") AND (maritime OR naval OR ship OR port) AND ("international maritime organization" OR IMO). Essa mesma sintaxe pode ser visualizada na seguinte forma: (([G1,T1] OR [G1,T2]) AND ([G2,T1] OR [G2,T2] OR [G2, T3] OR [G2, T4]) AND ([G3,T1] OR [G3,T2])). O primeiro termo, ([G1,T1] OR [G1,T2]) , objetiva encontrar referências que abordem o tema segurança cibernética. O segundo termo, ([G2,T1] OR [G2,T2] OR [G2, T3] OR [G2, T4]) , busca restringir os resultados a referências que abordem assuntos voltados para meios e instalações marítimas. Por fim, o último termo, ([G3,T1] OR [G3,T2])) , faz com que apenas as referências que mencionem a IMO apareçam nos resultados. No presente estudo, as referências incluídas

na análise tiveram como critérios a abordagem do tema, segurança cibernética em meios e instalações marítimas, identificação de riscos nesse contexto e apresentação de propostas de medidas mitigatórias.

2.1.1 Compilação dos Resultados

A sintaxe proposta foi aplicada em todas as bases de dados utilizadas, na janela temporal de 5 de julho de 2017 até 31 de março de 2021. O quantitativo de resultados obtidos encontra-se na Tabela 2.

Tabela 2 - Nº de resultados por base de dados

Base de dados	Nº de resultados
Scopus	63
IEEE Explore	2
ACM digital library	6
Open Grey	0
Google Scholar	100 (1620)

Fonte: O autor, 2021.

Quadro 2 - Ficha de avaliação de elegibilidade

Critérios				
Aborda segurança cibernética em meios e/ou instalações marítimas?	SIM		NÃO	
Identifica riscos?	SIM		NÃO	
Apresenta de propostas de medidas mitigatórias?	SIM		NÃO	
É posterior a 5 de julho de 2017?	SIM		NÃO	
Está em língua inglesa?	SIM		NÃO	
Observações:				
Sugere-se	INCLUIR		EXCLUIR	
Avaliador:				

Fonte: O autor, 2021.

Nota-se que o número de resultados provenientes do Google *Scholar* é demasiadamente grande, por isso foram utilizados apenas os 100 (cem) primeiros resultados. É importante comentar que o mecanismo de pesquisa Google ordena os resultados por relevância. Os resultados obtidos foram exportados das bases de dados no formato eletrônico *BibTeX* (.bib), específico para registro de referências bibliográficas, e carregados no gerenciador eletrônico de referências *Mendeley* (2021). Após a retirada dos resultados duplicados, restaram 163 para análise de critérios de elegibilidade, de acordo com a ficha apresentada no Quadro 2. As avaliações foram realizadas pelo autor. Para ser incluída, a referência deve atender a todos os critérios.

2.1.2 Adaptações e Limitações

O método apresentado foi adaptado e simplificado para utilização na presente pesquisa. Neste trabalho as referências foram avaliadas apenas pelo autor. Porém, sugere-se que ao menos dois pesquisadores avaliem as referências e que haja um terceiro para desempate, em caso de discordância. Algumas informações sugeridas no Quadro 1, para a apresentação do relato, foram suprimidas, ficando somente aquelas julgadas mais importantes pelo autor. Os dados extraídos das referências foram interpretados pelo autor, não havendo avaliação de outros.

2.2 Mineração de Dados em Texto

O desenvolvimento das tecnologias de armazenamento e processamento de dados, especialmente relacionados à virtualização, não pode ser ignorado. A *computação em nuvem* favoreceu a formação de empresas de tecnologia da informação, que fornecem infraestrutura computacional. Não é mais necessário ter um computador potente em uma residência ou local de trabalho para ter acesso a um volume significativo de armazenamento e processamento de dados. Os clientes hospedam seus dados em grandes centros de dados, que comportam muitos computadores trabalhando em conjunto. O aumento das massas de dados armazenadas por essas empresas gerou a necessidade de desenvolver novas metodologias para extrair valor desse importante ativo que é a informação. Assim, a ciência de dados tem ganhado cada vez mais espaço, fornecendo maneiras eficientes de extrair informações dessas grandes massas de dados, ou *big data*[1].

[1] Conjunto de dados tão volumoso e complexo que não pode ser analisado utilizando técnicas tradicionais, demandando grande capacidade de processamento para interpretação (ORACLE, 2021).

Nesse contexto a linguagem de programação python vem se destacando. Kumar e Panda (2019) descrevem Python como uma linguagem de programação de alto nível, criada em 1991, com alta versatilidade e simplicidade. Ao longo dos anos essa linguagem foi ganhando cada vez mais popularidade sendo hoje uma das mais utilizadas no mundo. Possui a capacidade de trabalhar utilizando bibliotecas e pacotes que simplificam a programação. Dentre esses pacotes há o *Natural Language Toolkit* (NLTK), especialmente voltado para a análise de texto e utilizado na presente pesquisa. Além desse pacote, foram utilizados na pesquisa o *collections*, ferramentas úteis para análises quantitativas, o *numpy*, que contém procedimentos de cálculos matemáticos e o *matplotlib*, que é responsável pela elaboração de gráficos.

Figura 5 - Importação de pacotes para o algoritmo

```
1   #Pacotes e funções utilizadas
2   import nltk
3   from nltk.corpus import stopwords
4   from nltk.tokenize import word_tokenize
5   from collections import Counter
6   import string
7   import numpy as np
8   import matplotlib.pyplot as plt
9   from wordcloud import WordCloud
10  #Pacotes e funções utilizadas
```

Fonte: O autor, 2021.

Jurafsky e Martin (2020), descrevem os conceitos básicos para o processamento de textos. Na abordagem adotada pelo presente trabalho foi adotada a contagem do número de vezes que as palavras se repetem em cada documento analisado. Após essa análise, foram contadas as palavras que contém o termo ciber, em português, e *cyber*, em inglês. Dessa forma, foi possível gerar um valor de referência utilizando o número de vezes que termos relacionados a ciber e *cyber* se repetem em relação ao total de palavras de cada documento. Com essa informação pretende-se avaliar o nível de discussão de assuntos relacionados a cibernética em relação aos demais presentes nos documentos de referência. O algoritmo utilizado na mineração de dados em texto, APÊNDICE A, se inicia com a importação dos pacotes empregados, conforme a Figura 5. Em um segundo momento, são carregadas as *stopwords*, na língua do documento que está sendo analisado, conforme a linha 13 da Figura 6, essas palavras são aquelas que podem ser desconsideradas no processamento do texto sem prejudicar o entendimento do assunto. É possível adicionar palavras nessa lista, como na linha 16 da Figura 6, conforme a necessidade do pesquisador, para refinar os dados obtidos, neste trabalho foram retirados os termos constantes nos APÊNDICES D e E. Além disso, os caracteres de pontuação

também devem ser carregados para posterior eliminação, de forma a facilitar o processamento dos dados, como na linha 22 da Figura 6.

Figura 6 - Retirada de termos e pontuação

```
12  #Termos que devem ser excluídos do texto
13  stop_words = (stopwords.words('portuguese'))
14
15  #Termos adicionados pelo autor
16  stop_words.append ('-')
17  #Termos adicionados pelo autor
18
19  #Termos que devem ser excluídos do texto
20
21  #Retirada de termos e pontuação
22  string_punctuation = string.punctuation
23
24  text = open ('arquivo.txt', mode='r', encoding='utf-8')
25
26  content = text.read()
27
28  word_tokens = word_tokenize(content)
29
30  filtered_sentence = [w for w in word_tokens if not w in stop_words]
31
32  filtered_sentence = []
33
34  for w in word_tokens:
39
40  filtered_sentence_punctuation = [q for q in filtered_sentence if not q in string_punctuation]
41
42  filtered_sentence_punctuation = []
43
44  for q in filtered_sentence:
49  #Retirada de termos e pontuação
```

Fonte: O autor, 2021.

Figura 7 - Extração de dados quantitativos

```
51  #Contagem da incidência de cada termo
52  contador = Counter(filtered_sentence_punctuation)
53  #Contagem da incidência de cada termo
54
55  #Ordenação de termos por incidência
56  contador_lista = []
57
58  for i in contador.most_common():
59
60      contador_lista.append(i)
61  #Ordenação de termos por incidência
62
63  #Exibição dos 10 termos mais citados
64  print(contador_lista[:10])
65  #Exibição dos 10 termos mais citados
66
67  #Conversão do tipo de dado (de lista para dicionário), necessário para gráfico e wordcloud
68  b = dict(contador_lista[:10])
69  #Conversão do tipo de dado (de lista para dicionário), necessário para gráfico e wordcloud
70
71  #Exibição para verificação
72  print (b)
73  #Exibição para verificação
```

Fonte: O autor, 2021.

O texto analisado é então carregado e *tokenizado*. Esse termo se refere ao procedimento de divisão do texto em palavras e símbolos, para processamento. Dessa forma, cada palavra, ou símbolo, pode ser comparada com os itens constantes em *stopwords* e *punctiation*. Assim, o texto analisado é filtrado para posterior extração de dados quantitativos, como frequência de repetição de palavras e palavras mais citadas. No algoritmo utilizado foram extraídas as frequências de palavras e as dez (10) mais citadas em cada arquivo, conforme apresentado no trecho da Figura 7. Além dos procedimentos apresentados, são utilizados métodos para produção de gráficos e nuvens de palavras para facilitar a exposição dos dados obtidos, conforme pode ser visualizado no algoritmo completo, APÊNDICE A.

2.2.1 Limitações

Na elaboração do código não foram consideradas técnicas de otimização, responsáveis por tornar o algoritmo de processamento mais eficiente. É importante comentar que o algoritmo utilizado ainda pode receber diversas melhorias, gerando outros produtos e aumentando a qualidade da análise. Essa vertente não foi explorada por se tratar de um campo de estudo ainda desconhecido para o autor.

2.3 Questionário

Gerhardt e Silveira (2009) descrevem a utilização de questionários como uma forma de obter informações e percepções de uma parcela de um determinado grupo e, por indução, inferir a percepção do grupo como um todo. As perguntas do questionário podem exigir respostas objetivas ou subjetivas, dependendo da intenção do indivíduo que o planeja. No presente estudo foram utilizadas questões objetivas baseadas nos resultados da revisão sistemática. Para operacionalizar o questionário utilizou-se a ferramenta aberta *Google Forms*, através da qual é possível criar formulários eletrônicos com facilidade. Foram considerados três grandes grupos alvo: sociedade civil, pesquisadores das áreas de segurança cibernética e defesa e Oficiais da MB alunos do Curso de Política e Estratégia Marítima (CPEM) e do Curso de Estado-Maior para Oficiais Superiores (CEMOS). A escolha desses grupos tem por objetivo entender as perspectivas da sociedade em geral, da academia e de Oficiais que, em breve, serão decisores de alto nível na MB.

Buscou-se alcançar a sociedade civil através da divulgação do questionário em redes sociais e aplicativos de mensagens, de forma que mesmo aqueles indivíduos que não são da

área pudessem tomar conhecimento. Como pesquisadores, foram considerados os integrantes do Laboratório de Simulações e Cenários (LSC) da Escola de Guerra Naval (EGN), alunos e instrutores do Programa de Pós-Graduação em Estudos Marítimos (PPGEM) da EGN, Oficiais da MB formados no Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações, pesquisadores do Instituto Meira Mattos (IMM), Oficiais do Comando Naval de Operações Especiais (CoNavOpEsp), responsáveis por operações cibernéticas, e pesquisadores do laboratório de Segurança da Informação, das Comunicações, dos Computadores e do Espaço Cibernético (SICCCiber) da Universidade Federal Fluminense (UFF). Para esses grupos o questionário foi divulgado através de contato com cada um deles.

No cabeçalho do questionário foi colocado em evidência a informação de que a identificação dos respondentes não seria divulgada. Foram elaboradas 4 perguntas, sendo a primeira e a segunda baseadas nos resultados da revisão sistemática:

- Dentre os fatores de risco à segurança cibernética no setor marítimo, sinalize os cinco (5) considerados mais preocupantes:

1	Carência de normas e regulações;
2	Pouca produção de pesquisas na área;
3	Falhas humanas e governança deficiente;
4	Vulnerabilidades em sistemas amplamente empregados para navegação, como o GPS, AIS, ECDIS;
5	Popularização de tecnologias de embarcações autônomas;
6	Falta de legislação específica;
7	Incidência crescente do número de ataques cibernéticos a instalações marítimas;
8	Falta de recursos financeiros para a implementação de sistemas de segurança satisfatórios;
9	Utilização, cada vez maior, de sistemas cibernéticos para controle de instalações marítimas;
10	Dicotomia entre os níveis de alerta público e privado;
11	Vulnerabilidades em softwares e tecnologias de prateleira;
12	Guerra eletrônica;
13	Conhecimento deficiente por parte de profissionais marítimos;
14	Lentidão do ramo para adoção de medidas de segurança cibernética;
15	Falta de padronização internacional em requisitos de segurança;
16	Informações sobre ataques não são compartilhadas;

17 Não há um sistema de certificação de segurança cibernética no ramo;

18 Operação remota.

- Dentre ações abaixo, sinalize as cinco (5) consideradas importantes para fortalecer o poder marítimo brasileiro no que se refere à segurança cibernética:

1 Reforçar o ensino;

2 Estabelecer normas e regulação;

3 Implementar gerenciamento de riscos cibernéticos;

4 Incentivar boas práticas de governança cibernética;

5 Implementar planos de contingência;

6 Compartilhar informações;

7 Empregar sistemas alternativos ao GPS para navegação;

8 Implementar autenticação de dados na recepção de sistemas de navegação;

9 Implementar auxílios a navegação com tecnologia laser;[2]

10 Estabelecer estrutura de verificação de conformidade/*compliance*;

11 Incentivar pesquisa em segurança cibernética marítima;

12 Criar laboratórios em parceria público-privada;

13 Empregar *ethical haking* para detecção de vulnerabilidades;

14 Incentivar *think-tanks* na área;

15 Criar de carreiras específicas, no setor marítimo, voltadas especificamente para segurança cibernética a bordo;

16 Incentivar o nivelamento internacional de requisitos mínimos de segurança cibernética;

17 Estabelecer requisitos mínimos de segurança para receptores de sinais de geolocalização, como GPS e AIS;

18 Acompanhar a consciência situacional cibernética no setor marítimo;

19 Implementar de uma base de ensino obrigatória para todos os profissionais do setor marítimo;

20 Conscientizar gestores e líderes de instituições voltadas para o setor marítimo;

21 Elaborar sistemas de inspeção para certificação de instituições;

---

[2] Essas tecnologias envolvem o emprego da faixa de micro-ondas do espectro eletromagnético. Hoje já estão disponíveis uma série de aplicações como o *Laser Imaging Detection and Ranging* (LIDAR), sistema que utiliza a mesma lógica do radar para gerar imagens com sinais *laser*.

22 Manter o ensino de métodos tradicionais de navegação, independentes de informações eletrônicas, para profissionais da área;
23 Normatizar centros de monitoramento de sistemas cibernéticos para instalações marítimas;
24 Elaborar legislação específica para o setor;
25 Fomentar parcerias público-privadas;
26 Realizar exercícios de segurança cibernética.

- Tendo em vista a atual tendência internacional de fortalecimento da segurança cibernética, a postura Brasileira, no que se refere a políticas públicas, em relação ao assunto pode ser considerada satisfatória? (considere neste caso um escopo mais amplo, não apenas focado no setor marítimo);

- Sim;
- Não.

- As ações da Marinha do Brasil, enquanto autoridade marítima, acompanham a tendência internacional de regulação cibernética no setor marítimo?

- Sim;
- Não;
- Não tenho informações sobre as ações da Marinha.

2.3.1 Limitações

O questionário foi distribuído para outras instituições, inclusive para representantes da iniciativa privada, porém não houve adesão significativa. Sendo assim, deve-se considerar que as respostas têm baixa representatividade no que se refere a percepção do setor privado brasileiro.

2.4 Síntese

No presente capítulo foram apresentadas as técnicas e os métodos utilizados para colher os resultados analisados nesta pesquisa. De maneira geral, foi aplicado o método der revisão

sistemática, baseado na técnica proposta pelo manual PRISMA, para sumarizar riscos e medidas mitigatórias no que se refere a segurança cibernética em instalações marítimas, propostos pela comunidade acadêmica internacional. Além disso, utiliza-se também o método de mineração de dados em texto, aplicando uma técnica baseada em python, para extrair a frequência de palavras relacionadas à segurança cibernética em documentos oficiais de nível político, brasileiros e americanos, como uma forma de representação do grau de discussão do assunto no nível político dos Estados referência. Por fim, o método de questionário é aplicado para colher a percepção brasileiras de Oficiais da Marinha, pesquisadores e sociedade civil. Vale ressaltar que as informações compiladas na revisão sistemática foram utilizadas na formulação dos questionários de maneira direta e que as respostas de outras perguntas, nº3 e º4, representam a percepção sobre o nível de discussão, colhido na mineração de dados em texto. Isso demonstra uma integração entre os métodos e técnicas, gerando, entre outros benefícios, a possibilidade de comparação entre os resultados de cada um.

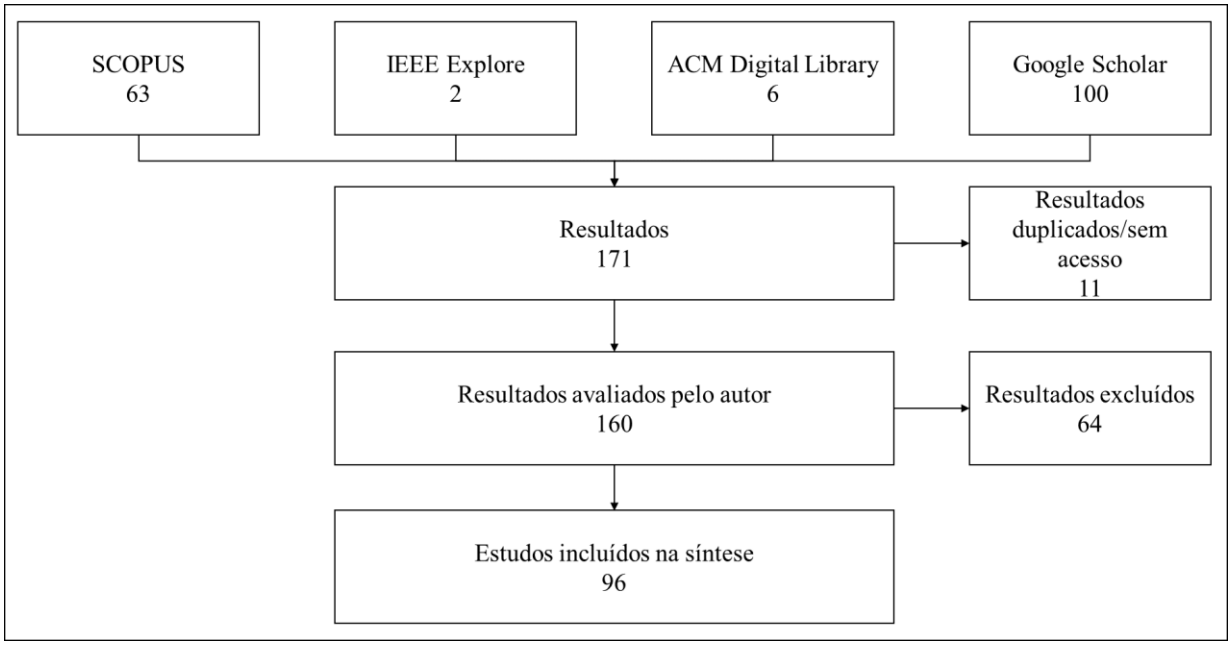
3 RESULTADOS E DISCUSSÃO

Neste capítulo são apresentados os resultados da revisão sistemática, da mineração de dados em texto e da aplicação do questionário, assim como reflexões relativas aos mesmos.

3.1 Revisão Sistemática de Literatura

As referências encontradas nas pesquisas eletrônicas foram agrupadas e ordenadas em sequência alfabética pelos nomes dos autores. Os resultados duplicados foram retirados, assim como os que não estavam disponíveis para acesso, no total de onze. Dessa forma, 160 referências foram apreciadas pelo autor e 96 atenderam todos os critérios estabelecidos previamente, conforme pode ser visualizado na Figura 8. A lista detalhada de referências no formato *BibTeX* encontra-se no link abaixo:
https://drive.google.com/file/d/1CNnFdXHFpmp06yTIa8UOb8Vh4ZsLVh7/view?usp=sharing.

Figura 8 – Fluxograma da revisão sistemática



Fonte: O autor, 2021.

A partir da leitura das referências incluídas na síntese é possível extrair uma série de informações valiosas. Dessa forma, são identificadas dezoito grandes fontes de risco para a segurança cibernética em instalações marítimas, Quadro 3, e vinte e seis propostas de medidas mitigatórias para essas ameaças, Quadro 4. As taxas de incidência de cada fonte de risco e

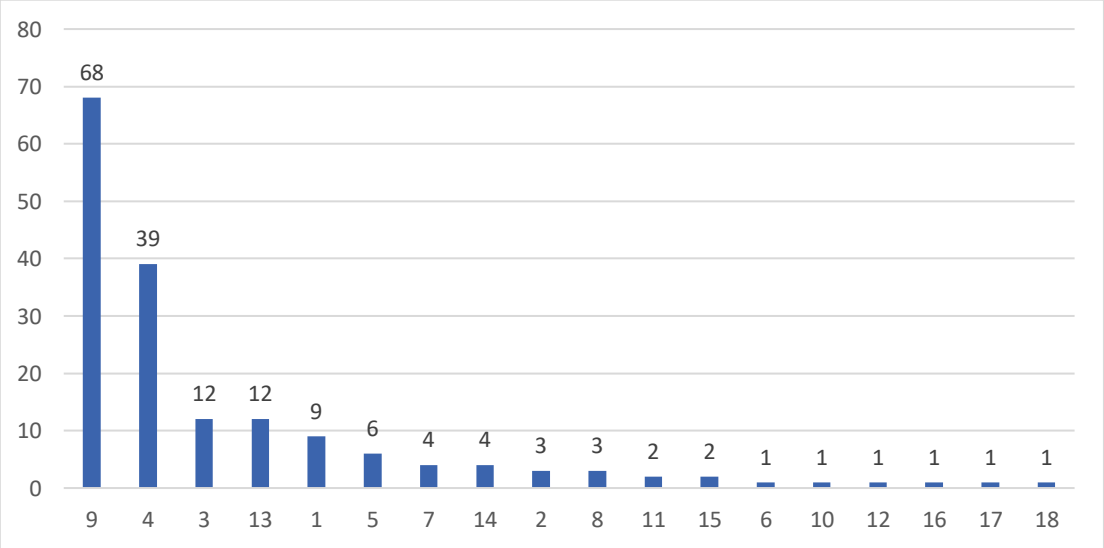
medida mitigatória em relação aos estudos podem sem visualizados nas figuras 9 e 10, respectivamente.

Quadro 3 – Fontes de riscos para a segurança cibernética em instalações marítimas

1	Carência de normas e regulações
2	Pouca produção de pesquisas na área
3	Falhas humanas e governança deficiente
4	Vulnerabilidades em sistemas amplamente empregados para navegação, como o GPS, AIS, ECDIS
5	Popularização de tecnologias de embarcações autônomas
6	Falta de legislação específica
7	Incidência crescente do número de ataques cibernéticos a instalações marítimas
8	Falta de recursos financeiros para a implementação de sistemas de segurança satisfatórios
9	Utilização, cada vez maior, de sistemas cibernéticos para controle de instalações marítimas
10	Dicotomia entre os níveis de alerta público e privado
11	Vulnerabilidades em softwares e tecnologias de prateleira
12	Guerra eletrônica
13	Conhecimento deficiente por parte de profissionais marítimos
14	Lentidão do ramo para adoção de medidas de segurança cibernética
15	Falta de padronização internacional em requisitos de segurança
16	Informações sobre ataques não são compartilhadas
17	Não há um sistema de certificação de segurança cibernética no ramo[3]
18	Operação remota

Fonte: O autor, 2021.

Figura 9 – Incidência da citação de cada risco nos estudos analisados



Fonte: O autor, 2021.

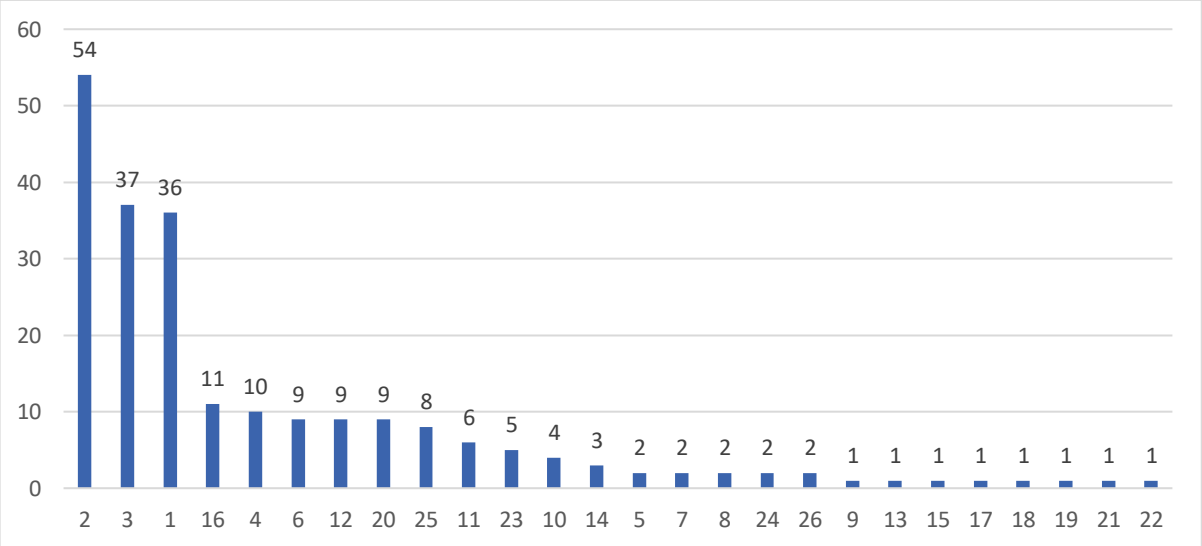
[3] Esse risco se refere a um sistema de certificação padronizado internacionalmente. É importante comentar que já existem iniciativas nacionais nesse sentido.

