

ESCOLA DE GUERRA NAVAL

CMG (EN) JOSÉ FRANCISCO DE ANDRADE JUNIOR

**COMANDO E CONTROLE (C²) NO NÍVEL ESTRATÉGICO:
Ameaças e Contingências aos Sistemas Satelitais
Geoestacionários na Marinha do Brasil**

Rio de Janeiro

2025

CMG (EN) JOSÉ FRANCISCO DE ANDRADE JUNIOR

**COMANDO E CONTROLE (C²) NO NÍVEL ESTRATÉGICO:
Ameaças e Contingências aos Sistemas Satelitais
Geoestacionários na Marinha do Brasil**

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas.

Orientador: CMG (RM1) Luís Fernando Nogueira Pompeu

Rio de Janeiro
Escola de Guerra Naval
2025

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

Declaro que este trabalho acadêmico: a) corresponde ao resultado de investigação por mim desenvolvida, enquanto discente da Escola de Guerra Naval (EGN); b) é um trabalho original, ou seja, que não foi por mim anteriormente utilizado para fins acadêmicos ou quaisquer outros; c) é inédito, isto é, não foi ainda objeto de publicação; e d) é de minha integral e exclusiva autoria.

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar. Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

Os direitos morais e patrimoniais deste trabalho acadêmico, nos termos da Lei 9.610/1998, pertencem ao seu Autor, sendo vedado o uso comercial sem prévia autorização. É permitida a transcrição parcial de textos do trabalho, ou mencioná-los, para comentários e citações, desde que seja feita a referência bibliográfica completa.

Os conceitos e ideias expressas neste trabalho acadêmico são de responsabilidade do Autor e não retratam qualquer orientação institucional da EGN ou da Marinha do Brasil.

AGRADECIMENTOS

“Deus nos concede, a cada dia, uma página de vida nova no livro do tempo. Aquilo que colocarmos nela, corre por nossa conta”.

Francisco Cândido Xavier

Em primeiro lugar, agradeço a Deus por todas as conquistas ao longo da minha vida.

À minha esposa, Ozaneide, pelo inestimável apoio, dedicação e compreensão, sem os quais não teria sido possível concluir este trabalho; e ao meu filho, Gabriel, pelas horas revitalizantes de convívio.

Aos meus pais, Andrade e Clotilde Fortunato (*in memoriam*), pelo zelo e pela dedicação com que me educaram. Aos meus avós, Benedito (*in memoriam*) e Nazaré de Andrade (*in memoriam*), pelo amor e por terem sido referências de educação e afeto, especialmente na ausência de minha mãe.

Ao meu orientador, CMG (RM1) Luís Fernando Nogueira Pompeu, pela atenção, serenidade e generosidade com que me acompanhou, e, sobretudo, pelas orientações sempre coerentes e precisas, fundamentais para o desenvolvimento deste trabalho.

Aos meus amigos e irmãos de infância, pelo constante incentivo e compreensão, que foram essenciais nesta jornada.

Ao CMG (RM1) Alexandre Sousa, Encarregado do C-PEM/2025, pela empatia, praticidade e liderança com que conduziu a turma ao longo dessa jornada, oferecendo indicações seguras e pertinentes.

Ao CF (RM1) Nagashima, pela constante disponibilidade e pelo conhecimento compartilhado de forma clara e objetiva, cujas contribuições foram muito importantes para a consecução desta pesquisa.

À Escola de Guerra Naval, por meio de seu Corpo Docente, pelos ensinamentos e pela dedicação, que tanto contribuíram para a ampliação dos meus conhecimentos e que certamente farão a diferença no desempenho das minhas futuras funções.

Por fim, aos amigos da Turma C-PEM/2025, pelos momentos e experiências compartilhadas, pelas novas amizades e pelo companheirismo cultivado ao longo desta trajetória.

RESUMO

Nesta tese investiga-se a vulnerabilidade das infraestruturas de comunicações militares baseadas em sistemas satelitais geoestacionários (GEO) diante das ameaças cibernéticas, eletrônicas e espaciais, propondo alternativas contingenciais que aumentem a resiliência dos Sistemas de Comando e Controle (C²) no nível estratégico da Marinha do Brasil. O foco recai sobre o Sistema Naval de Comando e Controle (SisNC²), sustentado pelo Sistema de Comunicações Militares por Satélite (SISCOMIS), cuja dependência exclusiva de satélites geoestacionários pode comprometer a disponibilidade e a integridade das operações, como evidenciado pelo ataque à rede ViaSat durante o conflito Rússia-Ucrânia. Para mitigar essas fragilidades, foram estudadas três alternativas tecnológicas: sistemas satelitais de baixa órbita (LEO), comunicações de banda larga em alta frequência (WBHF) e banda estreita em alta frequência (NBHF). Cada solução foi avaliada quanto à soberania tecnológica, resiliência a interferências, operação em ambientes contestados e latência. A metodologia integrou revisão bibliográfica, pesquisa documental e uma Análise Multicritério Híbrida (AHP, MACBETH e TOPSIS), que permitiu classificar as opções segundo sete critérios: ataques cibernéticos, interceptação, bloqueio, armas antissatélites, largura de banda, controle nacional e latência. Os resultados indicaram que os sistemas satelitais de baixa órbita (LEO) apresentaram o melhor desempenho global, seguidos de forma bastante próxima pelas comunicações WBHF, que se destacaram pela alta resiliência e pelo pleno controle nacional. Em sequência, foram classificadas as soluções GEO e NBHF. Por fim, propõe-se a integração gradual e complementar dessas tecnologias à infraestrutura atual do SisNC², em consonância com a Política Nacional de Cibersegurança e a Estratégia Nacional de Defesa, visando à proteção de infraestruturas críticas e à garantia de autonomia operacional.

Palavras-chave: Comando e Controle. Infraestrutura de Comunicações. Soberania Tecnológica. Sistemas Satelitais de Baixa Órbita (LEO). Comunicações de Banda Larga em Alta Frequência (WBHF). Vulnerabilidades Cibernéticas. SisNC². Resiliência Operacional. Guerra Eletrônica. Análise Multicritério.

ABSTRACT

Command and Control at the Strategic Level: Threats and Contingencies to Geostationary Satellite Systems in the Brazilian Navy

This thesis examines the vulnerabilities of military communications infrastructures based on geostationary (GEO) satellite systems in the face of cyber, electronic, and space threats, and proposes contingency alternatives to strengthen the resilience of Command and Control (C²) systems at the strategic level of the Brazilian Navy. The research focuses on the Naval Command and Control System (SisNC²), which relies on the Military Satellite Communications System (SISCOMIS). Exclusive dependence on this infrastructure can compromise operational availability and integrity, as demonstrated by the cyberattack on the ViaSat network during the Russia–Ukraine conflict. To address these challenges, three technological alternatives were analyzed: Low Earth Orbit (LEO) satellite systems, Wideband High Frequency (WBHF) communications, and Narrowband High Frequency (NBHF) systems. Each option was assessed regarding technological sovereignty, resilience to interference, contested environment operation, and latency. The methodology combined literature review, documentary research, and a Hybrid Multicriteria Analysis (AHP, MACBETH, and TOPSIS), enabling prioritization of the alternatives against seven evaluation criteria: cyberattacks, interception, jamming, susceptibility to anti-satellite weapons, bandwidth, national control, and latency. Results indicated that Low Earth Orbit (LEO) satellite systems achieved the best overall performance, closely followed by WBHF communications, which stood out for their high resilience and full national control. Subsequently, GEO and NBHF systems ranked third and fourth, respectively. Finally, the thesis proposes the gradual and complementary integration of these technologies into the SisNC² infrastructure to ensure operational continuity and decision-making autonomy in cases of access denial or satellite link degradation, in line with the National Cybersecurity Policy and National Defense Strategy, which stress technological sovereignty and the protection of critical information infrastructures.

Keywords: Command and Control. Communications Infrastructure. Technological Sovereignty. Low Earth Orbit Satellite Systems (LEO). Wideband High Frequency Communications (WBHF). Cyber Vulnerabilities. SisNC². Operational Resilience. Electronic Warfare. Multicriteria Analysis.

LISTA DE FIGURAS

Figura 1 – Fluxos Vertical e Horizontal de Informações entre os diversos níveis da estrutura de C ²	19
Figura 2 – Topologia da Rede LEO <i>Starlink</i>	34
Figura 3 – Taxas de dados (bps) versus largura de banda, de acordo com a MIL-STD-188-110D.....	37
Figura 4 – Comunicações em um Cenário sem Ameaças.....	40
Figura 5 – Perda de comunicações em um ambiente A2AD	41
Figura 6 – Restabelecimentos das comunicações por meio do emprego de sistemas WBHF	41

LISTA DE TABELAS

Tabela 1 – Sistemas LEO (Low Earth Orbit) versus GEO (Geoestacionários).....	31
Tabela 2 – Formas de Onda Típicas para um Canal de Banda Estreita.....	44
Tabela 3 – Escala de Saaty	50
Tabela 4 – Exemplo de escala verbal utilizada	51
Tabela 5 – Redução de Vieses Cognitivos e Motivacionais na Abordagem Híbrida .	54
Tabela 6 – Matriz de Comparação dos Critérios de Avaliação das Estruturas – Método AHP	64
Tabela 7 – Comparação, Par a Par, dos Critérios dos Critérios – Método AHP.....	65
Tabela 8 – Valor da Atratividade para o Critério C_1	66
Tabela 9 – Valor da Atratividade para o Critério C_2	67
Tabela 10 – Valor da Atratividade para o Critério C_3	69
Tabela 11 – Valor da Atratividade para o Critério C_4	70
Tabela 12 – Valor da Atratividade para o Critério C_5	71
Tabela 13 – Valor da Atratividade para o Critério C_6	71
Tabela 14 – Valor da Atratividade para o Critério C_7	72
Tabela 15 – Matriz de Decisão (sem ponderação/normalização)	73
Tabela 16 – Matriz de Decisão Ponderada	73
Tabela 17 – Figuras de Mérito do Método TOPSIS	73
Tabela 18 – Valor da Atratividade para o Critério C_1 - Primeira Entrevista.....	88
Tabela 19 – Valor da Atratividade para o Critério C_2 - Primeira Entrevista.....	88
Tabela 19 – Valor da Atratividade para o Critério C_3 - Primeira Entrevista.....	88
Tabela 21 – Valor da Atratividade para o Critério C_4 - Primeira Entrevista.....	88
Tabela 22 – Valor da Atratividade para o Critério C_5 - Primeira Entrevista.....	88
Tabela 23 – Valor da Atratividade para o Critério C_6 - Primeira Entrevista	88
Tabela 24 – Valor da Atratividade para o Critério C_7 - Primeira Entrevista.....	89
Tabela 25 – Valor da Atratividade para o Critério C_1 - Segunda Entrevista.....	89
Tabela 26 – Valor da Atratividade para o Critério C_2 - Segunda Entrevista.....	89
Tabela 27 – Valor da Atratividade para o Critério C_3 - Segunda Entrevista	90
Tabela 28 – Valor da Atratividade para o Critério C_4 - Segunda Entrevista.....	90
Tabela 29 – Valor da Atratividade para o Critério C_5 - Segunda Entrevista.....	90
Tabela 30 – Valor da Atratividade para o Critério C_6 - Segunda Entrevista.....	90
Tabela 31 – Valor da Atratividade para o Critério C_7 - Segunda Entrevista.....	90

Tabela 32 – Valor da Atratividade para o Critério C ₁ - Terceira Entrevista.....	91
Tabela 33 – Valor da Atratividade para o Critério C ₂ - Terceira Entrevista.....	91
Tabela 34 – Valor da Atratividade para o Critério C ₃ - Terceira Entrevista.....	91
Tabela 35 – Valor da Atratividade para o Critério C ₄ - Terceira Entrevista.....	91
Tabela 36 – Valor da Atratividade para o Critério C ₅ - Terceira Entrevista.....	91
Tabela 37 – Valor da Atratividade para o Critério C ₆ - Terceira Entrevista.....	92
Tabela 38 – Valor da Atratividade para o Critério C ₇ - Terceira Entrevista.....	92

LISTA DE ABREVIATURAS E SIGLAS

A2AD	–	Anti-Access/Area Denial – Antiacesso e Negação de Área
ASAT	–	Armas Antissatélites
AHP	–	<i>Analytic Hierarchy Process</i> – Processo de Hierarquia Analítica
CC ²	–	Centro de Comando e Controle
CC ² MD	–	Centro de Comando e Controle do Ministério da Defesa
CD-SisMC ²	–	Conselho Diretor do Sistema Militar de Comando e Controle
C ²	–	Comando e Controle
DCTIM	–	Diretoria de Comunicações e Tecnologia da Informação da Marinha
EGN	–	Escola de Guerra Naval
FEC	–	<i>Forward Error Correction</i> – Correção de Erros por Antecipação
GEO	–	<i>Geostationary Earth Orbit</i> – Órbita Terrestre Geoestacionária ou Satélite Geoestacionário
LEO	–	<i>Low Earth Orbit</i> – Órbita Terrestre Baixa
MACBETH	–	<i>Measuring Attractiveness by a Categorical Based Evaluation Technique</i> – Medida de Atratividade por Técnica de Avaliação Categórica
MB	–	Marinha do Brasil
MD	–	Ministério da Defesa
NBHF	–	<i>Narrow Band High Frequency</i> – Sistemas de Comunicações de Banda Estreita em Alta Frequência
RECIM	–	Rede de Comunicações Integradas da Marinha
ROD	–	Rede Operacional de Defesa
SATCOM	–	Sistemas de Comunicações Satelitais
SisMC ²	–	Sistema Militar de Comando e Controle
SisNC ²	–	Sistema Naval de Comando e Controle
TOPSIS	–	<i>Technique for Order Preference by Similarity to Ideal Solution</i> – Técnica para Ordenação por Similaridade com a Solução Ideal
WBHF	–	<i>Wide Band High Frequency</i> – Sistemas de Comunicações de Banda Larga em Alta Frequência

SUMÁRIO

1	INTRODUÇÃO.....	13
2	INFRAESTRUTURA DE COMANDO E CONTROLE NA MARINHA DO BRASIL	19
2.1	SISTEMA MILITAR DE COMANDO E CONTROLE	20
2.2	REDE DE COMUNICAÇÕES DAS FORÇAS.....	21
2.3	REDE OPERACIONAL DE DEFESA.....	21
2.4	INFRAESTRUTURA DE COMUNICAÇÕES DO SisNC ²	21
2.5	AMEAÇAS.....	22
2.6	REQUISITOS FUNDAMENTAIS.....	25
2.7	CONCLUSÕES PARCIAIS.....	27
3	SISTEMAS SATELITAIS DE BAIXA ÓRBITA (LEO)	29
3.1	CONCEITOS BÁSICOS DE SISTEMAS LEO	29
3.2	ARQUITETURA E PROTOCOLOS.....	31
3.3	AMEAÇAS.....	32
3.4	RESILIÊNCIA DOS SISTEMAS LEO.....	33
3.5	CONCLUSÕES PARCIAIS.....	34
4	SISTEMAS DE COMUNICAÇÕES DE BANDA LARGA EM ALTA FREQUÊNCIA	36
4.1	CONCEITOS BÁSICOS DE SISTEMAS WBHF.....	36
4.2	ARQUITETURA E PROTOCOLOS.....	37
4.3	AMEAÇAS.....	38
4.4	RESILIÊNCIA DOS SISTEMAS WBHF	39
4.5	CONCLUSÕES PARCIAIS.....	41
5	SISTEMAS DE COMUNICAÇÕES DE BANDA ESTREITA EM ALTA FREQUÊNCIA	43
5.1	CONCEITOS BÁSICOS DE SISTEMAS NBHF	43
5.2	ARQUITETURA E PROTOCOLOS.....	44
5.3	AMEAÇAS.....	45
5.4	RESILIÊNCIA DOS SISTEMAS NBHF	45
5.5	CONCLUSÕES PARCIAIS.....	46

6	AVALIAÇÃO MULTICRITÉRIO	48
6.1	FUNDAMENTOS DA ABORDAGEM MULTICRITÉRIO HÍBRIDA	48
6.2	INFRAESTRUTURAS E CRITÉRIOS DE AVALIAÇÃO	54
6.2.1	Matriz de Comparação, Par a Par, dos Critérios AHP	56
6.2.2	Vetor de Pesos Normalizados – AHP	64
6.2.3	Análise e Atribuição dos Valores de Atratividade – MACBETH	65
6.2.4	Matriz de Decisão Ponderada – MACBETH	72
6.2.5	Resultados Finais – TOPSIS	73
6.3	CONCLUSÕES PARCIAIS.....	73
7	CONSIDERAÇÕES FINAIS	76
	REFERÊNCIAS	80
	APÊNDICE A - QUESTIONÁRIO ESTRUTURADO	85
	APÊNDICE B – IMPLEMENTAÇÃO DA ANÁLISE MULTICRITÉRIO	93

1 INTRODUÇÃO

Em um ambiente de competição entre Estados, a crescente complexidade dos cenários operacionais modernos e as ameaças emergentes no campo das comunicações militares têm exigido uma reformulação estratégica das infraestruturas tecnológicas empregadas pelas Forças Armadas. No contexto da Marinha do Brasil (MB), a eficácia do Sistema Naval de Comando e Controle (SisNC²), parte integrante do Sistema Militar de Comando e Controle (SisMC²), depende da infraestrutura de comunicações formada pelo Sistema de Comunicações Militares por Satélite (SISCOMIS) e pela Rede de Comunicações Integradas da Marinha (RECIM). Assim, esses dois elementos representam os principais alicerces para o fluxo de informações entre os níveis tático, operacional e estratégico. Tais sistemas asseguram a conectividade e a interoperabilidade entre o SisNC² e o SisMC². (BRASIL, 2023b; BRASIL, 2015)

O segmento espacial do SISCOMIS possui infraestrutura de comunicações baseada em satélites geoestacionários e esse tipo de comunicação tem se revelado suscetível a vulnerabilidades, notadamente ameaças como: ações de bloqueio (guerra eletrônica); ataques cibernéticos; e emprego de armas antissatélite (ASAT), cinéticas e não-cinéticas, no domínio estratégico espacial, também denominado Quarto Domínio (BRASIL, 2025). O avanço das capacidades ofensivas por Estados e grupos organizados demonstra que não há garantias absolutas de inviolabilidade ou disponibilidade desses meios mesmo no Quarto Domínio, formado pelas operações e segmentos espaciais (STEVENSON et al., 2014; BBC Brasil, 2007).

O espaço cibernético, integrante do Quinto Domínio Operacional, que abrange os ambientes cibernético, eletromagnético e cognitivo (TILL, 2018; BRASIL, 2025) vem apresentando crescente relevância nos conflitos contemporâneos. O caso da empresa Crypto AG, revelado por Miller (2020), somado aos recentes ciberataques contra a ViaSat, demonstraram essa tendência. As vulnerabilidades decorrentes se tornaram evidentes durante a guerra da Ucrânia, quando ofensivas russas contra a empresa ViaSat comprometeram de forma significativa a capacidade de comunicação das Forças Armadas ucranianas e impactaram diversos usuários civis que dependiam desse provedor (NCSC, 2022). Esse episódio evidenciou, de forma prática, que mesmo grandes operadores comerciais de satélites não estão imunes a ameaças cibernéticas avançadas, o que ressalta a necessidade de resiliência, redundância e

soberania tecnológica na proteção das comunicações estratégicas. As ofensivas exploraram vulnerabilidades das estações terrenas, responsáveis pela integração dos enlaces satelitais por meio de redes fixas de telecomunicações interligadas à internet. Essa dependência da internet ampliou, de forma crítica, a superfície de exposição a ataques cibernéticos. Diante desse cenário, revela-se necessária a criação de alternativas seguras e redundantes aos sistemas satelitais geoestacionários. Essas medidas visam garantir comunicações críticas em situações de conflito, reduzir a dependência de sistemas vulneráveis e assegurar a continuidade operacional (NCSC, 2022).

Esses casos expõem vulnerabilidades estruturais que vão além de falhas tecnológicas pontuais, revelando a crescente sofisticação e impacto das ameaças cibernéticas no cenário militar global. Nesse contexto, a Dimensão Cibernética, também denominada espaço cibernético, vem se consolidando como componente essencial do Quinto Domínio operacional, ao lado dos domínios terrestre, marítimo, aéreo e espacial (BRASIL, 2025). Nele, os princípios de confidencialidade, integridade e disponibilidade da informação se tornaram pilares indispensáveis ao êxito das operações militares modernas. Considerando-se esse novo paradigma operacional, torna-se essencial, no âmbito da Marinha do Brasil (MB), estudar soluções que complementem a atual infraestrutura de comunicações que apoia o SisNC², tornando-o mais resiliente diante de ambientes contestados e ameaças cibernéticas constantes.

Embora o SisNC² não atue diretamente no nível estratégico — como será detalhado no Capítulo 2 —, o fortalecimento de sua infraestrutura de comunicações representa, em certa medida, um incremento da resiliência do SisMC², que se insere no nível estratégico.

Nesse sentido, destacam-se como candidatos a alternativas contingentes para a infraestrutura do segmento espacial do SISCOPIS os seguintes sistemas:

- a) Os Sistemas Satelitais de Baixa Órbita (LEO);
- b) Os Sistemas de Comunicações de Banda Larga em Alta Frequência (*Wide Band High Frequency* – WBHF); e
- c) Os Sistemas de Comunicações de Banda Estreita em Alta Frequência (*Narrow Band High Frequency* – NBHF).

A estrutura de C², no âmbito da MB exige que os dados fluam com segurança e celeridade entre os diferentes níveis da cadeia de comando. O SisNC² deve, portanto, ter uma infraestrutura de comunicações resiliente capaz de operar mesmo em condições adversas. Segundo Zacconi (2021), o fluxo de informações entre os níveis operacional e estratégico é essencial para a coesão das ações militares, e qualquer falha nesse sistema compromete o processo decisório em tempo hábil. Ademais, a interoperabilidade com estruturas superiores, como a Rede Operacional de Defesa (ROD) e o SISCOMIS, impõe exigências adicionais de flexibilidade, robustez e segurança.