Quadro 4 - Propostas de medidas mitigatórias

1	Reforçar o ensino
2	Estabelecer normas e regulação
3	Implementar gerenciamento de riscos cibernéticos
4	Incentivar boas práticas de governança cibernética
5	Implementar planos de contingência
6	Compartilhar informações
7	Empregar sistemas alternativos ao GPS para navegação
8	Implementar autenticação de dados na recepção de sistemas de navegação
9	Implementar auxílios a navegação com tecnologia laser
10	Estabelecer estrutura de verificação de conformidade/*compliance*
11	Incentivar pesquisa em segurança cibernética marítima
12	Criar laboratórios em parceria público-privada
13	Empregar *ethical haking* para detecção de vulnerabilidades
14	Incentivar *think-tanks* na área
15	Criar de carreiras específicas, no setor marítimo, voltadas especificamente para segurança cibernética a bordo
16	Incentivar o nivelamento internacional de requisitos mínimos de segurança cibernética
17	Estabelecer requisitos mínimos de segurança para receptores de sinais de geolocalização, como GPS e AIS
18	Acompanhar a consciência situacional cibernética no setor marítimo
19	Implementar de uma base de ensino obrigatória para todos os profissionais do setor marítimo
20	Conscientizar gestores e líderes de instituições voltadas para o setor marítimo
21	Elaborar sistemas de inspeção para certificação de instituições
22	Manter o ensino de métodos tradicionais de navegação, independentes de informações eletrônicas, para profissionais da área
23	Normatizar centros de monitoramento de sistemas cibernéticos para instalações marítimas
24	Elaborar legislação específica para o setor
25	Fomentar parcerias público-privadas
26	Realizar exercícios de segurança cibernética

Fonte: O autor, 2021.

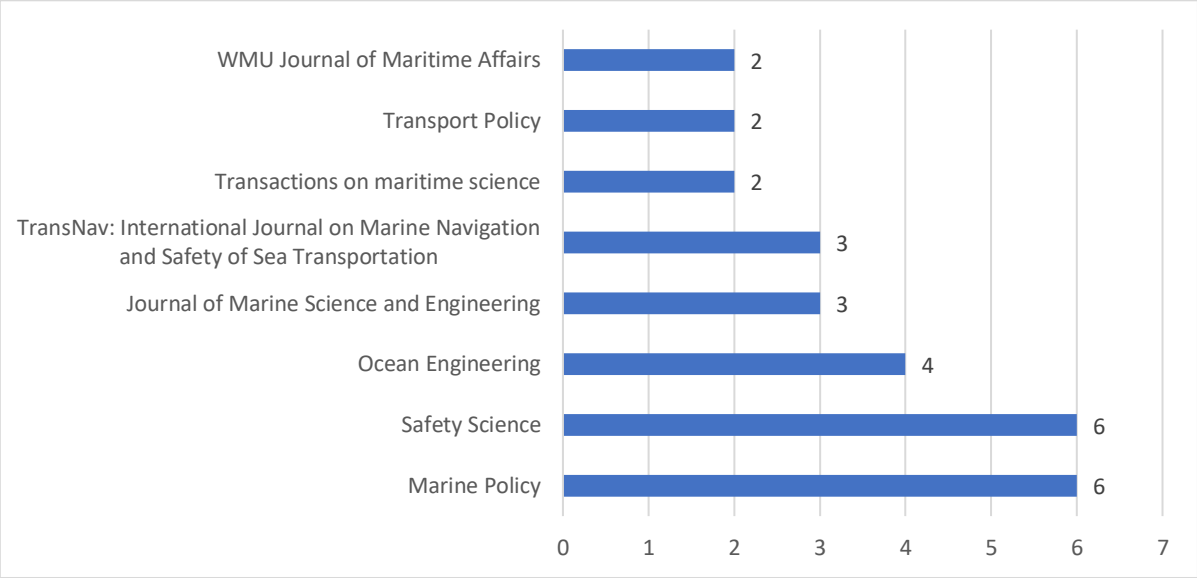
Figura 10 - Incidência da citação de cada medida mitigatória nos estudos analisados



Fonte: O autor, 2021.

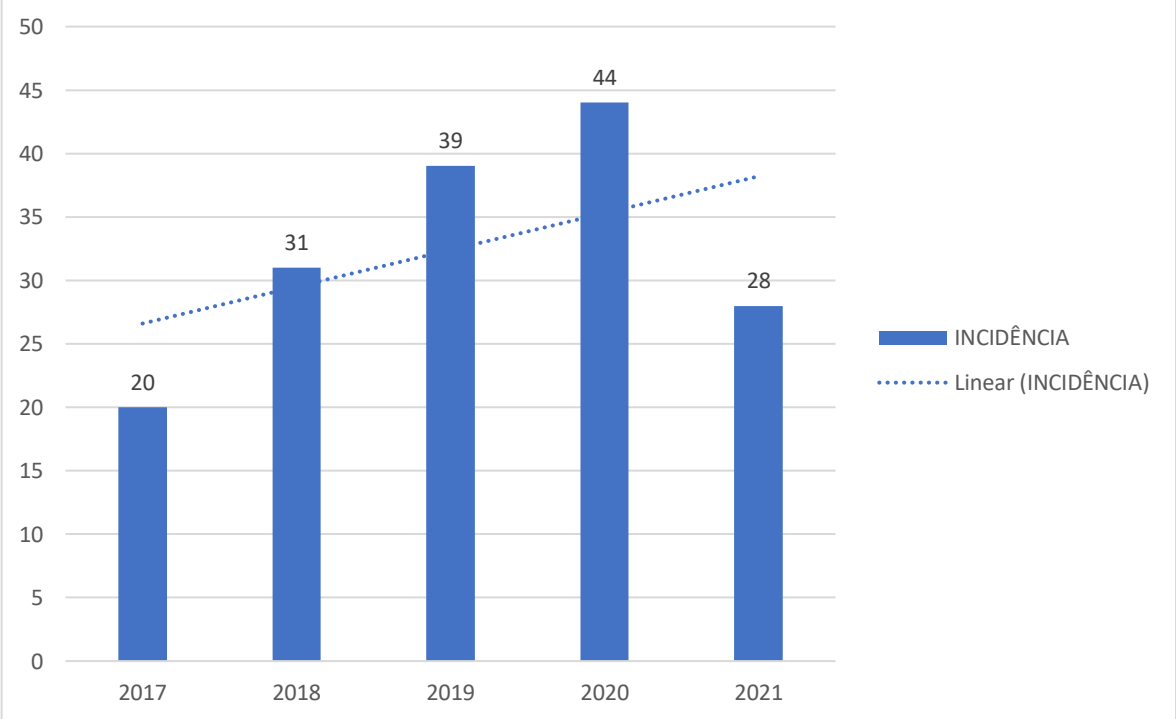
As análises individuais, sobre riscos e propostas de ações mitigatórias, de cada artigo podem ser visualizadas nos APÊNDICES B e C. Além desse levantamento foram realizadas análises, a partir dos dados de cada obra avaliada pelo autor. Foram mapeados os periódicos que com maior atuação entre os estudos avaliados, Figura 11, a distribuição dos estudos ao longo dos anos, Figura 12, e a distribuição global das filiações dos autores, Figura 13.

Figura 11 - Periódicos



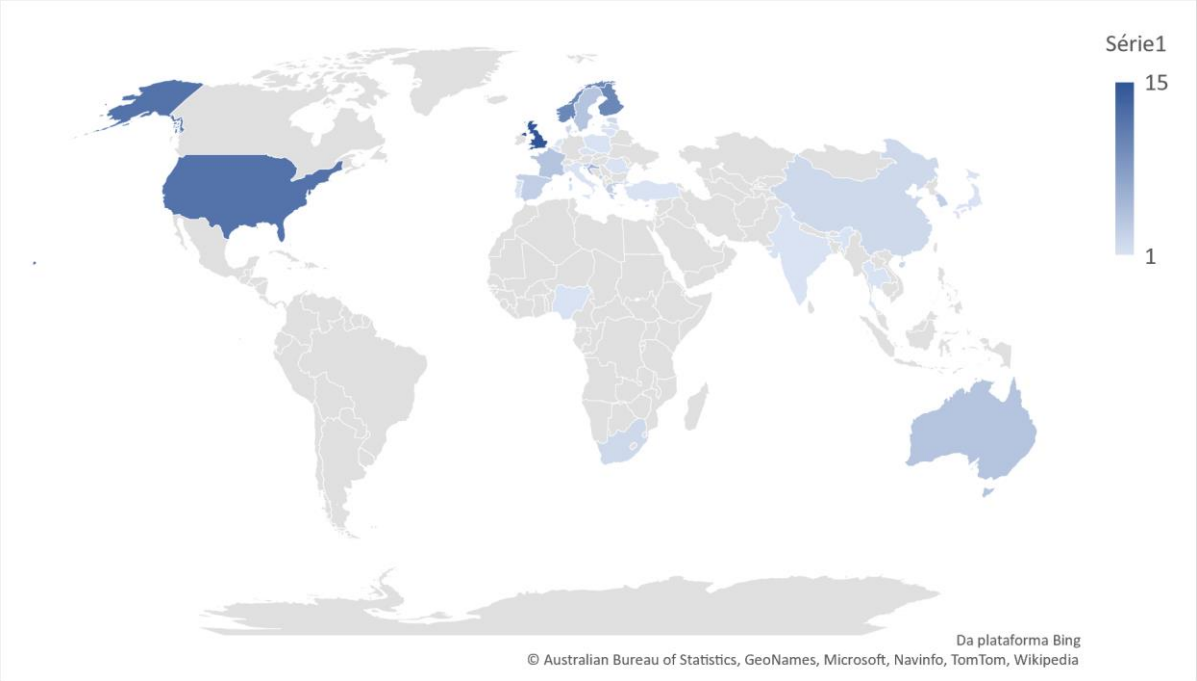
Fonte: O autor, 2021.

Figura 12 – Produções por ano



Fonte: O autor, 2021.

Figura 13 – Produções por país



Fonte: O autor, 2021.

A partir dos dados gerados, percebe-se que ao compilar as informações, dispersas em um conjunto de produções acadêmicas, foi possível criar uma visão geral de como o assunto, segurança cibernética em instalações marítimas, vem sendo tratado pela academia no nível internacional. Pode ser observado que, entre os riscos identificados, Quadro 3, os que mais chamam a atenção dos pesquisadores são o de nº9 (Utilização, cada vez maior, de sistemas cibernéticos para controle de instalações marítimas) e o de nº4 (Vulnerabilidades em sistemas amplamente empregados para navegação, como o GPS, AIS, ECDIS). Esse fato sinaliza para a necessidade de implementar ações para reforçar a segurança desses sistemas, cada vez mais presentes em instalações marítimas, e para conscientizar usuários. Já entre as ações mitigatórias identificadas, Quadro 4, as que apresentam uma maior incidência entre as obras analisadas são as de nº2 (Estabelecer normas e regulação), nº3 (implementar gerenciamento de riscos cibernéticos), e de nº1 (reforçar o ensino). As principais ações mitigatórias identificadas apresentam potencial para mitigar os principais riscos notados pela comunidade acadêmica internacional. De uma maneira geral os riscos mais amplos se referem a implementação de sistemas cibernéticos a bordo, fato que não pode ser contornado, e as vulnerabilidades inerentes a esses sistemas. As ações mitigatórias nº2, nº3 e nº1 fazem referências a fatores de governança essenciais para utilização, com segurança, desse tipo de sistema.

As análises secundárias apresentam outras informações importantes. Neste sentido, foram identificados poucos periódicos responsáveis pela publicação de mais de um artigo

acadêmico acerca do assunto tratado, Figura 11. Esse dado mostra que as iniciativas de estudos voltados para a área ainda se encontram dispersas. Ao refletir sobre a distribuição das obras por ano, Figura 12, fica clara a tendências crescente na produção de conteúdo, demonstrando um grande potencial para trabalhos futuros bem como o crescimento da preocupação acerca do tema na comunidade acadêmica internacional. Já a distribuição global de filiações, Figura 13, deixa claro que há uma concentração de estudos em alguns poucos Estados, com especial destaque para Reino Unido, Estados Unidos e Noruega. Percebe-se que países com tradição marítima se destacam nos estudos relacionados. É importante destacar a ausência do Estado brasileiro nesse contexto, demonstrando uma carência em pesquisa e desenvolvimento sobre o tema.

3.2 Mineração de Dados em Texto

Os documentos analisados foram o *Worldwide Threat Assessment* (WTA) *of the US Intelligence*, apresentado anualmente no congresso americano para expor ao nível político os temas mais desafiadores em relação à segurança nacional, o Relatório Anual da CREDN da câmara dos deputados do Brasil, documento onde são comentados os temas de maior relevo para essa comissão, e as ORCOM, documento através do qual o Comandante da Marinha do Brasil exprime suas orientações para a força. O WTA e o relatório anual da CREDN da câmara foram escolhidos por tratarem diversos assuntos no nível político dos Estados referência. Dessa forma espera-se que esses documentos sirvam como parâmetro de comparação sobre como cada Estado dispende sua atenção sobre os diversos assuntos discutidos. As ORCOM foram inseridas na análise com o objetivo de verificar o comportamento da MB em relação ao nível político brasileiro.

Tabela 3 - Anos analisados, por documento

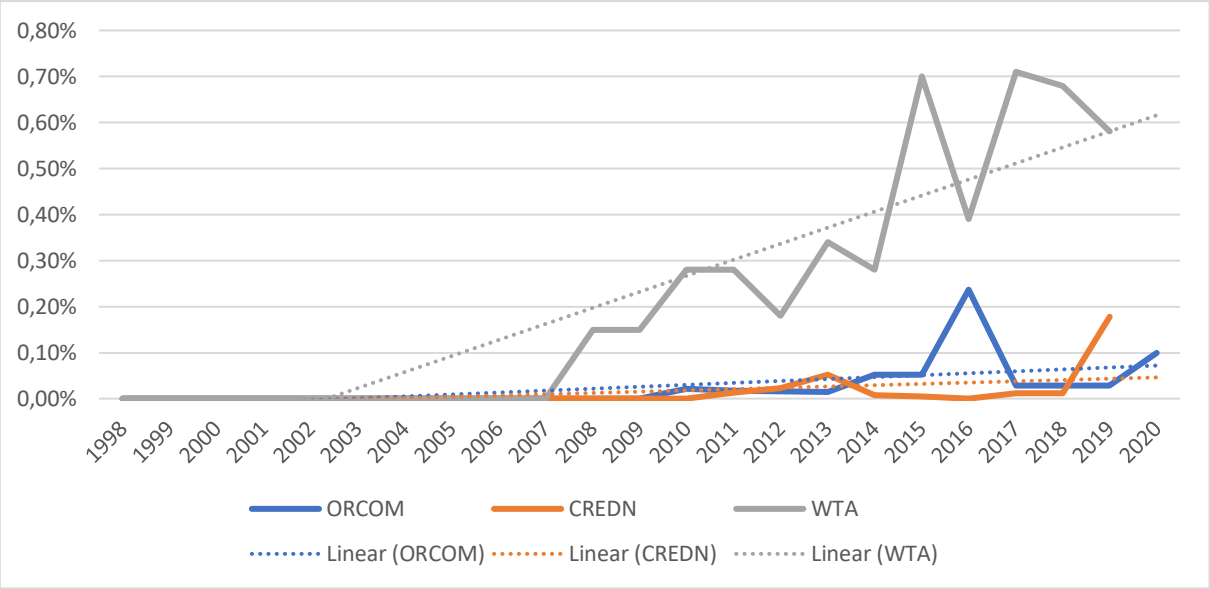
	Ano 20XX														
Documento	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20
WTA	X	X	X	X	X		X	X	X	X	X	X	X	X	
ORCOM	X	X	X	X	X	X	X	X	X		X	X			X
CREDN	X	X	X	X	X	X	X		X	X	X	X	X		

Fonte: O autor, 2021.

Foi considerada a janela temporal de 2006 até 2020, para a busca dos documentos, sendo encontrados os documentos referentes aos anos apresentados na Tabela 3. O algoritmo do

APÊNDICE A foi aplicado, sendo obtidas as frequências das palavras constantes nos documentos. Esses dados foram reunidos e apresentados na Figura 14, a unidade de referência considerada foi a porcentagem de palavras relacionadas em relação ao total de palavras no texto.

Figura 14 - Incidência de termos relacionados a segurança cibernética



Fonte: O autor, 2021.

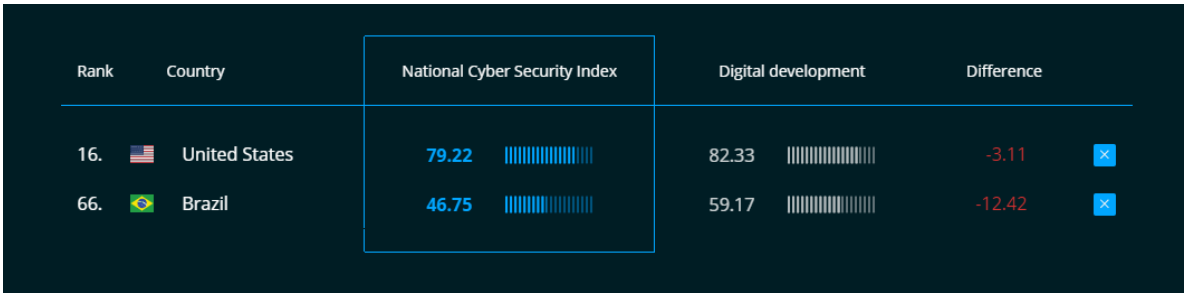
Além da informação citada anteriormente, foi possível listar as dez palavras mais citadas em cada documento analisado, por ano, conforme os APÊNDICES F, G e H. É interessante comentar que, no que se refere aos relatórios WTA, o termo *cyber* aparece entre os dez mais citados em 2015, 2017, 2018 e 2019. Isso reforça a ideia de que o tema segurança cibernética ganhou espaço no debate político referente a ameaças aos EUA, e que o nível de alerta sobre o assunto realmente é maior nos Estados Unidos. Por outro lado, nos documentos brasileiros analisados, esse mesmo termo não aparece entre os dez mais citados em nenhum ano. Dessa forma, fica claro que o assunto ainda carece de um tratamento apropriado. A MB acompanha o nível de discussão no nível político brasileiro, que está defasado em relação ao nível americano. Assim, nota-se que a segurança cibernética no mar pode receber uma maior atenção por parte da Autoridade Marítima brasileira, assim como o assunto, de forma ampla, deve receber maior atenção no nível político.

A análise, representada na Figura 14, deixa claro que há uma grande diferença na taxa de citações de termos relacionados à segurança cibernética, não apenas restrita ao ambiente marítimo, em documentos de nível político americanos e brasileiros. Essa informação pode ser confrontada com o índice de crescimento do número de usuários de internet nos Estados Unidos

e no Brasil, Figura 16. Nota-se que os dois Estados possuem uma taxa de crescimento semelhante. Dessa forma, entende-se que há uma deficiência na discussão do assunto no contexto brasileiro e essa deficiência se reflete em um nível mais baixo de segurança cibernética.

Esse fato pode ser observado no *National Cyber Security Index* (NCSI) (2021), um índice de segurança cibernética desenvolvido por uma iniciativa conjunta do governo da Estónia e do Programa de Desenvolvimento das Nações Unidas. Esse índice é construído a partir de 46 indicadores, divididos em 12 capacidades e 3 categorias (NCSI, 2021), pontuados por uma equipe de especialistas a partir de atos legais, documentos e websites oficiais dos Estados avaliados. Dessa forma, é possível notar que o tratamento do assunto em documentos oficiais reflete um maior índice de segurança, como pode ser observado nos casos brasileiro e americano.

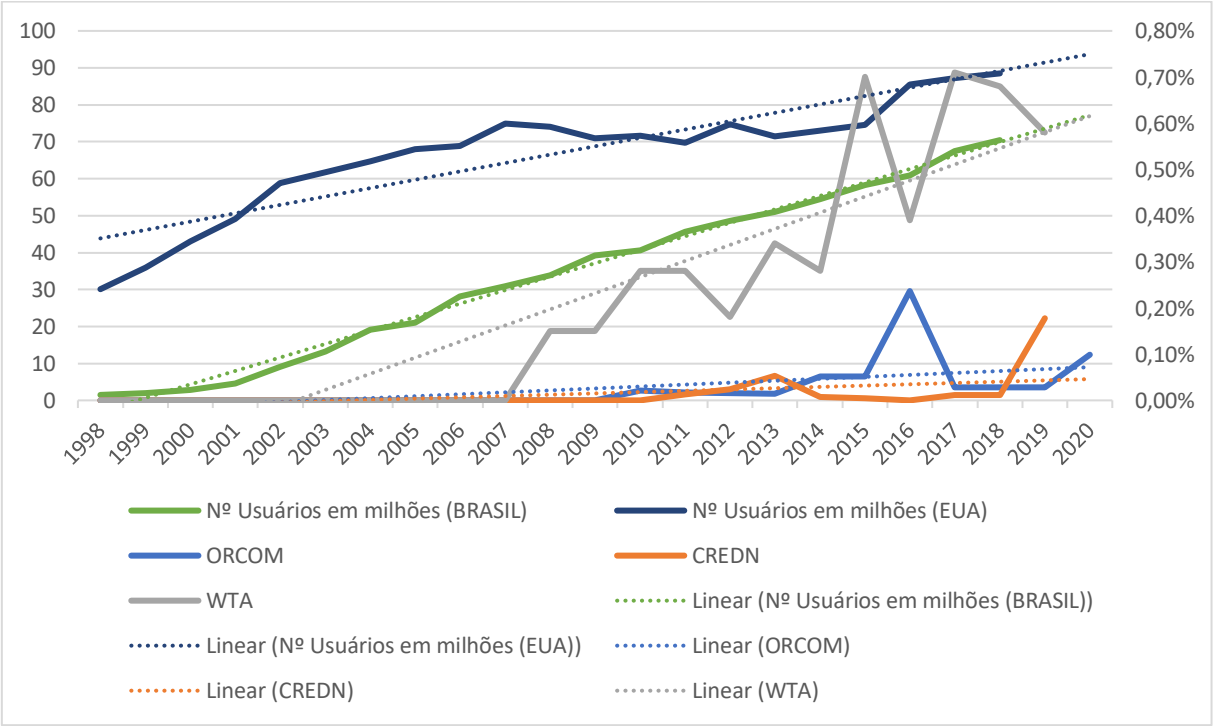
Figura 15 - Índice de segurança cibernética



Rank	Country	National Cyber Security Index	Digital development	Difference
16.	United States	79.22	82.33	-3.11
66.	Brazil	46.75	59.17	-12.42

Fonte: NCSI, 2021.

Figura 16 - Evolução do nº de usuários de internet ao longo dos anos



Fonte: The World Bank, 2021.

3.3 Questionário

O questionário para a sociedade foi distribuído por rede social e aplicativo de mensagens, LinkedIn e grupos de WhatsApp, alcançando 20 respondentes. O questionário para pesquisadores foi distribuído diretamente para os grupos de pesquisa, alcançando 34 respondentes. Como pesquisadores, foram considerados os integrantes do LSC/EGN, alunos e instrutores do PPGEM/EGN, Oficiais da MB formados no Curso de Aperfeiçoamento Avançado em Segurança da Informação e Comunicações, pesquisadores do IMM, Oficiais do CoNavOpEsp, responsáveis por operações cibernéticas, e pesquisadores do laboratório SICCCiber/UFF. O questionário para os Oficiais alunos do CPEM e CEMOS foi distribuído diretamente para os mesmos, alcançando 85 Oficiais alunos. Esses cursos foram considerados por atingirem um público de militares que estão sendo preparados para cargos de assessoria de alto nível (BRASIL, 2021). As respostas colhidas são apresentadas a seguir, por pergunta realizada.

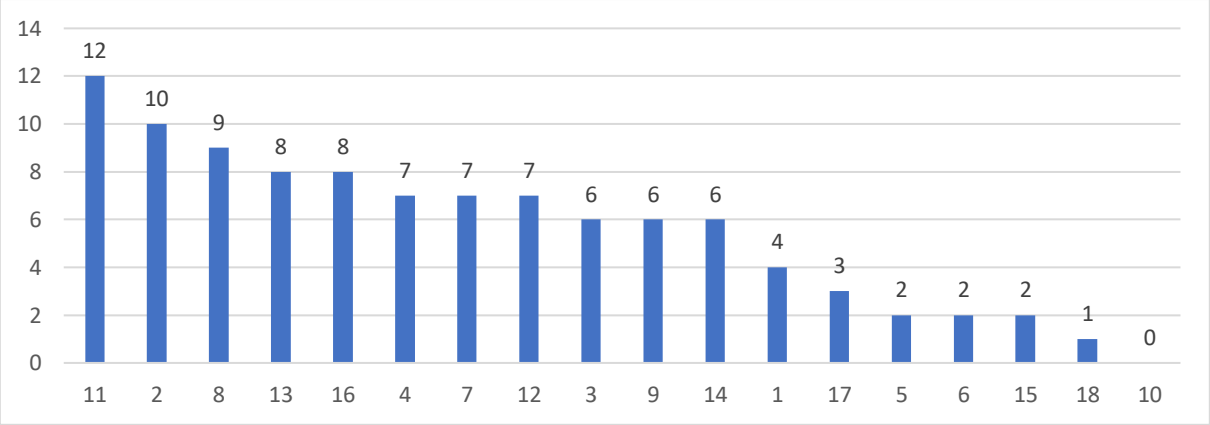
3.3.1 Primeira pergunta

Dentre os fatores de risco à segurança cibernética no setor marítimo, sinalize os cinco (5) considerados mais preocupantes:

1	Carência de normas e regulações;	7	Incidência crescente do número de ataques cibernéticos a instalações marítimas;
2	Pouca produção de pesquisas na área;	8	Falta de recursos financeiros para a implementação de sistemas de segurança satisfatórios;
3	Falhas humanas e governança deficiente;	9	Utilização, cada vez maior, de sistemas cibernéticos para controle de instalações marítimas;
4	Vulnerabilidades em sistemas amplamente empregados para navegação, como o GPS, AIS, ECDIS;	10	Dicotomia entre os níveis de alerta público e privado;
5	Popularização de tecnologias de embarcações autônomas;		
6	Falta de legislação específica;		

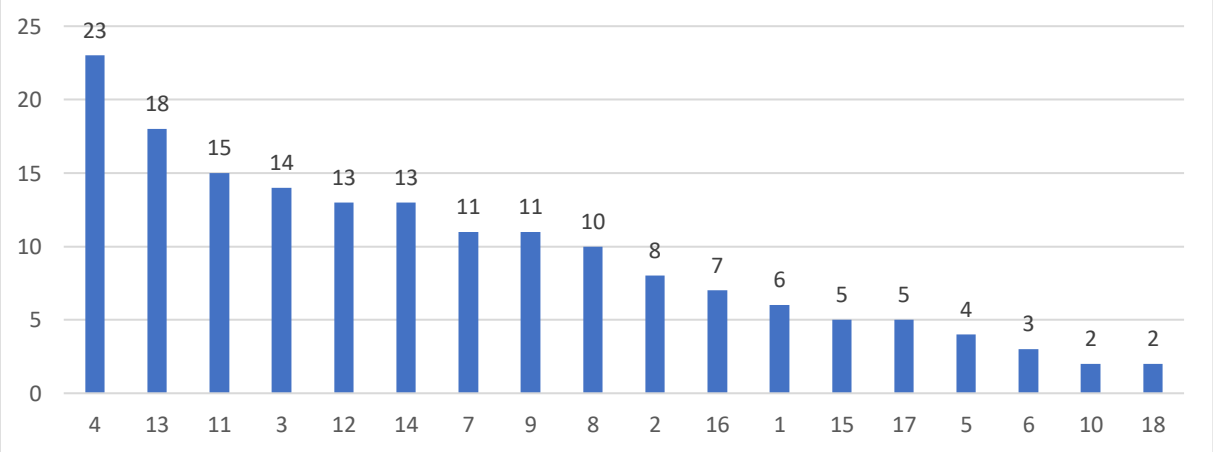
11	Vulnerabilidades em softwares e tecnologias de prateleira;	15	Falta de padronização internacional em requisitos de segurança;
12	Guerra eletrônica;		
13	Conhecimento deficiente por parte de profissionais marítimos;	16	Informações sobre ataques não são compartilhadas;
		17	Não há um sistema de certificação de segurança cibernética no ramo;
14	Lentidão do ramo para adoção de medidas de segurança cibernética;	18	Operação remota.

Figura 17 – Primeira pergunta/Sociedade



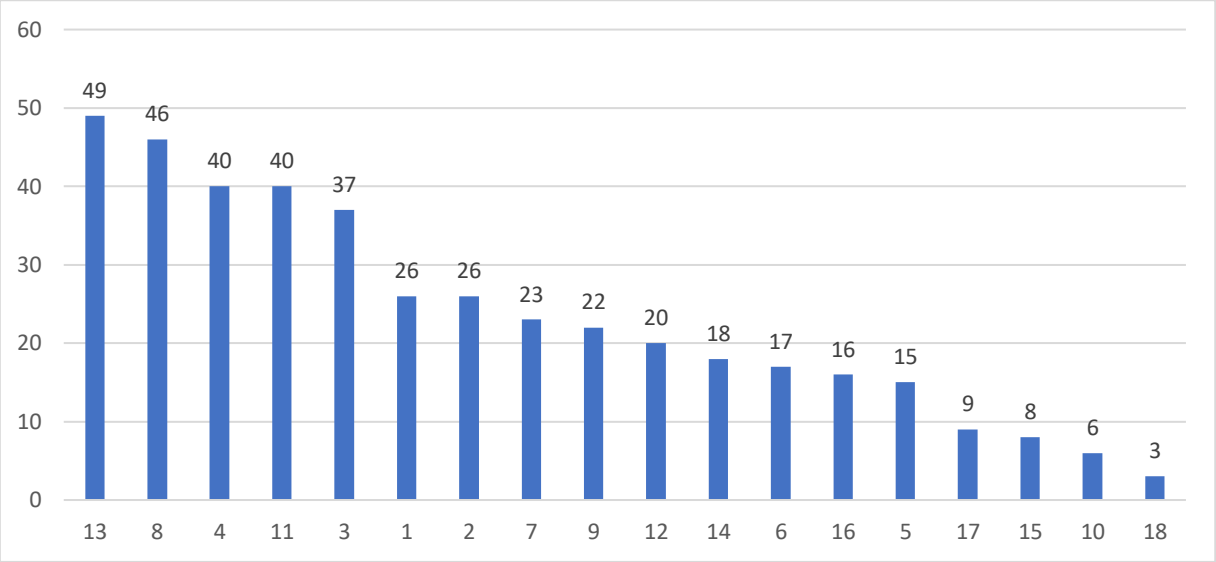
Fonte: O autor, 2021.

Figura 18 – Primeira pergunta/Pesquisadores



Fonte: O autor, 2021.

Figura 19 – Primeira Pergunta/Oficiais Alunos



Fonte: O autor, 2021.

É interessante notar a diferença de percepção entre os grupos analisados. Para a sociedade o maior risco foi o nº11 (vulnerabilidades em softwares e tecnologias de prateleira), para pesquisadores foi o nº4 (vulnerabilidades em sistemas amplamente empregados para navegação, como o GPS, AIS, ECDIS) e para os Oficiais alunos da MB foi o nº13 (conhecimento deficiente por parte de profissionais marítimos). Além dos fatores de risco apresentados nas opções da primeira pergunta, foram incluídos quatro outros por Oficiais Alunos da MB, Tabela 4.

Tabela 4 - Riscos idenficicados por Oficiais alunos da MB

Risco	Nº de citações
Inexistência de disciplina específica no curriculum de formação de profissionais marítimos	1
Desconhecimento sobre os impactos de um possível ataque cibernético	1
Falta de atualização dos conteúdos de cursos oferecidos sobre o assunto	1
Mentalidade de segurança cibernética deficiente	1

Fonte: O autor, 2021.

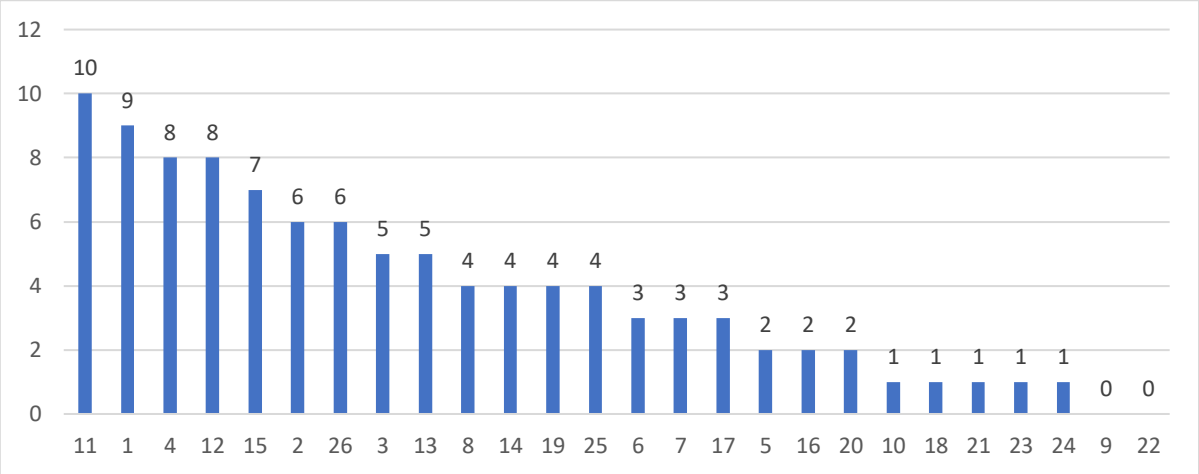
3.3.2 Segunda Pergunta

- Dentre ações abaixo, sinalize as cinco (5) consideradas importantes para fortalecer o poder marítimo brasileiro no que se refere à segurança cibernética:

1	Reforçar o ensino;		mínimos de segurança cibernética;
2	Estabelecer normas e regulação;	17	Estabelecer requisitos mínimos de segurança para receptores de sinais de geolocalização, como GPS e AIS;
3	Implementar gerenciamento de riscos cibernéticos;	18	Acompanhar a consciência situacional cibernética no setor marítimo;
4	Incentivar boas práticas de governança cibernética;	19	Implementar de uma base de ensino obrigatória para todos os profissionais do setor marítimo;
5	Implementar planos de contingência;	20	Conscientizar gestores e líderes de instituições voltadas para o setor marítimo;
6	Compartilhar informações;	21	Elaborar sistemas de inspeção para certificação de instituições;
7	Empregar sistemas alternativos ao GPS para navegação;	22	Manter o ensino de métodos tradicionais de navegação, independentes de informações eletrônicas, para profissionais da área;
8	Implementar autenticação de dados na recepção de sistemas de navegação;	23	Normatizar centros de monitoramento de sistemas cibernéticos para instalações marítimas;
9	Implementar auxílios a navegação com tecnologia laser;[4]	24	Elaborar legislação específica para o setor;
10	Estabelecer estrutura de verificação de conformidade/*compliance*;	25	Fomentar parcerias público-privadas;
11	Incentivar pesquisa em segurança cibernética marítima;	26	Realizar exercícios de segurança cibernética.
12	Criar laboratórios em parceria público-privada;		
13	Empregar *ethical haking* para detecção de vulnerabilidades;		
14	Incentivar *think-tanks* na área;		
15	Criar de carreiras específicas, no setor marítimo, voltadas especificamente para segurança cibernética a bordo;		
16	Incentivar o nivelamento internacional de requisitos		

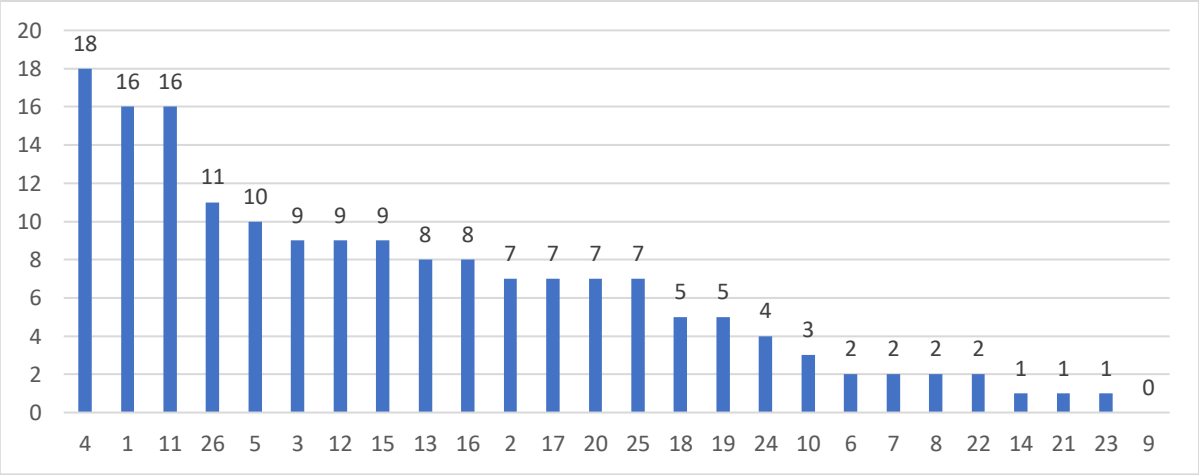
[4] Essas tecnologias envolvem o emprego da faixa de micro-ondas do espectro eletromagnético. Hoje já estão disponíveis uma série de aplicações como o *Laser Imaging Detection and Ranging* (LIDAR), sistema que utiliza a mesma lógica do radar para gerar imagens com sinais *laser.*

Figura 20 – Segunda pergunta/Sociedade



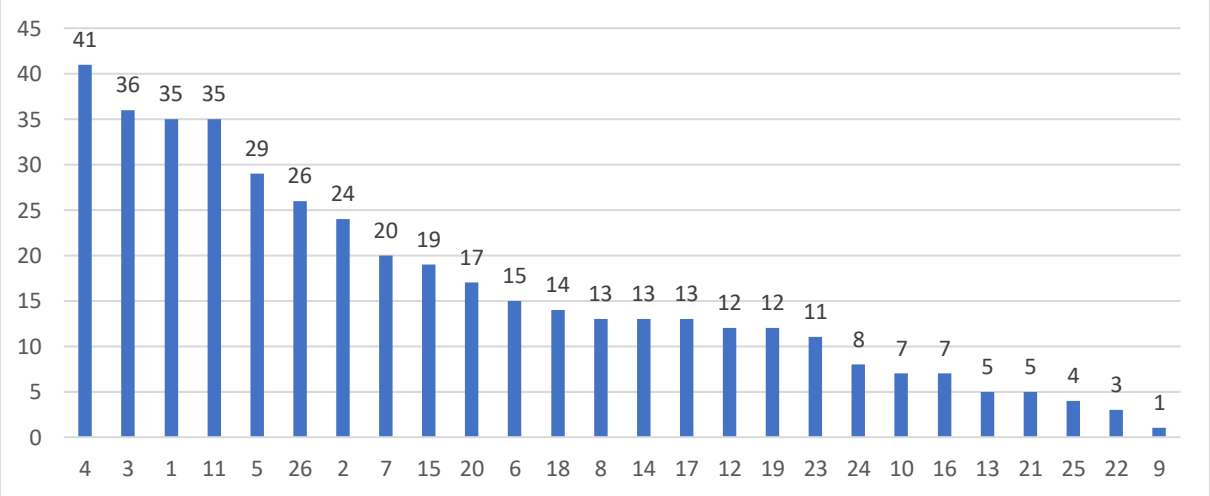
Fonte: O autor, 2021.

Figura 21 – Segunda pergunta/Pesquisadores



Fonte: O autor, 2021.

Figura 22 – Segunda pergunta/Oficiais Alunos



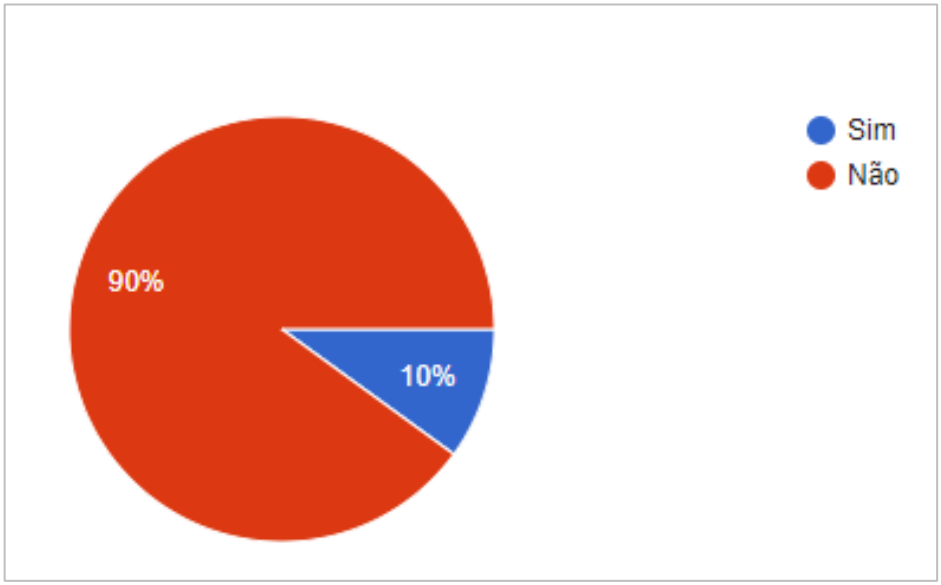
Fonte: O autor, 2021.

Em relação a medidas mitigatórias, para a sociedade a mais importante seria a de nº11 (incentivar pesquisa em segurança cibernética marítima), para pesquisadores e Oficiais alunos foi o nº4 (incentivar boas práticas de governança cibernética). Esses dados levam à percepção de que há um certo alinhamento entre o entendimento da academia e Oficiais alunos, no que se refere a medidas mitigatórias. Também é importante destacar que a medida mitigatória de nº9 (implementar auxílios a navegação com tecnologia laser) teve poucas citações, demonstrando que ainda carece de amadurecimento no Brasil.

3.3.3 Terceira pergunta

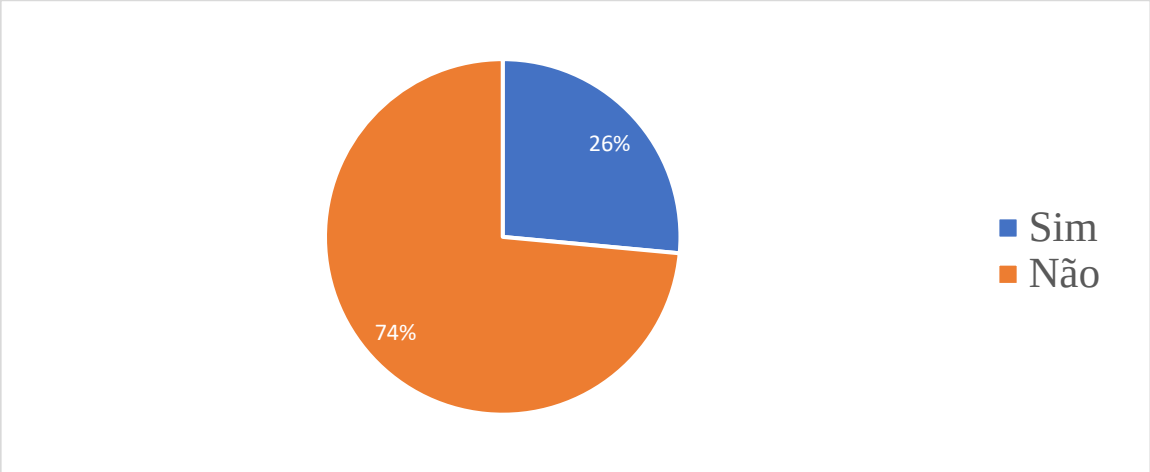
Tendo em vista a atual tendência internacional de fortalecimento da segurança cibernética, a postura Brasileira, no que se refere a políticas públicas, em relação ao assunto pode ser considerada satisfatória? (considere neste caso um escopo mais amplo, não apenas focado no setor marítimo);

Figura 23 – Terceira pergunta/Sociedade



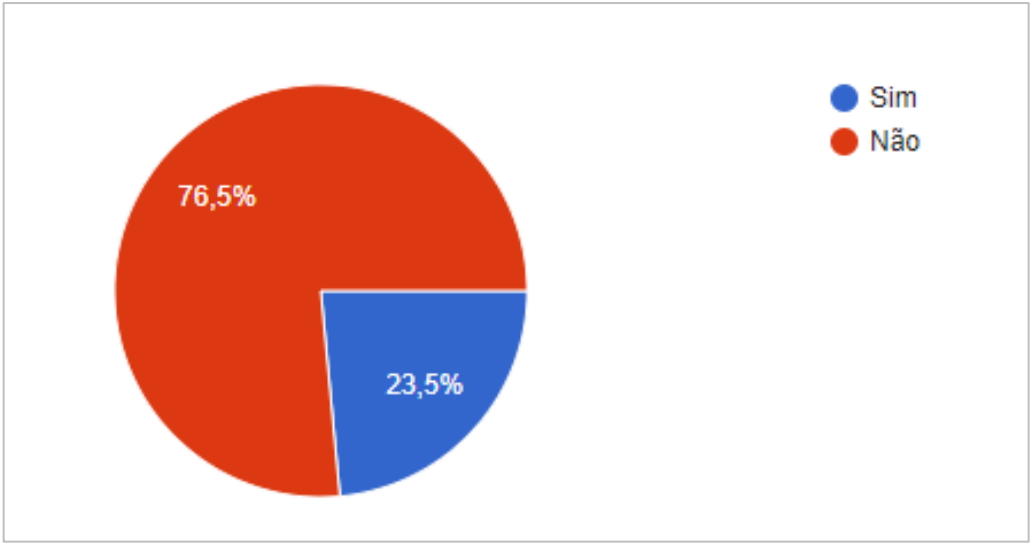
Fonte: O autor, 2021.

Figura 24 – Terceira pergunta/Pesquisadores



Fonte: O autor, 2021.

Figura 25 – Terceira pergunta/Oficiais Alunos



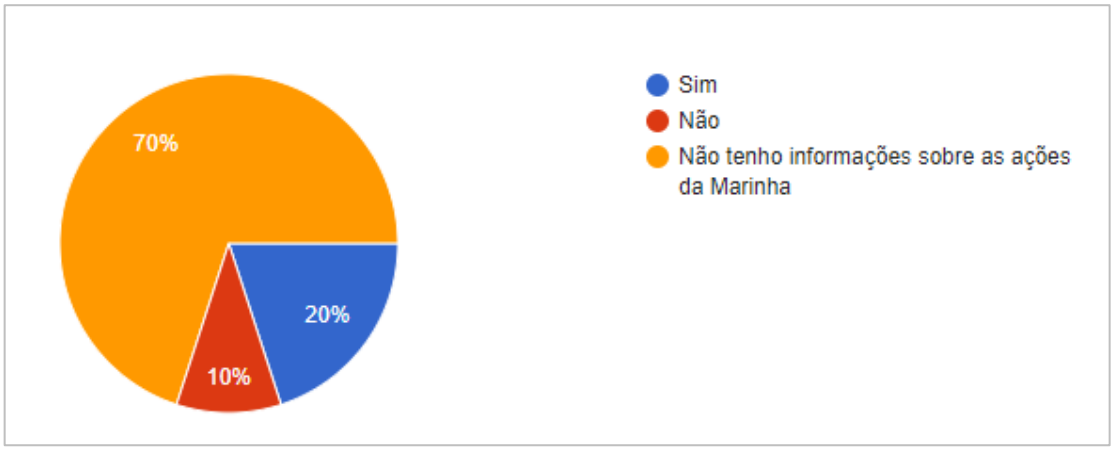
Fonte: O autor, 2021.

Em relação a terceira pergunta, fica claro de que existe, em todos os grupos, a percepção de que o Estado brasileiro não está atuando de maneira eficaz no que se refere a segurança cibernética de maneira ampla.

3.3.4 Quarta Pergunta

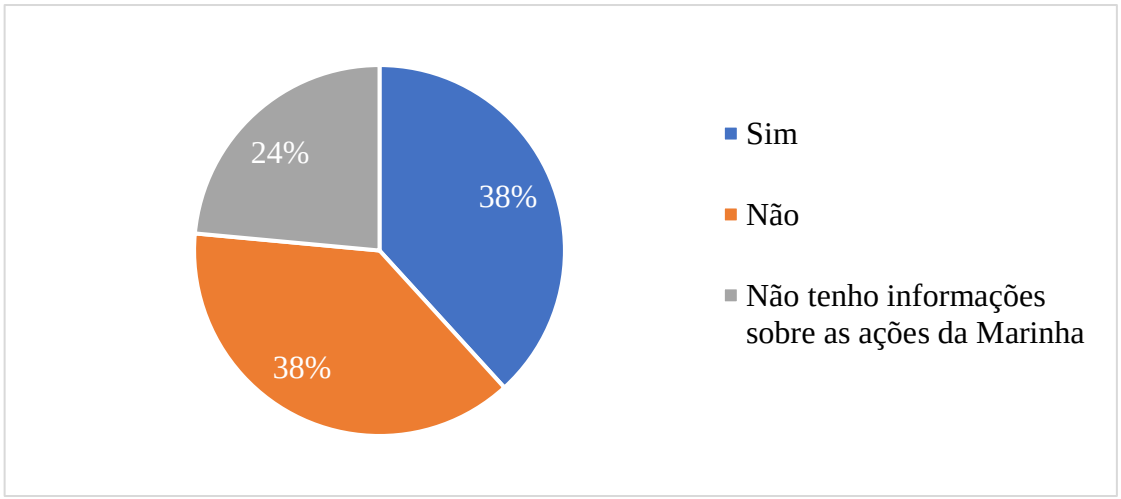
As ações da Marinha do Brasil, enquanto autoridade marítima, acompanham a tendência internacional de regulação cibernética no setor marítimo?

Figura 26 – Quarta pergunta/Sociedade



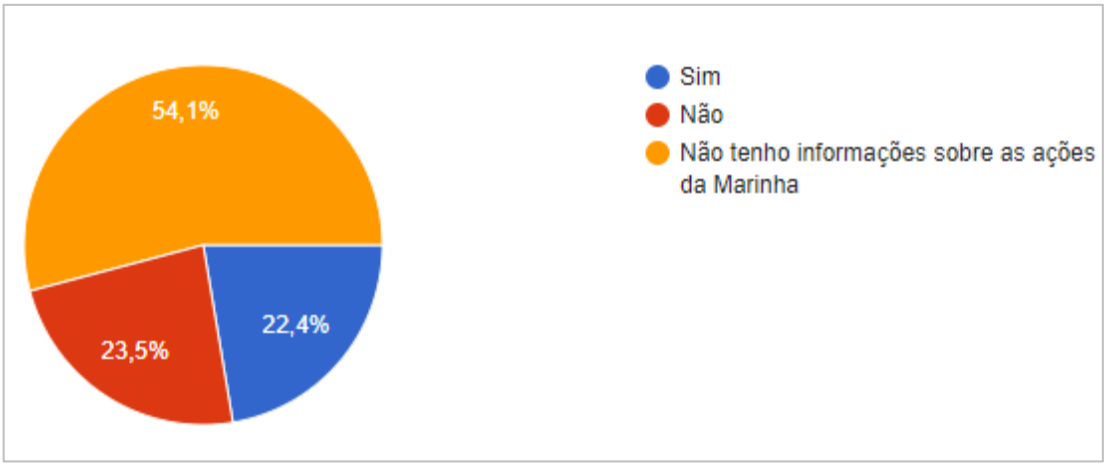
Fonte: O autor, 2021.

Figura 27 – Quarta pergunta/Pesquisadores



Fonte: O autor, 2021.

Figura 28 – Quarta pergunta/Oficiais Alunos



Fonte: O autor, 2021.

A quarta pergunta, deixa claro que, entre a sociedade civil e Oficiais alunos, há um grande índice de desconhecimento de ações da Marinha do Brasil sobre o tema. É necessário destacar que, em todos os grupos, uma minoria acredita que as ações da MB no setor têm sido satisfatórias, o que reflete a tendência observada sobre segurança cibernética em relação ao Estado brasileiro como um todo.

3.4 Discussão

Após a apresentação dos resultados é importante realizar alguns comentários. A revisão sistemática possibilitou a identificação de fontes de risco, Quadro 3, e medidas mitigatórias, Quadro 4, que foram utilizadas como parâmetro para a elaboração das perguntas 1 e 2 dos questionários. O fato de apenas quatro fontes de risco terem sido incluídas, Tabela 4, demonstra que as fontes identificadas atendem a maioria dos respondentes. No que se refere às propostas de medidas mitigatórias, não houve inclusão. Esses dados reforçam a confiabilidade dos resultados da revisão sistemática. Sendo assim, é possível notar que o Estado brasileiro, e a Marinha do Brasil, podem utilizar as fontes de risco e medidas mitigatórias encontradas na presente pesquisa para elaborar políticas de fortalecimento da segurança cibernética no ambiente marítimo.

Com a mineração de dados, foram extraídos dados secundários de grande importância para o entendimento do contexto atual. O mapeamento dos periódicos, Figura 11, que mais produzem conteúdo sobre os assuntos analisados facilita o acompanhamento do estado da arte e o monitoramento de novas tendências. A Figura 12 apresenta a evolução do número de obras analisadas, de acordo com o ano de publicação. Dessa forma, é possível notar que o assunto vem sendo cada vez mais abordado, indicando um gradativo crescimento em sua importância. Ao visualizar a Figura 13, nota-se que poucos países concentram a maior parte das produções sobre o tema em questão. É importante destacar que a participação brasileira na produção de conteúdo sobre o assunto ainda é baixa, mas demonstra sinais de que há potencial para o desenvolvimento na área, conforme Leite Junior e Sá (2020) e Leite Junior, *et al.* (2021). Os Apêndices F, G e H apresentam um outro subproduto que possui grande potencial para análises futuras, pois exprime de forma quantitativa os assuntos mais abordados em documentos de nível político. Algumas das palavras mais citadas ao longo dos anos nas ORCOM são pessoal e concurso. Essas palavras refletem os planos da força de expansão de sua força de trabalho para atender aos planos de criação da segunda esquadra e construção de meios. Dessa forma, essa técnica pode ser aplicada para analisar outros assuntos e outros documentos de interesse. Os

dados obtidos podem fornecer subsídios para análises de tendências nos contextos nacional e internacional.