A proposta de uma infraestrutura alternativa encontra respaldo teórico e estratégico nos princípios de redundância e dissuasão. Sistemas de comunicações em HF, por exemplo, são notoriamente resilientes, em virtude de sua propagação ionosférica que independe de infraestrutura física conectada à internet, sendo menos suscetíveis a interceptações e ataques cibernéticos (STEVENSON et al., 2014). Adicionalmente, os sistemas satelitais de baixa órbita, devido à sua dinâmica e densidade orbitais, possuem maior resistência e não permitem ataques físicos direcionados, conforme descrito em BBC Brasil (2007).

Outro aspecto relevante é a necessidade de soberania tecnológica. A adoção de sistemas autóctones, desenvolvidos no Brasil, que permitiriam maior controle sobre algoritmos, protocolos de segurança e arquitetura de hardware, evitaria o risco de vulnerabilidades intencionais inseridas por fornecedores estrangeiros. Além disso, é importante destacar que o desenvolvimento de soluções tecnológicas autóctones está alinhado com as diretrizes estabelecidas pela Política Nacional de Cibersegurança (PNCiber), instituída pelo Decreto nº 11.856/2023, a qual define requisitos como a autonomia tecnológica nacional, a resiliência de infraestruturas críticas e a proteção de ativos estratégicos de informação (BRASIL, 2023a). De forma consonante, a Estratégia Nacional de Defesa (END) reforça a soberania cibernética como eixo estruturante das Capacidades Nacionais de Defesa, destacando a necessidade de domínio tecnológico em áreas sensíveis, como sistemas de C² e Comunicações Estratégicas (BRASIL, 2020a). Tais documentos sustentam a importância de se investir em tecnologias desenvolvidas no país, com controle pleno sobre algoritmos, protocolos e processos de criptografia, de modo a garantir a inviolabilidade e a continuidade das operações militares em ambientes adversos.

Diversos episódios históricos evidenciam a relevância da autonomia tecnológica, especialmente, no que se refere às áreas de telecomunicações e tecnologia da informação:

- a) Um dos casos mais emblemáticos que ilustram os perigos da dependência de soluções tecnológicas estrangeiras para comunicações militares é o escândalo envolvendo a empresa suíça Crypto AG. Desde a década de 1950, essa companhia forneceu dispositivos de criptografia para mais de 120 governos e entidades diplomáticas. No entanto, descobriu-se que esses equipamentos, em especial o modelo CX-52, continham vulnerabilidades deliberadamente inseridas por meio de chaves-mestras. Tais falhas permitiam o acesso às mensagens criptografadas por agências de inteligência, como a Agência de Segurança Nacional dos Estados Unidos (NSA) e o Serviço de Inteligência Exterior da Alemanha (BND). Em 2020, uma apuração conjunta do jornal *The Washington Post* e das emissoras ZDF (Alemanha) e SRF (Suíça) revelou que a Crypto AG era secretamente controlada por essas duas agências, dentro das operações clandestinas denominadas “Thesaurus” e, mais tarde, “Rubicon”, em vigor até 2018. Esse caso reforça a necessidade de adoção de sistemas de comunicação autóctones, que assegurem a integridade e o controle das informações estratégicas em ambientes militares (MILLER, 2020);
- b) Outro exemplo importante ocorreu em agosto de 2008, quando a Geórgia foi alvo de uma ofensiva militar por parte da Rússia. Paralelamente à invasão terrestre, registrou-se uma série de ataques cibernéticos coordenados, protagonizados por hackers russos. Essa foi a primeira ocorrência conhecida de uma ofensiva digital de grande escala, concomitante a operações bélicas convencionais. O impacto psicológico e informacional foi profundo, resultando no isolamento digital da Geórgia perante o cenário internacional. É razoável considerar que, caso o país tivesse desenvolvido uma estrutura própria de defesa cibernética, os efeitos dessa campanha poderiam ter sido mitigados (MARKOFF, 2008); e
- c) Mais recentemente, em setembro de 2024, houve um incidente no Oriente Médio envolvendo explosões de pagers que deixaram mortos e feridos entre membros do Hezbollah. Esse evento acendeu o alerta sobre as

fragilidades dos sistemas de comunicação adquiridos sem processos rigorosos de validação quanto à sua procedência e segurança (REUTERS, 2024).

Adicionalmente, cabe destacar que tecnologias consideradas sensíveis, sobretudo aquelas voltadas à segurança das comunicações, são frequentemente submetidas a restrições de exportação. Quando a sua comercialização é permitida, é usual que contenham limitações em seus algoritmos ou funcionalidades, comprometendo o seu desempenho e a segurança em contextos críticos.

Assim, é importante que o SisNC² possua uma Infraestrutura autônoma e resiliente de comunicações, flexível e plenamente interoperável com o escalão superior (estratégico), a fim de permitir que as informações decorrentes do nível tático possam ser compartilhadas, via nível operacional, sem atrasos, interceptações ou bloqueios (STEVENS et al., 2014), até o nível estratégico, e vice-versa (POSADA, 2019). Para tanto, deve-se buscar uma Infraestrutura de Comunicações contingente à atual infraestrutura do SisNC², que é composta pela RECIM e pelo segmento espacial do Sistema de Comunicações Militares por Satélite (SISCOMIS) (BRASIL, 2015).

Parte-se da hipótese de que a adoção de alternativas tecnológicas autóctones e resilientes, em regime complementar ao SISCOMIS, pode incrementar significativamente a capacidade de C² da MB em ambientes contestados e sob ameaça cibernética, espacial ou eletrônica.

Diante do que foi exposto nesta fase introdutória, observa-se importante dependência da Marinha do Brasil em relação ao segmento espacial do Sistema de Comunicações Militares por Satélite (SISCOMIS), o que compromete a resiliência da infraestrutura de comunicações de Comando e Controle (C²), tornando-a suscetível a interferências eletrônicas, ataques cibernéticos e armas antissatélite (ASAT). Assim, observa-se como Problema de Pesquisa desse trabalho: “Uma forte dependência do SisNC² em relação ao segmento espacial do SISCOMIS”.

Nesse contexto, emerge a Questão Central que orienta esta pesquisa: “Como a Marinha do Brasil poderá mitigar os efeitos de interferências eletrônicas, ataques cibernéticos e armas antissatélite sobre a principal infraestrutura de comunicações que suporta o Sistema Naval de Comando e Controle (SisNC²)?”

Para responder a essa questão, o presente trabalho foi estruturado em sete capítulos, cujo detalhamento a seguir permite relacionar cada um deles aos níveis de aprendizagem propostos pela Taxonomia de Bloom (PINTO, 2023). Essa estruturação contempla Objetivos Estruturantes Específicos voltados ao Objeto de Estudo, que consiste na avaliação e proposição de infraestruturas de comunicações capazes de complementar ou substituir temporariamente o SISCOMIS em situações de degradação ou negação de acesso ao ambiente espacial. O propósito central é, portanto, garantir a resiliência, a soberania e a continuidade da infraestrutura de comunicações de C² no âmbito do SisNC².

No Capítulo 2, apresenta-se a fase diagnóstica, que tem como objetivo identificar e apresentar a atual Infraestrutura de Comando e Controle da Marinha do Brasil, com ênfase na Infraestrutura de Comunicações empregada no SisNC². Nesse contexto, são evidenciadas suas vulnerabilidades diante do atual cenário de ameaças tecnológicas, em ambientes operacionalmente contestados. No final do Capítulo 2, são apresentados argumentos que reforçam o Problema de Pesquisa, a Questão Central e o Objeto de Estudo deste trabalho (PINTO, 2023).

Nos Capítulos 3, 4 e 5 têm-se como propósito identificar, apresentar e analisar os Sistemas Satelitais de Baixa Órbita (LEO), os Sistemas de Comunicações de Alta Frequência de Banda Larga (WBHF) e os Sistemas de Comunicações de Banda Estreita (NBHF), respectivamente. Em cada capítulo, faz-se uma análise desses sistemas frente a critérios como capacidade de resposta, soberania, vulnerabilidade a interferências, ameaças cibernéticas e capacidade de operação em ambientes degradados.

No Capítulo 6, tem-se como objetivo formular e aplicar uma Análise Multicritério Híbrida, combinando os métodos AHP (*Analytic Hierarchy Process*), MACBETH (*Measuring Attractiveness by a Categorical Based Evaluation Technique*) e TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*), e comparar os resultados obtidos. A partir da avaliação de sete critérios estratégicos, pode-se **ordenar** as alternativas tecnológicas estudadas.

O Capítulo 7, tem-se por finalidade compilar os principais achados, interpretar os resultados à luz dos objetivos traçados e propor uma composição de sistemas de comunicações resilientes e contingentes à atual infraestrutura do SisNC².

2 INFRAESTRUTURA DE COMANDO E CONTROLE NA MARINHA DO BRASIL

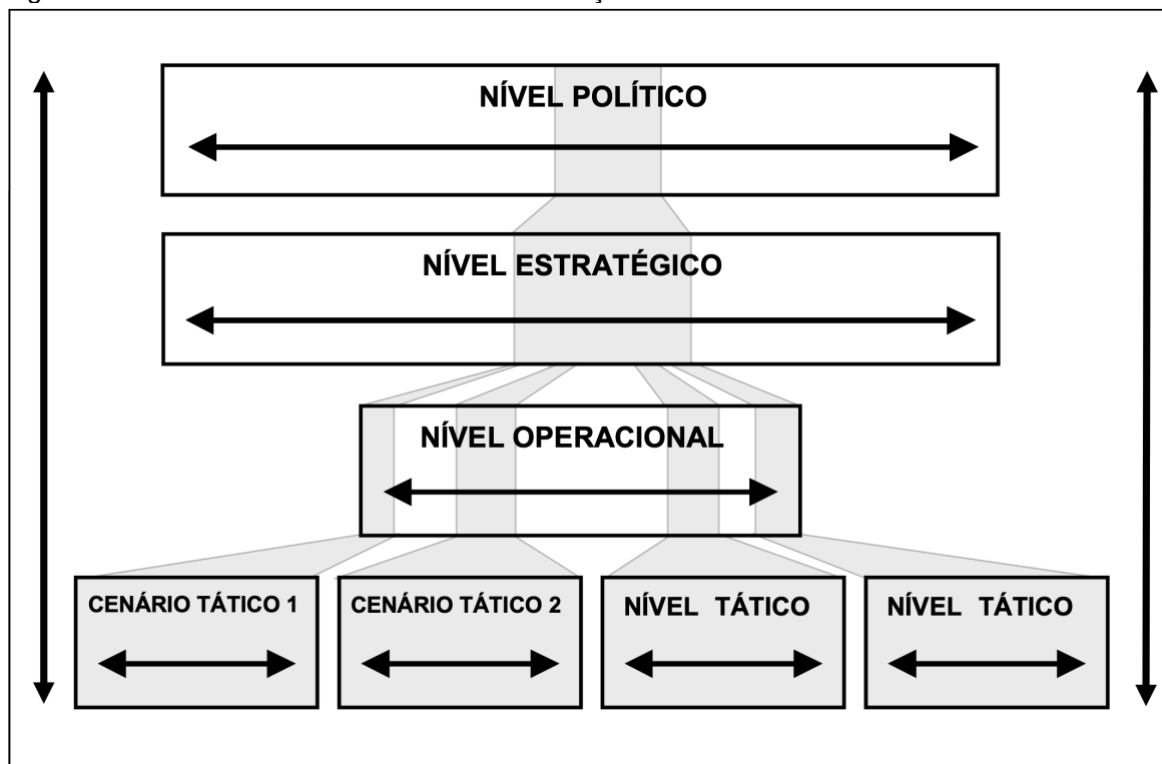
Neste capítulo aborda-se a infraestrutura do Sistema Naval de Comando e Controle (SisNC²), com ênfase na arquitetura de comunicações empregada, destacando também as principais ameaças que podem comprometer sua operacionalidade.

Quando da necessidade de adoção de doutrina e/ou procedimentos na condução de operações de C² em níveis mais altos, a publicação que trata do assunto é a Doutrina Militar de Comando e Controle (BRASIL, 2015). Segundo essa publicação:

O fluxo vertical ocorrerá entre os diversos níveis da estrutura de C², permitindo que informações sejam transmitidas entre os escalões subordinados e superiores. À medida que as informações sobem níveis hierárquicos, devem ser mais condensadas, evitando-se os detalhes inerentes aos níveis inferiores.

O fluxo horizontal ocorrerá entre os elementos do mesmo nível, dotando-os de consciência situacional do ambiente em que estarão inseridos (Brasil, 2015, p. 21).

Figura 1 – Fluxos Vertical e Horizontal de Informações entre os diversos níveis da estrutura de C²



Fonte: BRASIL (2015).

A Figura 1 evidencia que a infraestrutura de comunicações atua como a espinha dorsal de uma estrutura de Comando e Controle (C²), conectando os

diferentes níveis dessa cadeia. Assim, um aumento de resiliência nos níveis inferiores contribui para que as informações cheguem ao nível estratégico com segurança, mitigando atrasos, intercepções e/ou bloqueios. Como o foco deste trabalho está centrado no C² em nível estratégico, abordar-se-á nesta tese o problema considerando apenas o fluxo vertical de informações, entre os níveis, desde o tático até o estratégico, principalmente entre o tático e o operacional, no qual é empregado o segmento espacial do SISCOMIS.

2.1 SISTEMA MILITAR DE COMANDO E CONTROLE

De acordo com a Doutrina Militar de Comando e Controle, O SisMC² compreende a integração de instalações, meios de comunicação, sistemas de informação, doutrinas, procedimentos operacionais e recursos humanos indispensáveis ao exercício do C², com o objetivo de apoiar as atividades de preparo e emprego das Forças Armadas. Esse sistema abrange tanto os Sistemas Militares de C² das três Forças quanto aqueles diretamente subordinados ao Ministério da Defesa, tendo como finalidade prover os recursos de C² necessários ao funcionamento da Estrutura Militar de Defesa. Seu propósito é atender às demandas decorrentes do preparo e do emprego das Forças Armadas, devendo ainda possuir a capacidade de interagir com organizações nacionais e internacionais, militares ou civis (BRASIL, 2015).

Dentro da estrutura do SisMC², a MB atua por meio de um Centro de Comando e Controle (CC²) de caráter permanente, formado pelo do Comando de Operações Navais (ComOpNav), e de caráter temporário, formados pelos CC² dos Comandos Operacionais ativados e/ou contingentes brasileiros em Forças de Paz.

Como principal meio de transmissão de dados operacionais militares no âmbito do SisMC², tem-se o Sistema de Comunicações Militares por Satélite (SISCOMIS), sob a gestão da Subchefia de Comando e Controle (SC-1), vinculada à Chefia de Operações Conjuntas do Estado-Maior Conjunto das Forças Armadas (CHOC/EMCFA). Sua estrutura tecnológica é composta por uma infraestrutura de comunicações formada por satélites geoestacionários e redes de dados, distribuída em dois segmentos: o Espacial e o Terrestre. O SISCOMIS é responsável por garantir a conectividade segregada necessária para a transmissão de voz, dados e imagens, possibilitando o intercâmbio de informações em tempo real entre os CC² integrantes

do SisMC², de forma a atender às demandas operacionais conjuntas e específicas do Ministério da Defesa (BRASIL, 2015).

2.2 REDE DE COMUNICAÇÕES DAS FORÇAS

Além dos recursos disponibilizados pelo SISCOMIS, as redes internas de comunicação de dados e voz das três Forças Armadas estão interconectadas a esse sistema e devem ser utilizadas de forma complementar, sempre que contribuírem para o fortalecimento da estrutura de C² no contexto das Operações Militares (BRASIL, 2015).

2.3 REDE OPERACIONAL DE DEFESA

A Rede Operacional de Defesa (ROD) constitui um dos principais meios de comunicação militares operacionais no âmbito do SisMC². Estruturada como uma *Wide Area Network* (WAN), a ROD oferece conectividade segregada — caracterizada por ser restrita, segura e gerenciável — utilizando múltiplas vias, incluindo o SISCOMIS, as redes de dados das Forças Armadas, como a RECIM, a EBNET e a INTRAER, além da Internet. Seu protocolo de endereçamento baseia-se no *Internet Protocol* (IP) (BRASIL, 2015).

Projetada para sustentar os diversos sistemas e serviços hospedados no Centro de Comando e Controle do Ministério da Defesa (CC²MD), a ROD tem por finalidade viabilizar a condução eficiente das operações conjuntas e singulares sob responsabilidade do MD. Essa rede assegura o fluxo contínuo e seguro de informações em tempo real entre os diversos CC² vinculados ao SisMC², promovendo a interoperabilidade entre eles, sobretudo nos níveis estratégico e operacional.

Os CC² dos Comandos Operacionais ativados, bem como os Centros de suas respectivas Forças Componentes, devem operar de forma integrada à ROD, garantindo interoperabilidade e coordenação no emprego do poder militar.

2.4 INFRAESTRUTURA DE COMUNICAÇÕES DO SisNC²

No âmbito da Marinha do Brasil (MB), o SisNC², assim como o SisMC², conta com uma infraestrutura de comunicações composta por dois segmentos: o espacial,

representado pelo SISCOMIS, e o terrestre, formado pela RECIM. Esta última utiliza enlaces digitais de dados e infraestrutura contratada do tipo *Multiprotocol Label Switching* (MPLS¹).

A infraestrutura que interliga o SisNC² ao SisMC² também se baseia no SISCOMIS e na RECIM, garantindo a integração vertical das informações entre os diferentes níveis da estrutura de C². A RECIM, por sua vez, está integrada à ROD, o que permite a conectividade entre as Organizações Militares de terra pertencentes à estrutura de C².

Entretanto, apenas o segmento espacial do SISCOMIS assegura o fluxo contínuo de informações desde o nível tático (navios, viaturas etc.) até o estratégico. Esse segmento é composto por dois satélites: o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), sob controle do Ministério da Defesa e operado pela Aeronáutica, e o Star One C3, operado pela empresa Claro S/A (BRASIL, 2023b).

Dessa forma, a análise de ameaças desenvolvida neste trabalho será restrita àquelas que afetam especificamente os sistemas de comunicações satelitais geoestacionários.

2.5 AMEAÇAS

Considerando que o SISCOMIS, por meio de seu segmento espacial, representa o principal meio de transmissão de dados operacionais entre os níveis tático e estratégico no âmbito do SisMC² e do SisNC², torna-se essencial identificar os vetores de ameaça que possam comprometer sua disponibilidade, integridade e segurança. Para tanto, é suficiente concentrar-se nas ameaças associadas a satélites que operam em órbita geoestacionária. Atualmente, parte dos navios estrategicamente mais relevantes da MB operam com sistemas satelitais geoestacionários nas bandas “X” e “Ku”.

A seguir, são apresentadas as principais ameaças associadas à operação de sistemas satelitais geoestacionários (GEO):

¹ MPLS (Multiprotocol Label Switching) é uma técnica de encaminhamento de dados que utiliza rótulos (labels), em vez de endereços IP, para direcionar pacotes de forma mais rápida e eficiente através de redes complexas, com suporte a múltiplos protocolos e garantia de qualidade de serviço (QoS).

a) **Interceptação:** consiste na captura não autorizada de sinais de comunicação, seja por meio de técnicas passivas (como a recepção via antenas direcionais), seja por métodos mais sofisticados, que envolvem engenharia reversa ou análise de tráfego. No caso dos sistemas GEO, cuja operação se dá em bandas específicas, como a Banda X, por exemplo, a interceptação pode ocorrer por meio de:

- Captação de sinais de *downlink* (emitidos do satélite para as estações terrestres), caso não estejam adequadamente criptografados;
- Ausência de encriptação de ponta a ponta, permitindo que agentes hostis analisem o tráfego, mesmo sem decodificá-lo imediatamente; e
- Emprego de equipamentos adversários, comerciais ou militares, capazes de captar e decodificar sinais de comunicações via satélite (*SATCOM*).

A mitigação desse tipo de ameaça exige a aplicação rigorosa de protocolos criptográficos de Estado, autenticação mútua entre os terminais e a adoção de tecnologias anti-interceptação (BRASIL, 2015; RAMELLA, 2021).

b) **Bloqueio (*Jamming*):** refere-se à emissão deliberada de sinais interferentes com o objetivo de degradar ou interromper os enlaces de comunicação entre os terminais terrestres e o satélite geoestacionário. As formas mais comuns incluem:

- *Jamming* em *uplink*: direcionado ao satélite, impede a recepção de sinais oriundos das estações terrestres;
- *Jamming* em *downlink*: voltado às estações receptoras (terminais terrestres) em solo, gera interferência que suprime ou mascara a comunicação proveniente do satélite; e
- *Spoofing*: emissão de sinais falsos que imitam os legítimos, com o intuito de confundir os sistemas receptores.

Essas ações são típicas de cenários de guerra eletrônica e têm sido amplamente documentadas em conflitos recentes, como na Ucrânia (STEVENSON, 2014; NCSC, 2022).

c) Ataques cibernéticos: satélites geoestacionários, como o SGDC, não menos suscetíveis a ataques cibernéticos diretos, uma vez que operam com *firmware*² embarcado e isolado. No entanto, o segmento terrestre — composto por estações de controle, redes de apoio e terminais conectados à internet — constitui o principal ponto de vulnerabilidade. Os ataques cibernéticos podem envolver:

- Comprometimento das estações de controle, com alteração de comandos, desativação de enlaces ou desvio de tráfego;
- Acesso não autorizado às redes administrativas da Força, com consequente vazamento de informações sensíveis;
- Inserção de *malware*³ e/ou *backdoors*⁴ nos sistemas de gestão de enlaces ou nos equipamentos terminais; e
- Ataques distribuídos de negação de serviço (DDoS), afetando a disponibilidade dos serviços associados.

Sem a adoção de políticas robustas de segurança cibernética, segmentação lógica de redes, atualização contínua de sistemas e autenticação multifatorial, a crescente dependência de softwares integrados e sua interligação com redes convencionais expõem significativamente as infraestruturas de acesso aos sistemas satelitais geoestacionários (GEO) a riscos cibernéticos relevantes (MILLER, 2020; US-SC, 2024).

² *Firmware*: programa de baixo nível incorporado em memória não volátil de dispositivos eletrônicos, responsável por controlar suas funções básicas de operação e permitir a comunicação entre o hardware e camadas superiores de software.