A mineração de dados em texto também extraiu de maneira objetiva o grau de discussão do assunto segurança cibernética nos documentos oficiais analisados, Figura 14. É possível notar que o nível de discussão no Brasil está bem abaixo do que se observa nos Estado Unidos, e que essa tendência é seguida pelas ORCOM. Entretanto verifica-se que o número de usuários de internet nesses dois Estados demonstra uma taxa de crescimento semelhante, Figura 16, explicitando um descompasso entre a utilização de tecnologias digitais e a discussão sobre segurança. Ao observar o NCSI, Figura 15, nota-se que há uma grande diferença entre os índices de segurança cibernética entre os Estados avaliados. Assim, é possível perceber indícios de que o grau de discussão do assunto no nível político se reflete em um melhor índice de segurança cibernética. A terceira pergunta reforça essa percepção, de que o nível de discussão no Brasil ainda carece de amadurecimento. A quarta pergunta evidência o fato, já observado na mineração de texto, de que a autoridade marítima brasileira, assim como o nível político de maneira geral, ainda desenvolve pouco o assunto tratado no nível decisório.

Os resultados encontrados demonstram especial importância, pois fazem referência a um assunto que, apesar de pouco explorado no contexto nacional, apresenta uma adesão crescente por pesquisadores no nível internacional. O caráter estratégico do ambiente marítimo para o Estado brasileiro, como fonte de recursos e via de comunicações, faz com que a manutenção da estabilidade do meio seja fundamental para a defesa dos interesses nacionais. Para isso, a consciência situacional, no que se refere a ameaças, deve ser reforçada e o acompanhamento do estado da arte nas diversas questões de segurança envolvendo o mar deve ser constante. Nesse sentido, o presente estudo fornece informações relevantes para assessoria no que se refere a questões de segurança cibernética no ambiente marítimo.

Ao analisar os produtos provenientes da revisão sistemática, em especial as palavras mais citadas nos documentos analisados, Apêndices F, G e H. Nota-se que os documentos brasileiros apresentam um nível de maturidade mais baixo, quando comparados aos americanos. Como comentado anteriormente, o assunto segurança cibernética não aparece entre os 10 mais citados nos documentos brasileiros analisados, demonstrando uma lacuna no tratamento do assunto. Essa tendência se reflete na atuação da MB, que também deixa a desejar no tratamento do tema. Percebe-se que há uma tendência de que a MB acompanhe o comportamento do nível político brasileiro. Sendo assim, uma maior abordagem pelo nível político poderá ampliar a atuação da MB.

Os resultados dos questionários demonstram que há um nível preocupante de desconhecimento no que se refere ao assunto por Oficiais da MB. Sendo assim é necessário que haja um reforço por parte do sistema de ensino naval no que se refere ao tema. Um fator importante é a diferença de gerações, há uma tendência de que Oficias mais jovens apresentem um maior interesse no assunto, enquanto Oficiais de idade mais avançada podem apresentar resistência. Dessa forma, é importante criar canais de comunicação entre gerações na força, de forma a fazer com que os conhecimentos relacionados ao ambiente cibernético cheguem aos tomadores de decisão, através de assessoria apropriada.

Nesse contexto o desenvolvimento tecnológico também é fundamental. O domínio de tecnologias cibernéticas torna possível uma maior consciência situacional sobre capacidades e vulnerabilidades desses sistemas. O desenvolvimento nacional dessas tecnologias, associado a sistemas de certificação de segurança cibernética, apresenta um grande potencial de redução de riscos. Além disso, a capacidade de exportar tecnologias representa uma importante vantagem estratégica. O domínio tecnológico sobre sistemas utilizados por outros facilita o planejamento de estratégias de enfrentamento e funciona, também, como elemento dissuasório. Um exemplo a ser citado é o do submarino nuclear, que perderia grande parte de seu poder dissuasório caso fosse implantadas vulnerabilidades em seus sistemas cibernéticos. Dessa forma, é importante reforçar que o fomento ao desenvolvimento nacional na área é um elemento estratégico para o futuro.

Por fim, percebe-se que os métodos utilizados forneceram resultados complementares que, após análise qualitativa, se reforçaram e possibilitaram conclusões mais sólidas. A presente pesquisa também apresentou a característica de congregar análises quantitativa e qualitativas, demonstrando a possibilidade de aplicação de metodologias híbridas em ciências sociais. Assim, nota-se que o conjunto de métodos e técnicas empregado apresenta um caráter inovador, assim como um grande potencial para detecção de tendências, em assuntos diversos, e planejamento de políticas públicas.

4 CONCLUSÃO

A presente pesquisa foi capaz de identificar riscos referentes a segurança cibernética em instalações marítimas, assim como medidas mitigatórias para enfrentá-los, objetivo primário do trabalho. Os dados utilizados foram obtidos de maneira sistemática, utilizando uma abordagem híbrida, unindo três métodos distintos para formar um quadro maior sobre o tema proposto. Discutiu-se a importância da segurança cibernética nas relações de poder no contexto das relações internacionais e em questões de segurança marítima, trazendo à tona a necessidade de se enfrentar essa problemática, de acordo com o objetivo específico a. A literatura acadêmica internacional foi revisada, utilizando uma metodologia impessoal e de fácil reprodução, conforme o objetivo específico b. Os dados minerados em documentos oficiais, americanos e brasileiros, foram obtidos de maneira automatizada empregando técnicas de programação, atendendo o objetivo específico c. Por fim, as percepções de três grupos sociais distintos foram colhidas por meio de questionários e tratadas, fornecendo ao leitor uma amostra da percepção destes grupos acerca da realidade brasileira, satisfazendo o objetivo específico d. A reunião das informações geradas permite responder as questões básica e secundárias do trabalho, assim como a hipótese proposta. Dessa forma, é possível observar que a pesquisa atingiu seus objetivos, produzindo conhecimento que contribuirá para a formulação de políticas públicas que objetivem o fortalecimento da segurança cibernética no ambiente marítimo. É importante destacar que o conjunto de métodos e técnicas empregado, com características inovadoras no contexto das ciências sociais, apresenta grande potencial para aplicações futuras.

4.1 Considerações Finais

O presente estudo demonstrou, de acordo com a questão básica proposta, que há medidas de segurança cibernéticas, específicas para o meio marítimo, propostas pela comunidade acadêmica internacional que apresentam potencial para serem implementadas no Brasil, como políticas públicas. Se observou que a presença do tema segurança cibernética nas ORCOM e nos relatórios da CREDN não são compatíveis com as necessidades brasileiras, conforme questão secundária a. Também se constatou que a presença do tema segurança cibernética nas ORCOM acompanha a tendência dos relatórios da CREDN da câmara dos deputado, respondendo a questão secundária b. Assim, provou-se a hipótese levantada de que há medidas de segurança cibernética, focadas no meio marítimo, propostas pela comunidade acadêmica internacional que podem servir de base para a criação de políticas públicas no Brasil.

Os riscos e propostas de medidas mitigatórias apresentados são úteis como referências para que a Marinha do Brasil possa desenvolver políticas públicas capazes de suprir as lacunas identificadas. A metodologia utilizada pode ser expandida utilizando mão de obra especializada, com tempo e recursos para pesquisa, abordando mais bases de dados e ampliando o número de referências analisadas. Além disso, é possível estudar cada medida mitigatória proposta, individualmente, e como seria possível implementá-las na realidade brasileira. Essa expansão apresenta um grande potencial para fornecer uma visão ainda mais precisa do estado da arte sobre o assunto, dando aos decisores da Marinha do Brasil ainda mais subsídios. Sugere-se que a Marinha direcione esforços para a conscientização de seus militares, especialmente aqueles com possibilidade de ocupar funções com grande poder decisório.

4.2 Sugestões para Trabalhos Futuros

Sugere-se que os riscos identificados sejam analisados individualmente, no contexto das marinhas de guerra e mercante brasileiras, para identificação de vulnerabilidades e implementação de modelos apropriados para o gerenciamento dos mesmos. As medidas mitigatórias propostas também devem ser avaliadas de maneira minuciosa, servindo como referência para a elaboração de propostas de políticas públicas por parte da autoridade marítima brasileira. Assim, sugere-se o estudo aprofundado de cada medida mitigatória proposta, suas possibilidades e limitações para o caso brasileiro, e de propostas de implementação. Com isso será possível melhor o nível de segurança cibernética no Brasil, aumentando a confiabilidade das infraestruturas críticas nacionais.

REFERÊNCIAS

ADEE, S. The Hunt for the Kill Switch. **IEEE Spectrum**, v. 45, n. 5, p.34-39, 2008.

ALMSLMANY, A., WANG, C. e CAO, Q. Advanced deceptive jamming model based on DRFM sub-Nyquist sampling. In: 2016 13th **International Bhurban Conference on Applied Sciences and Technology**, IEEE, p. 727-73.

BARRETT, M. P. **Framework for Improving Critical Infrastructure Cybersecurity**. 2018. Disponível em: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11. Acesso em: 26 de abr. de 2021.

BEIRÃO, A. P. "Segurança no Mar": que segurança? In: BEIRÃO, A.P E PEREIRA, A.C. ALVES. (Org.), **Reflexões sobre a Convenção do Direito do Mar**. Brasília: FUNAG, 2014. P. 127-166. Disponível em: http://funag.gov.br/loja/download/1091-Convencao_do_Direito_do_Mar.pdf. Acesso em: 07 de mar. de 2021.

BERLIN, I. **Against the Current** – Essays in the History of Ideas. New York: The Viking Press, 1980.

BHATTI, J.; HUMPHREYS, T. E. Hostile control of ships via false GPS signals: Demonstration and detection. **NAVIGATION: Journal of the Institute of Navigation**, v. 64, n. 1, p. 51-66, 2017.

BIMCO. **The Guidelines on Cyber Security Onboard Ships**. Versão 4. 2020. Disponível em: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships. Acesso em: 26 de abr. de 2021.

BRASIL. Estado Maior da Armada. EMA-305 – **Doutrina Militar Naval**. Brasília, 2017.

BRASIL. **Lei Complementar Nº97, de 9 de junho de 1999**. Dispõe sobre as normas gerais para a organização, o preparo e o emprego das Forças Armadas. 1999.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília, 2020a.

BRASIL. Senado Federal. **Relatório de Avaliação de Política Pública**: a política nacional sobre defesa cibernética. Brasília, 2019.

BRASIL. **Plano Estratégico da Marinha** (PEM 2040). Marinha do Brasil. Estado-Maior da Armada, Brasília, DF, 2020b.

BRASIL. **Decreto nº10.569, de 9 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. 2020c. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm. Acesso em: 26 de abr. de 2021.

BRASIL. Escola de Guerra Naval. **Cursos.** 2021. Disponível em: https://www.marinha.mil.br/egn/cursos. Acesso em: 04 de ago. de 2021.

BUERGER, C. What is Maritime Security? **Marine Policy**, v. 53, p. 159–164, 2015. Disponível em: http://bueger.info/wp-content/uploads/2014/12/Bueger-2014-What-is-Maritime-Security-final.pdf. Acesso em: Acesso em: 07 de mar. de 2021.

CASTRO, T. **Teoria das Relações Internacionais**. Brasília: FUNAG, 2012.

CENTENO, M. A.; ENRIQUEZ, E. **War and Society**. Cambridge: Polity Press, 2016.

DUNNE, T.; KURKI, M.; SMITH, S. **International Relations Theories**: discipline and diversity. Oxford: Oxford University Press, 2016.

ECO, Umberto. **Como se faz uma tese**. São Paulo: Perspectiva, 2012.

EUA. **Critical Infrastructures Protection Act of 2001**. 2001. Disponível em: https://www.govinfo.gov/app/details/USCODE-2010-title42/USCODE-2010-title42-chap68-subchapIV-B-sec5195c/context. Acesso em: 26 de abr. de 2021.

EUA. CISA. **Critical Infrastructure Sectors**. 2020a. Disponível em: https://www.cisa.gov/critical-infrastructure-sectors. Acesso em: 26 de abr. de 2021.

EUA. **National Maritime Cybersecurity Plan**. Washington, 2020b.

FALLEIRO, F. D. **Conversor Analógico-Digital com Capacitores Mínimos Integrado na Tecnologia CMOS**. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2015.

FARIAS, Claudio M. De; LI, Wei; DELICATO, Flávia C.; PIRMEZ, Luci; ZOMAYA, Albert Y.; PIRES, Paulo F.; SOUZA, José N. De. A Systematic Review of Shared Sensor Networks. **ACM Comput. Surv**., New York, NY, USA, v. 48, n. 4, 2016. ISSN: 0360-0300. DOI: 10.1145/2851510. Disponível em: https://doi.org/10.1145/2851510.

FERRARI, P., *et al*. Model-Based Stealth Attack to Networked Control System Based on Real-Time Ethernet. **IEEE Transactions on Industrial Electronics**, 2020.

FREUND, J. **Sociologia Del Conflicto**. Ediciones do Ejército. Madrid. 1995.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de Pesquisa**. Porto Alegre: UFRGS, 2009.

GIL, A. C. **Como Elaborar Projetos de Pesquisa**. 4ª ed. São Paulo: Atlas, 2002.

GOUGH, B. **Naval Warfare**: Its Ruling Principles and Practice Historically Treated by P.H. Colomb. Annapolis: Naval Institute Press, 1990.

GROVE, E. Sea Power. In R. A. Denemark (Ed.), **The International Studies Encyclopedia**. p. 1-16, 2010.

KATSURAI, M. Bursty research topic detection from scholarly data using dynamic Co-word networks: A preliminary investigation. **IEEE 2nd International Conference on Big Data Analysis**, Beijing, p. 115-119. 2017.

KUMAR, A.; PANDA, S. P. A Survey: How Python Pitches in IT-World. **International Conference on Machine Learning, Big Data, Cloud and Parallel Computing**. Índia, 2019.

HAM, C.; HILL, M. **O processo de elaboração de políticas no Estado capitalista moderno**. Campinas, SP: Editora da Unicamp, 1993.

HAYES, C. R. **Maritime cybersecurity**: the future of national security. Naval Postgraduate School. Monterey, 2016.

IMO. **Guidelines on Maritime Cyber Risk Management**. London, 2017.

ISO.**ISO/IEC 27001**: Information Technology – Security Techniques – Information Security Management Systems –Requirements. 2018.

JURAFSKY, D.; MARTIN, J. H. **Speech and Language Processing:** An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition. 2020.

LEITE JUNIOR, W. C.; SÁ, A. O. Triggering Cyber electronic Attacks in Naval Radar Systems. In: **2020 IMEKO TC-19 International Workshop on Metrology for the Sea**, 2020, Nápoles. Proceedings of the 2020 IMEKO TC-19 International Workshop on Metrology for the Sea, 2020.

LEITE JUNIOR, W. C.; DE MORAES, C. C.; DE ALBUQUERQUE, C. E. P.; MACHADO, R. C. S.; SÁ, A. O. A Triggering Mechanism for Cyber-Attacks in Naval Sensors and Systems. **SENSORS**, v. 21, p. 3195, 2021.

LIBERATI A, *et al*. **The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions**: explanation and elaboration. PLoS Med, 21 de jul. de 2009.

MAHAN, A. **The Influence of Sea Power upon History 1660-1783**. New York: Dover, 1987.

MALESEVIC, S. **The Sociology of War and Violence**. Cambridge University Press. 2014.

MARCONDES, D. **Textos Básicos de Ética**: de Platão a Foucault. Rio de Janeiro: Editora Zahar, 2007.

MARCONI, M. A. LAKATOS, E. M. **Fundamentos de Metodologia Científica**. São Paulo: Atlas, 2003.

MARX, K.; ENGELS, F. **Manifesto do Partido Comunista**. 9. ed. Petrópolis, RJ: Vozes, 1999.

MCLAUGHLIN, S. *et al*. The Cybersecurity Landscape in Industrial Control Systems. **Proceedings of the IEEE**, v. 104, n. 5, p.1039-1057, 2016.

MENDELEY. **Mendeley**. Versão 1.19.8. Disponível em: https://www.mendeley.com/download-desktop-new/. Acesso em: 29 de mar. de 2021.

NCSI. **National Cyber Security Index**. 2021. Disponível em: https://ncsi.ega.ee/. Acesso em: 6 de jun. de 2021.

ORACLE. **O que é Big Data**? 2021. Disponível em: https://www.oracle.com/br/big-data/what-is-big-data/. Acesso em: 07 de ago. de 2021.

PARCHARIDIS, M. D. **Simulation of Cyber Attacks Against Scada Systems**. International Hellenic University. Thessaloniki, 2018.

PYTHON. **Python**. Versão 3.9.2. 19 fev. 2021. Disponível em: https://www.python.org/. Acesso em: 29 de mar. de 2021.

REINO UNIDO. **Code of Practice**: Cyber Security for Ships. Londres, 2017.

SÁ, A. O.; MACHADO, R. C. S.; ALMEIDA, N. N. O Encontro da Guerra Cibernética com as Guerras Eletrônica e Cinética no Âmbito do Poder Marítimo. **Revista da Escola de Guerra Naval**, Rio de Janeiro, v. 25, n. 1, p. 89-128. janeiro/abril. 2019.

SADEK, N. Shipping Companies Confront Cyber Crooks as Economies Reopen. **Bloomberg**. 2021. Disponível em: https://about.bgov.com/news/shipping-companies-confront-cyber-crooks-as-economies-reopen/. Acesso em: 20 de set. de 2021.

SANGER, D. E. **The Perfect Weapon**: War, Sabotage and Fear in the Cyber Age. Nova Iorque: Broadway Books, 2018.

SOUZA, C. Políticas Públicas: uma revisão da literatura. **Caderno Sociologias**, Porto Alegre, n. 16, p.20-45, jul./dez. 2006.

THE WORLD BANK. **Individuals using the Internet**. 2021. Disponível em: https://data.worldbank.org/indicator/IT.NET.USER.ZS. Acesso em: 11 de jun. de 2021.

TILL, G. **Sea Power**: a guide for the 21st century. London: Routledge, 2009.

VAN EVERA, S. **Guide to Methods for Students of Political Science**. Ithaca: Cornell University House, 1997.

WARRICK, J.; NAKASHIMA, E. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. **The Washington Post**. 2020. Disponível em: https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html. Acesso em: 26 de abr. de 2021.

ZETTER, K. **Countdown to Zero Day:** Stuxnet and Launch of the World's First Digital Weapon. Nova Iorque: Broadway Books, 2015.

APÊNDICE A – ALGORÍTIMO DE MINERAÇÃO DE DADOS EM TEXTO

```
#Pacotes e funções utilizadas
import nltk
from nltk.corpus import stopwords
from nltk.tokenize import word_tokenize
from collections import Counter
import string
import numpy as np
import matplotlib.pyplot as plt
from wordcloud import WordCloud
#Pacotes e funções utilizadas
#Termos que devem ser excluídos do texto
stop_words = (stopwords.words('portuguese/english'))
#Termos adicionados pelo autor
stop_words.append ('–')
#Termos adicionados pelo autor
#Termos que devem ser excluídos do texto
print (stop_words)
#Retirada de termos e pontuação
string_punctuation = string.punctuation
text = open ('file.txt', mode='r', encoding='utf-8')
content = text.read()
word_tokens = word_tokenize(content)
filtered_sentence = [w for w in word_tokens if not w in stop_words]
filtered_sentence = []
for w in word_tokens:
 if w not in stop_words:
  filtered_sentence.append(w)
filtered_sentence_punctuation = [q for q in filtered_sentence if not q in string_punctuation]
filtered_sentence_punctuation = []
for q in filtered_sentence:
 if q not in string_punctuation:
  filtered_sentence_punctuation.append(q)
```

```
#Retirada de termos e pontuação
#Contagem da incidência de cada termo
contador = Counter(filtered_sentence_punctuation)
#Contagem da incidência de cada termo
#Ordenação de termos por incidência
contador_lista = []
for i in contador.most_common():
 contador_lista.append(i)
#Ordenação de termos por incidência
#Exibição dos 10 termos mais citados
print(contador_lista[:10])
#Exibição dos 10 termos mais citados
#Conversão do tipo de dado (de lista para dicionário), necessário para gráfico e wordcloud
b = dict(contador_lista[:10])
#Conversão do tipo de dado (de lista para dicionário), necessário para gráfico e wordcloud
#Exibição para verificação
print (b)
#Exibição para verificação
#Gráfico
palavras = b.keys()
y_pos = np.arange(len(palavras))
contagem = b.values()
plt.bar(y_pos, contagem, align='center', alpha=0.5)
plt.xticks(y_pos, palavras)
plt.ylabel('Frequencia')
plt.title('Frequencia das palavras')
plt.savefig('file_10mais.png', format='png')
plt.show()
#Gráfico
#Criação de aqruivo onde será escrito o texto após a remoção de termos e pontuação
arquivo = open("file_filtered.txt", "a")
#Criação de aqruivo onde será escrito o texto após a remoção de termos e pontuação
#Conversão do tipo de dado (de lista para string), necessário para salvar o arquivo como txt
string = " ".join(filtered_sentence_punctuation)
```

```
#Conversão do tipo de dado (de lista para string), necessário para salvar o arquivo como txt
#wordcloud
text = string
wordcloud = WordCloud(max_font_size=100,width = 1520, height = 535).generate(text)
plt.figure(figsize=(16,9))
plt.imshow(wordcloud)
plt.axis("off")
plt.show()
wordcloud.to_file("file_worcloud.png")
#wordcloud
#Gravação da informação no arquivo criado anteriormente
arquivo.write(string)
arquivo.close()
#Gravação da informação no arquivo criado anteriormente
```

APÊNDICE B – RISCOS

As referências encontram-se numeradas conforme a ordem do arquivo no link: https://drive.google.com/file/d/1CNnFdXHFpmp06yTIa8UOb8Vh4ZsLVh7/view?usp=sharing.

incluídos	96
excluídos	64
Sem acesso	3
TOTAL	163

REF.	RISCOS																	
Nº	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1																		
2																		
3																		
4																		
5																		
6	1		1	1														
7	1	1																
8																		
9			1	1														1
10			1	1							1							
11	1				1													
12	1				1													
13				1	1		1											
14	1		1					1										
15																		
16																		
17									1									
18							1											
19									1	1								
20			1															
21			1	1	1				1									
22			1	1														
23			1					1										
24				1					1									
25																		
26				1														
27				1					1									
28				1					1			1						
29			1										1					
30																		
31									1					1				

32									1									
33																		
34																		
35					1				1					1				
36																		
37																		
38																		
39																		
40									1									
41																		
42		1							1									
43																		
44									1									
45																		
46									1									
47																		
48	1								1									
49																		
50									1									
51																		
52																		
53									1									
54																		
55																		
56																		
57																		
58																		
59									1									
60																		
61																		
62				1														
63									1									
64									1									
65													1					
66				1					1									
67					1													
68																		
69									1					1				
70				1					1									
71									1									
72				1					1									
73				1					1									
74				1					1									
75				1														
76																		

77																		
78				1					1									
79									1									
80							1											
81																		
82				1					1									
83									1									
84				1					1				1					
85				1					1									
86																		
87																		
88									1				1					
89																		
90	1								1									
91	1						1		1									
92																		
93																		
94																		
95									1									
96		1													1			
97				1					1									
98				1				1	1				1					
99									1									
100				1					1				1					
101				1					1				1					
102									1									
103									1									
104																		
105																		
106																		
107																		
108									1									
109																		
110																		
111	1					1							1		1	1	1	
112									1					1				
113																		
114									1									
115																		
116																		
117																		
118			1										1					
119			1								1		1					
120													1					
121									1									

122				1					1									
123									1									
124									1									
125			1						1				1					
126																		
127									1									
128				1					1									
129																		
130				1					1									
131				1					1									
132				1					1									
133				1					1									
134				1					1									
135				1					1									
136																		
137				1					1									
138				1					1									
139									1									
140																		
141									1									
142																		
143				1					1									
144				1					1									
145																		
146																		
147				1					1									
148																		
149																		
150																		
151																		
152																		
153																		
154																		
155																		
156									1									
157																		
158				1					1									
159																		
160																		
161																		
162																		
163																		
TOTAL	9	3	12	39	6	1	4	3	68	1	2	1	12	4	2	1	1	1

APÊNDICE C – AÇÕES MITIGATÓRIAS

As referências encontram-se numeradas conforme a ordem do arquivo no link: https://drive.google.com/file/d/1CNnFdXHFpmp06yTIa8UOb8Vh4ZsLVh7/view?usp=sharing.

incluídos	96
excluídos	64
Sem acesso	3
TOTAL	163

REF.	AÇÕES																									
Nº	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1																										
2																										
3																										
4																										
5																										
6	1	1																								
7		1																								
8																										
9	1	1																								
10		1	1																							
11			1	1																						
12			1	1	1																					
13	1					1	1	1	1																	
14	1		1	1																						
15																										
16																										
17		1																								
18			1																							
19	1	1	1			1				1		1														
20	1																									
21			1																							

22		1									1														
23	1	1								1															
24	1	1										1												1	
25																									
26		1								1															
27	1																								
28		1	1																						
29	1	1	1	1																					
30																									
31			1										1												
32												1												1	
33																									
34																									
35		1	1											1											
36																									
37																									
38																									
39																									
40		1																							
41																									
42		1	1									1												1	
43																									
44	1	1												1											
45																									
46		1	1																						

47																									
48	1	1										1			1	1								1	
49																									
50				1																					
51																									
52																									
53		1	1			1																			
54																									
55																									
56																									
57																									
58																									
59		1																							
60																									
61																									
62																1									
63	1																								
64	1	1				1											1								
65	1																	1							
66		1	1																						1
67		1																							
68																									
69		1																							
70				1												1									
71		1																							

72		1	1																						
73				1												1									
74																						1			
75																1									
76																									
77																									
78		1	1																						
79		1	1																1						
80		1	1																						
81																									
82		1														1									
83				1												1									
84	1	1																		1					
85			1								1										1				
86																									
87																									
88	1															1						1			
89																									
90	1		1																						
91		1	1			1													1						
92																									
93																									
94																									
95	1	1	1													1									
96								1			1			1											

97							1																		
98	1	1	1			1																			
99		1																							
100	1																								
101	1	1	1																1						
102		1																							
103																						1			
104																									
105																									
106																									
107																									
108												1												1	
109																									
110																									
111	1	1				1																	1		
112	1	1																							
113																									
114		1	1																						

115																									
116																									
117																									
118	1	1				1																	1		
119	1			1							1	1								1			1	1	
120	1																								1
121	1	1	1																						
122		1	1																						
123		1								1															
124				1																					
125	1															1				1					
126																									
127																1									
128	1	1																							
129																									
130		1	1																						
131		1	1																						

132		1	1																						
133	1	1	1													1						1			
134		1	1																						
135			1																						
136																									
137	1											1												1	
138	1	1																		1					
139	1	1	1																	1					
140																									
141	1	1	1																	1					
142																									
143	1																			1					
144		1	1			1					1														
145																									
146																									
147											1														
148																									

149																									
150																									
151																									
152																									
153																									
154																									
155																									
156					1																				
157																									
158												1												1	
159																									
160																									
161																									
162																									
163																									
TOTAL	36	54	37	10	2	9	2	2	1	4	6	9	1	3	1	11	1	1	1	9	1	1	5	2	8	2