³ *Malware*: termo derivado de “*malicious software*”, refere-se a qualquer programa ou código desenvolvido com o objetivo de comprometer a integridade, a confidencialidade ou a disponibilidade de sistemas e dados.

⁴ *Backdoor*: recurso ou código inserido em sistemas ou aplicações que permite o acesso remoto e não autorizado, contornando mecanismos legítimos de autenticação, frequentemente utilizado para espionagem ou controle persistente de dispositivos comprometidos.

d) Armas antissatélites (ASAT): constituem uma das ameaças mais críticas à continuidade operacional dos satélites geoestacionários. Esses armamentos podem ser classificados em:

- Cinéticos: mísseis lançados a partir da superfície ou de aeronaves, com capacidade de interceptar fisicamente o satélite, como evidenciado no teste chinês de 2007 (BBC, 2007);
- Não cinéticos: feixes de laser ou micro-ondas de alta energia, capazes de danificar sensores ou sistemas ópticos, sem contato físico direto (DoD, 2020); e
- Cibernéticos: ações que comprometem os sistemas de controle e navegação do satélite, por meio de invasão às redes da estação terrena controladora (US-SC, 2024).

A destruição ou neutralização de um satélite geoestacionário representa um risco estratégico, com potencial de interromper por tempo indeterminado o fluxo de informações sensíveis. Ademais, os detritos espaciais gerados podem comprometer a operação de outros sistemas orbitais. A mitigação dessa ameaça pode ser realizada pelo emprego de constelações satelitais redundantes, estratégias de reposição rápida — inclusive com satélites de órbita baixa (LEO) — e o desenvolvimento de capacidades nacionais para resposta autônoma a incidentes no Domínio Espacial.

2.6 REQUISITOS FUNDAMENTAIS

Para que a infraestrutura de comunicações destinada ao suporte dos sistemas de C^2 , no âmbito do SisNC², seja robusta e eficaz, é necessário que seus componentes atendam a requisitos técnicos e operacionais rigorosos, de modo a garantir disponibilidade, integridade, confidencialidade e continuidade operacional. A seguir, apresentam-se alguns requisitos de interesse selecionados pelo autor:

- a) Redundância multinível: a arquitetura de comunicações deve assegurar continuidade operacional por meio de múltiplos enlaces — satelitais (GEO

e LEO), terrestres (fibra óptica e micro-ondas) e rádio (HF, VHF, UHF, WBHF) —, mitigando riscos de interrupção por ataque ou falha técnica (STEVENSON, 2014);

- b) Interoperabilidade: é essencial a adoção de protocolos compatíveis com padrões internacionais (como STANAG 5066, STANAG 4539 e MIL-STD-188-110), de modo a favorecer operações conjuntas e multinacionais, com redes flexíveis e interoperáveis entre os diversos sistemas de Defesa;
- c) Baixa latência e alta disponibilidade: para garantir o suporte ao ciclo de decisão e resposta em tempo real, especialmente em ambientes operacionais dinâmicos, a infraestrutura deve apresentar latência reduzida e alta disponibilidade (US-SC, 2024);
- d) Resiliência a ambientes contestados: a infraestrutura deve operar sob condições de negação de acesso e guerra eletrônica, por meio de modulações adaptativas, uso de enlaces com espectro disperso e protocolos autoconfiguráveis (STEVENSON, 2014; NCSC, 2022);
- e) Cibersegurança: a proteção das comunicações deve ser assegurada por criptografia ponta a ponta, autenticação multifator, monitoramento contínuo de ameaças, segmentação de redes e políticas rigorosas de atualização e controle de acesso (BRASIL, 2015; MILLER, 2020; US-SC, 2024);
- f) Capacidade de operação em movimento (*on-the-move*): os terminais móveis — embarcados, aerotransportados ou terrestres — devem manter conectividade contínua, inclusive em deslocamento;
- g) Gestão de redes com consciência situacional: as redes devem possibilitar visualização em tempo real, roteamento automático, monitoramento da integridade dos enlaces e priorização dinâmica de tráfego, assegurando a manutenção do comando mesmo em situações de contingência;
- h) Integração com sensores e efetores: a infraestrutura deve ser capaz de transportar dados de sensores (radar, sonar, SIGINT, entre outros) e comandos para sistemas de armas, de modo a sustentar o ciclo OODA (Observar-Orientar-Decidir-Agir); e
- i) Portabilidade e modularidade: a adoção de sistemas transportáveis e escaláveis possibilita rápida instalação em zonas temporárias de operação ou em ambientes hostis, conferindo maior flexibilidade.

2.7 CONCLUSÕES PARCIAIS

A análise da infraestrutura de Comando e Controle (C²) na Marinha do Brasil (MB) revelou um cenário caracterizado por avanços relevantes, mas também por desafios estruturais e operacionais significativos, especialmente no que se refere à segurança, resiliência e continuidade das comunicações em ambientes contestados e de negação de acesso. Constatou-se, ainda, a existência de lacunas doutrinárias e organizacionais no tratamento do C² nos níveis superiores ao tático, parcialmente supridas pela Doutrina Militar de Comando e Controle do Ministério da Defesa.

A espinha dorsal das comunicações que sustentam o Sistema Naval de Comando e Controle (SisNC²) está centrada no Sistema de Comunicações Militares por Satélite (SISCOMIS), cuja infraestrutura, composta pelos segmentos espacial e terrestre, garante o fluxo vertical de informações entre os níveis tático, operacional e estratégico. A integração desse sistema com a RECIM e a ROD assegura a interoperabilidade entre os Centros de Comando e Controle (CC²), ampliando as capacidades operacionais e o alcance informacional da Força.

Entretanto, a forte dependência do segmento espacial do SISCOMIS para assegurar esse fluxo de informações representa um ponto crítico de vulnerabilidade, configurando o Problema Central desta pesquisa. Essa dependência compromete a resiliência da infraestrutura de comunicações, tornando-a suscetível a interferências eletrônicas, ataques cibernéticos e armas antissatélite (ASAT), que são ameaças cada vez mais recorrentes em conflitos contemporâneos.

A relevância dessa questão é reforçada por casos documentados de comprometimento de infraestruturas de comunicação consideradas seguras, como evidenciado por Miller (2020) ao revelar a atuação clandestina da CIA e da BND no uso de equipamentos da Crypto AG, o que reforça a importância da independência tecnológica e da transparência criptográfica nos sistemas de defesa nacionais.

Dessa forma, esta pesquisa definiu como Objeto de Estudo a avaliação e proposição de infraestruturas de comunicações capazes de complementar ou substituir temporariamente o SISCOMIS em situações de degradação ou negação de acesso ao ambiente espacial, garantindo assim a resiliência, a soberania e a continuidade da infraestrutura de comunicações para de C² no âmbito da MB.

É, portanto, imprescindível a busca por alternativas contingentes, ainda que parciais à atual infraestrutura, que possibilitem à MB preservar sua capacidade de C²

mesmo em ambientes com antiacesso e negação de área⁵ ou avaria satelital. Nos capítulos seguintes, analisar-se-ão alternativas tecnológicas, incluindo os sistemas satelitais de baixa órbita (LEO) e as comunicações em alta frequência, tanto em banda larga (WBHF) quanto em banda estreita (NBHF), com o objetivo de identificar caminhos viáveis para o fortalecimento da resiliência e da soberania tecnológica da Marinha do Brasil no âmbito do SisNC², diante de cenários operacionais cada vez mais desafiadores.

⁵ Ambientes com antiacesso e negação de área (Anti-Access/Area Denial - A2AD) se caracterizam por áreas de operações militares onde as forças hostis buscam negar o acesso e as condições de operação às forças aliadas, fazendo uso de bloqueios eletrônicos, mísseis de longo alcance, interferência em comunicações e ações antissatélites.

3 SISTEMAS SATELITAIS DE BAIXA ÓRBITA (LEO)

Neste capítulo, tem-se como objetivo identificar e apresentar os Sistemas de Comunicações Satelitais de Baixa Órbita (*Low Earth Orbit* – LEO) frente às ameaças de interceptação, bloqueio, ataques cibernéticos e armas antissatélites (NCSC, 2022; STEVENS, 2014). Ao evidenciar sua resiliência diante dessas ameaças contemporâneas, os sistemas LEO são avaliados como alternativas estratégicas à crescente vulnerabilidade dos sistemas espaciais geoestacionários em ambientes contestados.

As crescentes ameaças à infraestrutura espacial, baseada em satélites geoestacionários, representadas por armas antissatélite (ASAT), ataques cibernéticos e interferências eletromagnéticas intencionais, tem impulsionado a busca por alternativas mais resilientes de comunicação (BBC, 2007; NCSC, 2022; STEVENS, 2014).

Nesse contexto, os sistemas LEO despontam como uma alternativa viável e promissora para os sistemas C2, especialmente em ambientes caracterizados por A2AD, nos quais há intensa disputa pelo espectro eletromagnético (STEVENS, 2014). Com latência reduzida, elevada taxa de atualização de cobertura e capacidade para conexões persistentes, as constelações LEO oferecem redundância estratégica às redes geossíncronas e terrestres (KRATOS DEFENSE, 2022).

3.1 CONCEITOS BÁSICOS DE SISTEMAS LEO

Os satélites de órbita baixa operam em órbitas compreendidas entre aproximadamente 500 km e 2.000 km. Devido a essa proximidade, completam uma órbita completa em períodos de 90 a 120 minutos, o que possibilita alta taxa de revisitação sobre determinadas regiões e reduz significativamente a latência nas comunicações, alcançando valores inferiores a 50 milissegundos (TELARUS, 2024).

Segundo Al-Hraishawi et al. (2021), uma das principais vantagens operacionais dos satélites LEO, em comparação com os sistemas GEO, reside na menor distância de propagação dos sinais, o que viabiliza o uso de terminais de comunicação mais leves, compactos e de baixa potência. Essa característica é especialmente vantajosa para plataformas móveis — como navios, veículos terrestres e aeronaves — que podem manter comunicações contínuas sem a necessidade de antenas com plataformas estabilizadas.

A altitude reduzida das órbitas dos satélites LEO favorece o acesso direto entre terminais e satélites, possibilitando comunicações persistentes com menor latência e maior confiabilidade. Para tanto, os terminais modernos empregam sistemas de rastreamento automático, capazes de alinhar dinamicamente o feixe de transmissão ao movimento orbital do satélite. Muitos desses terminais empregam antenas de arranjo em fases (*phased array antennas*), que permitem a formação simultânea de múltiplos feixes e diagrama de radiação adaptativo, eliminando a necessidade de partes móveis e proporcionando menor tempo de aquisição de sinal, bem como maior robustez mecânica de construção, mesmo sob condições ambientais adversas (HE et al., 2021).

Os sistemas LEO atuais baseiam-se no conceito de constelações de satélites, compostas por dezenas, centenas ou milhares de unidades operando de forma sincronizada. Exemplos notáveis incluem os projetos Starlink, OneWeb e Project Kuiper (Amazon), que, por meio da interligação entre satélites da mesma rede, têm demonstrado a viabilidade técnica de fornecer cobertura global, persistente e em alta velocidade (US-SC, 2024).

Uma característica operacional relevante dessas constelações é a resiliência estrutural, decorrente do elevado número de satélites em operação. Mesmo que algumas unidades sejam inutilizadas por falhas técnicas, ações hostis ou colisões com detritos espaciais, o sistema permanece funcional graças à redundância orbital e à possibilidade de reposicionamento e reposição rápida por meio de lançamentos em massa com veículos reutilizáveis (CAPELLA et al., 2017).

Tais características tornam os satélites de baixa órbita especialmente atrativos para aplicações em defesa, sobretudo no contexto dos sistemas de C², pois viabilizam comunicações persistentes em tempo quase real, além de facilitar a integração com plataformas operacionais móveis. A capacidade de operar além da linha de visada (*Beyond Line of Sight* – BLOS), combinada à interoperabilidade com redes táticas e ao suporte a protocolos militares — como a norma STANAG 5066 (NATO, 2022) — reforça o papel estratégico das constelações LEO como infraestrutura crítica de apoio a operações militares contemporâneas.

Na Tabela 1, é apresentado um quadro comparativo sumarizando as características técnicas dos Sistemas LEO e GEO.

Tabela 1 – Sistemas LEO (Low Earth Orbit) versus GEO (Geoestacionários)

Características	Satélites LEO	Satélites GEO
Altitude típica	De 500 – 2.000 km	35.786 km
Período orbital	De 90 a 120 minutos	24 horas
Latência	Baixa (20–50 ms)	Alta (500–700 ms)
Cobertura	De local a global	Continental
Nº para cobertura global	De dezenas a milhares	Três
Rastreamento de satélites	Necessário	Desnecessário
Operação Móvel	Alta viabilidade	Plataformas estabilizadas
Custo de Lançamento (UN)	Mais baixo (menores e mais leves)	Alto (grandes e complexos)
Resiliência	Alta (múltiplos satélites)	Baixa (menos unidades)
Susceptibilidade a ASAT	Mais resiliente	Mais vulnerável

Fonte: Elaborado pelo autor.

3.2 ARQUITETURA E PROTOCOLOS

A arquitetura dos sistemas satelitais de baixa órbita (LEO) modernos é caracterizada por constelações densas, compostas por centenas ou milhares de satélites dispostos em planos orbitais sobrepostos, o que assegura cobertura global e alta redundância. Esse modelo arquitetônico permite que múltiplos satélites estejam simultaneamente visíveis a um terminal terrestre, garantindo a continuidade dos enlaces mesmo em caso de falhas ou bloqueios parciais na constelação (TURNER, 2015).

Um dos principais diferenciais técnicos desses sistemas é a presença de enlaces intersatélites, denominados *Inter-Satellite Links* (ISL), geralmente implementados por meio de tecnologia óptica. Esses enlaces possibilitam comunicação direta entre satélites vizinhos, criando uma rede de dados orbital. Dessa forma, é possível interligar, ponto a ponto, terminais terrestres ou unidades móveis, dispensando a intermediação de estações terrenas centrais de controle — o que reduz a latência, aprimora a segurança e aumenta a autonomia operacional do sistema (SPACEX, 2025; SPACENEWS, 2023; KRATOS DEFENSE, 2022).

No que se refere às camadas de rede e transporte, destacam-se protocolos adaptados a ambientes de alta mobilidade e latência variável, como o *Dynamic Link Exchange Protocol* (DLEP). Esse protocolo permite que dispositivos de roteamento

identifiquem, de forma dinâmica, as características dos enlaces disponíveis — como largura de banda, latência e disponibilidade — otimizando a seleção de rotas em tempo real, inclusive em contextos táticos (IETF, 2017). Além disso, interfaces baseadas em IP encapsulado com criptografia, ponto a ponto, são empregadas para assegurar a integridade e a confidencialidade dos dados transmitidos. Essa abordagem viabiliza a integração direta com redes militares que adotam o padrão STANAG 5066, utilizado em redes HF e em soluções de interoperabilidade com infraestruturas legadas de Comando e Controle (NATO, 2017).

Com essa estrutura, as constelações LEO podem atuar como extensões satelitais das redes táticas modernas, oferecendo conectividade persistente mesmo em ambientes degradados ou sob condições de A2AD.

3.3 AMEAÇAS

A seguir, são apresentadas as principais ameaças que podem comprometer a infraestrutura de comunicações de um sistema de C², com foco em suas implicações para os sistemas LEO:

- a) Interceptação: embora as comunicações por satélites LEO possam ser monitoradas por adversários, a criptografia e autenticação dos usuários, juntamente com a constante mobilidade dos satélites, dificultam a realização de interceptações persistentes;
- b) Bloqueio (*Jamming*): a mobilidade orbital das constelações LEO, associada à diversificação de frequências e ao emprego de antenas com conformação de feixes adaptativos, dificulta sobremaneira bloqueios duradouros. Essas características reduzem a eficácia de tentativas de *jamming* e tornam os sistemas LEO notavelmente mais resilientes a esse tipo de ameaça (ANDRADE, 2015);
- c) Ataques Cibernéticos: segundo o *United States Studies Centre* (2024), os satélites têm se tornado alvos recorrentes de ataques cibernéticos, exigindo a implementação de protocolos robustos de autenticação, criptografia, ponto a ponto, e segurança de *firmware* embarcado. Contudo, a arquitetura distribuída dos sistemas LEO, com múltiplas estações terrenas e Pontos de Presença (*Point of Presence* - PoP), confere maior resiliência às suas redes

de dados, quando comparadas aos sistemas geoestacionários (GEO), conforme será detalhado na próxima seção; e

- d) Armas Antissatélites (ASAT): apesar de vulneráveis a ASAT, os satélites LEO, quando organizados em constelações densas, apresentam resiliência estrutural. A elevada quantidade de unidades operacionais dificulta o comprometimento integral da rede, assegurando continuidade funcional por meio de redundância em massa.

3.4 RESILIÊNCIA DOS SISTEMAS LEO

A resiliência dos sistemas satelitais de órbita baixa é uma característica fundamental que os torna especialmente adequados para aplicações críticas de C^2 , sobretudo em ambientes adversos e de alta mobilidade. Essa resiliência decorre de fatores técnicos e topológicos que viabilizam a continuidade operacional, mesmo diante de falhas parciais ou ameaças cibernéticas (ZHAO; ZHU, 2022).

As constelações LEO são compostas por centenas ou milhares de satélites distribuídos em múltiplos planos orbitais. Essa configuração permite que múltiplos satélites estejam simultaneamente visíveis a um terminal terrestre, assegurando a continuidade dos enlaces mesmo diante de bloqueios ou falhas parciais da constelação. Além disso, a presença de numerosas estações terrestres, distribuídas globalmente, contribui para a redundância da malha orbital e para a robustez dos canais de comunicação. Segundo Pan (2024), a constelação Starlink, operada pela SpaceX, contava, em 2024, com aproximadamente 37 Pontos de Presença (PoP) globais, incluindo diversas estações estrategicamente distribuídas para otimizar a latência e a capacidade da rede.

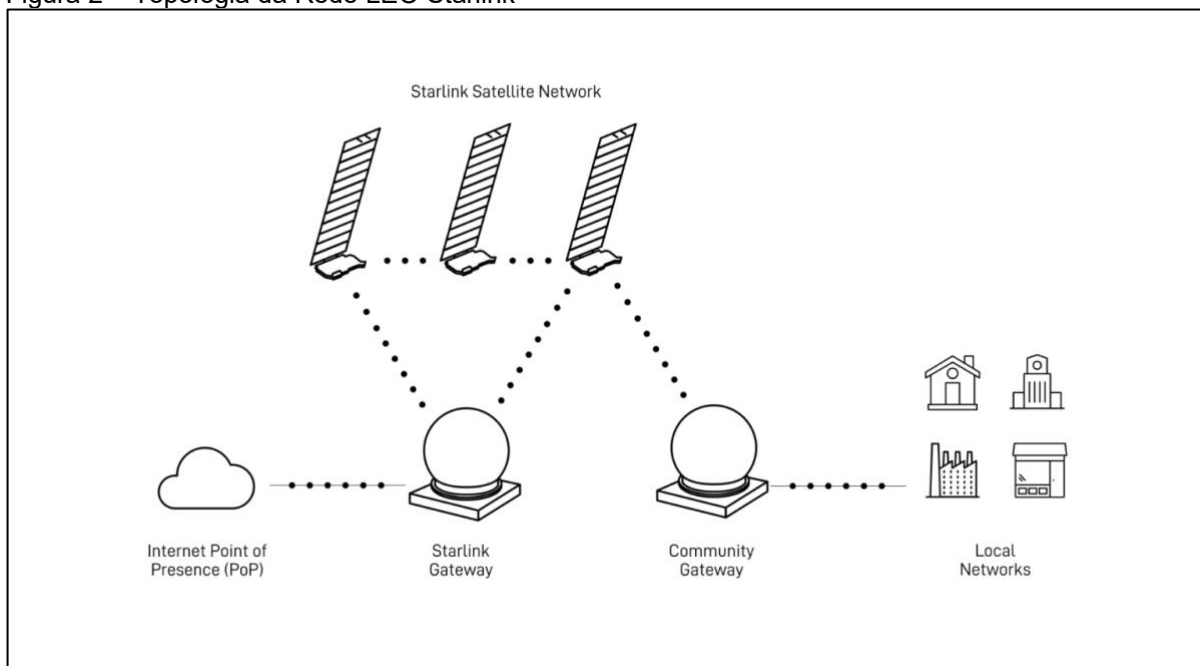
A integração dos sistemas LEO aos sistemas de C^2 pode ocorrer por meio de *gateways* de internet compatíveis com redes táticas e satelitais, viabilizando a interoperabilidade com sistemas GEO, WBHF e NBHF. Essa interoperabilidade permite que as Forças Armadas e outras instituições de Estado mantenham comunicações seguras e contínuas, mesmo em cenários de degradação ou negação de serviço.

Além disso, os sistemas LEO permitem que plataformas móveis — como navios, viaturas terrestres e aeronaves — mantenham conectividade estável por meio de terminais compactos com rastreamento automático. A baixa latência inerente à

órbita LEO, já abordada anteriormente, é essencial para aplicações que demandam resposta em tempo quase real — como sistemas de C², navegação satelital e veículos autônomos (ASSAM; REIS, 2025).

Outro aspecto relevante é a capacidade de segmentação por prioridade de tráfego, viabilizada por arquiteturas de rede inteligente. Essa funcionalidade assegura que comunicações críticas recebam tratamento preferencial, especialmente em situações de congestionamento ou sob ataque cibernético, aumentando a confiabilidade e a eficiência do sistema em condições operacionais extremas (ASSAM; REIS, 2025). Na Figura 2, é apresentada, como exemplo de segmentação e distribuição das estações terrestres, a topologia da rede LEO Starlink.

Figura 2 – Topologia da Rede LEO Starlink



Fonte: PAN (2024).

3.5 CONCLUSÕES PARCIAIS

Para a Marinha do Brasil, os satélites de órbita baixa (LEO) representam não apenas uma oportunidade de modernização, mas também uma estratégia para o fortalecimento da infraestrutura de ambientes marítimos necessária ao SisNC². A ampliação da arquitetura de comunicações para incluir constelações LEO pode reduzir a dependência exclusiva de sistemas GEO, mitigando os riscos associados à degradação, ao bloqueio ou à destruição desses ativos por ameaças cibernéticas ou cinéticas.

A integração dos sistemas LEO ao SISCOMIS, por meio de gateways interoperáveis e terminais navais compatíveis, pode expandir significativamente a capilaridade e a resiliência das redes de C². Tais sistemas oferecem baixa latência, capacidade de operação em plataformas móveis, escalonamento dinâmico de cobertura e priorização de tráfego, o que os torna adequados para atender aos diversos níveis de comando, do estratégico ao tático-operacional.

A arquitetura distribuída das constelações LEO proporciona redundância intrínseca, roteamento dinâmico e continuidade do enlace, mesmo diante da perda de múltiplos satélites ou estações terrestres — características essenciais em cenários contestados.

Apesar das vantagens operacionais, a adoção de sistemas LEO impõe desafios significativos. A implantação de constelações em órbita baixa exige investimentos elevados em lançamentos múltiplos, bem como acesso a tecnologias críticas de construção e manutenção, frequentemente concentradas em empresas e países detentores do *know-how* espacial. Além disso, a necessidade de renovação periódica dos satélites — decorrente da vida útil limitada em órbita baixa — amplia os custos de operação e logística, impactando a sustentabilidade financeira no longo prazo. Para a MB, tais fatores implicam não apenas dependência de parcerias internacionais e de fornecedores estrangeiros, mas também a necessidade de consolidar competências nacionais em integração, manutenção e operação de terminais compatíveis. Esses aspectos configuram obstáculos relevantes à plena autonomia tecnológica e à soberania no emprego de comunicações estratégicas baseadas em constelações LEO.

Por fim, destaca-se a possibilidade de adoção gradual e complementar, em coexistência com redes legadas em HF (NBHF), e sistemas GEO, viabilizando uma transição escalonada em conformidade com os orçamentos disponíveis, as doutrinas em vigor e as necessidades operacionais projetadas. No capítulo seguinte, serão identificados e apresentados identificar e apresentar os Sistemas de Comunicações de Banda Larga em Alta Frequência. No capítulo seguinte, serão identificados e apresentados os Sistemas de Comunicações de Banda Larga em Alta Frequência (WBHF).

4 SISTEMAS DE COMUNICAÇÕES DE BANDA LARGA EM ALTA FREQUÊNCIA

Neste capítulo, tem-se como objetivo identificar e apresentar os Sistemas de Comunicações de Banda Larga em Alta Frequência (*Wideband High Frequency – WBHF*), frente às ameaças de interceptação, bloqueio, ataques cibernéticos e armas antissatélites. Ao evidenciar sua resiliência diante dessas ameaças contemporâneas, os sistemas WBHF são avaliados como alternativas estratégicas à crescente vulnerabilidade dos sistemas espaciais geoestacionários em ambientes contestados.

O avanço das ameaças no ambiente de guerra eletrônica e cibernética tem impulsionado a necessidade de sistemas de comunicação mais resilientes e autônomos. Os WBHF representam uma evolução das comunicações em alta frequência (HF) tradicionais, oferecendo maior largura de banda, maior taxa de transmissão de dados e maior robustez frente a interferências.

Neste capítulo, essa tecnologia será analisada quanto ao seu potencial de emprego como infraestrutura de comunicações para os sistemas de C², particularmente em cenários de A2AD, nos quais a continuidade das operações militares depende de meios independentes de satélites ou redes terrestres vulneráveis.

4.1 CONCEITOS BÁSICOS DE SISTEMAS WBHF

Os sistemas WBHF ampliam significativamente as capacidades das comunicações em alta frequência (HF) tradicionais, permitindo atingir taxas de transferência de dados superiores a 120 kbps, por meio do uso de modulações e codificações digitais avançadas (DoD, 2012). Em determinadas condições operacionais, essas taxas podem alcançar até 240 kbps, conforme especificado na norma MIL-STD-188-110D (DoD, 2017a). Esse desempenho é viabilizado por modulações como 256-QAM e por técnicas robustas de codificação de canal, com o uso de códigos de correção de erro (*Forward Error Correction – FEC*). O *interleaving* — técnica que reorganiza os bits transmitidos para dispersar possíveis erros e facilitar sua correção —, aliado à detecção adaptativa da qualidade do canal e ao uso de protocolos de retransmissão automática (*Automatic Repeat Request – ARQ*), contribui para o aumento da confiabilidade do enlace. A norma STANAG 4539 estabelece o emprego de múltiplos esquemas de modulação, que se adaptam

dinamicamente à qualidade do canal e aos níveis de degradação, conforme as características do ambiente de propagação (NATO, 2017).

Segundo Stevens *et al.* (2014), o WBHF, ao contrário dos sistemas GEO, opera de forma autônoma e com alcance global, independente de infraestrutura de redes físicas, permitindo a comunicação mesmo em áreas remotas ou degradadas. Além disso, os sistemas WBHF demonstram maior imunidade a bloqueios e interferências eletromagnéticas, devido às características inerentes à propagação em HF — como a reflexão ionosférica e o amplo espectro de frequências disponíveis —, dificultando a obstrução completa do sinal.

4.2 ARQUITETURA E PROTOCOLOS

Na Figura 3, é apresentada uma tabela baseada nos parâmetros da norma MIL-STD-188-110D, relacionando as taxas de transmissão de dados com a razão sinal-ruído mínima (*Signal-to-Noise Ratio* – SNR) exigida para garantir comunicações confiáveis em canais de alta frequência (HF) (MOTTA, 2021).

Figura 3 – Taxas de dados (bps) versus largura de banda, de acordo com a MIL-STD-188-110D

Wave Form ID	Min SNR	3 kHz	6 kHz	9 kHz	12 kHz	15 kHz	18 kHz	21 kHz	24 kHz	30 kHz	36 kHz	42 kHz	48 kHz
Walsh	-8	75	150	300	300	300	600	300	600	600	1,200	1,200	1,200
2PSK	0	150	300	600	600	600	1,200	600	1,200	1,200	2,400	2,400	2,400
2PSK	2	300	600	1,200	1,200	1,200	2,400	1,200	2,400	2,400	4,800	4,800	4,800
2PSK	5	600	1,200	2,400	2,400	2,400	4,800	2,400	4,800	4,800	9,600	9,600	9,600
2PSK	7	1,200	2,400	-	4,800	4,800	-	4,800	9,600	9,600	12,800	14,400	16,000
2PSK	8	1,600	3,200	4,800	6,400	8,000	9,600	9,600	12,800	16,000	19,200	19,200	24,000
4PSK(a)	9	2,400	-	-	-	-	-	-	-	-	-	-	-
4PSK(b)	11	3,200	6,400	9,600	12,800	16,000	19,200	19,200	25,600	32,000	38,400	38,400	48,000
8PSK	14	4,800	9,600	14,400	19,200	24,000	28,800	28,800	38,400	48,000	57,600	57,600	72,000
16QAM	17	6,400	12,800	19,200	25,600	32,000	38,400	38,400	51,200	64,000	76,800	76,800	96,000
32QAM	20	8,000	16,000	24,000	32,000	40,000	48,000	48,000	64,000	80,000	96,000	96,000	120,000
64QAM(1)	23	9,600	19,200	28,800	38,400	48,000	57,600	57,600	76,800	96,000	115,200	115,200	144,000
64QAM(2)	25	12,000	24,000	36,000	48,000	57,600	72,000	76,800	96,000	120,000	144,000	160,000	192,000
256QAM	28	16,000	32,000	48,000	64,000	76,800	90,000	115,200	120,000	160,000	192,000	192,000	240,000

Fonte: MOTTA (2021).

Os valores indicados representam estimativas com base em condições ideais de canal e podem variar conforme o uso de técnicas de correção de erro (*Forward Error Correction* – FEC), *interleaving* e diversidade de recepção. De modo geral, quanto maior a taxa de dados desejada, maior será a exigência de qualidade do canal, refletida pela SNR. As especificações técnicas do WBHF são definidas por documentos como os STANAG 5066 e 5070 da OTAN, que estabelecem padrões de

interoperabilidade para comunicações em HF (NATO, 2022; NATO, 2013). A norma STANAG 5066, por exemplo, define a camada de enlace para redes de dados em HF, assegurando a entrega ordenada e confiável dos pacotes. A norma MIL-STD-188-110 -C/D estabelece os parâmetros de desempenho para MODEM de dados, incluindo os modos WBHF com altas taxas de transmissão, enquanto o STANAG 4539 trata da estrutura de modulação e codificação voltada à operação eficiente em ambientes ruidosos e sob interferência (DoD, 2012; DoD, 2017a; NATO, 2017).

Os requisitos definidos nas normas MIL-STD-188-110D e STANAG 4539 contemplam também as taxas de transmissão utilizadas pelos padrões legados, o que permite aos sistemas WBHF manterem interoperabilidade plena com os Sistemas de Comunicações de Banda Estreita em Alta Frequência (*Narrowband High Frequency* – NBHF).

4.3 AMEAÇAS

A seguir, são apresentadas as principais ameaças que podem comprometer infraestruturas de comunicações de um sistema de C², com foco nas particularidades dos sistemas de Comunicações de Banda Larga em Alta Frequência (WBHF):

- a) Interceptação: técnicas de escuta e decodificação representam riscos à segurança operacional. No entanto, os sistemas WBHF podem empregar criptografia robusta, que, embora possa ser interceptada, impede a decodificação do conteúdo transmitido. Adicionalmente, a variabilidade dos parâmetros de modulação e codificação dificulta a interceptação sistemática por parte de agentes adversários;
- b) Bloqueio (*Jamming*): a emissão deliberada de sinais interferentes por forças hostis visa comprometer os enlaces de comunicação. Os sistemas WBHF empregam técnicas de detecção adaptativa e ajuste dinâmico da largura de banda para mitigar tais efeitos. A própria natureza da propagação em HF — com base na reflexão ionosférica — confere maior resistência ao bloqueio, pois nem sempre é possível estabelecer um enlace entre dois pontos distantes utilizando a mesma frequência, em um mesmo instante. Além disso, as redes WBHF podem operar com estações remotas,

permitindo o uso de diversidade espacial, que se mostra virtualmente imune ao *jamming* (STEVENS, 2014);

- c) Ataques Cibernéticos: devido à baixa dependência de redes de dados externas, os sistemas WBHF apresentam uma superfície de contato com a dimensão cibernética reduzida. Exigem, portanto, apenas a proteção local de hardware, o que os torna intrinsecamente mais resilientes a ataques cibernéticos em comparação a sistemas baseados em redes de dados convencionais; e
- d) Armas Antissatélites: os sistemas WBHF são imunes a ataques antissatélites, uma vez que não dependem de ativos em órbita. Sua operação totalmente autônoma os torna estratégicos em cenários contestados, especialmente quando há comprometimento ou negação de acesso ao Domínio Espacial.

4.4 RESILIÊNCIA DOS SISTEMAS WBHF

Os sistemas de Comunicações de Banda Larga em Alta Frequência (WBHF) utilizam técnicas como criptografia, saltos de frequência e protocolos de correção de erros para manter a integridade e a confidencialidade dos dados. Em ambientes de antiacesso e negação de área (A2AD), sua capacidade de operar de forma autônoma, sem depender de infraestrutura externa, torna-os ideais para comunicações persistentes e seguras (STEVENS, 2014).

Adicionalmente, o emprego da tecnologia ALE⁶ (*Automatic Link Establishment*) facilita significativamente a seleção automática de canais e frequências com melhor qualidade de enlace, reduzindo o tempo de estabelecimento da comunicação e aumentando a disponibilidade operacional. A terceira geração dessa tecnologia (ALE 3G), padronizada pelas normas STANAG 4538 e MIL-STD-188-141B, permite o gerenciamento de redes complexas, com troca automatizada de mensagens, verificação de integridade, troncalização de canais e manutenção de múltiplos enlaces (NATO, 2007; DoD, 1999).

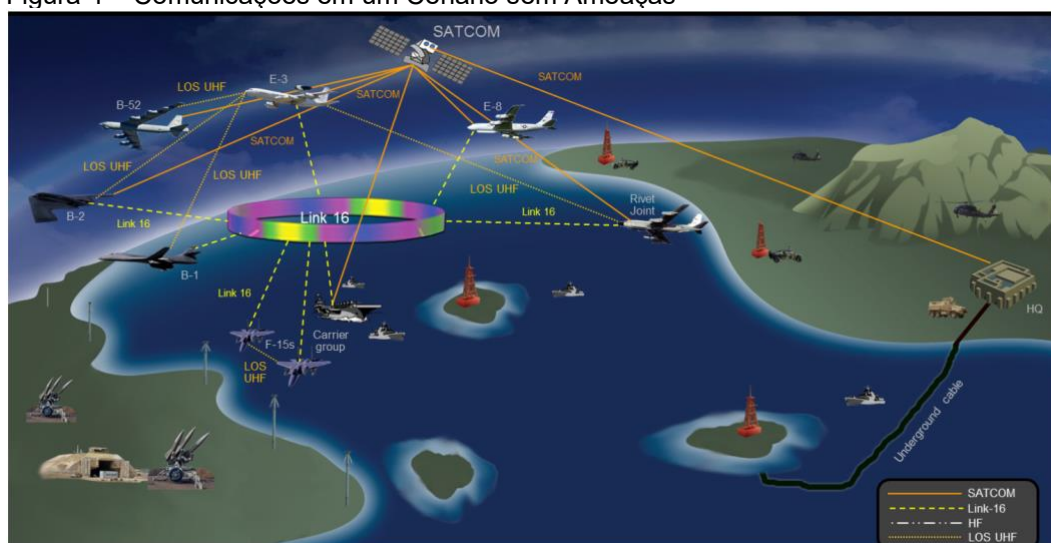
⁶ ALE – *Automatic Link Establishment*, tecnologia que automatiza a escolha da melhor frequência de comunicação em HF.

A quarta geração (ALE 4G), conforme descrita na MIL-STD-188-141D, representa um avanço significativo, ao incorporar funcionalidades como varredura de espectro, negociação dinâmica de largura de banda e suporte a enlaces assimétricos, operando com taxas de sinalização de até 900 bps. Nos sistemas WBHF, o ALE 4G prioriza a formação de enlaces e assegura maior robustez em canais degradados, tolerando SNR negativos, altos níveis de dispersão e atrasos prolongados — fatores críticos em cenários de guerra eletrônica e ambientes de alta mobilidade. A varredura síncrona ou assíncrona, aliada à compatibilidade reversa com versões anteriores, torna o ALE 4G uma tecnologia essencial para operações no nível tático (NATO, 2017b).

A robustez dos sistemas WBHF foi comprovada em testes operacionais conduzidos com aeronaves militares. Segundo Stevens et al. (2014), foi possível transmitir vídeo em tempo real por enlaces WBHF, evidenciando sua viabilidade para aplicações de alta largura de banda em ambientes dinâmicos e sujeitos a interferências.

As Figuras Figura 4, Figura 5 e Figura 6 ilustram três condições distintas de comunicação em um Sistema de Comando e Controle: (i) operação em cenário sem ameaças, (ii) perda de comunicações em ambiente A2AD e (iii) restabelecimento contingencial por meio do emprego de sistemas WBHF.

Figura 4 – Comunicações em um Cenário sem Ameaças



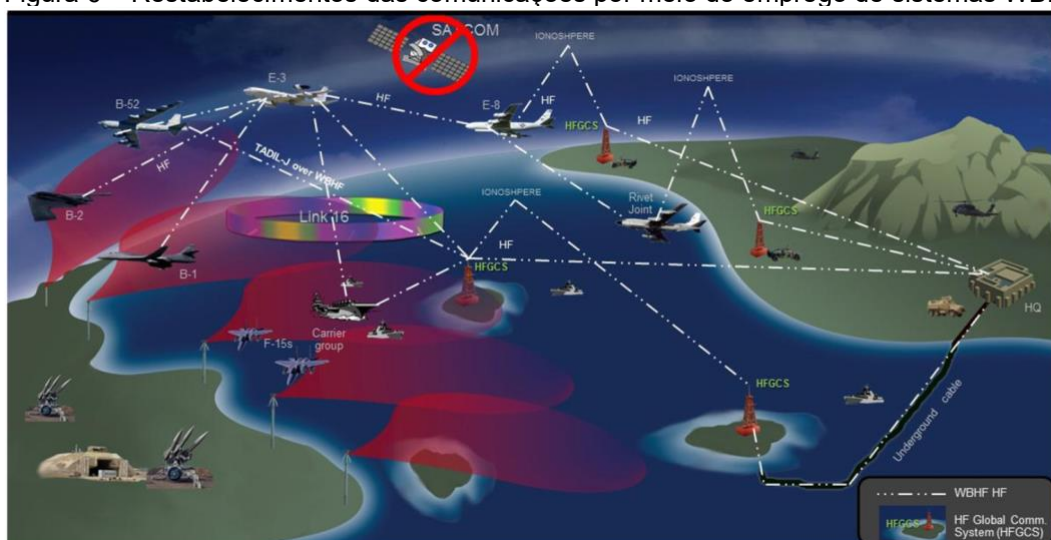
Fonte: STEVENS (2014).

Figura 5 – Perda de comunicações em um ambiente A2AD



Fonte: STEVENS (2014).

Figura 6 – Restabelecimentos das comunicações por meio do emprego de sistemas WBHF



Fonte: STEVENS (2014).

4.5 CONCLUSÕES PARCIAIS

O ataque cibernético à rede da ViaSat (NCSC, 2022), ocorrido poucas horas antes da invasão russa à Ucrânia, exemplifica os riscos concretos de paralisação estratégica de meios de comunicação em um conflito, com efeitos danosos às capacidades de C² de um país. Tal evento reforça a importância de estruturas alternativas e contingenciais aos sistemas GEO.

Os experimentos descritos por Stevens et al. (2014), envolvendo a transmissão de vídeo via WBHF a partir de plataformas aéreas, demonstram sua aplicabilidade em

missões táticas e de reconhecimento. A tecnologia permite operar além da linha de visada (*Beyond Line of Sight* – BLOS), sem dependência de enlaces satelitais, viabilizando o fluxo de informações entre os níveis tático, operacional e estratégico. Os testes indicaram taxas de dados compatíveis com aplicações de alta exigência, mesmo sob condições adversas de propagação atmosférica e em cenários com elevada mobilidade.

Adicionalmente, estudos revelam que redes baseadas em WBHF mantêm enlaces estáveis mesmo sob simulações de guerra eletrônica intensa, envolvendo o bloqueio deliberado de comunicações via sistemas GEO e a degradação proposital de sinais GPS. Nessas condições, os sistemas WBHF demonstraram ser essenciais para assegurar comunicações críticas de apoio aos sistemas de C² (STEVENSON, 2014).

Por apresentarem limitações de banda e dependerem das condições estatísticas da propagação ionosférica, os sistemas WBHF não se propõem a substituir integralmente os modernos sistemas GEO. Contudo, representam uma camada estratégica adicional de segurança, com elevada resiliência frente a ataques e ambientes contestados, consolidando-se como componente fundamental da arquitetura de contingência em sistemas de comunicações militares.

Diante do atual cenário geopolítico instável e das ameaças crescentes nos domínios Cibernético e Espacial (BRASIL, 2025), os sistemas WBHF, como recursos contingenciais às comunicações satelitais, constituem uma alternativa viável e eficaz. Sua integração em arquiteturas híbridas, autônomas e resilientes reforça a segurança das infraestruturas de informação que sustentam os sistemas de C². No capítulo seguinte, serão identificados e apresentados os Sistemas de Comunicações de Banda Estreita em Alta Frequência (NBHF).

5 SISTEMAS DE COMUNICAÇÕES DE BANDA ESTREITA EM ALTA FREQUÊNCIA

Neste capítulo, tem-se por objetivo identificar e apresentar os Sistemas de Comunicações de Banda Estreita em Alta Frequência, *Narrowband High Frequency* (NBHF), no contexto das ameaças contemporâneas, como interceptação, bloqueio, ataques cibernéticos e o emprego de armas antissatélites. Evidenciando sua resiliência frente a essas ameaças modernas, os sistemas NBHF são avaliados como alternativas estratégicas diante da crescente vulnerabilidade dos sistemas espaciais geoestacionários em ambientes contestados.

Os atuais sistemas de comunicações NBHF representam um avanço tecnológico em relação às comunicações analógicas HF tradicionais. Mantêm-se as características de banda estreita (tipicamente 3 kHz), mas com a adoção de técnicas digitais avançadas de modulação e codificação, otimizadas para ampliar a eficiência espectral e a robustez operacional. Essa evolução tecnológica responde à crescente necessidade de sistemas de comunicação resilientes em ambientes A2AD, marcados por restrições severas ao uso do espectro eletromagnético (STEVENS, 2014).

Nesse contexto, os sistemas NBHF despontam como alternativa relevante frente à vulnerabilidade cada vez maior das redes satelitais, sujeitas a ataques cibernéticos, interferências eletromagnéticas e ASAT.

5.1 CONCEITOS BÁSICOS DE SISTEMAS NBHF

Os sistemas NBHF empregam canais com largura de banda padrão de 3 kHz, cuja otimização ocorre por meio de modulações e codificações digitais aplicadas à banda base (canal de áudio), com o objetivo de alcançar taxas de dados superiores. O uso de canais de 3 kHz garante compatibilidade com a infraestrutura existente composta por transceptores legados, sendo este um dos principais diferenciais da tecnologia NBHF.

Seu desempenho foi aprimorado por meio da combinação de técnicas modernas de modulação digital, com adoção de formas de onda adaptativas, que se ajustam de acordo com a qualidade do canal. Entre as modulações utilizadas destacam-se BPSK, QPSK, 8-PSK e 16-QAM, associadas a codificações robustas de correção de erros, como FEC concatenada (*Viterbi + Reed-Solomon*), Turbo Codes ou LDPC (*Low-Density Parity-Check*) (LIN; COSTELLO, 2004).