APÊNDICE D – PALAVRAS RETIRADAS DA ANÁLISE/PORTUGÊS

Análise das ORCOM

['de', 'a', 'o', 'que', 'e', 'é', 'do', 'da', 'em', 'um', 'para', 'com', 'não', 'uma', 'os', 'no', 'se', 'na', 'por', 'mais', 'as', 'dos', 'como', 'mas', 'ao', 'ele', 'das', 'à', 'seu', 'sua', 'ou', 'quando', 'muito', 'nos', 'já', 'eu', 'também', 'só', 'pelo', 'pela', 'até', 'isso', 'ela', 'entre', 'depois', 'sem', 'mesmo', 'aos', 'seus', 'quem', 'nas', 'me', 'esse', 'eles', 'você', 'essa', 'num', 'nem', 'suas', 'meu', 'às', 'minha', 'numa', 'pelos', 'elas', 'qual', 'nós', 'lhe', 'deles', 'essas', 'esses', 'pelas', 'este', 'dele', 'tu', 'te', 'vocês', 'vos', 'lhes', 'meus', 'minhas', 'teu', 'tua', 'teus', 'tuas', 'nosso', 'nossa', 'nossos', 'nossas', 'dela', 'delas', 'esta', 'estes', 'estas', 'aquele', 'aquela', 'aqueles', 'aquelas', 'isto', 'aquilo', 'estou', 'está', 'estamos', 'estão', 'estive', 'esteve', 'estivemos', 'estiveram', 'estava', 'estávamos', 'estavam', 'estivera', 'estivéramos', 'esteja', 'estejamos', 'estejam', 'estivesse', 'estivéssemos', 'estivessem', 'estiver', 'estivermos', 'estiverem', 'hei', 'há', 'havemos', 'hão', 'houve', 'houvemos', 'houveram', 'houvera', 'houvéramos', 'haja', 'hajamos', 'hajam', 'houvesse', 'houvéssemos', 'houvessem', 'houver', 'houvermos', 'houverem', 'houverei', 'houverá', 'houveremos', 'houverão', 'houveria', 'houveríamos', 'houveriam', 'sou', 'somos', 'são', 'era', 'éramos', 'eram', 'fui', 'foi', 'fomos', 'foram', 'fora', 'fôramos', 'seja', 'sejamos', 'sejam', 'fosse', 'fôssemos', 'fossem', 'for', 'formos', 'forem', 'serei', 'será', 'seremos', 'serão', 'seria', 'seríamos', 'seriam', 'tenho', 'tem', 'temos', 'tém', 'tinha', 'tínhamos', 'tinham', 'tive', 'teve', 'tivemos', 'tiveram', 'tivera', 'tivéramos', 'tenha', 'tenhamos', 'tenham', 'tivesse', 'tivéssemos', 'tivessem', 'tiver', 'tivermos', 'tiverem', 'terei', 'terá', 'teremos', 'terão', 'teria', 'teríamos', 'teriam', '–', 'DA', 'ser', 'O', 'CAPÍTULO', 'A', '“', 'RESERVADO', 'ORIM-98', 'DE', '43', 'ORIGINAL', 'deverá', 'OM', '2', 'ABR98', '1', 'sobre', 'a.', 'b.', 'c.', 'h', 'dar', 'f.', 'O', 'd.', 'e.', 'f.', 'g.', '0', 'b', 'o.', 'o', 'C', 'E', 'b', 'ORIM-99', '27-', 'deverão', '3', 'apresentar', 'Os', '12', 'cargo', 'ORCOM-2000', '”', 'M', 'p', 'P', 'Orientações', 'COMARE', 'Comentários', 'relatório', 'atenção', 'apreciação', 'sistema', 'Relatório', 'MB', 'conceitos', 'Comandante', 'Marinha', 'ORCOM-2001', '15', 'via', 'ORCOM-2002', 'Dar', 'ORCOM-2003', '16', 'ORCOM-2004', '2004', 'ORCOM-2006', 'visando', 'ORCOM-2007', 'CM', 'Sistema', 'todos', 'ORCOM-2008', 'ORCOM', 'encaminhar', 'SITREP', 'Mensagem', '31OUT2008', 'ORCOM-2009', '30OUT2009', 'medidas', 'ORCOM-2010', 'ORCOM-2012', 'ORCOM-2011', 'ORCOM-2013', 'ORCOM-2014', 'ORCOM-2014', '--', 'S', 'mensagem', 'R', 'OSTENSIVO', 'EMA-300', '05DEZ', 'REV.3', '18OUT', '"', 'forma', 'SGM', 'ODS', 'apresentados', 'Almirantado', 'junto', 'ação', 'ações', 'execução', 'execução', 'Navais', 'planejamento', 'existirem', 'DGPM', 'controle', 'dados', '4', 'MM', 'recursos', 'ter', 'Quando', 'Naval', 'prioridade', 'manter', 'uso', 'JUN99', 'As', 'Manter', 'especial', 'Prosseguir', 'continuidade', 'projeto', 'DGMM', 'Obter', 'navais', 'níveis', 'área', 'Abrigo', '2000', 'naval', 'procedimentos', 'EMA', 'SET/2001', 'JUN/2001', 'resultados', 'Proposição', 'MAI/2001', 'MAI/2001', 'capacidade', '01SET2003', 'implementação', 'estudos', 'Programa', 'atividades', 'Plano', 'bem', 'Setor', '01OUT2008', 'sistemas', '2008', '15OUT2008', 'âmbito', '29OUT2010', 'maior', 'processo', '15OUT2010', '14OUT2011', 'Defesa', '22NOV', '25OUT', 'encaminhará', 'Órgãos', '``', 'PPA', 'Poder', 'Força', 'Estratégico', 'Iniciativa', 'emprego', 'Direção', 'Setorial', 'estratégico', 'objetivos', 'NAVAIS', 'ESTRATÉGICO', 'MARINHA', 'PLANO', 'Brasil', 'interesses', 'defesa', 'mar', 'deve', 'marítimos', 'áreas', 'interesses', 'marítima', 'Marítimo', 'marítimas', '5', 'ambiente', 'nacional', 'AÇÕES', 'ESTRATÉGICAS', 'marítimo', 'interesses', 'nacionais', 'Nesse', 'Marítima', 'nível', 'AEN', 'operações', 'Estratégica', 'Nacional', 'contribuir', 'Aprimorar', 'OBNAV', 'apoio', 'Operações', '15NOV', '08NOV', 'demais', 'consolidada', '01NOV', '11OUT', 'outros', 'despacho', 'Ministério', '31OUT2014', 'fim', 'modo', '15OUT2012', '01OUT2010', '01OUT2009', '15OUT2009', 'setores', '2007', 'cumprimento', '31OUT2007', 'ORIENTAÇÕES', 'serem', 'necessidades', 'operativos', '–', '2006', 'propor', 'relação', 'ano', 'nº', 'Lei', 'proposta', 'documentos', 'necessário', '01OUT2003', '10', '2003', 'considerando',

'01OUT2002', 'revisão', 'Relatórios', 'necessárias', 'Revisão', 'devem', 'existentes', 'Ampliação', 'JUL/2001', 'normas', 'Classe', 'anos', 'seguintes', 'aprovado', 'Executivo', 'MSC', 'PL', 'COMISSÃO', 'Sr.', 'RELAÇÕES', 'EXTERIORES', 'DEFESA', 'NACIONAL', '6.1.99', '4.11.98', 'rejeitado', '21.1.98', '17.6.98', '27.1.99', '20.5.98', '13.1.99', '1998', '6.1.99', '4.11.98', 'rejeitado', '21.1.98', '17.6.98', '27.1.99', '20.5.98', '13.1.99', '1998', 'CREDN', 'Relações', 'Comissão', 'Exteriores', 'Atividades', '2018', 'Pinto', 'Nilson', 'deputado', 'acordo', 'Marcelo', 'Texto', 'Rech', 'Foto', 'ainda', 'PARECER', 'afirmou', 'Nº', 'EM', 'APROVADO', 'dois', 'Brasília', 'países', 'país', 'presidente', 'Câmara', 'Deputados', 'Deputado', 'República', 'relações', 'quarta-feira', 'explicou', 'Estados', 'REQUERIMENTO', 'Estado', 'Acordo', 'texto', 'Em', 'Congresso', 'aprovação', 'destacou', 'De', 'temas', 'brasileira', 'Para', 'Furlan', 'Bruna', 'deputada', 'Aprovado', 'parecer', 'PSDB-SP', 'Sepulvida', 'Na', 'Benjamim', 'dia', '2017', 'pública', 'Segundo', 'audiência', 'Parecer', '2016', 'RELATOR', 'Gab', 'MENSAGEM', 'Federativa', 'PODER', 'EXECUTIVO', 'Requer', 'realização', 'assinado', 'Pedro', 'Vilela', 'Carlos', 'Presidente', 'EMENDA', 'II', 'Dep', '•', 'Luiz', 'Audiência', 'reuniões', 'presidência', 'Parlamentar', 'PSDB/AL', 'Zarattini', 'Moraes', 'Jô', 'Ministro', 'maio', 'Pública', 'Anexo', 'Sala', 'Cajado', 'destinada', '2010', 'Plenário', 'autoria', 'Deputada', 'abril', 'deputados', 'SUGESTÃO', '1º', 'Subtenente', 'Gonzaga', 'discutir', 'Penal', '24', 'julho', 'dezembro', 'Unidos', 'participar', 'União', 'artigo', 'desta', 'PROJETO', 'outubro', '2015', 'http', '//www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/', 'debater', 'política', 'Horário', 'brasileiro', 'Requerimento', 'Secretaria', 'encontro', 'Submete', 'consideração', 'MORAES', '2014', 'RELATÓRIO', 'Barbosa', 'Eduardo', 'EDUARDO', 'BARBOSA', 'MARCELO', 'RECH', 'Trabalho', 'afirmou', 'PSDB-MG', '2012', 'Perpétua', 'Almeida', 'realizada', 'PCdoB/AC', 'Rio', 'Brasileira', 'Sra', 'representantes', 'Seminário', 'À', 'V', 'Grupo', 'COMISSÕES', 'Federal', 'Subcomissão', 'parlamentares', '2011', 'Relator', 'submete', 'Senhor', 'CARLOS', 'REUNIÃO', 'ORDINÁRIA', 'DELIBERATIVA', 'Excelentíssimo', 'Casa', 'ALBERTO', 'ANTONIO', 'esclarecimentos', 'LERÉIA', 'vaga', '2009', 'Exercício', 'Mesa', 'aprove', 'Dependentes', 'Unidas', 'PATRIOTA', 'encaminhe', 'ALFREDO', 'brasileiros', 'Diretor', 'Legislativa', '11', 'MENDES', 'SIRKIS', 'celebrado', '29', 'Parlamento', 'prestar', 'Diretora', 'Fernando', 'William', 'Woo', 'Aprovada', 'Emanuel', 'Fernandes', 'apresentado', 'art', 'N°', 'TEMA', 'Raul', 'Rocha', 'Mourão', 'Jungmann', 'Hauly', 'CONVIDADOS', 'outras', 'Paulo', 'Antônio', 'junho', 'deliberação', '9', 'Brasileiro', 'Silva', 'unanimemente', 'Dr.', 'Req', 'Severiano', 'Alves', 'acompanhado', 'Exposição', 'Motivos', 'novembro', 'LEI', 'Senhores', '13', 'Rosinha', 'José', 'Marcondes', 'Gadelha', 'Especial', '7', 'agosto', 'Damião', 'Feliciano', 'Oliveira', 'Gabeira', 'COM', '18', 'NELSON', 'JOBIM', 'Autor', 'ATIVIDADES', 'DO', 'Reunião', 'Conferência', 'cada', 'Membro', 'Representante', 'Unanimidade', 'Ano', 'MSC-', 'presença', 'Tipo', 'Data', 'Encerrada', 'Final', 'Vieira', 'Cunha', 'Amorim', 'setembro', '¨', 'Celso', 'VIEIRA', 'FERNANDO', 'CUNHA', '22/11/06', '2005', 'ocupa', 'Relatora', '20/12/06', 'Maninha', 'Técnica', 'Matéria', 'Área', 'Convenção', 'JOÃO', 'Lima', 'Emenda', 'André', '6', 'Alceu', 'Collares', 'Protocolo', 'Decisão', 'Ana', 'João', 'PFL-BA', '24/05/06', 'PSOL-DF', 'Gomes', 'confirmado', 'Resultado', 'unanimidade', 'requer', 'Deliberativa', 'autor', 'pauta', 'MANINHA', 'dá', 'retirado', 'providências', 'voto', 'contra', 'DATA', 'ção', 'Senado', 'ofício', 'solicita', '25', 'Cedraz', 'Antonio', 'Pannunzio', '24/08/2005', 'redação', '09/11/2005', '13/04/2005', 'Coo-', 'peração', 'Rejeitada', 'Aroldo', '17/08/2005', '14/09/2005', 'dispõe', '15/06/2005', '19', '14', 'Dispõe', '21', 'Apreciação', 'Ementa', 'Última', 'Ação', 'Apresentação', 'Regime', 'tramitação', 'Situação', 'Ordinária', 'Arquivada', 'Despacho', 'Sujeita', 'Prioridade', 'Aguardando', '54', 'Comissões', '2002', 'Redação', 'Zulaiê', 'Transformada', 'Artigo', 'Art', 'Recebimento', 'Encaminhamento', 'Cobra', 'favorável', 'Favorável', 'Rep.', 'Encaminhado', 'relator', 'Não', 'Gov', 'Apensado', '4.10.00', 'Alberto', 'PROPOSIÇÃO', 'Do', 'apresentadas', 'Fraga', '2001', 'substitutivo', 'AUTOR', 'EMENTA', 'DISTRIBUIÇÃO', 'PRAZO', 'P/', 'EMENDAS', 'VISTA', 'ÚLTIMA', 'AÇÃO', 'Segunda-feira', '05', 'Fevereiro', 'Página', 'Solicita', 'Próximas', 'Virgílio', 'c/', 'cons', 'CN', 'Guimarães',

'Aprovação', 'JOSÉ', 'MATÉRIAS', 'PAULO', 'JORGE', '20', '1999', 'LUIZ', 'MOREIRA', '1997', 'PROPOSIÇÕES', 'DAS', 'TRAMITAÇÃO', 'trabalho', 'PLP', '1º.7.98', '3.6.98', 'Dia', 'Martins', 'Ferreira', 'V.', 'Diniz', '1º.4.98', '15.4.98', '28.1.98', '20.1.99', 'Convidado', 'Criação', 'SECRETÁRIA', 'Denise', 'Moreira', 'Lana', 'Alencar', 'Araripe', 'Viégas', 'PÚBLICA', 'ANO', 'Ordinárias', 'Extraordinárias', 'Subcomissões', 'Conjuntas', 'APRECIADAS', 'Informais', 'Expositores', 'Wilson', '219/98', 'Adylson', 'Motta', '6.5.98', 'Brasileiros', 'RODRIGUES', 'Termos', 'reunião', 'Ofícios', 'CORPO', 'Walbia', 'Lóra', 'TÉCNICO', 'SUBSTITUTO', '2', 'SUBSTITUTA', 'Francisca', 'PRESIDENTE', '2ª', 'Fátima', 'Moura', 'Campos', 'Ivana', 'Antonete', 'Mazurek', 'ATAS', 'PUBLICAÇÕES', 'Terezinha', 'J.', 'Pitangui', 'CONTROLE', '', '', '', '', '', '', '', '']

Análise dos Relatórios da CREDN

['de', 'a', 'o', 'que', 'e', 'é', 'do', 'da', 'em', 'um', 'para', 'com', 'não', 'uma', 'os', 'no', 'se', 'na', 'por', 'mais', 'as', 'dos', 'como', 'mas', 'ao', 'ele', 'das', 'à', 'seu', 'sua', 'ou', 'quando', 'muito', 'nos', 'já', 'eu', 'também', 'só', 'pelo', 'pela', 'até', 'isso', 'ela', 'entre', 'depois', 'sem', 'mesmo', 'aos', 'seus', 'quem', 'nas', 'me', 'esse', 'eles', 'você', 'essa', 'num', 'nem', 'suas', 'meu', 'às', 'minha', 'numa', 'pelos', 'elas', 'qual', 'nós', 'lhe', 'deles', 'essas', 'esses', 'pelas', 'este', 'dele', 'tu', 'te', 'vocês', 'vos', 'lhes', 'meus', 'minhas', 'teu', 'tua', 'teus', 'tuas', 'nosso', 'nossa', 'nossos', 'nossas', 'dela', 'delas', 'esta', 'estes', 'estas', 'aquele', 'aquela', 'aqueles', 'aquelas', 'isto', 'aquilo', 'estou', 'está', 'estamos', 'estão', 'estive', 'esteve', 'estivemos', 'estiveram', 'estava', 'estávamos', 'estavam', 'estivera', 'estivéramos', 'esteja', 'estejamos', 'estejam', 'estivesse', 'estivéssemos', 'estivessem', 'estiver', 'estivermos', 'estiverem', 'hei', 'há', 'havemos', 'hão', 'houve', 'houvemos', 'houveram', 'houvera', 'houvéramos', 'haja', 'hajamos', 'hajam', 'houvesse', 'houvéssemos', 'houvessem', 'houver', 'houvermos', 'houverem', 'houverei', 'houverá', 'houveremos', 'houverão', 'houveria', 'houveríamos', 'houveriam', 'sou', 'somos', 'são', 'era', 'éramos', 'eram', 'fui', 'foi', 'fomos', 'foram', 'fora', 'fôramos', 'seja', 'sejamos', 'sejam', 'fosse', 'fôssemos', 'fossem', 'for', 'formos', 'forem', 'serei', 'será', 'seremos', 'serão', 'seria', 'seríamos', 'seriam', 'tenho', 'tem', 'temos', 'tém', 'tinha', 'tínhamos', 'tinham', 'tive', 'teve', 'tivemos', 'tiveram', 'tivera', 'tivéramos', 'tenha', 'tenhamos', 'tenham', 'tivesse', 'tivéssemos', 'tivessem', 'tiver', 'tivermos', 'tiverem', 'terei', 'terá', 'teremos', 'terão', 'teria', 'teríamos', 'teriam', '–', 'DA', 'ser', 'O', 'CAPÍTULO', 'A', '“', 'RESERVADO', 'ORIM-98', 'DE', '43', 'ORIGINAL', 'deverá', 'OM', '2', 'ABR98', '1', 'sobre', 'a.', 'b.', 'c.', 'h', 'dar', 'f.', 'O', 'd.', 'e.', 'f.', 'g.', '0', 'b', 'o.', 'o', 'C', 'E', 'b', 'ORIM-99', '27-', 'deverão', '3', 'apresentar', 'Os', '12', 'cargo', 'ORCOM-2000', '”', 'M', 'p', 'P', 'Orientações', 'COMARE', 'Comentários', 'relatório', 'atenção', 'apreciação', 'sistema', 'Relatório', 'MB', 'conceitos', 'Comandante', 'Marinha', 'ORCOM-2001', '15', 'via', 'ORCOM-2002', 'Dar', 'ORCOM-2003', '16', 'ORCOM-2004', '2004', 'ORCOM-2006', 'visando', 'ORCOM-2007', 'CM', 'Sistema', 'todos', 'ORCOM-2008', 'ORCOM', 'encaminhar', 'SITREP', 'Mensagem', '31OUT2008', 'ORCOM-2009', '30OUT2009', 'medidas', 'ORCOM-2010', 'ORCOM-2012', 'ORCOM-2011', 'ORCOM-2013', 'ORCOM-2014', 'ORCOM-2014', '--', 'S', 'mensagem', 'R', 'OSTENSIVO', 'EMA-300', '05DEZ', 'REV.3', '18OUT', '"', 'forma', 'SGM', 'ODS', 'apresentados', 'Almirantado', 'junto', 'ação', 'ações', 'execução', 'execução', 'Navais', 'planejamento', 'existirem', 'DGPM', 'controle', 'dados', '4', 'MM', 'recursos', 'ter', 'Quando', 'Naval', 'prioridade', 'manter', 'uso', 'JUN99', 'As', 'Manter', 'especial', 'Prosseguir', 'continuidade', 'projeto', 'DGMM', 'Obter', 'navais', 'níveis', 'área', 'Abrigo', '2000', 'naval', 'procedimentos', 'EMA', 'SET/2001', 'JUN/2001', 'resultados', 'Proposição', 'MAI/2001', 'MAI/2001', 'capacidade', '01SET2003', 'implementação', 'estudos', 'Programa', 'atividades', 'Plano', 'bem', 'Setor', '01OUT2008', 'sistemas', '2008', '15OUT2008', 'âmbito', '29OUT2010', 'maior', 'processo', '15OUT2010', '14OUT2011', 'Defesa', '22NOV', '25OUT', 'encaminhará', 'Órgãos', '``', 'PPA', 'Poder', 'Força', 'Estratégico', 'Iniciativa', 'emprego', 'Direção', 'Setorial', 'estratégico', 'objetivos', 'NAVAIS', 'ESTRATÉGICO', 'MARINHA', 'PLANO', 'Brasil',

'interesses', 'defesa', 'mar', 'deve', 'marítimos', 'áreas', 'interesses', 'marítima', 'Marítimo', 'marítimas', '5', 'ambiente', 'nacional', 'AÇÕES', 'ESTRATÉGICAS', 'marítimo', 'interesses', 'nacionais', 'Nesse', 'Marítima', 'nível', 'AEN', 'operações', 'Estratégica', 'Nacional', 'contribuir', 'Aprimorar', 'OBNAV', 'apoio', 'Operações', '15NOV', '08NOV', 'demais', 'consolidada', '01NOV', '11OUT', 'outros', 'despacho', 'Ministério', '31OUT2014', 'fim', 'modo', '15OUT2012', '01OUT2010', '01OUT2009', '15OUT2009', 'setores', '2007', 'cumprimento', '31OUT2007', 'ORIENTAÇÕES', 'serem', 'necessidades', 'operativos', '–', '2006', 'propor', 'relação', 'ano', 'nº', 'Lei', 'proposta', 'documentos', 'necessário', '01OUT2003', '10', '2003', 'considerando', '01OUT2002', 'revisão', 'Relatórios', 'necessárias', 'Revisão', 'devem', 'existentes', 'Ampliação', 'JUL/2001', 'normas', 'Classe', 'anos', 'seguintes', 'aprovado', 'Executivo', 'MSC', 'PL', 'COMISSÃO', 'Sr.', 'RELAÇÕES', 'EXTERIORES', 'DEFESA', 'NACIONAL', '6.1.99', '4.11.98', 'rejeitado', '21.1.98', '17.6.98', '27.1.99', '20.5.98', '13.1.99', '1998', '6.1.99', '4.11.98', 'rejeitado', '21.1.98', '17.6.98', '27.1.99', '20.5.98', '13.1.99', '1998', 'CREDN', 'Relações', 'Comissão', 'Exteriores', 'Atividades', '2018', 'Pinto', 'Nilson', 'deputado', 'acordo', 'Marcelo', 'Texto', 'Rech', 'Foto', 'ainda', 'PARECER', 'afirmou', 'Nº', 'EM', 'APROVADO', 'dois', 'Brasília', 'países', 'país', 'presidente', 'Câmara', 'Deputados', 'Deputado', 'República', 'relações', 'quarta-feira', 'explicou', 'Estados', 'REQUERIMENTO', 'Estado', 'Acordo', 'texto', 'Em', 'Congresso', 'aprovação', 'destacou', 'De', 'temas', 'brasileira', 'Para', 'Furlan', 'Bruna', 'deputada', 'Aprovado', 'parecer', 'PSDB-SP', 'Sepulvida', 'Na', 'Benjamim', 'dia', '2017', 'pública', 'Segundo', 'audiência', 'Parecer', '2016', 'RELATOR', 'Gab', 'MENSAGEM', 'Federativa', 'PODER', 'EXECUTIVO', 'Requer', 'realização', 'assinado', 'Pedro', 'Vilela', 'Carlos', 'Presidente', 'EMENDA', 'II', 'Dep', '•', 'Luiz', 'Audiência', 'reuniões', 'presidência', 'Parlamentar', 'PSDB/AL', 'Zarattini', 'Moraes', 'Jô', 'Ministro', 'maio', 'Pública', 'Anexo', 'Sala', 'Cajado', 'destinada', '2010', 'Plenário', 'autoria', 'Deputada', 'abril', 'deputados', 'SUGESTÃO', '1º', 'Subtenente', 'Gonzaga', 'discutir', 'Penal', '24', 'julho', 'dezembro', 'Unidos', 'participar', 'União', 'artigo', 'desta', 'PROJETO', 'outubro', '2015', 'http', '//www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/noticias/', 'debater', 'política', 'Horário', 'brasileiro', 'Requerimento', 'Secretaria', 'encontro', 'Submete', 'consideração', 'MORAES', '2014', 'RELATÓRIO', 'Barbosa', 'Eduardo', 'EDUARDO', 'BARBOSA', 'MARCELO', 'RECH', 'Trabalho', 'afirmou', 'PSDB-MG', '2012', 'Perpétua', 'Almeida', 'realizada', 'PCdoB/AC', 'Rio', 'Brasileira', 'Sra', 'representantes', 'Seminário', 'À', 'V', 'Grupo', 'COMISSÕES', 'Federal', 'Subcomissão', 'parlamentares', '2011', 'Relator', 'submete', 'Senhor', 'CARLOS', 'REUNIÃO', 'ORDINÁRIA', 'DELIBERATIVA', 'Excelentíssimo', 'Casa', 'ALBERTO', 'ANTONIO', 'esclarecimentos', 'LERÉIA', 'vaga', '2009', 'Exercício', 'Mesa', 'aprove', 'Dependentes', 'Unidas', 'PATRIOTA', 'encaminhe', 'ALFREDO', 'brasileiros', 'Diretor', 'Legislativa', '11', 'MENDES', 'SIRKIS', 'celebrado', '29', 'Parlamento', 'prestar', 'Diretora', 'Fernando', 'William', 'Woo', 'Aprovada', 'Emanuel', 'Fernandes', 'apresentado', 'art', 'N°', 'TEMA', 'Raul', 'Rocha', 'Mourão', 'Jungmann', 'Hauly', 'CONVIDADOS', 'outras', 'Paulo', 'Antônio', 'junho', 'deliberação', '9', 'Brasileiro', 'Silva', 'unanimemente', 'Dr.', 'Req', 'Severiano', 'Alves', 'acompanhado', 'Exposição', 'Motivos', 'novembro', 'LEI', 'Senhores', '13', 'Rosinha', 'José', 'Marcondes', 'Gadelha', 'Especial', '7', 'agosto', 'Damião', 'Feliciano', 'Oliveira', 'Gabeira', 'COM', '18', 'NELSON', 'JOBIM', 'Autor', 'ATIVIDADES', 'DO', 'Reunião', 'Conferência', 'cada', 'Membro', 'Representante', 'Unanimidade', 'Ano', 'MSC-', 'presença', 'Tipo', 'Data', 'Encerrada', 'Final', 'Vieira', 'Cunha', 'Amorim', 'setembro', '¨', 'Celso', 'VIEIRA', 'FERNANDO', 'CUNHA', '22/11/06', '2005', 'ocupa', 'Relatora', '20/12/06', 'Maninha', 'Técnica', 'Matéria', 'Área', 'Convenção', 'JOÃO', 'Lima', 'Emenda', 'André', '6', 'Alceu', 'Collares', 'Protocolo', 'Decisão', 'Ana', 'João', 'PFL-BA', '24/05/06', 'PSOL-DF', 'Gomes', 'confirmado', 'Resultado', 'unanimidade', 'requer', 'Deliberativa', 'autor', 'pauta', 'MANINHA', 'dá', 'retirado', 'providências', 'voto', 'contra', 'DATA', 'ção', 'Senado', 'ofício', 'solicita', '25', 'Cedraz', 'Antonio', 'Pannunzio', '24/08/2005', 'redação', '09/11/2005', '13/04/2005', 'Coo-', 'peração', 'Rejeitada', 'Aroldo', '17/08/2005',