Adicionalmente, os sistemas NBHF podem fazer uso da técnica ISB (*Independent Sideband*), que permite a transmissão simultânea de fluxos independentes nas bandas laterais superior e inferior. Essa técnica viabiliza o uso de dois canais de 3 kHz, dobrando assim a capacidade de transmissão de dados, desde que os transceptores utilizados suportem tal operação e que, na recepção, existam filtros adequados para a separação desses sinais (NATO, 2017).

5.2 ARQUITETURA E PROTOCOLOS

A Tabela 2 apresenta os parâmetros definidos pela norma MIL-STD-188-110C, que estabelece a relação entre a taxa de transmissão de dados e a razão sinal-ruído mínima (SNR) necessária para assegurar uma comunicação confiável em canais HF de banda estreita (NBHF). Essa norma, adotada pelo Departamento de Defesa dos Estados Unidos (DoD, 2012) e referenciada por alianças como a OTAN (NATO, 2017), fornece especificações técnicas fundamentais para o dimensionamento de sistemas de comunicações militares, especialmente em ambientes marcados por severas restrições espectrais, alta variabilidade nas condições de propagação e suscetibilidade a interferências, sejam naturais ou deliberadas.

Tabela 2 – Formas de Onda Típicas para um Canal de Banda Estreita

Modulação	Codificação de Canal (FEC)	Banda	Taxa (bps)	SNR
BPSK	Viterbi + Reed-Solomon	3 kHz	75 – 600	≥ 0 dB
QPSK	Concatenada ou Turbo-Codes	3 kHz	600 – 2400	≥ 3 dB
8-PSK	Turbo ou LDPC	3 kHz	2400 – 3200	≥ 8 dB
16-QAM	LDPC / Turbo Codes	3 kHz	3200 – 4800	≥ 12 dB
QPSK+QPSK	Concatenada (dois fluxos)	6 kHz	Até 4800	≥ 10 dB

Fonte: Adaptado de MIL-STD-188-110C; NATO STANAG 4539 Appendix H (DoD, 2012; NATO, 2017).

Os parâmetros apresentados abrangem diferentes esquemas de modulação e codificação, detalhando as condições mínimas necessárias para garantir desempenho adequado em cenários operacionais típicos. Essas informações são essenciais para o planejamento de enlaces que utilizam sistemas NBHF, permitindo a avaliação da robustez, da eficiência espectral e da resiliência das comunicações (NATO, 2022).

5.3 AMEAÇAS

A seguir, apresentam-se as principais ameaças que podem comprometer a infraestrutura de comunicações de um sistema de C2 e sua relação com os sistemas NBHF:

- a) Interceptação: os sistemas NBHF podem empregar técnicas de criptografia robusta que, embora passíveis de interceptação, não permitem a decodificação do conteúdo transmitido. Ademais, as grandes distâncias envolvidas e a variabilidade das condições de propagação entre diferentes pontos dificultam a interceptação eficaz, especialmente quando a estação receptora se encontra em uma posição com propagação desfavorável;
- b) Bloqueio (*Jamming*): devido à variabilidade espacial e temporal das condições de propagação em HF, os sistemas NBHF apresentam elevada resiliência a bloqueios intencionais. A impossibilidade de replicar as condições de propagação em locais distintos dificulta a efetividade de ataques por *jamming*;
- c) Ataques Cibernéticos: devido à baixa dependência de redes de dados externas, os sistemas NBHF apresentam uma superfície de contato com a dimensão cibernética reduzida. Exigem, portanto, apenas a proteção local de hardware, o que os torna intrinsecamente mais resilientes a ataques cibernéticos em comparação a sistemas baseados em redes de dados convencionais; e
- d) Armas Antissatélites: os sistemas NBHF são imunes a ataques antissatélites, uma vez que não dependem de ativos em órbita. Sua operação totalmente autônoma os torna estratégicos em cenários contestados, especialmente quando há comprometimento ou negação de acesso ao Domínio Espacial.

5.4 RESILIÊNCIA DOS SISTEMAS NBHF

Os sistemas NBHF são compatíveis com os protocolos ALE 3G, que viabilizam a seleção automática de canais e enlaces com base na qualidade do canal. Além disso, podem ser integrados a sensores e sistemas de combate por meio de links de dados, como o Link 16 e o Link 22, permitindo o escoamento seguro de informações para os sistemas de C² (DoD, 2022; NILE PMO, 2020).

A adoção de sistemas NBHF, como complemento aos SATCOM e/ou WBHF, pode viabilizar comunicações confiáveis e resilientes, especialmente em ambientes A2AD. Sua interoperabilidade com sistemas legados e sua flexibilidade espectral os tornam adequados para operações em cenários contestados.

Destaca-se, ainda, a relevância da nacionalização dos MODEM por meio do desenvolvimento de softwares dedicados, bem como da adoção de criptografia autóctone integrada aos sistemas NBHF. A Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM) desenvolveu, recentemente, o sistema ComSec-DV (Comunicações Seguras por Dados e Voz), o qual pode ser empregado em sistemas legados, de modo a assegurar a transmissão segura de dados e mensagens de voz.

Essas medidas são estratégicas para a consolidação da soberania operacional (BRASIL, 2023a; BRASIL, 2020a), pois fortalecem a autonomia tecnológica nacional, mitigam vulnerabilidades decorrentes da dependência de soluções estrangeiras e ampliam a segurança das comunicações militares.

5.5 CONCLUSÕES PARCIAIS

Em um cenário global caracterizado por disputas pelo espectro eletromagnético, ameaças cibernéticas crescentes e a crescente vulnerabilidade das infraestruturas espaciais, os sistemas de Comunicações de Banda Estreita em Alta Frequência (NBHF) reaparecem como solução tecnológica estratégica complementar. Tais sistemas oferecem a vantagem da reutilização da infraestrutura legada de transceptores, representando não apenas economia de recursos, mas também uma resposta ágil às demandas por resiliência complementar às comunicações militares via satélite.

Embora apresentem taxas de dados mais modestas, quando comparados às comunicações via satélite ou aos sistemas WBHF, os sistemas NBHF se destacam por sua robustez, confiabilidade e adaptabilidade. O uso de formas de onda adaptativas, técnicas modernas de codificação e a possibilidade de operação com modulação ISB (*Independent Sideband*) permitem sua atuação eficaz mesmo em ambientes contestados — marcados por guerra eletrônica, interferências intencionais e ausência de infraestrutura de suporte.

Adicionalmente, sua arquitetura descentralizada e a independência em relação a sistemas espaciais os tornam imunes a ataques antissatélite (ASAT), o que reforça sua relevância em um contexto geopolítico em que o Domínio Espacial se torna cada vez mais disputado.

Outro aspecto de destaque é a baixa exposição ao ciberespaço ao operarem de forma autônoma e com equipamentos dedicados. Essa característica é particularmente crítica em cenários de guerra híbrida, nos quais a proteção e continuidade das comunicações podem ser determinantes para o sucesso das operações. Além disso, por se tratar de sistemas de banda estreita, torna-se viável a adoção de solução criptográfica autóctone já desenvolvida pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), por meio do sistema ComSec-DV (Comunicações Seguras por Dados e Voz), que assegura a transmissão segura de dados e mensagens de voz.

Dessa forma, os sistemas NBHF não apenas complementam as demais soluções de comunicação (como os sistemas GEO, WBHF e LEO), mas também assumem papel estratégico contingente na manutenção da continuidade operacional dos sistemas de C², sobretudo em ambientes degradados, contestados ou imprevisíveis.

No capítulo seguinte, será apresentada e aplicada a Análise Multicritério para a avaliação das quatro alternativas de infraestrutura de comunicações já apresentadas: satélites geoestacionários (GEO), satélites de baixa órbita (LEO), comunicação de alta Frequência de banda larga (WBHF) e comunicação de alta frequência de banda estreita (NBHF).

6 AVALIAÇÃO MULTICRITÉRIO

Neste capítulo, tem-se como objetivo apresentar os fundamentos teóricos da Análise Multicritério, com ênfase na aplicação de uma abordagem híbrida voltada à seleção comparativa entre diferentes alternativas de infraestrutura de comunicações. A proposta metodológica baseia-se na integração dinâmica de três métodos multicritério de decisão — AHP, MACBETH e TOPSIS — considerados métodos complementares com enfoques avaliativos distintos, com o intuito de combinar seus pontos fortes e oferecer uma solução robusta e bem fundamentada.

Nesse contexto, realizou-se uma comparação sistemática entre quatro alternativas de infraestrutura: satélites geoestacionários (GEO), satélites de baixa órbita (LEO), comunicação de alta Frequência de banda larga (WBHF) e comunicação de alta frequência de banda estreita (NBHF). A infraestrutura GEO foi utilizada como referência na análise conjunta com as demais alternativas candidatas a compor soluções de comunicação contingente ao SisNC². A aplicação dos métodos multicritério supracitados considerará sete critérios estratégicos de avaliação previamente definidos, permitindo hierarquizar as alternativas de forma objetiva, transparente e alinhada a requisitos operacionais.

6.1 FUNDAMENTOS DA ABORDAGEM MULTICRITÉRIO HÍBRIDA

Nesta seção são apresentados, de forma conceitual, os três métodos que compõem a análise multicritério híbrida, com destaque para suas principais características:

- a) AHP (*Analytic Hierarchy Process*): é um método de apoio à decisão multicritério que permite decompor um problema complexo em uma estrutura hierárquica, facilitando a avaliação das alternativas com base em critérios múltiplos. A partir de comparações par a par entre os elementos da hierarquia, o método gera matrizes de julgamento que são processadas para a obtenção dos pesos relativos dos critérios e da prioridade das alternativas. Essa abordagem fornece um mecanismo eficaz para capturar as preferências do decisor, assegurando maior clareza e consistência no processo de escolha (SILVA; OLIVEIRA; SOUSA, 2021);

- b) MACBETH (*Measuring Attractiveness by a Categorical Based Evaluation Technique*): é uma abordagem de análise multicritério que se destaca por utilizar exclusivamente julgamentos qualitativos sobre as diferenças de valor entre alternativas, dispensando a necessidade de atribuições numéricas diretas. Essa metodologia tem como objetivo apoiar o decisor — ou um grupo consultivo — na quantificação da atratividade relativa entre as opções disponíveis, com base em comparações verbais como “ligeiramente melhor”, “muito melhor” ou “incomparável”. Essas expressões são convertidas, por meio de um processo interativo e lógico, em uma escala de valor cardinal e intervalar. A escala resultante permite representar numericamente as preferências, preservando a coerência dos julgamentos expressos e facilitando a construção de modelos decisórios consistentes, especialmente úteis quando os decisores não se sentem confortáveis em fornecer estimativas numéricas exatas (BANA E COSTA; DE CORTE; VANSNICK, 2012); e
- c) TOPSIS (*Technique for Order Preference by Similarity to Ideal Solution*): é um método de decisão multicritério que busca identificar a alternativa mais próxima da solução ideal e mais distante da solução anti-ideal. A técnica parte da normalização da matriz de decisão, seguida da ponderação dos critérios e do cálculo das distâncias euclidianas entre cada alternativa e os pontos de referência (ideal e anti-ideal). O índice de similaridade (C_i) é utilizado para classificar as alternativas, indicando aquela com maior grau de preferência. Sua aplicação é valorizada por fornecer uma hierarquização intuitiva e tecnicamente robusta das opções avaliadas (HWANG; YOON, 1981).

Com a integração dos métodos AHP, TOPSIS e MACBETH, busca-se uma abordagem abrangente que aproveita as vantagens específicas de cada um, proporcionando uma solução mais robusta que produz resultados decorrentes de aspectos quantitativos e avaliações subjetivas. Souza et al. (2018) e Morita et al. (2023) desenvolveram uma análise híbrida integrando os métodos AHP e TOPSIS.

A seguir, apresenta-se a sequência lógica que orienta essa integração:

a) AHP – Estruturação do Problema e Definição dos Pesos

- Cada critério C_i e C_j comparado, par a par, segundo a escala de Saaty, gera uma matriz $A = [a_{ij}]$, onde: $a_{ij} = \frac{1}{a_{ji}}$, $a_{ii} = 1$.

Tabela 3 – Escala de Saaty

Avaliação	Valor
Igual importância	1
Importância moderada	3
Importância forte	5
Importância muito forte	7
Importância extrema	9
valores intermediários	2, 4, 6, 8

Fonte: Adaptado de Saaty (2008).

- Construção da Matriz de Comparação par a par: $a_{ij} = \frac{1}{a_{ji}}$, com $a_{ii} = 1$.
- Cálculo do vetor de Pesos Normalizados se dá pela média normalizada das colunas ou pelo autovetor principal da matriz A :

$$w_i = \frac{1}{n} \sum_{j=1}^n \frac{a_{ij}}{\sum_{k=1}^n a_{kj}} \quad (6.1)$$

- Cálculo do Índice de Consistência:

$$IC = \frac{\lambda_{\max} - n}{n - 1} \quad (6.2)$$

Onde $\lambda_{\max}$ é o maior autovalor⁷ da matriz A , n é o número de critérios, e RI é o índice aleatório de Saaty, que pode ser encontrado em Donegan e Dodd (1991).

⁷ O autovalor de uma matriz representa a quantidade pela qual um autovetor é escalado quando a matriz é aplicada a ele. Ou seja, é um número que indica o fator de ampliação ou redução de certos vetores que mantêm sua direção ao serem transformados pela matriz.

- Cálculo da Consistência Relativa:

$$CR = \frac{IC}{RI} \quad (6.3)$$

Se o valor de $CR \leq 0,10$, a matriz é considerada consistentemente aceitável (MU; PEREYRA-ROJAS, 2017, p. 15).

b) MACBETH – Valoração Qualitativa das Alternativas:

- Definição de Alternativas e Critérios, listando as alternativas ($A_1, A_2, \dots, A_n$) e os critérios de avaliação ($C_1, C_2, \dots, C_m$);
- Conversão dos julgamentos verbais em restrições matemáticas via programação linear, realizando comparações pareadas entre alternativas, com uso das categorias: Indiferente, Muito Fraca, Fraca, Moderada, Forte, Muito Forte e Extrema;

Tabela 4 – Exemplo de escala verbal utilizada

Verbal	Valor Cardinal Atribuído
Indiferente	0,0
Muito Fraca	0,2
Fraca	0,4
Moderada	0,5
Forte	0,6
Muito Forte	0,8
Extrema	1,0

Fonte: Adaptado de Bana e Costa & Vansnick (2004).

- Construção da Matriz MACBETH por critério, denominada Matriz de Decisão Ponderada, representando numericamente as intensidades verbais de preferência entre pares de alternativas;

c) Integração AHP + MACBETH

O método AHP é utilizado para atribuir pesos aos critérios com base em julgamentos estruturados e consistentes. O método MACBETH é empregado para

quantificar, de forma qualitativa, o desempenho das alternativas em cada critério. Então a combinação desses métodos resulta em uma matriz de decisão, proveniente do método MACBETH, ponderada pelos pesos produzidos pelo método AHP, que é então empregada como entrada para o método TOPSIS e calculada por meio das equações 6.4 e 6.5.

- Normalização da Matriz de Decisão:

$$r_{ij} = \frac{x_{ij}}{\sqrt{\sum_{i=1}^m x_{ij}^2}} \quad (6.4)$$

- Aplicação dos pesos w_j , vindos do AHP, sobre os elementos normalizados r_{ij} , gerando a Matriz de Decisão Ponderada:

$$v_{ij} = w_j \cdot r_{ij} \quad (6.5)$$

d) TOPSIS – Hierarquização Final das Alternativas

Inicialmente, define-se como Solução Ideal (A^+) a solução formada pelos valores máximos observados na matriz de decisão ponderada e normalizada. Em outras palavras, ela corresponde a uma alternativa idealizada, que reúne simultaneamente o melhor desempenho em todos os critérios considerados.

De mesma forma, Define-se como Solução Anti-Ideal (A^-) a solução formada pelos valores mínimos observados na matriz de decisão ponderada e normalizada. Em outras palavras, ela corresponde a uma alternativa hipotética oposta à ideal, que reúne simultaneamente o pior desempenho em todos os critérios considerados.

- Determinação da Solução Ideal (A^+) e Anti-ideal (A^-):

$$A^+ = \{ \max(v_{ij}) \mid j \in J \} \quad (6.6)$$

$$A^- = \{ \min(v_{ij}) \mid j \in J \} \quad (6.7)$$

- Cálculo das distâncias euclidianas:

$$D_i^+ = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^+)^2} \quad (6.8)$$

$$D_i^- = \sqrt{\sum_{j=1}^n (v_{ij} - v_j^-)^2} \quad (6.9)$$

Onde v_j^+ é o valor ideal do critério j , isto é, o melhor desempenho possível entre todas as alternativas e v_j^- é o valor anti-ideal do critério j , isto é, o pior desempenho possível entre todas as alternativas.

- Cálculo do Índice de Similaridade:

$$C_i = \frac{D_i^-}{D_i^+ + D_i^-} \quad (6.10)$$

Ao final dos cálculos dos valores de mérito no método TOPSIS, a alternativa com maior valor de C_i é considerada a mais próxima da solução ideal. De forma resumida, os pesos dos critérios são atribuídos por meio do método AHP. Em seguida, os desempenhos das alternativas são medidos qualitativamente por meio do método MACBETH. A matriz ponderada resultante é então utilizada como base para a hierarquização final no método TOPSIS.

Segundo Xu et al. (2023), a combinação de métodos subjetivos e objetivos contribui para aumentar a robustez e a imparcialidade das avaliações multicritério. Nesse sentido, a adoção conjunta dos métodos AHP, MACBETH e TOPSIS se justifica por sua capacidade de integrar o rigor quantitativo à flexibilidade qualitativa, promovendo uma análise decisória mais abrangente. Essa integração dos três métodos apresentados constitui uma proposição e iniciativa original deste trabalho, cujo propósito é converter aspectos subjetivos, como os julgamentos de atratividade realizados por especialistas, em valores estruturados e compatíveis com modelos matemáticos de avaliação. A Tabela 5 sintetiza de que forma a abordagem híbrida

descrita neste capítulo contribui para mitigar a influência de vieses cognitivos e motivacionais nos resultados da análise multicritério (PINTO, 2023).

Tabela 5 – Redução de Vieses Cognitivos e Motivacionais na Abordagem Híbrida

Viés	Tipo	Estratégia de Mitigação do Viés	Método(s)
Excesso de confiança	Motivacional	Verificação de consistência nas comparações evita certeza injustificada	AHP-Índice CR
Ancoragem	Cognitivo	Comparações múltiplas e cruzadas dificultam fixação em um único valor inicial	AHP-MACBETH
Influência do Grupo	Motivacional	Julgamentos individuais são fragmentados e reavaliados em diferentes estágios	MACBETH-TOPSIS
Disponibilidade	Cognitivo	Cálculo objetivo baseado em dados normalizados evita julgamentos impulsivos	TOPSIS
Subjetividade excessiva	Cognitivo	Tradução verbal → cardinalidade e ponderação matemática equilibram percepções	MACBETH-TOPSIS
Falta de rastreabilidade	Cognitivo	Etapas formalizadas permitem auditoria e revisão de decisões	Abordagem Híbrida

Fonte: Elaborado pelo autor.

Ao considerar simultaneamente critérios qualitativos (como julgamentos de valor e atratividade) e critérios quantitativos (como pesos relativos e distâncias numéricas), o processo decisório torna-se estatisticamente mais equilibrado e robusto, possibilitando a classificação das alternativas com menor grau de subjetividade

6.2 INFRAESTRUTURAS E CRITÉRIOS DE AVALIAÇÃO

Com o objetivo de viabilizar uma análise comparativa consistente, optou-se por consultar três especialistas da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), quanto à avaliação de atratividade necessária para a aplicação do método MACBETH. Para o método AHP, em decorrência da complexidade e da quantidade de comparações exigidas, não houve consulta aos especialistas; o próprio Autor realizou os julgamentos pareados entre os critérios identificados como essenciais, atribuindo escalas de importância relativa conforme a escala fundamental de Saaty. No caso do método MACBETH, os especialistas forneceram julgamentos

objetivos de atratividade para cada uma das alternativas de infraestrutura, considerando cada critério, o que permitiu a construção de escalas cardinais. As respostas foram coletadas por meio de questionários estruturados (Apêndice A), e a média dos julgamentos foi utilizada como variável de entrada na análise multicritério híbrida, alimentando o programa implementado pelo Autor em linguagem MATLAB (Apêndice B).

Com o intuito de garantir que os aspectos operacionais e estratégicos essenciais à proposição de uma infraestrutura confiável para sistemas de C^2 fossem contemplados, selecionaram-se selecionou três infraestruturas candidatas, uma estrutura de referência (existente) e sete critérios de avaliação:

a) Infraestruturas:

- A_1 – Sistemas GEO (existente);
- A_2 – Sistemas LEO;
- A_3 – Sistemas WBHF; e
- A_4 – Sistemas NBHF; e

b) Critérios:

- C_1 – Ataques Cibernéticos;
- C_2 – Interceptação;
- C_3 – Bloqueio;
- C_4 – Susceptibilidade a Armas Antissatélites;
- C_5 – Largura de Banda;
- C_6 – Controle Nacional; e
- C_7 – Latência.

Na seção seguinte, é apresentada a avaliação comparativa das infraestruturas consideradas, resultando na hierarquização das alternativas frente aos critérios selecionados.

6.2.1 Matriz de Comparação, Par a Par, dos Critérios AHP

A atribuição de pesos referentes às comparações par a par foi realizada de acordo com a importância relativa de cada critério. Na diagonal principal da matriz, todos os valores são iguais a 1, uma vez que cada critério é comparado consigo mesmo. As demais células tiveram seus valores atribuídos conforme o detalhamento presente nos subitens seguintes.

I - Linha 1 – Ataques Cibernéticos C₁

- C₁ versus C₂ (Interceptação)

Os ataques cibernéticos apresentam importância moderadamente superior em relação à interceptação, por serem considerados uma ameaça mais abrangente e com maior potencial de comprometer de forma ampla os sistemas de comunicação. No entanto, essa superioridade não caracteriza uma diferença extrema de relevância entre os dois critérios. Por esse motivo, na escala Saaty, foi atribuída a importância moderada (3), indicando que os ataques cibernéticos possuem prioridade relativa em comparação ao critério interceptação.

- C₁ versus C₃ (Bloqueio)

Os ataques cibernéticos apresentam importância significativamente superior em relação ao bloqueio, considerando que este último representa uma vulnerabilidade operacional pontual, ao passo que os ciberataques têm potencial para comprometer de maneira abrangente a integridade e a disponibilidade de todo o sistema. Assim, atribuiu-se a importância forte (5), indicando que os ataques cibernéticos possuem relevância substancialmente maior em comparação ao critério bloqueio.

- C₁ versus C₄ (ASAT)

As armas antissatélites exercem impacto prioritariamente sobre sistemas baseados em satélites geoestacionários, ao passo que os ataques cibernéticos comprometem de forma abrangente qualquer infraestrutura de telecomunicações, incluindo satélites. Além disso, o emprego de

capacidades ASAT envolve custos elevados e apresenta menor probabilidade de ocorrência em comparação aos ciberataques, que podem ser conduzidos de forma mais recorrente e com menor barreira de acesso tecnológico. Por essa razão, na escala Saaty, foi atribuída a importância muito forte (7), indicando que os ataques cibernéticos possuem relevância significativamente superior em relação ao critério armas antissatélites.

- C₁ versus C₅ (Largura de Banda)

A largura de banda destinada aos sistemas de C² apresenta importância equivalente à dos ataques cibernéticos, considerando que ambos são fatores determinantes para garantir a eficiência operacional. A largura de banda desempenha papel essencial ao permitir o fluxo ágil e contínuo de mensagens e dados críticos em um sistema de C². Dessa forma, considerando a escala Saaty, foi atribuída a importância igual (1), indicando que esses critérios possuem o mesmo nível de relevância para o desempenho e a segurança das operações.

- C₁ versus C₆ (Controle Nacional)

Os ataques cibernéticos são considerados significativamente mais críticos do que o controle nacional. Isso porque, sem uma proteção cibernética eficaz, a soberania sobre o sistema se torna insuficiente para garantir sua operação segura e contínua. A vulnerabilidade a ataques pode comprometer imediatamente a integridade e a disponibilidade das comunicações, anulando qualquer vantagem derivada do controle nacional. Por essa razão, na escala Saaty, foi atribuído o valor 5, correspondente a uma importância forte dos ataques cibernéticos em relação ao critério controle nacional.

- C₁ versus C₇ (Latência)

Considera-se que os ataques cibernéticos possuem importância moderadamente superior em relação à latência. Enquanto a latência impacta de forma parcial a execução das operações — afetando principalmente a velocidade de transmissão e a capacidade de resposta —, os ciberataques podem comprometer integralmente a disponibilidade, a

integridade e a confiabilidade dos sistemas de comando e controle. Logo, foi empregado o valor 3, indicando importância moderada de ataques cibernéticos sobre o critério latência.

II - Linha 2 – Interceptação C₂

- C₂ versus C₃ (Bloqueio)

A interceptação tem importância moderada sobre bloqueio, uma vez que interceptar comunicações, obtendo-se seu conteúdo, pode ser considerado mais grave que bloqueá-las temporariamente. Assim, dentro da escala Saaty, este critério recebeu importância moderada (3).

- C₂ versus C₄ (ASAT)

A interceptação é muito mais relevante que armas antissatélite, uma vez que possui mais probabilidade de ocorrência que o emprego de armas antissatélite. Assim, dentro da escala Saaty, este critério recebeu importância forte (5).

- C₂ versus C₅ (Largura de Banda)

Em cenários de combate contemporâneo, a insuficiência de largura de banda pode inviabilizar o uso de sensores, enlaces de vídeo e a gestão de munições inteligentes. Esse requisito constitui uma condição mínima para assegurar a plena capacidade operacional no contexto do C², superando, em termos relativos, a relevância do risco de interceptação. Embora este risco represente uma ameaça significativa, sua mitigação é viável por meio de técnicas criptográficas robustas e da restrição à transmissão de informações sensíveis. Assim, o critério interceptação foi considerado menos importante que a largura de banda (C₅), recebendo, na escala de Saaty, o valor recíproco ao grau de importância moderada (1/3), o que indica que o critério C₅ é três vezes mais relevante que o critério C₂.

- C₂ versus C₆ (Controle Nacional)

A interceptação de comunicações constitui uma ameaça imediata ao êxito operacional, pois permite ao adversário acessar dados sensíveis,

comprometendo o sigilo e a surpresa estratégica. Esse risco pode gerar reações adversas instantâneas, como o redirecionamento de forças ou o bloqueio de operações críticas. Em contraste, o critério Controle Nacional se refere à soberania tecnológica e política sobre os sistemas de comunicações, cuja perda tende a produzir efeitos estratégicos graduais, como a dependência de fornecedores estrangeiros e a exposição a ingerências políticas. Considerando essa distinção temporal e operacional, a interceptação foi avaliada como moderadamente mais importante que o controle nacional, recebendo, na escala de Saaty, o valor 3.

III - Linha 3 – Bloqueio C₃

- C₃ versus C₄ (ASAT)

O bloqueio apresenta importância moderadamente superior em relação às armas antissatélites, considerando que a possibilidade de obstruir comunicações pode ocorrer em qualquer meio tecnológico, independentemente da arquitetura empregada. Além disso, o emprego de capacidades ASAT envolve custos elevados e apresenta menor probabilidade de ocorrência, em comparação a técnicas de bloqueio, que são mais acessíveis e passíveis de uso recorrente. Por essa razão, na escala Saaty, foi atribuída a importância moderada (3), indicando prioridade relativa do bloqueio sobre o critério armas antissatélites.

- C₃ versus C₅ (Largura de Banda)

A largura de banda é considerada mais importante do que o bloqueio, uma vez que a capacidade de transmitir dados com eficiência constitui requisito essencial para assegurar o funcionamento pleno dos sistemas de C². Por esse motivo, foi utilizado o valor recíproco de 3 (1/3), na escala Saaty, indicando que a largura de banda possui importância moderada em relação ao bloqueio.

- C₃ versus C₆ (Controle Nacional)

O bloqueio apresenta importância moderadamente superior em comparação ao controle nacional, tendo em vista que a capacidade

adversária de interromper transmissões pode comprometer, de forma imediata, a execução de operações, enquanto a ausência de soberania tecnológica tende a produzir efeitos mais graduais. Por essa razão, na escala Saaty, foi atribuída a importância moderada (3), indicando prioridade relativa do bloqueio sobre o critério controle nacional.

- C₃ versus C₇ (Latência)

O bloqueio foi considerado moderadamente mais importante do que a latência, dado que a interrupção deliberada das comunicações representa um risco direto e imediato à continuidade operacional, podendo resultar na completa indisponibilidade de informações críticas para a tomada de decisão. Esse impacto compromete severamente a execução coordenada de ações, a transmissão de ordens e a atualização situacional em tempo real. Por outro lado, o aumento da latência, embora prejudique a eficiência e a agilidade na resposta, não inviabiliza por completo o funcionamento do sistema de comando e controle. Essa distinção entre o efeito potencialmente total do bloqueio e o impacto parcial da latência fundamenta a atribuição da importância moderada (3) na escala Saaty, indicando prioridade relativa do bloqueio em comparação ao critério latência.

IV - Linha 4 – Armas Antissatélites C₄

- C₄ versus C₅ (Largura de Banda)

A largura de banda apresenta importância substancialmente superior em relação às armas antissatélites, uma vez que a capacidade de transmitir informações em alta velocidade é indispensável ao desempenho operacional dos sistemas de C². Além disso, a ameaça ASAT está restrita a sistemas espaciais específicos, envolve elevados custos de emprego e possui menor probabilidade de ocorrência em comparação a outras formas de ameaça. Por esse motivo, foi atribuído o valor recíproco de 5 (1/5) na escala de Saaty, indicando que a largura de banda é cinco vezes mais importante que o critério armas antissatélites.

- C₄ versus C₆ (Controle Nacional)

As armas antissatélites e o controle nacional foram considerados de importância equivalente, por ambos representarem riscos estratégicos equivalentes, mas sob perspectivas distintas. A neutralização física de satélites por meio de capacidades ASAT compromete diretamente a disponibilidade de enlaces espaciais, podendo provocar a interrupção prolongada dos serviços de comunicação e sensoriamento, mas possui baixa probabilidade de ocorrência. Por sua vez, a ausência de controle nacional implica dependência de terceiros na gestão e operação das infraestruturas de telecomunicações, gerando vulnerabilidades políticas, jurídicas e logísticas que reduzem a autonomia decisória. Dessa forma, foi atribuída a importância igual (1) na escala de Saaty, indicando equivalência entre os critérios, ainda que com naturezas distintas de impacto.

- C₄ versus C₇ (Latência)

As armas antissatélites e a latência foram avaliadas como critérios de igual importância, por representarem ameaças que, embora distintas em natureza, impactam diretamente a eficiência e a segurança das operações de Comando e Controle. A latência afeta continuamente o desempenho operacional, ao comprometer o tempo de resposta, a coordenação entre unidades e a efetividade na execução de ações em tempo real. Já a ameaça ASAT, embora baixa probabilidade de ocorrência e limitada a cenários específicos, possui elevado potencial disruptivo, podendo causar a degradação prolongada ou a perda completa de enlaces satelitais. Assim, considerando a frequência e a intensidade dos impactos, ambos os critérios foram considerados de relevância estratégica equivalente. Por esse motivo, foi atribuída a importância igual (1) na escala de Saaty, reconhecendo a paridade entre os riscos associados à latência e às capacidades antissatélites.

V - Linha 5 – Largura de Banda C₅

- C₅ versus C₆ (Controle Nacional)

A largura de banda apresenta importância moderadamente superior em relação ao critério de controle nacional, uma vez que a capacidade de transmitir dados em alta velocidade é um requisito operacional imediato e essencial para o funcionamento dos sistemas de Comando e Controle. A insuficiência desse recurso compromete diretamente o fluxo contínuo de informações, a consciência situacional e a coordenação eficiente entre os diferentes níveis de comando. Em contrapartida, o controle nacional representa um problema de médio e longo prazo, relacionado à autonomia na gestão, manutenção e evolução tecnológica das infraestruturas de telecomunicações. Embora a soberania sobre os sistemas seja relevante para mitigar riscos políticos e reduzir a dependência externa, seus efeitos tendem a se manifestar de forma gradual, diferentemente da limitação de largura de banda, que impacta de forma imediata a capacidade operacional. Por essa razão, foi atribuída, na escala de Saaty, a importância moderada (3), indicando prioridade relativa da largura de banda em comparação ao critério controle nacional.

- C₅ versus C₇ (Latência)

A largura de banda foi considerada moderadamente mais importante do que a latência, uma vez que a insuficiência de capacidade de transmissão compromete, de forma ampla e direta, o fluxo de informações essencial ao funcionamento eficaz dos sistemas de C². A limitação desse recurso pode ocasionar congestionamento de dados, perda de pacotes e severa restrição na troca de informações críticas entre as unidades operacionais. Em contraste, o impacto da latência, embora prejudique a agilidade na tomada de decisão e na coordenação em tempo real, se restringe ao aumento do tempo de resposta, sem necessariamente impedir a transmissão do conteúdo. Essa diferença, quanto à abrangência e à gravidade dos efeitos, justifica a atribuição da importância moderada (3) na escala de Saaty, indicando prioridade relativa da largura de banda em relação ao critério latência.

VI - Linha 6 – Controle Nacional C₆

- C₆ versus C₇ (Latência)

O critério controle nacional apresenta importância moderadamente superior em relação à latência, por estar associado à manutenção da soberania sobre as infraestruturas de comunicação — fator estratégico que assegura autonomia decisória, independência tecnológica e menor vulnerabilidade a pressões políticas externas. O domínio nacional sobre os sistemas permite definir políticas de segurança, garantir a continuidade dos serviços e proteger informações sensíveis ao longo de todo o ciclo operacional. Embora os efeitos da perda de soberania se manifestem de forma gradual, podem comprometer, progressivamente, a confiabilidade e a resiliência das comunicações estratégicas. Em contraste, a latência, embora relevante para a eficiência operacional imediata, restringe-se ao aumento do tempo de resposta e à redução da agilidade nas ações, sem afetar diretamente o controle ou a integridade dos ativos. Diante dessa diferença de escopo e profundidade dos impactos, foi atribuída, na escala de Saaty, a importância moderada (3), indicando prioridade relativa do controle nacional sobre o critério latência.

VII - Linha 7 – Latência C₇

Na linha correspondente ao critério latência (C₇), não foram realizadas novas comparações, uma vez que todas as avaliações, par a par, envolvendo esse critério já haviam sido efetuadas nas linhas anteriores da matriz. Conforme os procedimentos do método AHP, as comparações situadas abaixo da diagonal principal são automaticamente definidas como os valores recíprocos das avaliações localizadas acima da diagonal, assegurando a coerência e a consistência matemática da matriz. Dessa forma, a parte inferior da matriz é composta pelos inversos das relações previamente atribuídas, dispensando a necessidade de novas atribuições nesta etapa, conforme apresentado na Tabela 6.

Concluído o processo de comparação par a par e de atribuição de pesos aos sete critérios selecionados, verificou-se que o critério C₁ – Ataques Cibernéticos obteve o maior peso relativo, conforme apresentado na Tabela 7. Em razão disso, esse critério exercerá influência predominante no cálculo da Matriz de Decisão

Ponderada, especialmente nas etapas iniciais do método TOPSIS voltadas à seleção da infraestrutura mais adequada.

Tabela 6 – Matriz de Comparação dos Critérios de Avaliação das Estruturas – Método AHP

Comparação Direta	Comparação Indireta – Valor Recíproco						
	C ₁	C ₂	C ₃	C ₄	C ₅	C ₆	C ₇
C₁ - Ataques Cibernéticos	1,000	3,000	5,000	7,000	1.000	5.000	3.000
C₂ - Interceptação	0,333	1,000	3,000	5,000	0.333	3.000	3.000
C₃ - Bloqueio	0,200	0,333	1,000	3,000	0.333	3.000	3.000
C₄ - Armas Antissatélites	0,143	0,200	0,333	1,000	0.200	1.000	1.000
C₅ - Largura de Banda	1,000	3,000	3,000	5,000	1.000	3.000	3.000
C₆ - Controle Nacional	0,200	0,333	0,333	1,000	0.333	1.000	3.000
C₇ - Latência	0,333	0,333	0,333	1,000	0.333	0.333	1.000

Fonte: Elaborado pelo autor.

Por meio do programa implementado e executado em MATLAB (APÊNDICE B), foram calculados os demais parâmetros do método AHP:

- $\lambda_{max} = 7,5784$;
- $IC = 0,0964$;
- $RI(n = 7) = 1,32$; e
- $CR = 0,0730$, que está dentro do valor aceitável ($CR < 0,10$).

6.2.2 Vetor de Pesos Normalizados – AHP

Por meio da equação 6.1, foi calculado o vetor de Pesos Normalizados, cujas componentes estão listadas na Tabela 7 – Comparação, Par a Par, dos Critérios dos Critérios – Método AHP. Com destaque para a componente referente ao Critério Ataques Cibernéticos:

Tabela 7 – Comparação, Par a Par, dos Critérios dos Critérios – Método AHP

Critério	Peso Normalizado
C₁ - Ataques Cibernéticos	0,3133
C₅ - Largura de Banda	0,2568
C₂ - Interceptação	0,1635
C₃ - Bloqueio	0,1046
C₆ - Controle Nacional	0,0665
C₇ - Latência	0,0524
C₄ - Armas Antissatélites	0,0430

Fonte: Elaborado pelo autor.

6.2.3 Análise e Atribuição dos Valores de Atratividade – MACBETH

a) C₁ - Ataques Cibernéticos

A atratividade do critério C₁ avalia a capacidade dos sistemas avaliados de resistirem a ataques cibernéticos, assegurando a continuidade das comunicações mesmo diante de ameaças sofisticadas. Esse critério está diretamente relacionado à robustez da infraestrutura, ao grau de independência tecnológica e à presença de mecanismos de segurança autóctones.

Os sistemas WBHF obtiveram valor de atratividade média igual a 0,9000, em razão de sua operação sobre infraestrutura própria, desvinculada de redes comerciais, e da utilização de protocolos de criptografia dedicados, o que reduz substancialmente a sua superfície de exposição a ameaças cibernéticas.

Os sistemas NBHF foram avaliados com atratividade média igual a 0,9667, devido a características semelhantes às do WBHF no que se refere à independência de infraestrutura e à menor suscetibilidade à interceptação. Sua arquitetura de comunicação ponto a ponto, associada ao emprego de modulações robustas, contribui para elevada resiliência frente a ameaças cibernéticas.

Os sistemas LEO receberam valor de atratividade média igual a 0,7000. Essa avaliação considera o grande número de estações terrestres estrategicamente distribuídas, que aumentam a resiliência da rede por meio da segmentação do tráfego e da redundância de enlaces. Contudo, sua operação ainda depende, em grande parte, de gateways comerciais interligados à internet, o que introduz vulnerabilidades residuais a ataques cibernéticos distribuídos e exploração de superfícies expostas.

Os sistemas GEO foram avaliados com atratividade média igual a 0,5667. Apesar de parte da infraestrutura — como no caso do SGDC — estar sob controle

nacional, esses sistemas permanecem vulneráveis a ataques cibernéticos indiretos por meio de redes terrestres e enlaces compartilhados com satélites comerciais. Sua dependência de redes fixas e a exposição a infraestruturas mistas aumentam a suscetibilidade a ações hostis no domínio cibernético.

Tabela 8 – Valor da Atratividade para o Critério C₁

Dado	A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
I	0,7000	0,7000	0,9000	1,0000
II	0,5000	0,6000	0,8000	1,0000
III	0,5000	0,8000	1,0000	0,9000
Médias	0,5667	0,7000	0,9000	0,9667

Fonte: APÊNDICE A.

b) C₂ - Interceptação

A atratividade do critério C₂ avalia a vulnerabilidade dos sistemas de comunicação à interceptação por terceiros, considerando fatores como largura de banda, técnicas de modulação, controle de emissão, robustez dos mecanismos de criptografia empregados e integração com redes de dados.

Os sistemas GEO obtiveram valor de atratividade média igual a 0,5667. Sua posição geossíncrona fixa, combinada à ampla área de cobertura, facilita a detecção, o rastreamento e o monitoramento das transmissões. A previsibilidade dos enlaces e a concentração do tráfego tornam esses sistemas mais suscetíveis à interceptação, especialmente em cenários onde o sigilo operacional é essencial.

Os sistemas LEO apresentaram valor de atratividade média igual a 0,6333. Embora a órbita baixa reduza a exposição individual de cada satélite, a dependência de estações-base comerciais (gateways) introduz vetores potenciais de interceptação. Essa arquitetura híbrida, ao combinar ativos espaciais com infraestrutura terrestre externa, amplia os riscos à segurança da informação, sobretudo diante de adversários tecnologicamente avançados.

Os sistemas WBHF obtiveram valor médio de atratividade igual a 0,8000. Apesar de operarem com largura de banda de até 48 kHz — faixa que facilita a detecção espectral —, fazem uso de modulações digitais avançadas e, em determinadas aplicações, de criptografia proprietária. Esses recursos dificultam a interceptação do conteúdo, especialmente em cenários táticos onde não há a presença de sistemas modernos de guerra eletrônica.

Os sistemas NBHF também obtiveram valor de atratividade média igual a 0,8000, por operarem em canais estreitos de 3 kHz e, em geral, apresentarem baixa assinatura eletromagnética. Esses atributos, associados ao uso de criptografia proprietária, controle rigoroso de emissão, não integração com redes de dados e dependência das condições de propagação para o estabelecimento de enlaces, conferem elevada discrição e resistência a tentativas de interceptação não autorizada.

Dessa forma, a suscetibilidade à interceptação varia entre as alternativas — desde os sistemas GEO, mais expostos, até os NBHF e WBHF, mais discretos. Esse fator se revela importante na seleção de soluções de comunicação voltadas a operações nas quais o sigilo representa um requisito estratégico.

Tabela 9 – Valor da Atratividade para o Critério C₂

Dado	A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
I	0,7000	0,7000	0,8000	0,8000
II	0,5000	0,6000	0,7000	0,7000
III	0,5000	0,6000	0,9000	0,9000
Médias	0,5667	0,6333	0,8000	0,8000

Fonte: APÊNDICE A.

c) C₃ - Resiliência ao Bloqueio de Sinais (*Jamming*)

A atratividade do critério C₃ avalia a capacidade dos sistemas de comunicação de resistirem ou mitigarem interferências deliberadas (*jamming*). A diversidade espacial de propagação, as técnicas modernas de modulação digital e o controle espectral adaptativo constituem requisitos essenciais para a resiliência ao *jamming*, considerando que, em HF, as técnicas de salto de frequência apresentam baixa eficiência devido às limitações impostas pelas características da propagação ionosférica.

Os sistemas GEO obtiveram valor de atratividade média igual a 0,4000. Por manterem posição orbital fixa e utilizarem feixes de comunicação previsíveis, tornam-se alvos estáticos e vulneráveis à interferência deliberada. A dificuldade de realocação, somada à centralização dos enlaces, compromete sua resiliência em ambientes contestados e sujeitos à ataques decorrentes de guerra eletrônica.

Os sistemas LEO obtiveram valor de atratividade média igual a 0,9667, considerado elevado. A mobilidade orbital contínua e a capacidade de estabelecer múltiplos enlaces com diferentes estações terrestres, em momentos distintos,

proporcionam elevada redundância operacional. Essa arquitetura distribuída confere resiliência a bloqueios localizados ou temporários, ainda que a dependência de infraestrutura terrestre represente um vetor residual de vulnerabilidade frente a outras ameaças.

Os sistemas WBHF obtiveram valor de atratividade média igual a 1,0000. Sua elevada resiliência ao *jamming* decorre, primeiramente, das particularidades da propagação em HF, que oferece múltiplos caminhos por reflexão ionosférica e permite a seleção dinâmica da frequência ótima (MUF – *Maximum Usable Frequency*) para cada enlace. Além disso, técnicas como diversidade espacial, saltos de frequência coordenados e alocação dinâmica de espectro contribuem para mitigar a exposição a interferências.