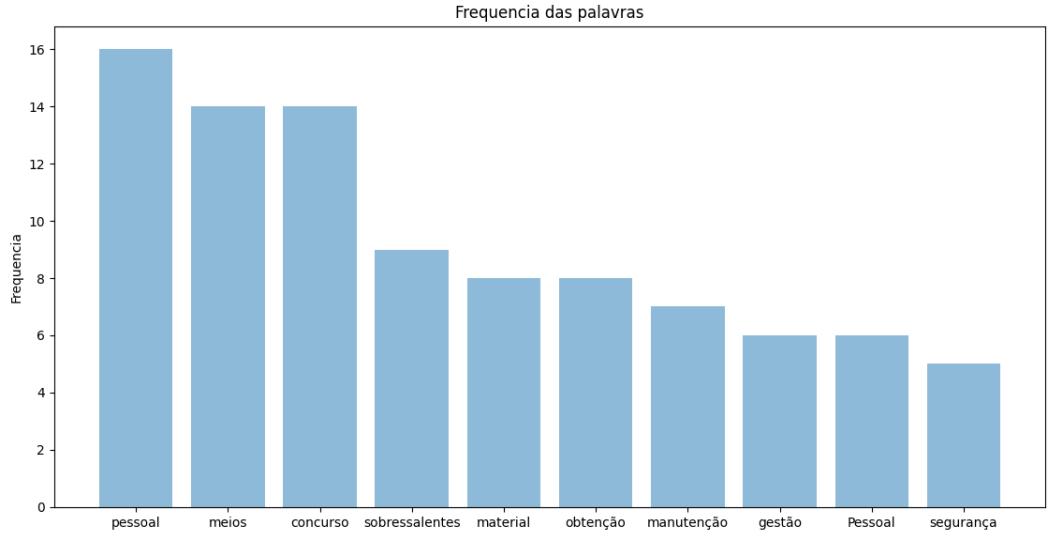
'14/09/2005', 'dispõe', '15/06/2005', '19', '14', 'Dispõe', '21', 'Apreciação', 'Ementa', 'Última', 'Ação', 'Apresentação', 'Regime', 'tramitação', 'Situação', 'Ordinária', 'Arquivada', 'Despacho', 'Sujeita', 'Prioridade', 'Aguardando', '54', 'Comissões', '2002', 'Redação', 'Zulaiê', 'Transformada', 'Artigo', 'Art', 'Recebimento', 'Encaminhamento', 'Cobra', 'favorável', 'Favorável', 'Rep.', 'Encaminhado', 'relator', 'Não', 'Gov', 'Apensado', '4.10.00', 'Alberto', 'PROPOSIÇÃO', 'Do', 'apresentadas', 'Fraga', '2001', 'substitutivo', 'AUTOR', 'EMENTA', 'DISTRIBUIÇÃO', 'PRAZO', 'P/', 'EMENDAS', 'VISTA', 'ÚLTIMA', 'AÇÃO', 'Segunda-feira', '05', 'Fevereiro', 'Página', 'Solicita', 'Próximas', 'Virgílio', 'c/', 'cons', 'CN', 'Guimarães', 'Aprovação', 'JOSÉ', 'MATÉRIAS', 'PAULO', 'JORGE', '20', '1999', 'LUIZ', 'MOREIRA', '1997', 'PROPOSIÇÕES', 'DAS', 'TRAMITAÇÃO', 'trabalho', 'PLP', '1º.7.98', '3.6.98', 'Dia', 'Martins', 'Ferreira', 'V.', 'Diniz', '1º.4.98', '15.4.98', '28.1.98', '20.1.99', 'Convidado', 'Criação', 'SECRETÁRIA', 'Denise', 'Moreira', 'Lana', 'Alencar', 'Araripe', 'Viégas', 'PÚBLICA', 'ANO', 'Ordinárias', 'Extraordinárias', 'Subcomissões', 'Conjuntas', 'APRECIADAS', 'Informais', 'Expositores', 'Wilson', '219/98', 'Adylson', 'Motta', '6.5.98', 'Brasileiros', 'RODRIGUES', 'Termos', 'reunião', 'Ofícios', 'CORPO', 'Walbia', 'Lóra', 'TÉCNICO', 'SUBSTITUTO', '2', 'SUBSTITUTA', 'Francisca', 'PRESIDENTE', '2ª', 'Fátima', 'Moura', 'Campos', 'Ivana', 'Antonete', 'Mazurek', 'ATAS', 'PUBLICAÇÕES', 'Terezinha', 'J.', 'Pitangui', 'CONTROLE', 'Representações', 'PSDB-PA', 'internacionais', '', '', '', '', '']

APÊNDICE E – PALAVRAS RETIRADAS DA ANÁLISE/INGLÊS

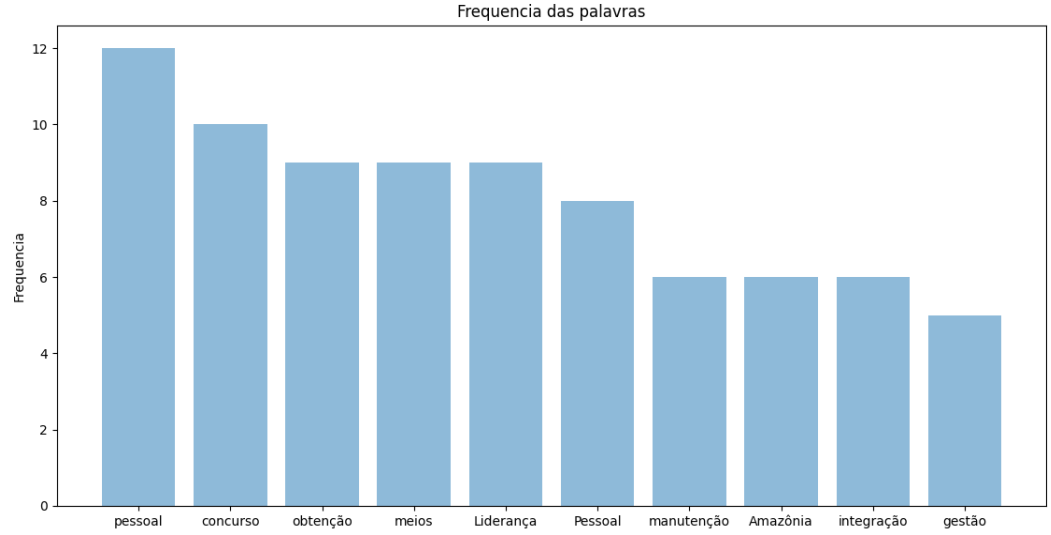
['i', 'me', 'my', 'myself', 'we', 'our', 'ours', 'ourselves', 'you', "you're", "you've", "you'll", "you'd", 'your', 'yours', 'yourself', 'yourselves', 'he', 'him', 'his', 'himself', 'she', "she's", 'her', 'hers', 'herself', 'it', "it's", 'its', 'itself', 'they', 'them', 'their', 'theirs', 'themselves', 'what', 'which', 'who', 'whom', 'this', 'that', "that'll", 'these', 'those', 'am', 'is', 'are', 'was', 'were', 'be', 'been', 'being', 'have', 'has', 'had', 'having', 'do', 'does', 'did', 'doing', 'a', 'an', 'the', 'and', 'but', 'if', 'or', 'because', 'as', 'until', 'while', 'of', 'at', 'by', 'for', 'with', 'about', 'against', 'between', 'into', 'through', 'during', 'before', 'after', 'above', 'below', 'to', 'from', 'up', 'down', 'in', 'out', 'on', 'off', 'over', 'under', 'again', 'further', 'then', 'once', 'here', 'there', 'when', 'where', 'why', 'how', 'all', 'any', 'both', 'each', 'few', 'more', 'most', 'other', 'some', 'such', 'no', 'nor', 'not', 'only', 'own', 'same', 'so', 'than', 'too', 'very', 's', 't', 'can', 'will', 'just', 'don', "don't", 'should', "should've", 'now', 'd', 'll', 'm', 'o', 're', 've', 'y', 'ain', 'aren', "aren't", 'couldn', "couldn't", 'didn', "didn't", 'doesn', "doesn't", 'hadn', "hadn't", 'hasn', "hasn't", 'haven', "haven't", 'isn', "isn't", 'ma', 'mightn', "mightn't", 'mustn', "mustn't", 'needn', "needn't", 'shan', "shan't", 'shouldn', "shouldn't", 'wasn', "wasn't", 'weren', "weren't", 'won', "won't", 'wouldn', "wouldn't", '’', '\uf0b7', 'The', 'United', 'continue', 'We', 'States', 'influence', 'capabilities', 'political', '2019', 'likely', 'countries', '2018', 'interests', 'including', 'threat', 'assess', 'efforts', 'probably', 'use', 'operations', '2017', '2016', 'also', 'In', 'remain', 'support', 'US', '2015', 'groups', 'might', '2014', 'international', 'government', 'forces', '2013', 'global', 'growth', 'new', 'foreign', '2012', 'year', 'regime', 'could', 'However', 'region', '2011', 'percent', 'judge', 'ida', 'STATEMENT', 'FOR', 'THE', 'RECORD', '2010–IC', 'FEB', '•', 'I', '2009', 'ability', '2008', '2009–IC', '2008–IC', 'last', '', '', '', '', '', '', '', '', '', '', '', '', '', '']