Os sistemas NBHF receberam valor de atratividade média igual a 0,8000. Embora compartilhem com os WBHF as vantagens inerentes à propagação em HF, geralmente não operam com diversidade espacial nem utilizam protocolos de detecção e mitigação de interferência, o que limita sua capacidade de resposta diante de bloqueios intencionais.

Importa destacar que a interferência deliberada é, em muitos casos, inviável para sistemas que operam em HF. As frequências eficazes para propagação dependem da localização geográfica das estações, da hora do dia, da estação do ano e das condições solares. Assim, para uma determinada estação interferidora, situada em posição geográfica distinta, pode não haver propagação favorável entre sua posição e as estações da rede-alvo, resultando em sinais de *jamming* que não alcançam o receptor ou que chegam com intensidade insuficiente para negar o serviço. Esses fatores, aliados à capacidade de comutação automática de frequência dos terminais WBHF, dificultam a interrupção integral do enlace, mesmo sob intensa atividade de guerra eletrônica.

Em síntese, todos os sistemas analisados apresentam algum grau de proteção contra *jamming*; contudo, as arquiteturas HF — especialmente o WBHF, seguidas pelo NBHF — e as constelações LEO destacam-se pela superior resiliência. A complexidade estatística da propagação ionosférica, aliada à seleção dinâmica de frequências (no caso do HF), bem como a redundância numérica e espacial das constelações LEO, tornam essas soluções particularmente robustas frente a bloqueios hostis de sinal.

Tabela 10 – Valor da Atratividade para o Critério C₃

Dado	A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
I	0,6000	0,9000	1,0000	0,8000
II	0,3000	1,0000	1,0000	0,7000
III	0,3000	1,0000	1,0000	0,9000
Médias	0,4000	0,9667	1,0000	0,8000

Fonte: APÊNDICE A.

d) C₄ - Armas Antissatélites (ASAT)

A atratividade do critério C₄ avalia o grau de resiliência dos sistemas de comunicações frente a ameaças orbitais, com ênfase em cenários de negação de acesso ao espaço, como os representados por ataques de armas antissatélites (ASAT).

Os sistemas WBHF e NBHF receberam valor de atratividade média igual a 1,0000, por não operarem no domínio espacial. Sua independência em relação a satélites os torna imunes a ataques ASAT, cujo escopo de atuação se restringe a ativos orbitais. Essa característica lhes confere elevada resiliência em ambientes operacionais contestados, especialmente em teatros onde o espaço possa ser negado de forma temporária ou permanente.

Os sistemas LEO foram avaliados com valor de atratividade média igual a 0,9000. Embora estejam sujeitos ao engajamento por armas ASAT, a elevada densidade orbital — viabilizada por constelações com dezenas ou centenas de satélites —, combinada à mobilidade contínua, reduz a efetividade de ações pontuais. Essa arquitetura distribuída fortalece a resiliência operacional, permitindo a continuidade do serviço mesmo diante de perdas parciais da infraestrutura espacial.

Em contrapartida, os sistemas GEO foram classificados com valor de atratividade média igual a 0,3000. Por operarem em posições fixas e isoladas, a cerca de 36.000 km da superfície terrestre, tornam-se alvos previsíveis e vulneráveis a ataques ASAT dirigidos. Sua função estratégica, ao concentrar enlaces críticos de comunicação, amplia o impacto potencial da neutralização, caracterizando-os como pontos únicos de falha com elevado risco operacional.

Tabela 11 – Valor da Atratividade para o Critério C₄

Dado	A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
I	0,2000	0,9000	1,0000	1,0000
II	0,5000	0,8000	1,0000	1,0000
III	0,2000	1,0000	1,0000	1,0000
Médias	0,3000	0,9000	1,0000	1,0000

Fonte: APÊNDICE A.

e) C₅ - Largura de Banda

A atratividade do critério C₅ avalia a capacidade de transmissão de dados de cada sistema, aspecto determinante para a eficiência das comunicações no contexto dos sistemas de C².

Os sistemas LEO obtiveram valor de atratividade média igual a 1,0000, por oferecerem a maior largura de banda entre as alternativas analisadas. Sua estrutura orbital viabiliza enlaces com baixa latência e altas taxas de transferência, favorecendo aplicações de dados intensivos, como transmissão de vídeo, telemetria avançada e integração de sensores em tempo real em ambientes operacionais complexos.

Os sistemas GEO foram classificados com valor de atratividade média igual a 0,9000. Apesar da latência mais elevada, sua ampla capacidade de banda larga os torna adequados para o tráfego de grandes volumes de informação em redes militares estratégicas, incluindo replicação de bancos de dados, videoconferência e enlaces de Estado-Maior.

Os sistemas WBHF obtiveram valor de atratividade média igual a 0,6000, com base em sua capacidade de alcançar taxas de até 240 kbps, conforme especificado na norma MIL-STD-188-110D. Embora inferiores às taxas dos sistemas satelitais, essas velocidades são consideradas satisfatórias para aplicações contingenciais para sistemas de C², sobretudo em cenários degradados ou de negação de acesso ao espectro, nos quais as comunicações via satélite podem estar comprometidas.

Por sua vez, os sistemas NBHF receberam o menor valor de atratividade média, igual a 0,2000, em razão das limitações técnicas relacionadas à largura de banda disponível. Esse fator restringe seu uso a comunicações de voz e à transferência de pequenos arquivos, tornando-os inadequados para aplicações multimídia ou transmissões de dados volumosos que exijam maior capacidade de enlace.

Tabela 12 – Valor da Atratividade para o Critério C₅

Dado	A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
I	0,9000	1,0000	0,6000	0,2000
II	0,9000	1,0000	0,5000	0,1000
III	0,9000	1,0000	0,7000	0,3000
Média	0,9000	1,0000	0,6000	0,2000

Fonte: APÊNDICE A.

f) C₆ - Controle Nacional

A atratividade do critério C₆ avalia a autonomia operacional e a soberania tecnológica, com base no grau de controle nacional sobre a infraestrutura de comunicações empregada — um fator crítico para a independência estratégica e a segurança institucional em operações militares.

Os sistemas WBHF e NBHF obtiveram valor de atratividade média igual a 1,0000, por serem integralmente operados sob domínio nacional, garantindo soberania relativa sobre sua operação e a segurança da informação.

Os sistemas GEO, neste caso se referindo ao segmento espacial do SISCOMIS, obtiveram atratividade média igual a 0,9000. Embora o SISCOMIS empregue o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC), controlado e operado pela Força Aérea Brasileira (FAB), também faz uso do satélite Star One C3, gerenciado por uma empresa privada (Claro S/A), o que reduz o nível de controle exclusivamente nacional. Ainda assim, por dispor de um satélite estratégico sob controle integral da FAB, a alternativa A₁ – Sistemas GEO – mantém alta atratividade para o critério ora analisado.

Por sua vez, os sistemas LEO – obteve atratividade média nula (0,0000), devido à inexistência de uma constelação LEO nacional. Essa dependência compromete a autonomia operacional e a soberania tecnológica.

Tabela 13 – Valor da Atratividade para o Critério C₆

Dado	A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
I	0,9000	0,0000	1,0000	1,0000
II	0,9000	0,0000	1,0000	1,0000
III	0,9000	0,0000	1,0000	1,0000
Média	0,9000	0,0000	1,0000	1,0000

Fonte: APÊNDICE A.

g) C₇ - Latência

A atratividade do critério C₇ avalia a latência ou atraso no envio e recebimento de mensagens. Trata-se de um fator crítico para a eficácia das operações de C², especialmente em ambientes táticos e em cenários que demandam tomada de decisão em tempo real.

Os sistemas WBHF e NBHF receberam valor de atratividade média igual a 1,0000, por operarem com enlaces rádio ponto a ponto e em tempo real, apresentando latência mínima. Por não dependerem de infraestrutura externa ou interconexões via redes de longa distância, esses sistemas proporcionam comunicações quase imediatas, ideais para ambientes operacionais que exigem respostas rápidas, coordenação ágil e sincronização precisa.

Os sistemas LEO foram classificados com valor de atratividade média igual a 0,8000. Apesar de serem sistemas satelitais, operam em órbitas baixas, o que lhes confere latência reduzida, tipicamente entre 20 e 50 milissegundos. Esse desempenho é satisfatório para a maioria das aplicações militares.

Por outro lado, os sistemas GEO receberam valor de atratividade média igual a 0,2000, em função da latência elevada — geralmente em torno de 500 milissegundos — decorrente da distância orbital de aproximadamente 36.000 km. Essa latência pode comprometer aplicações críticas que exigem resposta imediata, como, por exemplo, controle de plataformas remotamente pilotadas.

Tabela 14 – Valor da Atratividade para o Critério C₇

Dado	A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
I	0,2000	0,7000	1,0000	1,0000
II	0,3000	0,9000	1,0000	1,0000
III	0,1000	0,8000	1,0000	1,0000
Média	0,2000	0,8000	1,0000	1,0000

Fonte: APÊNDICE A.

6.2.4 Matriz de Decisão Ponderada – MACBETH

Por meio das equações 6.4 e 6.5, a partir dos pesos normalizados calculados pelo método AHP e da matriz de decisão derivada do método MACBETH, apresentada na Tabela 15, é construída a matriz de decisão ponderada, apresentada na Tabela 16, cujos elementos são utilizados para o cálculo dos diversos resultados apresentados pelo método TOPSIS.

Tabela 15 – Matriz de Decisão (sem ponderação/normalização)

Alternativa	C₁	C₂	C₃	C₄	C₅	C₆	C₇
A ₁ - Satélite GEO	0,5670	0,5670	0,4000	0,3000	0,9000	0,9000	0,2000
A ₂ - Satélite LEO	0,7000	0,6330	0,9670	0,9000	1,0000	0,0000	0,8330
A ₃ - WBHF	0,9000	0,8000	1,0000	1,0000	0,6000	1,0000	1,0000
A ₄ - NBHF	0,9670	0,8000	0,8000	1,0000	0,2000	1,0000	1,0000

Fonte: APÊNDICE B.

Tabela 16 – Matriz de Decisão Ponderada

Alternativa	C₁	C₂	C₃	C₄	C₅	C₆	C₇
A ₁ - Satélite GEO	0,1837	0,1159	0,0419	0,0129	0,2311	0,0599	0,0105
A ₂ - Satélite LEO	0,2268	0,1293	0,1012	0,0387	0,2568	0,0000	0,0436
A ₃ - WBHF	0,2916	0,1635	0,1046	0,0430	0,1541	0,0665	0,0524
A ₄ - NBHF	0,3133	0,1635	0,0837	0,0430	0,0514	0,0665	0,0524

Fonte: APÊNDICE B.

6.2.5 Resultados Finais – TOPSIS

Conforme descrito na seção 6.1, a partir dos resultados obtidos pelos métodos AHP e MACBETH, e com base nas equações 6.6 a 6.10, calculam-se as figuras de mérito do método TOPSIS, apresentadas na Tabela 17, as quais permitem classificar, por meio do Índice de Similaridade C_i , as infraestruturas de comunicações avaliadas.

Tabela 17 – Figuras de Mérito do Método TOPSIS

Infraestruturas de Comunicações	Distância Ideal (D_i^+)	Distância Anti-Ideal (D_i^-)	Índice C_i	Classificação
A ₂ - Satélite LEO	0,1148	0,2225	0,6597	1º
A ₃ - WBHF	0,1624	0,1884	0,6421	2º
A ₁ - Satélite GEO	0,1050	0,1895	0,5385	3º
A ₄ - NBHF	0,2065	0,1670	0,4472	4º

Fonte: APÊNDICE B.

6.3 CONCLUSÕES PARCIAIS

A adoção de uma abordagem híbrida de Análise Multicritério, conforme proposta neste estudo, contribuiu significativamente para mitigar vieses cognitivos e motivacionais frequentemente presentes em processos baseados em julgamento especializado, tais como excesso de confiança, ancoragem em avaliações anteriores

e influência de consenso em grupos técnicos. A integração dos métodos AHP, MACBETH e TOPSIS, operacionalizados em etapas sistemáticas com validação cruzada, fortaleceu a rastreabilidade, a coerência e a objetividade analítica das escolhas realizadas.

A aplicação prática dessa metodologia permitiu classificar quatro alternativas de infraestrutura de comunicações (A_1 – GEO, A_2 – LEO, A_3 – WBHF e A_4 – NBHF), com base em sete critérios estratégicos previamente definidos: C_1 – Ataques Cibernéticos, C_2 – Interceptação, C_3 – Bloqueio, C_4 – Susceptibilidade a Armas Antissatélites, C_5 – Largura de Banda, C_6 – Controle Nacional e C_7 – Latência. Os resultados obtidos por meio do método TOPSIS indicaram que o Sistema A_2 – Satélite LEO apresentou o melhor desempenho global ($C_i = 0,6597$), seguido de forma bastante próxima pelo Sistema A_3 – WBHF ($C_i = 0,6421$). As alternativas GEO (A_1) e NBHF (A_4) ocuparam a terceira e quarta posições, respectivamente.

Embora o Sistema LEO tenha se destacado em largura de banda e baixa latência, a ausência de controle nacional — evidenciada pelo valor zero de atratividade atribuído a esse critério — reduziu seu índice C_i e limitou a vantagem sobre o Sistema WBHF, resultando em um desempenho geral sensivelmente equilibrado entre essas duas alternativas. A fim de reduzir riscos associados à dependência de operadores estrangeiros no emprego de satélites LEO, a Marinha, por intermédio do Conselho Diretor do Sistema Militar de Comando e Controle (CD-SisMC²), poderá acompanhar e subsidiar tecnicamente o desenvolvimento do Sistema de Comunicações Táticas de Órbita Baixa (ComLEO), sob coordenação do Comando da Aeronáutica. Esse projeto, sucessor do Projeto Attícora (BRASIL, 2018; GUEDES, 2015), integra o Programa Estratégico de Sistemas Espaciais (PESE).

O Sistema WBHF, por sua vez, apresentou desempenho mais balanceado, com destaque para a elevada resiliência a ataques cibernéticos e ao bloqueio de sinais, além do pleno controle nacional. Esses fatores explicam sua pontuação próxima à do Sistema LEO, mesmo apresentando menor capacidade de largura de banda.

Dessa forma, os resultados apresentados neste capítulo reforçam a viabilidade e a relevância da adoção de uma arquitetura de comunicações híbrida e resiliente, combinando sistemas satelitais (GEO/LEO) e enlaces em alta frequência (WBHF/NBHF), de modo a atender, com flexibilidade e robustez, às demandas do SisNC² e, em nível estratégico, do SisMC². Ademais, a fim de melhor atender ao critério C_6 – Controle Nacional, os representantes da MB no CD-SisMC² poderão

continuar participando do desenvolvimento da Forma de Onda de Altas Taxas em HF para o Rádio Definido por Software de Defesa (RDS-Defesa) (RAMELLA, 2021) e, assim, a assegurar o emprego efetivo de tecnologias nacionais nas comunicações militares. Por fim, destaca-se que os requisitos operacionais encaminhados à equipe técnica desenvolvimento do RDS-Defesa devem contemplar a interoperabilidade em plataformas navais e a capacidade de operação em banda larga, em conformidade com os padrões internacionais MIL-STD-188-110 C/D, garantindo robustez, eficiência espectral e segurança criptográfica.

O código-fonte referente à implementação da abordagem multicritério híbrida se encontra disponível no Apêndice B, desenvolvido em linguagem MATLAB (formato *.m*), podendo ser reutilizado para a hierarquização de alternativas, segundo outros critérios.

Por fim, os resultados apresentados neste capítulo podem subsidiar decisões estratégicas quanto ao investimento, planejamento e desenho arquitetônico de redes resilientes, contribuindo para o aumento da autonomia, segurança e eficácia das operações de C^2 no contexto da Defesa Nacional. No capítulo a seguir, serão apresentadas as considerações finais e recomendações decorrentes dos resultados obtidos por este trabalho.

7 CONSIDERAÇÕES FINAIS

O desenvolvimento deste trabalho permitiu identificar, analisar e propor alternativas para o fortalecimento da resiliência e da soberania das comunicações estratégicas para C² no âmbito do Sistema Naval de Comando e Controle (SisNC²), considerando a dependência do segmento espacial do Sistema de Comunicações Militares por Satélite (SISCOMIS).

No Capítulo 1, a introdução contextualizou o ambiente estratégico e tecnológico das comunicações navais como infraestrutura para o SisNC², destacando a vulnerabilidade associada à dependência do segmento espacial do SISCOMIS diante de interferências eletrônicas, ataques cibernéticos e armas antissatélite (ASAT). A partir desse diagnóstico, foram definidos o Problema de Pesquisa, a Questão Central e o Objeto de Estudo, que orientaram toda a investigação constante deste trabalho.

O Capítulo 2 tratou da infraestrutura de C² da MB como elemento integrante do Sistema Militar de Comando e Controle (SisMC²), evidenciando que o SisNC² depende fortemente do segmento espacial do SISCOMIS e da RECIM. Constatou-se que o aumento da resiliência dos níveis inferiores de comunicação reflete diretamente na segurança das informações transmitidas ao nível estratégico. Concluiu-se, portanto, que o SisNC² deve dispor de infraestrutura alternativa de comunicações autônoma, flexível e interoperável como SISCOMIS, capaz de assegurar o fluxo vertical de informações entre os escalões, mesmo sob interferência, bloqueio ou degradação do enlace satelital.

O Capítulo 3 apresentou as conclusões sobre os Sistemas Satelitais de Baixa Órbita (LEO), que se mostraram alternativas promissoras por oferecerem baixa latência, maior largura de banda e cobertura global. Entretanto, observou-se que a dependência de operadores estrangeiros e a ausência de controle nacional constituem limitações importantes. Assim, destacou-se que o desenvolvimento de capacidades nacionais em órbita baixa representa uma oportunidade estratégica para a MB, especialmente em cooperação com o Comando da Aeronáutica e com o setor industrial de defesa.

O Capítulo 4 analisou os Sistemas de Comunicações em Alta Frequência de Banda Larga (WBHF), concluindo que apresentam elevado potencial de resiliência, principalmente em cenários de negação de acesso ao espaço. O WBHF permite taxas de dados significativamente superiores às comunicações HF convencionais e pode

atuar como sistema contingente ao SISCOMIS, assegurando a continuidade do C² em situações de interferência ou interrupção satelital. Sua principal vantagem reside no pleno controle nacional da tecnologia, na robustez operacional e na perspectiva de futura do RDS-Defesa incorporar formas de onda de banda larga, garantindo interoperabilidade e segurança cibernética.

O Capítulo 5 abordou os Sistemas de Comunicações de Banda Estreita em Alta Frequência (NBHF), ressaltando seu papel estratégico como solução complementar e de baixo custo para a manutenção da conectividade em ambientes degradados. Apesar das menores taxas de transmissão, os sistemas NBHF se destacam pela robustez, confiabilidade e independência de infraestruturas espaciais, sendo imunes a ataques ASAT e menos expostos a vulnerabilidades cibernéticas. Sua compatibilidade com a infraestrutura legada, que permite o emprego do aplicativo ComSec-DV desenvolvido pela Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), reforçam seu valor como componente essencial de uma arquitetura de comunicações resiliente.

O Capítulo 6 consolidou os resultados da análise multicritério híbrida (AHP, MACBETH e TOPSIS), mitigando vieses de julgamento e aprimorando a objetividade analítica. Os resultados indicaram que os sistemas LEO apresentaram o melhor desempenho global ($C_i = 0,6597$), seguidos de perto pelos sistemas WBHF ($C_i = 0,6421$). As alternativas — GEO ($C_i = 0,5385$) e NBHF ($C_i = 0,4472$) — ocuparam, respectivamente, a terceira e a quarta posições. Embora os sistemas LEO tenham se destacado tecnicamente quanto à largura de banda e à baixa latência, a ausência de controle nacional — refletida pela nota zero no critério correspondente — limitou sua vantagem potencial. A proximidade entre LEO e WBHF confirmou a viabilidade de uma integração entre sistemas satelitais e ionosféricos como a solução mais robusta para o SisNC², garantindo redundância, segurança e autonomia operacional.

Com base nos resultados da análise multicritério e nas conclusões técnicas, recomenda-se que os navios com sistemas satelitais geoestacionários (bandas “X” e “Ku”) empreguem Sistemas WBHF como solução de contingência, dada sua resiliência a bloqueios e robustez a ataques cibernéticos, além da possibilidade de pleno controle nacional, quando do emprego do RDS-Defesa. Já para os meios que ainda não dispõem de enlaces satelitais, sugere-se a adoção de Sistemas LEO, em função de seu desempenho técnico superior, menor custo e praticidade de instalação, sendo, nesses Meios, o NBHF empregado como elemento de contingência aos

Sistemas LEO para manutenção parcial de enlaces com o SisNC² em condições de negação do espaço.

Para mitigar os riscos associados à dependência de operadores estrangeiros, recomenda-se que a MB, por meio do CD-SisMC², apoie tecnicamente o desenvolvimento do Sistema de Comunicações Táticas de Órbita Baixa (ComLEO), coordenado pelo Comando da Aeronáutica. A MB deverá pleitear que essa constelação atenda a requisitos compatíveis com as demandas estratégicas de C², como largura de banda, baixa latência, cobertura contínua e interoperabilidade com sistemas navais embarcados, inclusive em ambientes sujeitos bloqueios e ataques cibernéticos.

Para garantir a segurança das informações transmitidas via NBHF, torna-se indispensável a adoção de soluções de criptografia autóctone e interoperável. Nesse contexto, recomenda-se o emprego do aplicativo ComSec-DV, desenvolvido pela DCTIM, que possibilita a troca segura de dados e mensagens de voz.

De forma integrada, a configuração modular e escalável ora proposta, que combina sistemas LEO, WBHF e NBHF, conforme o perfil operacional de cada Meio, contribui significativamente para o fortalecimento da resiliência, soberania e continuidade das comunicações em C², assegurando interoperabilidade e flexibilidade estratégica ao SisNC².