APÊNDICE F – 10 PALAVRAS MAIS CITADAS NAS ORCOM, POR ANO

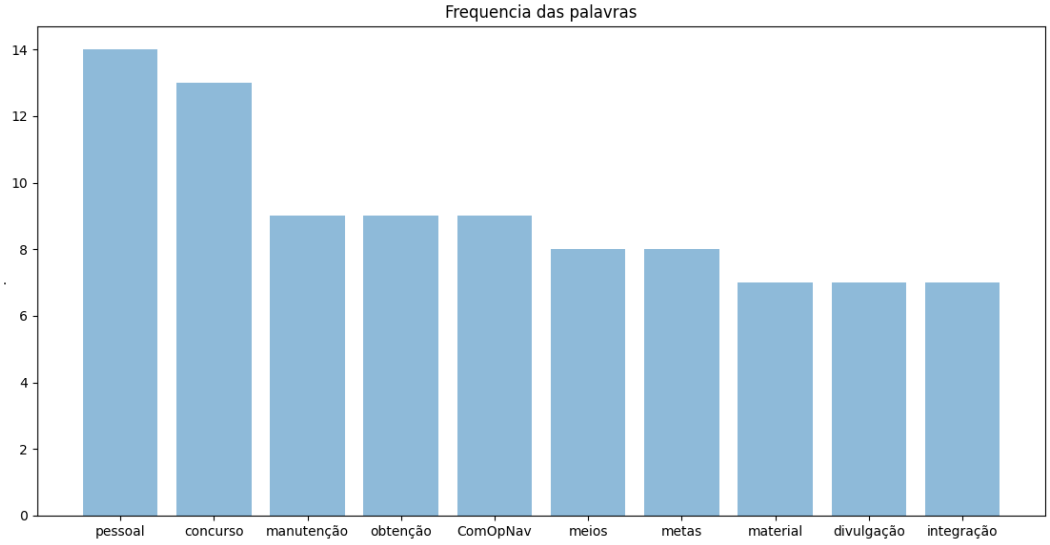
2006



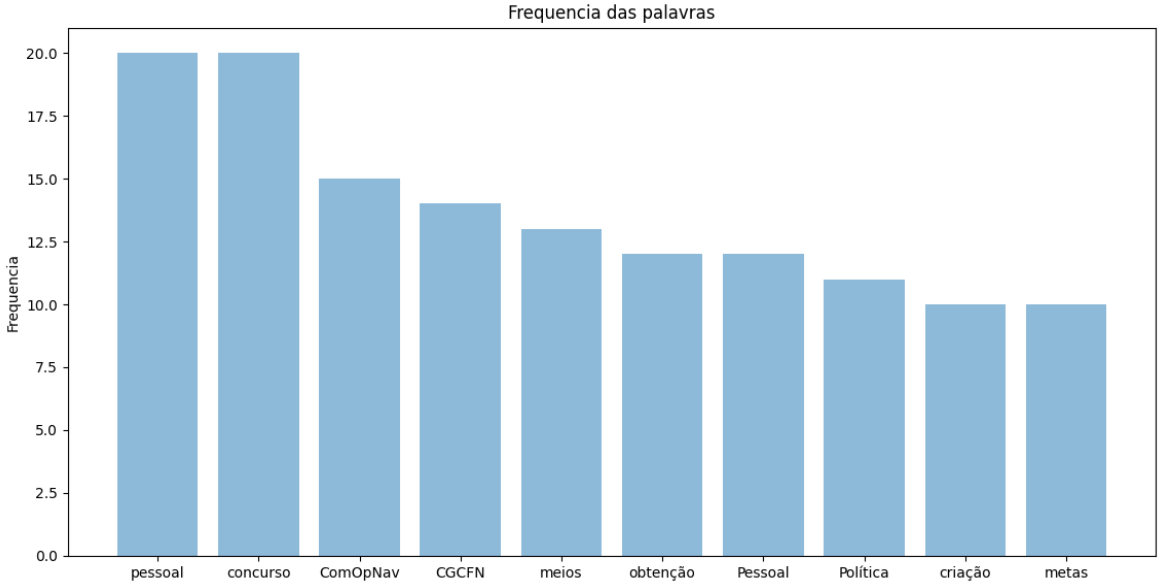
2007



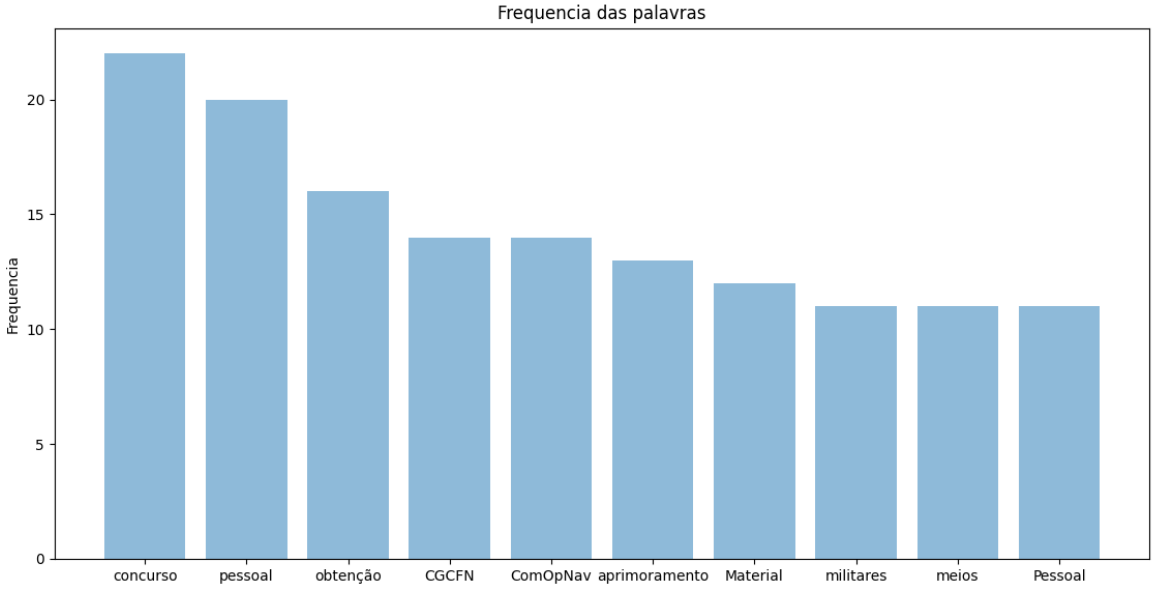
2008



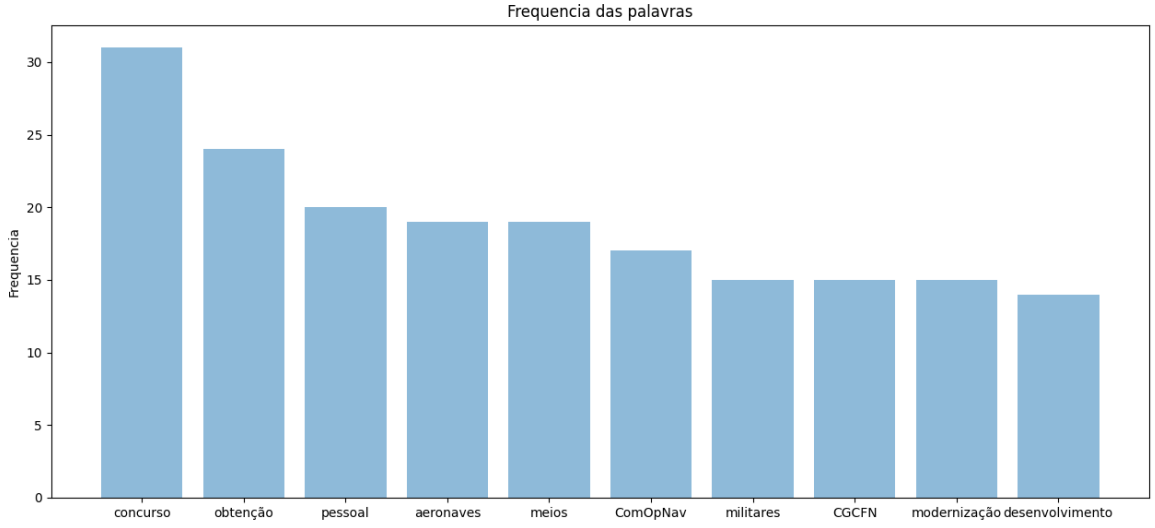
2009



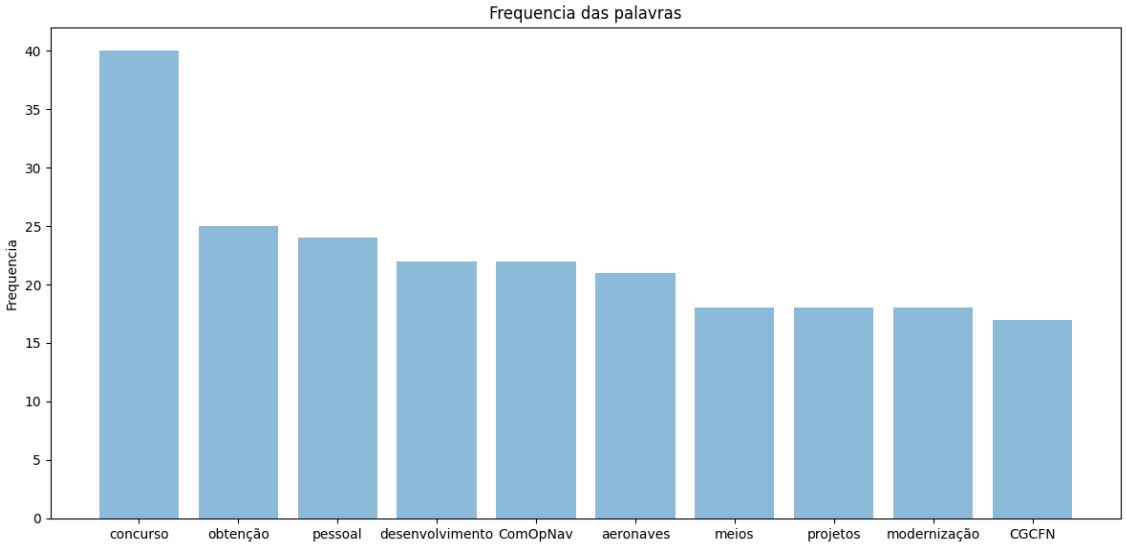
2010



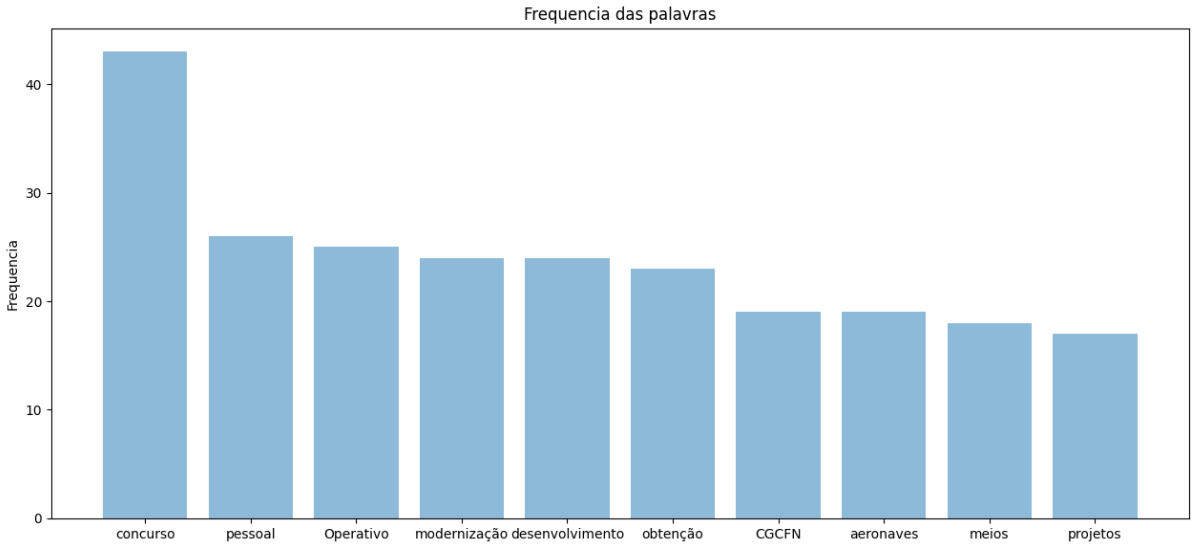
2011



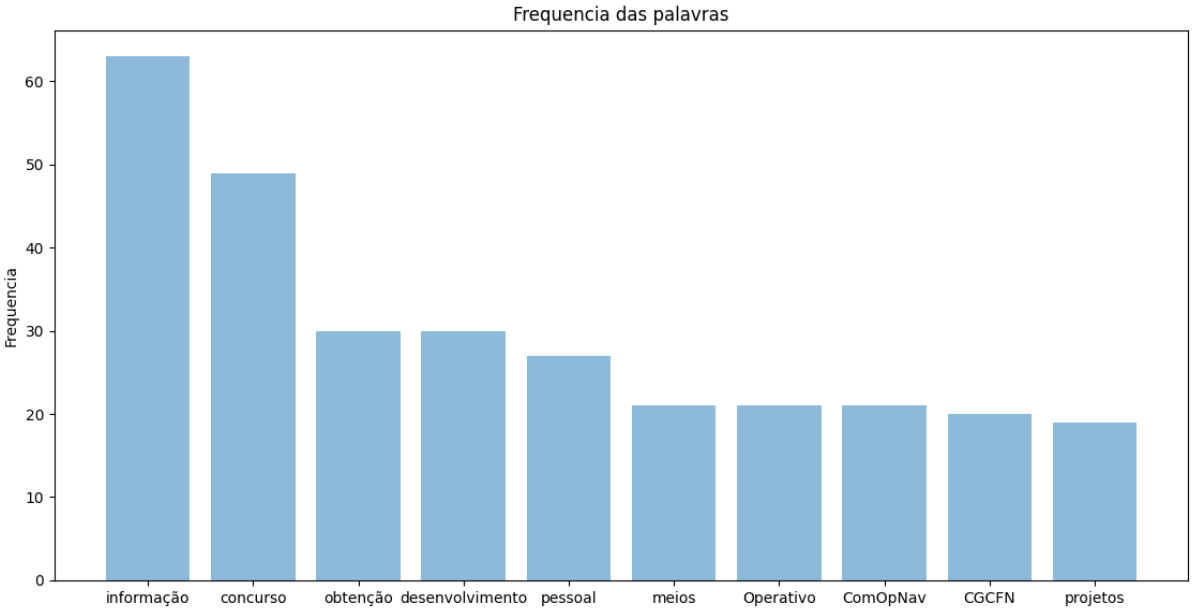
2012



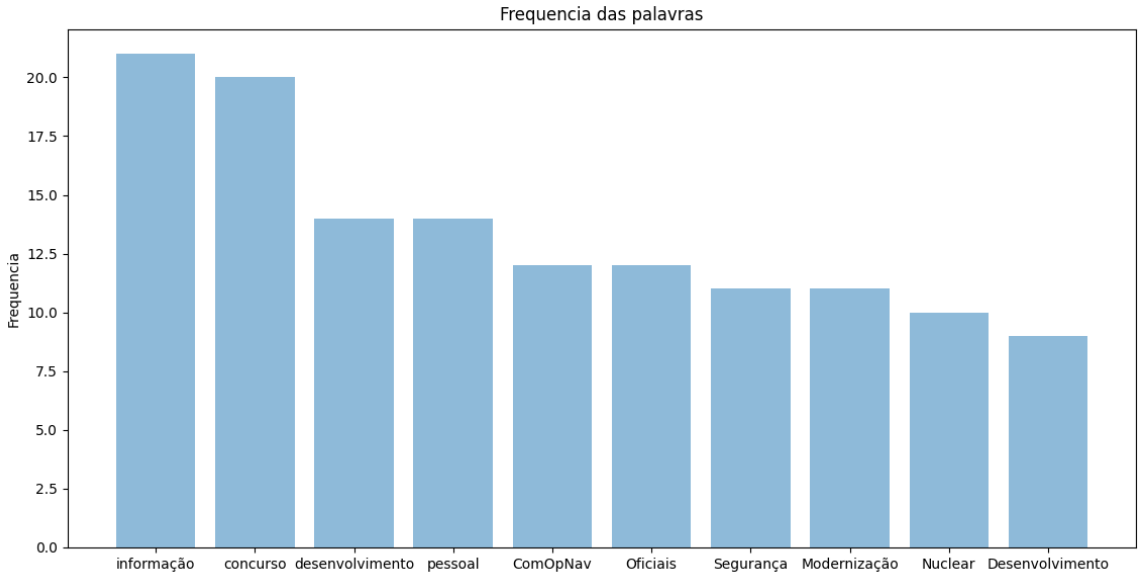
2013



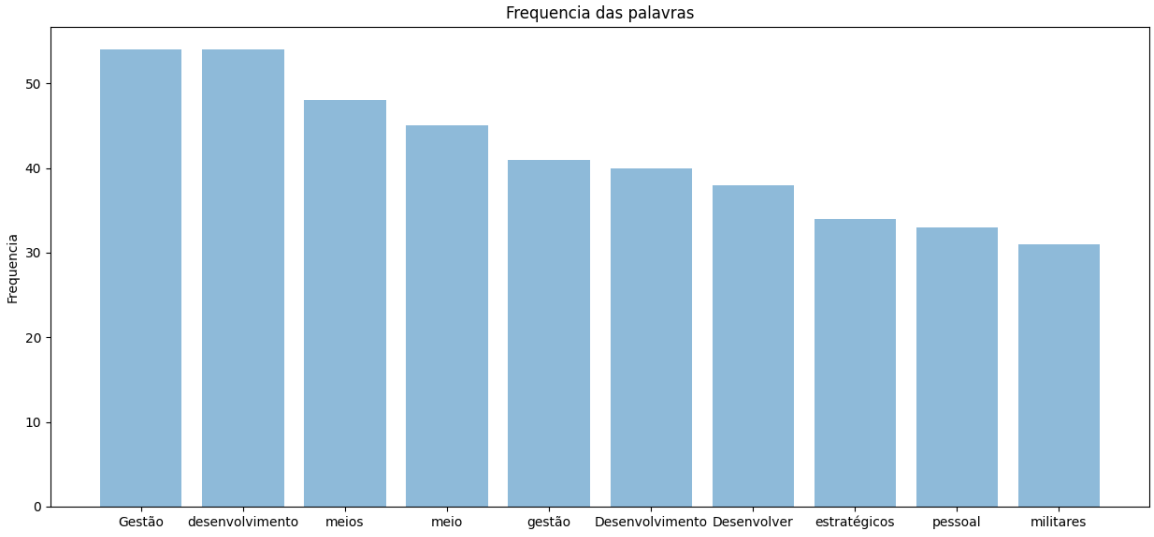
2014



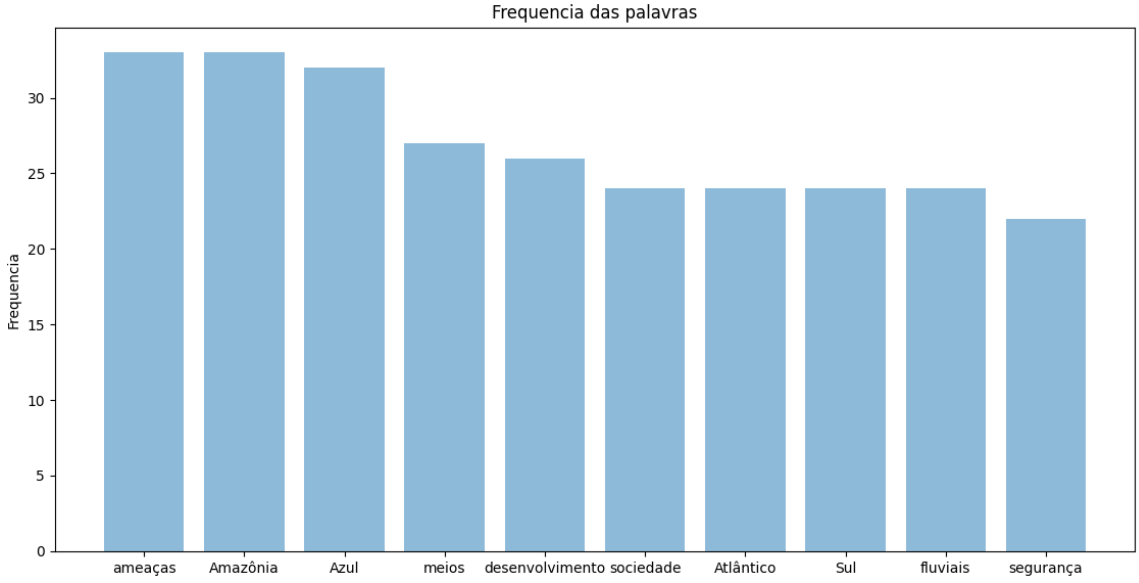
2016



2017

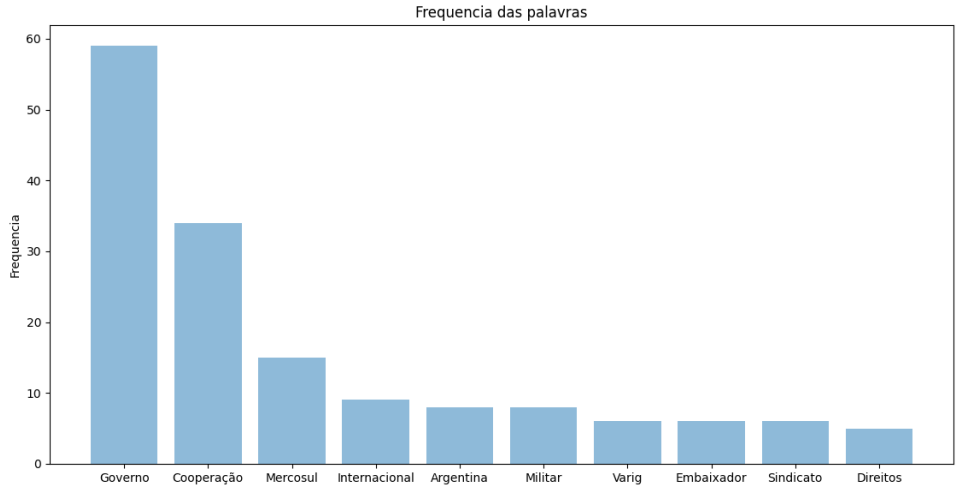


2020

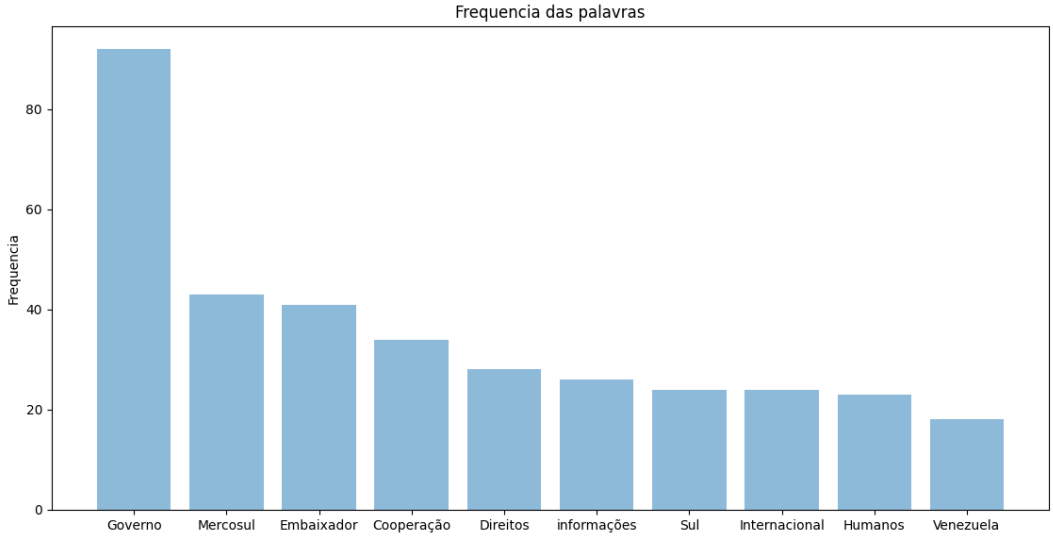


APÊNDICE G – 10 PALAVRAS MAIS CITADAS NOS RELATÓRIOS DA CREDN, POR ANO

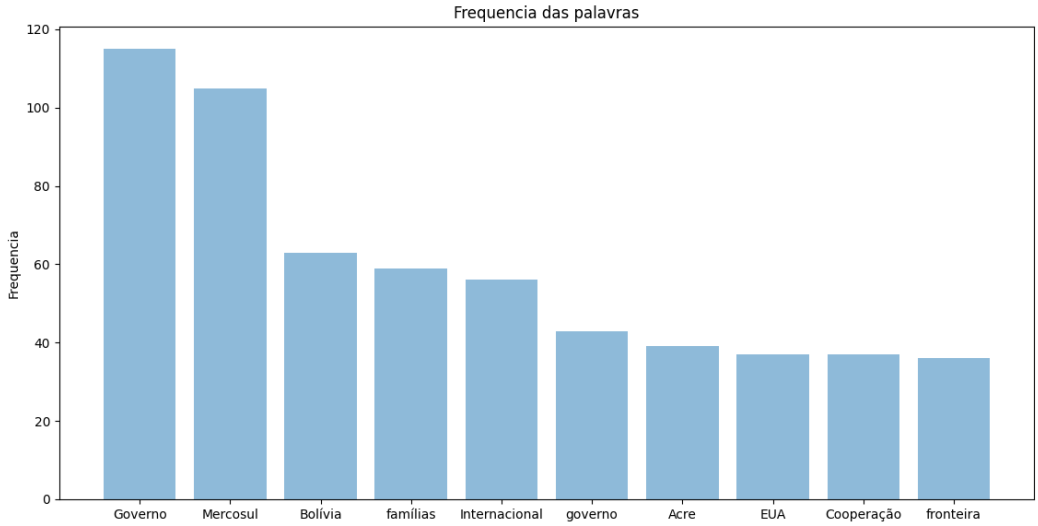
2006



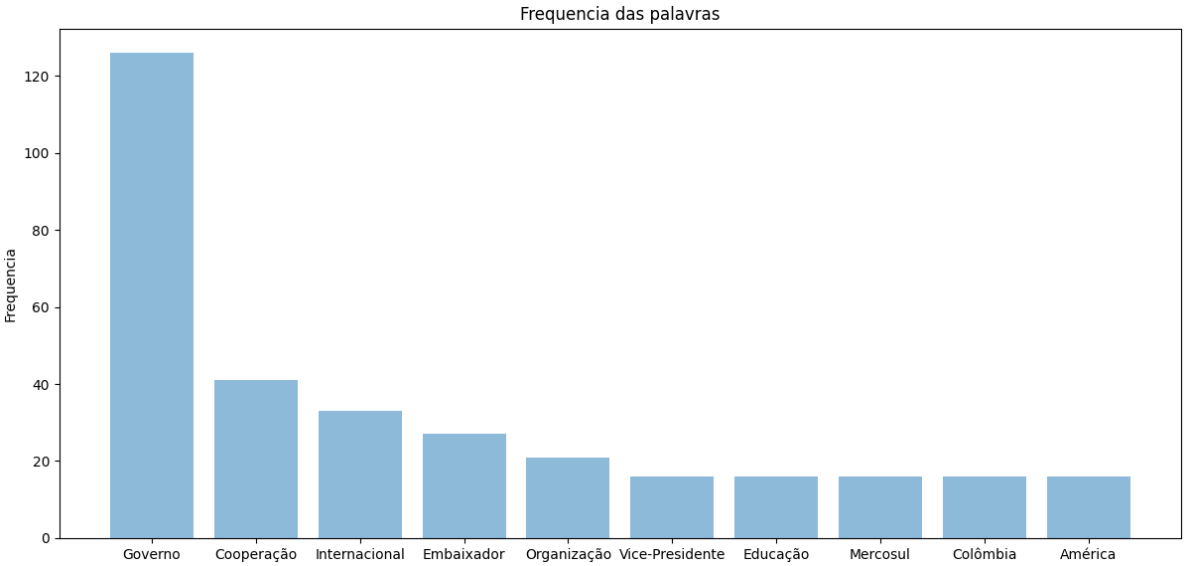
2007



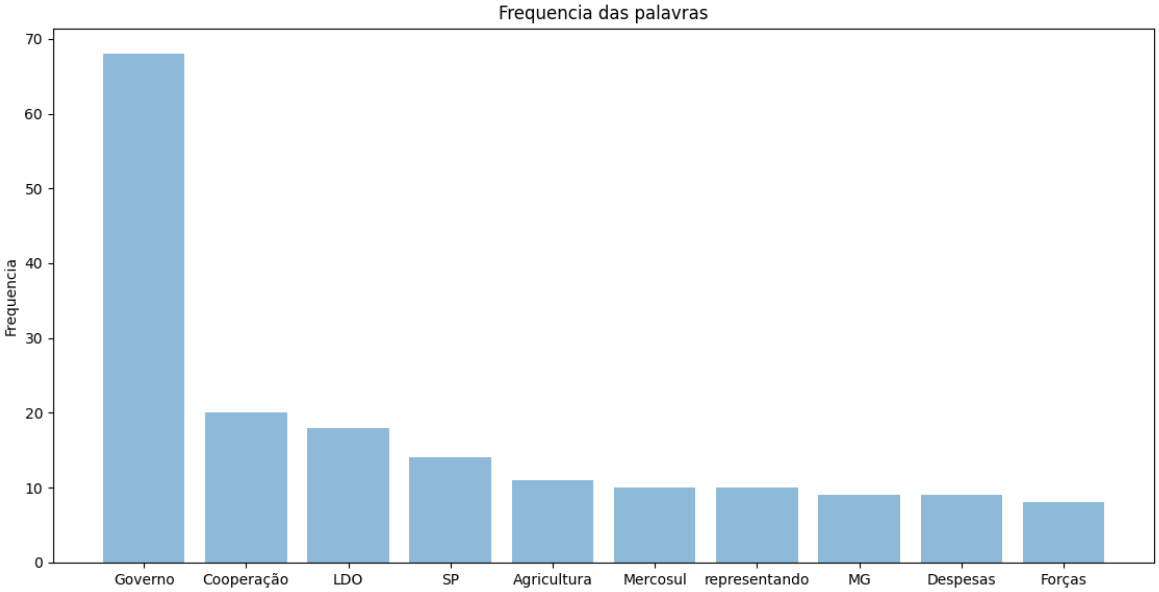
2008



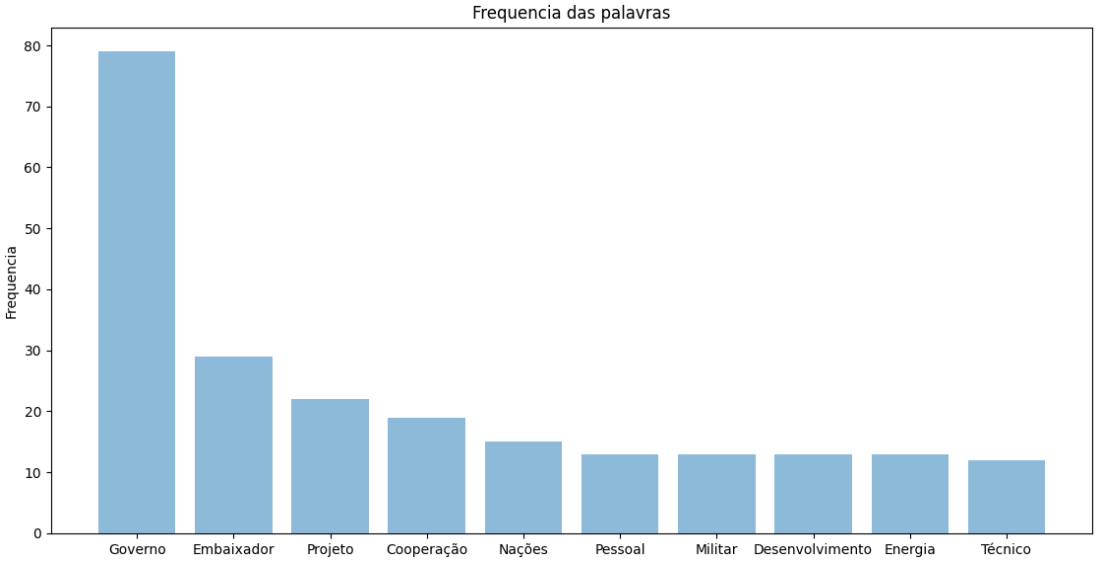
2009



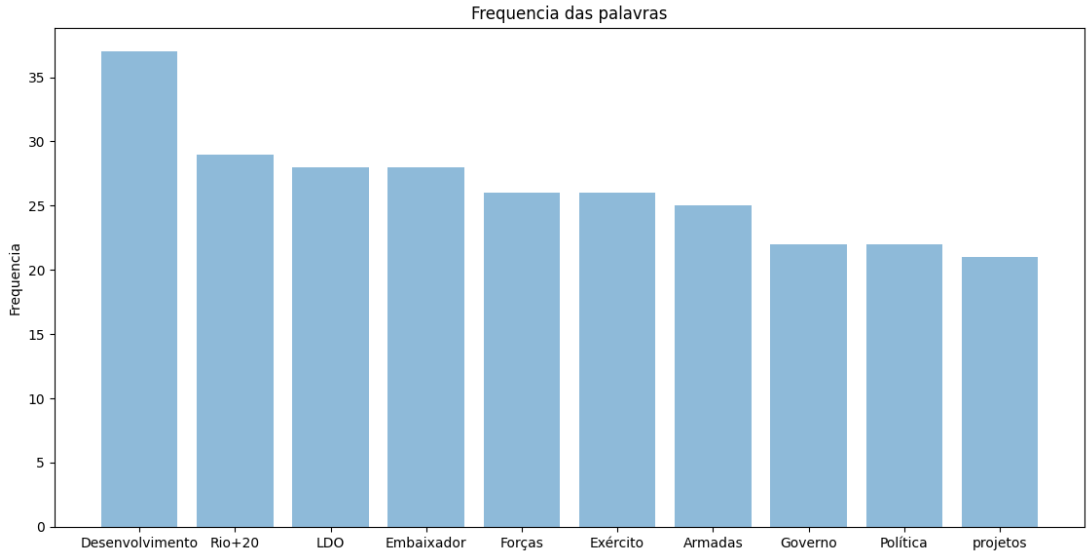
2010



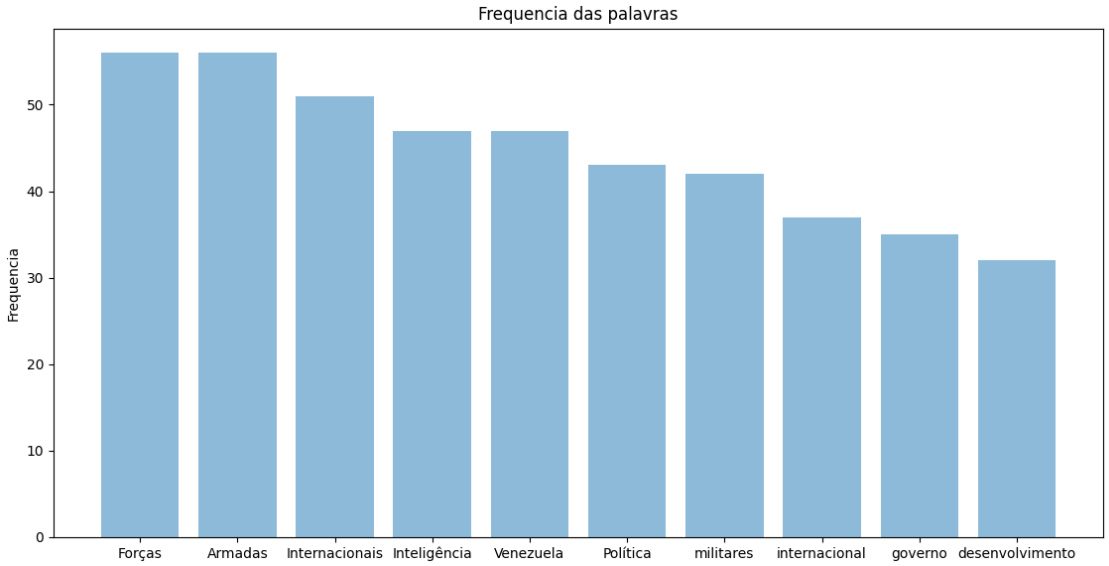
2011



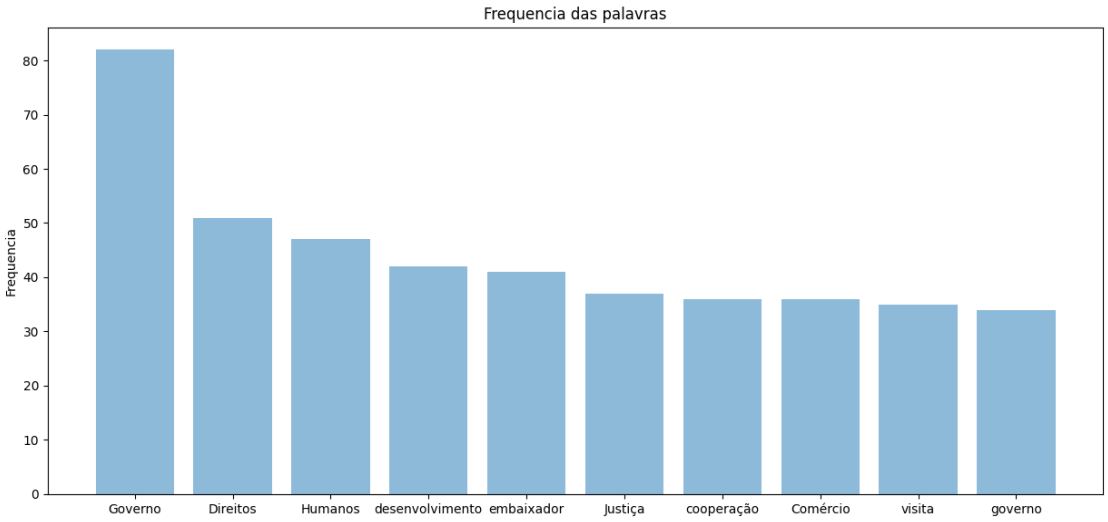
2012



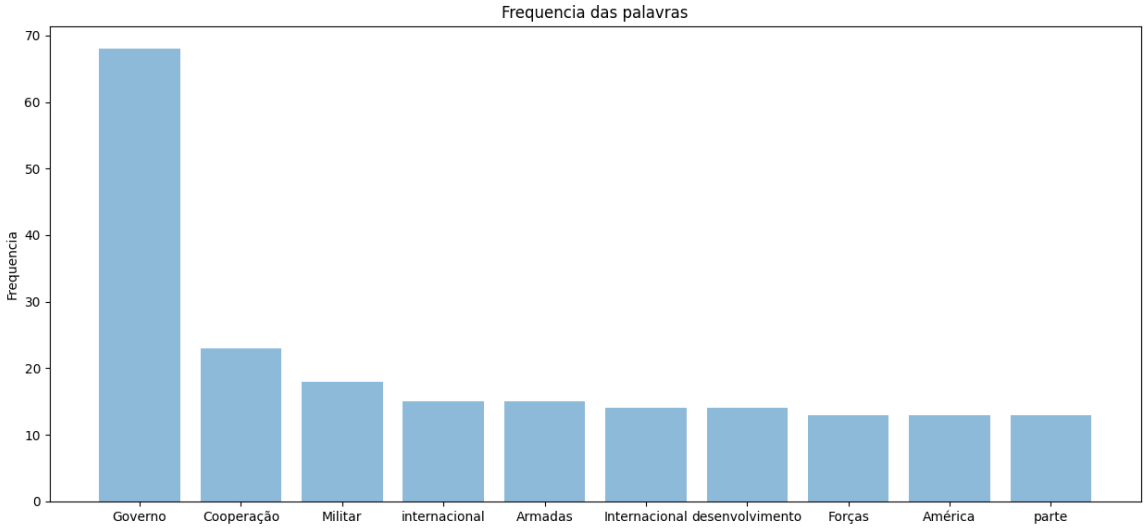
2014



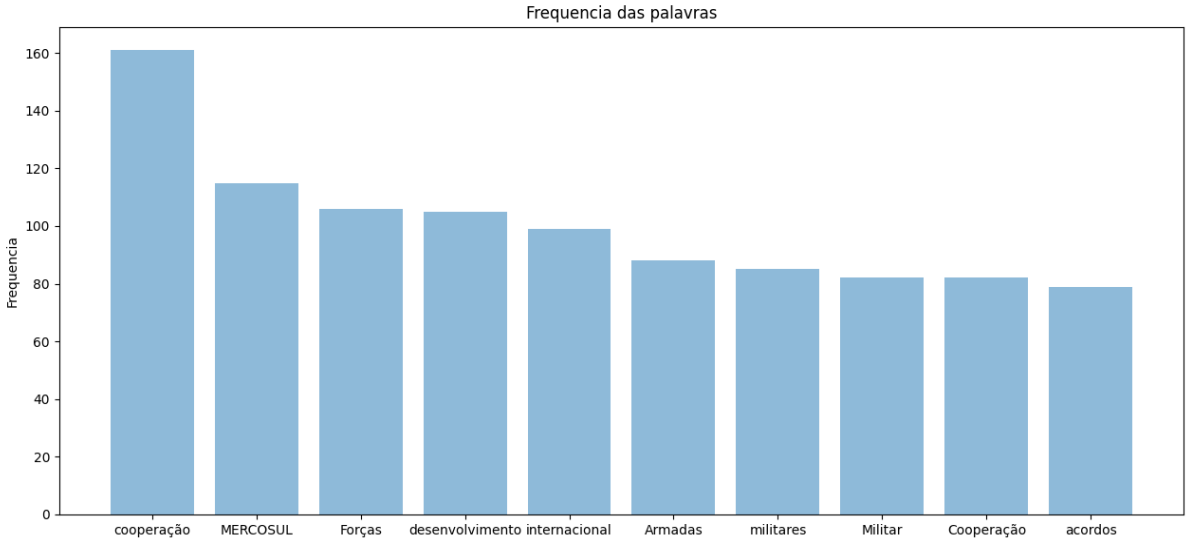
2015



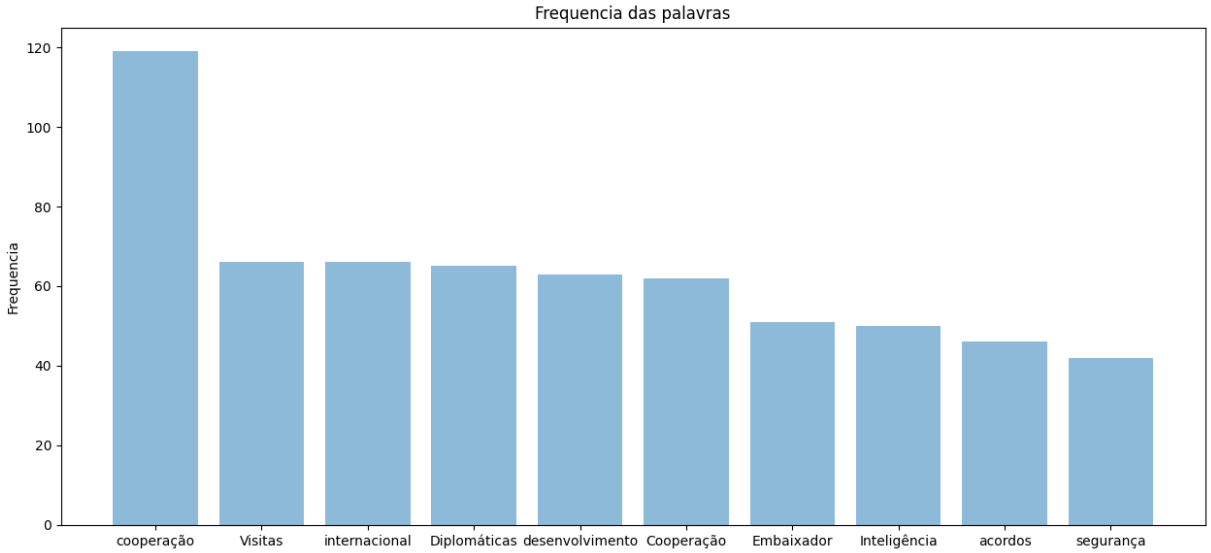
2016



2017

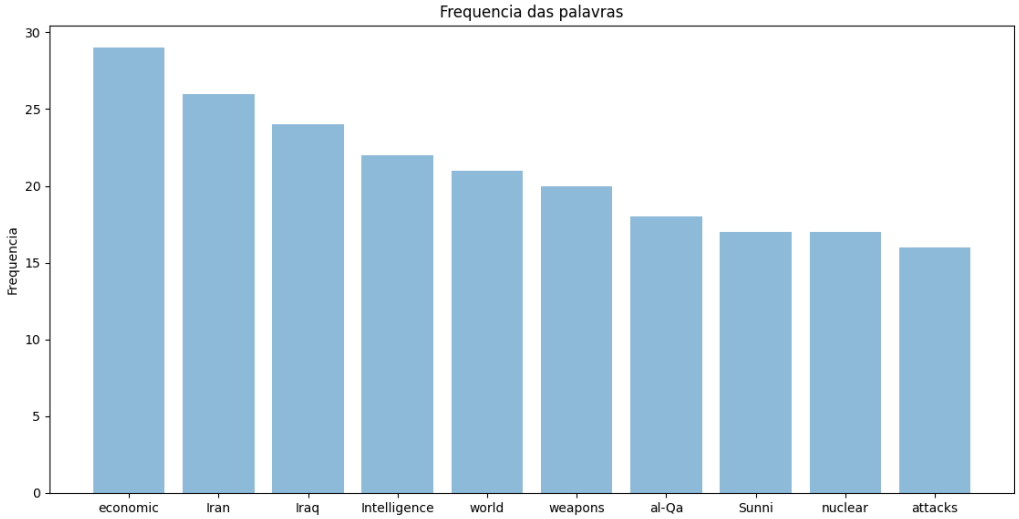


2018

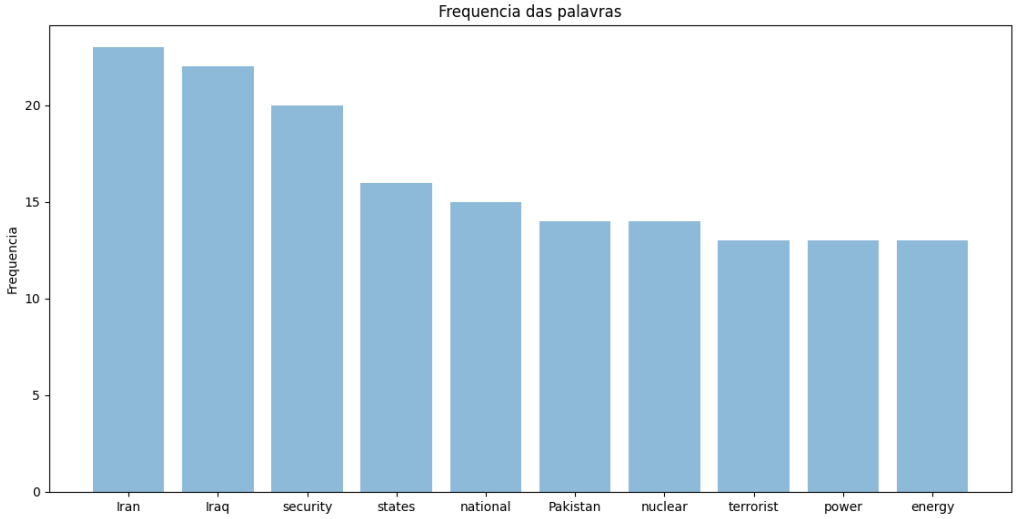


APÊNDICE H – 10 PALAVRAS MAIS CITADAS NOS RELATÓRIOS WTA, POR ANO

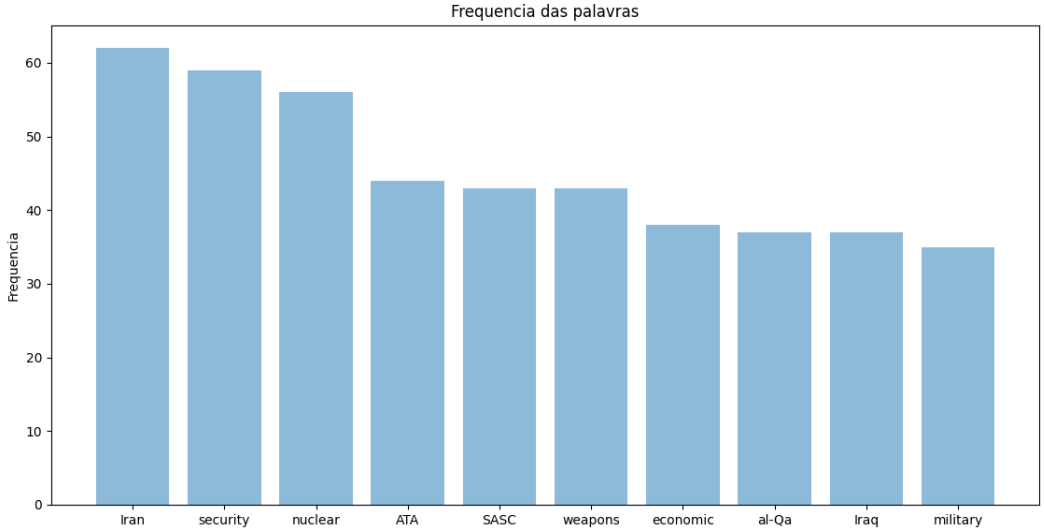
2006



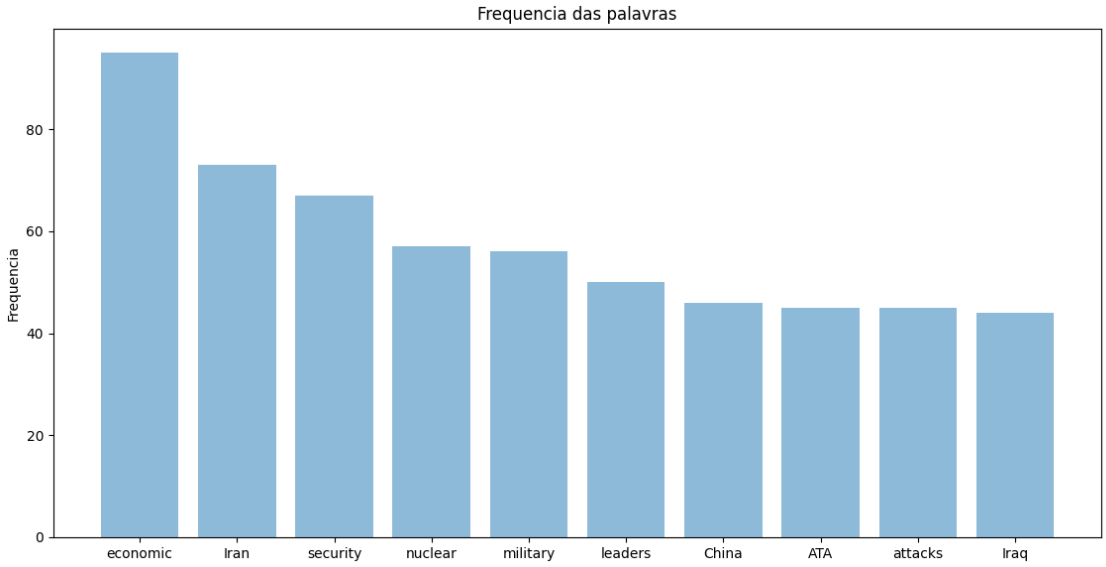
2007



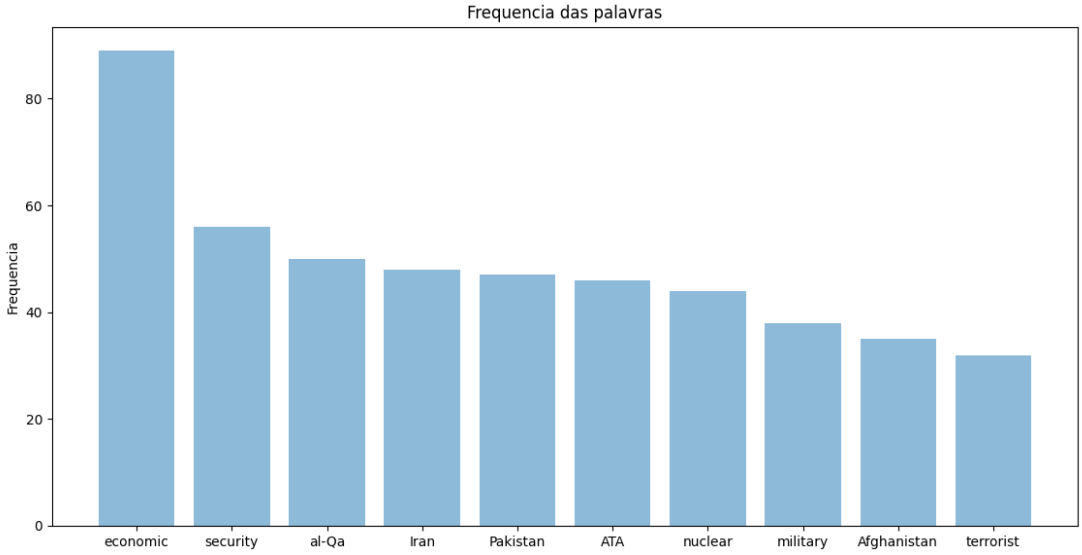
2008



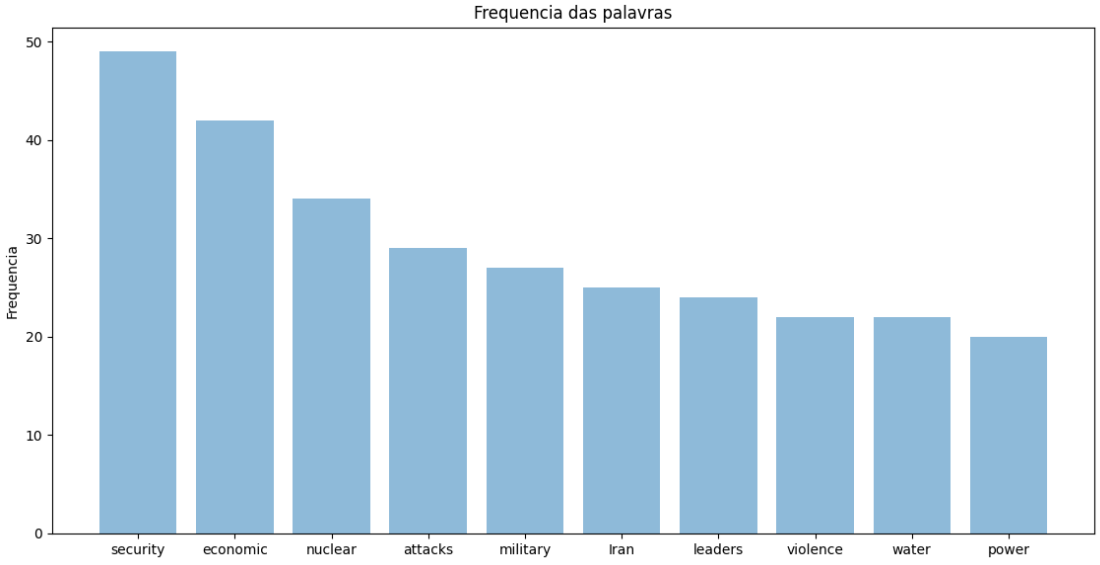
2009



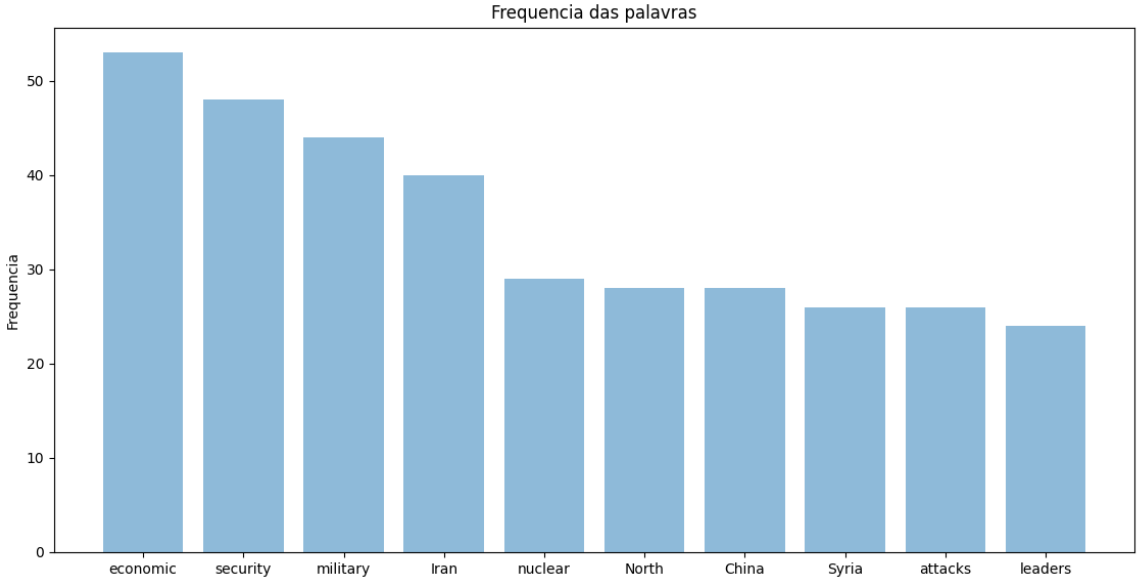
2010



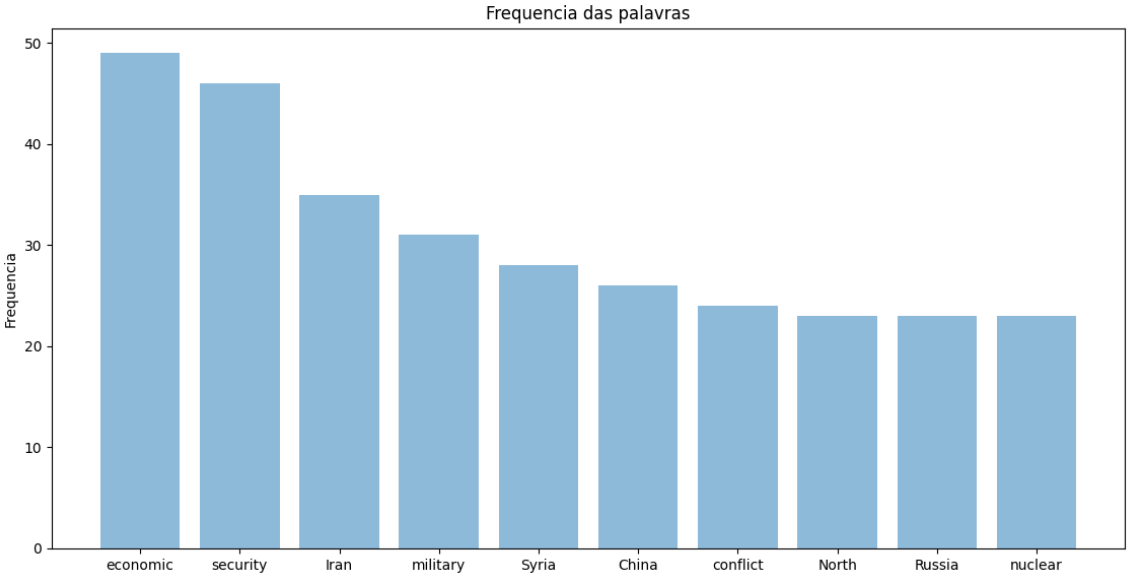
2012



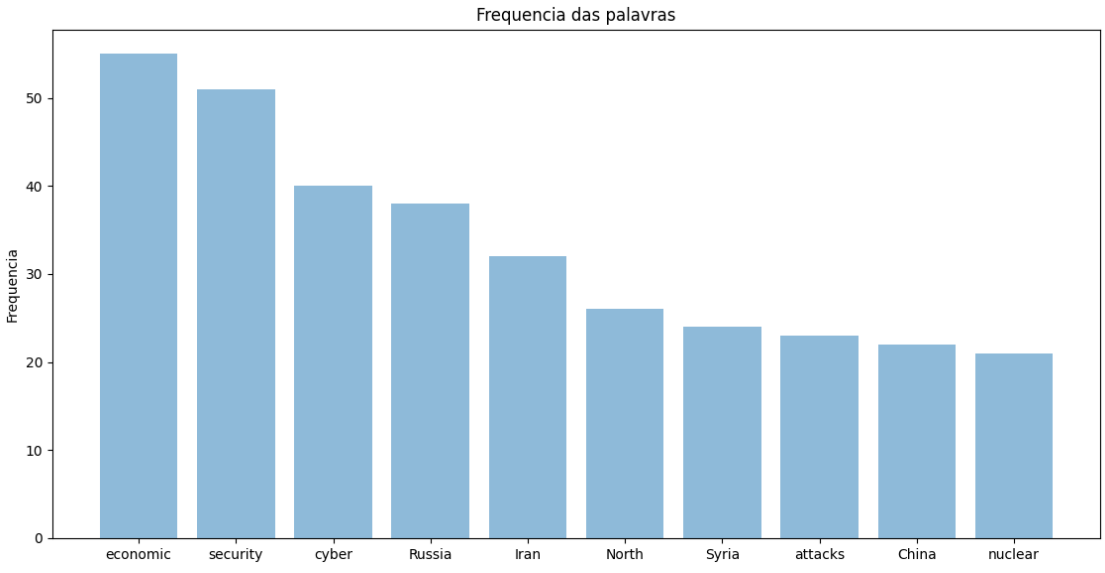
2013



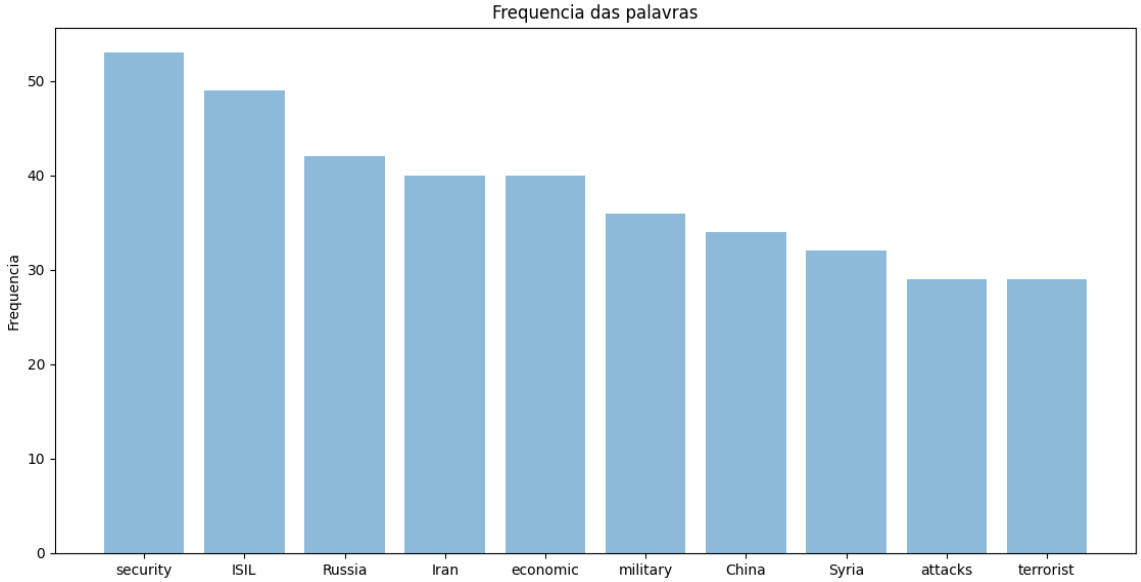
2014



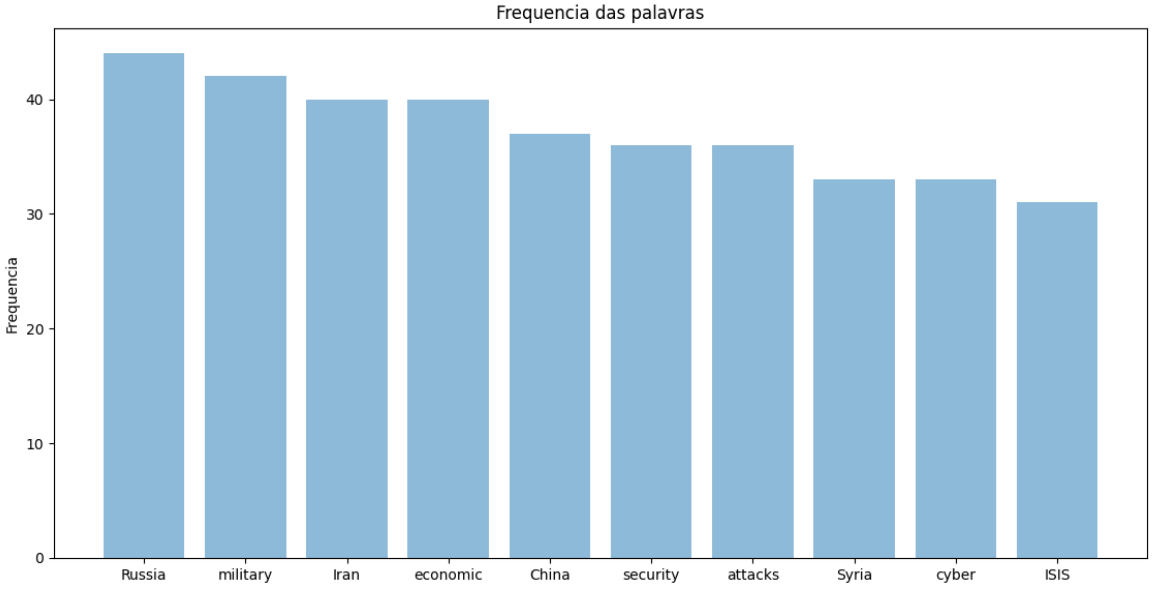
2015



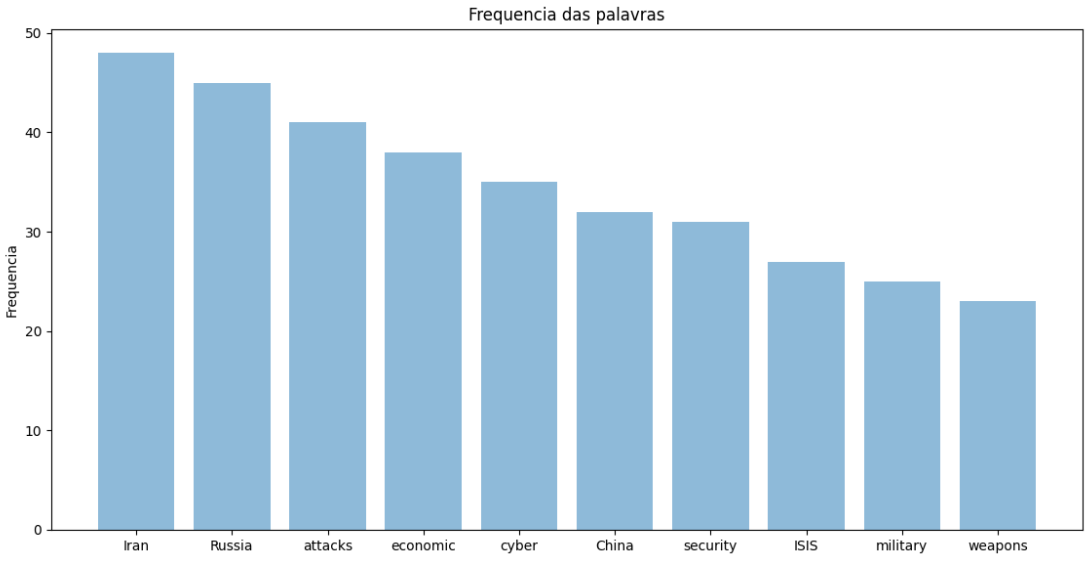
2016



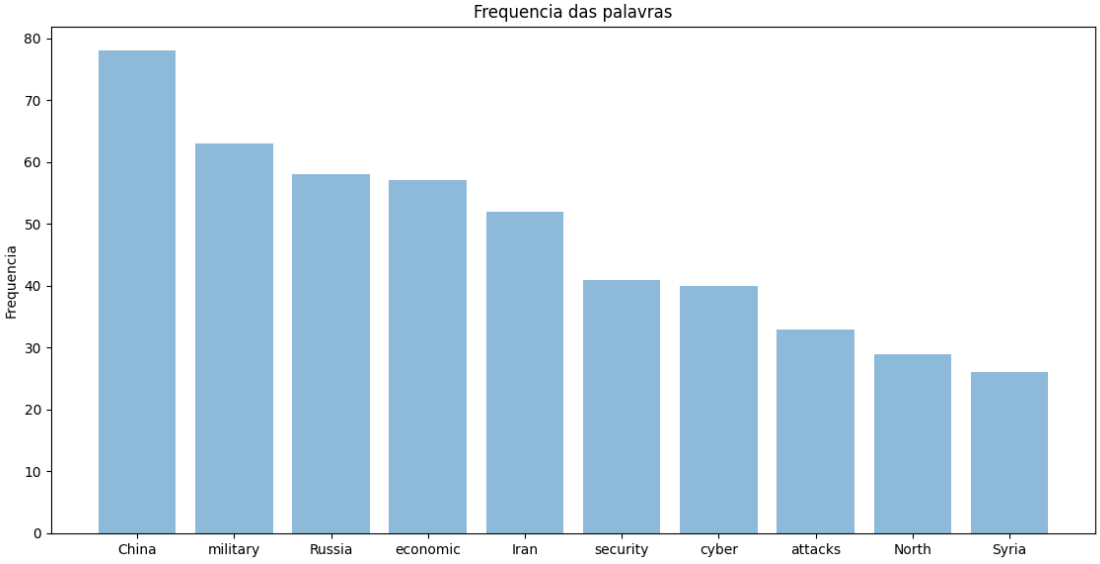
2017



2018



2019


Frequencia das palavras
Frequencia
0
10
20
30
40
50
60
70
80
China
military
Russia
economic
Iran
security
cyber
attacks
North
Syria