Com base nas conclusões parciais dos capítulos anteriores, verifica-se que a dependência exclusiva do SISCOMIS pode representar um risco concreto à continuidade do C² no âmbito da MB em uma real situação de A2AD. Assim, em resposta à Questão Central da pesquisa, conclui-se que a MB pode assegurar a continuidade, a soberania e a resiliência das comunicações estratégicas de C² por meio da integração de infraestruturas híbridas de comunicação, combinando sistemas LEO, WBHF e NBHF, de forma complementar e interoperável ao SISCOMIS. Essa integração, associada à consolidação de políticas de autonomia tecnológica e segurança criptográfica, permitirá à Força dispor de uma arquitetura de comunicações segura, redundante e nacionalmente controlada, essencial ao fortalecimento do SisNC² e ao cumprimento de sua missão institucional em quaisquer condições operacionais.

Adicionalmente, recomenda-se que a MB, por meio do CD-SisMC², mantenha sua colaboração ativa no projeto da Forma de Onda Conjunta para o Rádio Definido de Defesa (RDS-Defesa), assegurando que os requisitos operacionais contemplem

interoperabilidade em plataformas navais e operação em banda larga, conforme os padrões MIL-STD-188-110 C/D. Essa iniciativa está alinhada à Estratégia Nacional de Defesa (END) e à Política Nacional de Cibersegurança (PNCiber), que orientam o desenvolvimento de capacidades autônomas e seguras em comunicações militares.

A implementação das propostas apresentadas, mesmo que de forma parcial, tende a elevar significativamente a confiabilidade, disponibilidade e resiliência operacional do SisNC², contribuindo também para o atendimento das demandas do Sistema Militar de Comando e Controle (SisMC²) e, conseqüentemente, para o fortalecimento do C² no nível estratégico.

REFERÊNCIAS

- AL-HRAISHAWI, Hayder; CHOUGRANI, Houcine; KISSELEFF, Steven; LAGUNAS, Eva; CHATZINOTAS, Symeon. **A survey on non-geostationary satellite systems: the communication perspective**. arXiv preprint, arXiv:2107.05312, 2021. Disponível em: <https://arxiv.org/abs/2107.05312>.
- ANDRADE, J. F. de; CAMPOS, M. L. R. de; APOLINÁRIO, J. A. **L1-Constrained Normalized LMS Algorithms for Adaptive Beamforming**. IEEE Transactions on Signal Processing, v. 63, n. 24, p. 6524–6539, 15 dez. 2015. DOI: <https://doi.org/10.1109/TSP.2015.2474302>.
- ASSAM, Andrey de Oliveira; REIS, Ilmar Duarte dos. **Avanços em Sistemas de Satélites em Baixa Órbita: Protocolos de Comunicação, Navegação e Aprendizado Federado**. Engenharias, v. 29, n. 143, fev. 2025. DOI: 10.69849/revistaft/pa10202502282015. Disponível em: <https://revistaft.com.br/.../>. Acesso em: 23 abr. 2025.
- BANA E COSTA, Carlos A.; VANSNICK, Jean-Marie. **MACBETH – An interactive path towards the construction of cardinal value functions**. *International Transactions in Operational Research*, v. 11, n. 1, p. 1–34. 2004.
- BANA E COSTA, C. A.; DE CORTE, J.-M.; VANSNICK, J.-C. **MACBETH: Overview of MACBETH multicriteria decision analysis approach**. 2012. Disponível em: <https://www.researchgate.net/publication/230674197>.
- BBC Brasil. **China confirma teste de míssil contra satélite**. BBC Brasil, 23 de janeiro de 2007. Disponível em: https://www.bbc.com/...china_teste_crg. Acesso em: 18 fev. 2025.
- BRASIL. Marinha do Brasil. **Doutrina Militar Naval (DMN)**. 1. revisão preliminar. Brasília: Comando de Operações Navais, 2025.
- BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. **Institui a Política Nacional de Cibersegurança – PNCiber e dispõe sobre a governança da cibersegurança**. Diário Oficial da União, Brasília, DF, 27 dez. 2023a.
- BRASIL. Ministério da Defesa. Estado-Maior Conjunto das Forças Armadas. **Instrução Normativa EMCFA-MD nº 3, de 9 de fevereiro de 2023**. Estabelece, no âmbito do Sistema Militar de Comando e Controle – SisMC2, os procedimentos gerais para o emprego do Sistema de Comunicações Militares por Satélite – SISCOMIS. *Diário Oficial da União*, Brasília, DF, 20 mar. 2023b. Seção 1, p. 33.
- BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasília: Ministério da Defesa, 2020a.
- BRASIL. Ministério da Defesa. **MD20-S-01 – Programa Estratégico de Sistemas Espaciais (PESE)**. 1. ed. Brasília: Ministério da Defesa, 2018.

BRASIL. Ministério da Defesa. **MD31-M-03: Doutrina para o Sistema Militar de Comando e Controle**. Brasília, DF: Ministério da Defesa, 2015.

CAPELLA, Matthew R.; YOO, Peter J.; CUNNINGHAM, Daniel E.; WAKAYAMA, Cherry Y. **Mission Assurance Framework for Small Satellite Missions**. In: AIAA/USU Conference on Small Satellites, 31., 2017, Logan, UT. Proceedings [...]. Logan: Utah State University, 2017.

DONEGAN, H. A.; DODD, F. J. **A note on Saaty's random indexes**. Mathematical and Computer Modelling, v. 15, n. 10, p. 135–137, 1991. DOI: [10.1016/0895-7177\(91\)90098-R](https://doi.org/10.1016/0895-7177(91)90098-R).

GUEDES, Éric Cézzane Cólen. **O Programa Estratégico de Sistemas Espaciais**. Palestra apresentada na Escola Superior de Guerra, Rio de Janeiro, 19 maio 2025. Curso Superior de Defesa (CSD).

HE, Guolong; GAO, Xin; SUN, Liangliang; ZHANG, Rentian. **A Review of Multibeam Phased Array Antennas as LEO Satellite Constellation Ground Station**. IEEE Access, v. 9, p. 151–160, 2021. DOI: 10.1109/ACCESS.2021.3124318. Disponível em: https://www.researchgate.net/publication/355763236_A_Review_of_Multibeam_Phased_Array_Antennas_as_LEO_Satellite_Constellation_Ground_Station. Acesso em: 23 abr. 2025

HWANG, Ching-Lai; YOON, Kwangsun. **Multiple Attribute Decision Making: Methods and Applications**. New York: Springer, 1981.

KRATOS DEFENSE. **Inter-Satellite Links Are Making Space Networks a Reality**. 2022. Disponível em: <https://www.kratosdefense.com/constellations/articles/inter-satellite-links-are-making-space-networks-a-reality>. Acesso em: 23 abr. 2025.

IETF. **Dynamic Link Exchange Protocol (DLEP)**. RFC 8175, 2017. Disponível em: <https://datatracker.ietf.org/doc/html/rfc8175>. Acesso em: 23 abr. 2025

LIN, Shu; COSTELLO, Daniel J. **Error Control Coding: Fundamentals and Applications**. 2. ed. Upper Saddle River, NJ: Pearson Prentice Hall, 2004.

MARKOFF, John. **Before the Gunfire, Cyberattacks**. The New York Times, 13 ago. 2008. Disponível em: <https://www.nytimes.com/2008/08/13/technology/13cyber.html>. Acesso em: 18 fev. 2025.

MILLER, Greg. **The intelligence coup of the century**. The Washington Post, 11 de fevereiro de 2020. Disponível em: <https://www.washingtonpost.com/graphics/.../cia-crypto-encryption-machines-espionage/>. Acesso em: 18 fev. 2025.

MORITA, P. L. S. et al. **Método multicritério AHP-TOPSIS-2N aplicado à decisão de compra de imóvel em Manaus (Brasil)**. Revista Contemporânea, v. 3, n. 12, p. 31544–31569, dez. 2023. DOI: 10.56083/RCV3N12-341.

MOTTA, Marcelo Jorge de Assis. **Comunicações em alta frequência (HF): banda larga – uma nova realidade**. Revista Passadiço, Rio de Janeiro, n. 58, p. 58-60, 2021.

MU, Enrique; PEREYRA-ROJAS, Milagros. **Practical Decision Making: An Introduction to the Analytic Hierarchy Process (AHP) Using Super Decisions V2**. Cham: Springer, 2017. (SpringerBriefs in Operations Research). ISBN 978-3-319-33860-6. DOI: [10.1007/978-3-319-33861-3](https://doi.org/10.1007/978-3-319-33861-3).

NATO STANDARDIZATION OFFICE (NATO). **STANAG 4538: Technical Standards for 3rd Generation Automatic Link Establishment (3G ALE)**. Bruxelas: NATO, 2007.

NATO STANDARDIZATION OFFICE (NATO). **STANAG 5066: Profile for HF Radio Data Communications**. Bruxelas: NATO, 2022.

NATO STANDARDIZATION OFFICE (NATO). **STANAG 5070: HF Interoperability Standard**. Bruxelas: NATO, 2013.

NATO STANDARDIZATION OFFICE (NATO). **STANAG 4539: Standard for High-speed Data Transmission over HF**. Bruxelas: NATO, 2017.

NATIONAL CYBER SECURITY CENTRE (NCSC). **Russia behind cyber-attack with Europe-wide impact hour before Ukraine invasion**. NCSC, 10 de maio de 2022. Disponível em: <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion>. Acesso em: 18 fev. 2025.

NILE PROJECT MANAGEMENT OFFICE (NILE PMO). **Common Interface Guide – NATO Improved Link Eleven – Link 22**. Versão 2.3. San Diego, 2020. Disponível em: <https://www.link22.org/uploads/7/9/3/2/7932022/2020100>. Acesso em: 28 jul. 2025

PAN, Jianping. **What Is a Starlink POP? How Ground Stations Improve Latency and Capacity**. PCMag, 2024. Disponível em: <https://www.pcmag.com/news/what-is-a-starlink-pop-how-ground-stations-improve-latency-capacity>. Acesso em: 23 abr. 2025.

PINTO, Ítalo de Melo. **Estruturação de Problemas em Blocos**. Rio de Janeiro: Letras e Versos, 2023.

POSADA, Carlos Alberto. **O Sistema de Gerenciamento da Amazônia Azul (SisGAAz): impactos na doutrina e estrutura de comando e controle nas atividades de emprego limitado da Força da Marinha do Brasil**. Rio de Janeiro: Escola de Guerra Naval, 2019.

RAMELLA, Ítalo. **Uma arquitetura de comunicações para a interoperabilidade das Forças Armadas Brasileiras**. Rio de Janeiro: Escola de Guerra Naval, 2021.

REUTERS. **What we know about the deadly pager blasts in Lebanon.** Reuters News, 18 de setembro de 2024. Disponível em: <https://www.reuters.com/world/middle-east/what-we-know-so-far-about-deadly-pager-blasts-lebanon-2024-09-17/>. Acesso em: 18 fev. 2025.

SAATY, Thomas L. **Decision Making with the Analytic Hierarchy Process.** International Journal of Services Sciences, v. 1, n. 1, p. 83-98, 2008.

SOUZA, L. P., GOMES, C. F. S., & DE BARROS, A. P. 2018. **Implementation of new hybrid AHP–TOPSIS-2N method in sorting and prioritizing of an it CAPEX project portfolio.** International Journal of Information Technology & Decision Making, 17(04), 977-1005.

SILVA, E. F. da; OLIVEIRA, C. G. de; SOUSA, R. J. de. **Aplicação do método AHP como apoio à tomada de decisão na aquisição de um robô industrial.** Revista Científica Multidisciplinar Núcleo do Conhecimento, v. 6, n. 11, p. 141–158, 2021.

SPACENEWS. **Project Kuiper prototypes successfully test inter-satellite optical links.** 2023. Disponível em: <https://spacenews.com/project-kuiper-prototypes-successfully-test-inter-satellite-optical-links/>. Acesso em: 23 abr. 2025. SpaceNews.

SPACEX. **Starlink Tech.** 2025. Disponível em: <https://www.starlink.com/technology>. Acesso em: 23 abr. 2025.

STEVENS, J. A.; PAUL, L.; SNODGRASS, T. E.; NELSON, R. W. **Wideband High Frequency (WBHF) for Anti-access Area-Denial (A2AD) Environments.** In: IEEE MILITARY COMMUNICATIONS CONFERENCE (MILCOM), 2014, Baltimore: IEEE, 2014. p. 1522-1527. DOI: 10.1109/MILCOM.2014.251.

TELARUS. **LEO, MEO, and GEO, Oh My! Modern Satellite Connectivity, Explained.** 2024. Disponível em: <https://www.telarus.com/blog/modern-satellite-connectivity-explained/>. Acesso em: 23 abr. 2025.

TILL, Geoffrey. **Seapower: A Guide for the Twenty-First Century.** 4. ed. Abingdon: Routledge, 2018. (Cass Series: Naval Policy and History)

TURNER, Andrew E. **Constellation Design Considerations for Smallsats.** In: AIAA/USU CONFERENCE ON SMALL SATELLITES, 29., 2015, Logan, UT. Proceedings [...]. Logan: Utah State University, 2015.

UNITED STATES STUDIES CENTRE (US-SC). **The importance of satellite cybersecurity.** University of Sydney, 2024. Disponível em: <https://www.ussc.edu.au/the-importance-of-satellite-cybersecurity>. Acesso em: 23 abr. 2025.

UNITED STATES DEPARTMENT OF DEFENSE (DoD). **MIL-STD-6016: Tactical Data Exchange - Link 16.** Washington, D.C.: DoD, 2022.

UNITED STATES DEPARTMENT OF DEFENSE (DoD). **Directed Energy Weapons: Technologies, Applications and Implications**. Washington, D.C.: Office of the Secretary of Defense, 2020.

UNITED STATES DEPARTMENT OF DEFENSE (DoD). **MIL-STD-188-110C: Interoperability and Performance Standards for Data Modems**. Washington, D.C.: Department of Defense, 2012.

UNITED STATES DEPARTMENT OF DEFENSE (DoD). **MIL-STD-188-110D: Interoperability and Performance Standards for Data Modems**. Washington, D.C.: DoD, 2017a.

UNITED STATES DEPARTMENT OF DEFENSE (DoD). **MIL-STD-188-141D: Interoperability and Performance Standards for ALE 4G Systems**. Washington, D.C.: DoD, 2017b.

UNITED STATES DEPARTMENT OF DEFENSE (DoD). **MIL-STD-188-141B: Interoperability and Performance Standards for Medium and High Frequency Radio Systems**. Washington, D.C.: DoD, 1999.

XU, Yueying et al. **A hybrid multi-criteria decision-making approach based on ANP-entropy TOPSIS for building materials supplier selection**. *Entropy*, Basel, v. 25, n. 7, p. 1047, 2023. DOI: 10.3390/e25071047.

ZACCONI, Christiano Limoeiro. **O comando e controle nas operações conjuntas no nível estratégico: a situação do fluxo de informações entre o nível operacional (comando conjunto ativado) e o nível estratégico (Ministério da Defesa), da estrutura do sistema militar de comando e controle utilizado nas operações conjuntas**. Trabalho de Conclusão de Curso (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2021.

ZHAO, Yuhan; ZHU, Quanyan. **Autonomous and Resilient Control for Optimal LEO Satellite Constellation Coverage Against Space Threats**. arXiv preprint arXiv:2203.02050, 2022. Disponível em: <https://arxiv.org/abs/2203.02050>. Acesso em: 23 abr. 2025.

APÊNDICE A - QUESTIONÁRIO ESTRUTURADO

ENTREVISTAS COM ESPECIALISTAS EM COMUNICAÇÕES NAVAIS PARA ATRIBUIÇÃO DE VALORES de ATRATIVIDADE PARA O MÉTODO MACBETH

1 PROPÓSITO

A fim de permitir uma análise comparativa consistente, o Autor optou por consultar três especialistas da Diretoria de Comunicações e Tecnologia da Informação da Marinha (DCTIM), quanto aos parâmetros necessários à aplicação do método e *MACBETH*. Os especialistas deverão fornecer valores de atratividade entre alternativas com base em cada critério, permitindo a construção de escalas cardinais por meio de programação linear. A média dos valores obtidos com as respostas do Questionários Estruturados será usada para o cálculo da análise multicritério híbrida.

Com o intuito de garantir que os aspectos operacionais e estratégicos essenciais à proposição de uma infraestrutura contingente confiável para sistemas de Comando e Controle (C^2), o autor selecionou três infraestruturas candidatas e uma estrutura de referência (existente), e sete critérios de avaliação para essas estruturas:

a) Infraestruturas:

- A_1 – Sistemas GEO (existente);
- A_2 - Sistemas LEO;
- A_3 – Sistemas WBHF; e
- A_4 – Sistemas NBHF; e

b) Os critérios de análise considerados são os seguintes:

- C_1 – Ataques Cibernéticos;
- C_2 – Interceptação;
- C_3 – Bloqueio;
- C_4 – Susceptibilidade a Armas Antissatélites;
- C_5 – Largura de Banda;
- C_6 – Controle Nacional; e
- C_7 – Latência.

2 DEFINIÇÃO DOS CRITÉRIOS – *MACBETH*

a) C₁ - Ataques Cibernéticos

A análise do critério C₁ considera a capacidade dos sistemas avaliados de resistirem a ataques cibernéticos, garantindo a continuidade das comunicações mesmo sob ameaças avançadas. Esse critério está diretamente associado à robustez da infraestrutura de comunicação, ao grau de independência tecnológica e à presença de mecanismos de segurança autóctones.

b) C₂ - Interceptação

A análise do critério C₂ avalia a vulnerabilidade dos sistemas de comunicação à interceptação por terceiros, considerando fatores como largura de banda, técnicas de modulação, controle de emissão e robustez dos mecanismos de criptografia empregados.

c) C₃ - Resiliência ao Bloqueio de Sinais (*Jamming*)

A análise do critério C₃ considera a capacidade dos sistemas de comunicação em resistir ou mitigar tentativas de interferência deliberada, conhecidas como *jamming*. Esse critério avalia atributos como robustez do sinal e diversidade de propagação, reconhecendo que técnicas como salto de frequência são ineficazes em HF devido às características da propagação ionosférica.

d) C₄ - Armas Antissatélites (ASAT)

A análise do critério C₄ avalia o grau de exposição dos sistemas de comunicações a ameaças orbitais, com ênfase em cenários de negação de acesso ao espaço, como os representados por ataques antissatélite (ASAT).

e) C₅ - Largura de Banda

A avaliação do critério C₅ considera a capacidade de transmissão de dados de cada sistema, fator determinante para a eficiência das comunicações em tempo real no contexto de Comando e Controle.

f) C₆ - Controle Nacional

A análise do critério C₆, referente à Autonomia Operacional e à Soberania Tecnológica, avalia o grau de controle nacional sobre a infraestrutura de comunicações empregada — um fator crítico para a independência estratégica e a segurança institucional em operações militares.

g) C₇ - Latência

A avaliação do critério C₇ considera a latência das comunicações, ou seja, o tempo necessário entre o envio e o recebimento de uma informação. Trata-se de um fator crítico para a eficácia de operações de Comando e Controle, especialmente em ambientes táticos e em cenários que demandam tomada de decisão em tempo real.

3 PRIMEIRA ENTREVISTA

3.1 QUALIFICAÇÃO RESUMIDA DO ENTREVISTADO

- Posto, Especialidade e Nome do entrevistado: CF (EN) André Vinícius **PINHO** Luiz.
- Formação e Experiência do especialista:
 - Engenheiro Eletricista com ênfase em Telecomunicações; e
 - Mestre em Engenharia de Telecomunicações.
- Funções exercidas correlacionadas às Comunicações Militares Navais:
 - Superintendente de Telecomunicações da DCTIM;
 - Comandante da ERMRJ;
 - Chefe do Departamento de Enlaces da DCTIM;
 - Encarregado da Divisão de Enlaces do CTIM; e
 - Encarregado da Divisão de Operações da ERM CN.

3.2 TRIBUIÇÃO DE VALORES CARDINAIS – *MACBETH*

a) C₁ - Ataques Cibernéticos

Tabela 18 – Valor da Atratividade para o Critério C₁- Primeira Entrevista

A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
0,7	0,7	0,9	1,0

b) C₂ - Interceptação

Tabela 19 – Valor da Atratividade para o Critério C₂ - Primeira Entrevista

A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
0,7	0,7	0,8	0,8

c) C₃ - Resiliência ao Bloqueio de Sinais (*Jamming*)

Tabela 20 – Valor da Atratividade para o Critério C₃ - Primeira Entrevista

A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
0,6	0,9	1,0	0,8

h) C₄ - Armas Antissatélites (ASAT)

Tabela 21 – Valor da Atratividade para o Critério C₄ - Primeira Entrevista

A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
0,2	0,9	1,0	1,0

i) C₅ - Largura de Banda

Tabela 22 – Valor da Atratividade para o Critério C₅ - Primeira Entrevista

A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
0,9	1,0	0,6	0,2

j) C₆ - Controle Nacional

Tabela 23 – Valor da Atratividade para o Critério C₆ - Primeira Entrevista

A₁ - Satélite GEO	A₂ - Satélite LEO	A₃ - WBHF	A₄ - NBHF
0,9	0,0	1,0	1,0

k) C₇ - LatênciaTabela 24 – Valor da Atratividade para o Critério C₇ - Primeira Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,2	0,7	1,0	1,0

4 SEGUNDA ENTREVISTA**4.1 QUALIFICAÇÃO RESUMIDA DO ENTREVISTADO**

- Posto, Especialidade e Nome do entrevistado: CC (EN) **LEONARDO** de Lima FREITAS.

- Formação e Experiência do especialista:

- Engenheiro de Telecomunicações; e
- Mestre em Rádio Propagação.

- Funções exercidas correlacionadas às Comunicações Militares Navais:

- Oficial de ligação da área técnica da MB para o Sistema de Comunicações;
- Militares por Satélite (SISCOMIS);
- Chefe do Departamento de Enlaces da DCTIM; e
- Encarregado da Divisão de Enlaces por Satélite da DCTIM.

4.2 ATRIBUIÇÃO DE VALORES CARDINAIS – MACBETHa) C₁ - Ataques CibernéticosTabela 25 – Valor da Atratividade para o Critério C₁ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,5	0,6	0,8	1,0

b) C₂ - InterceptaçãoTabela 26 – Valor da Atratividade para o Critério C₂ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,5	0,6	0,7	0,7

c) C₃ - Resiliência ao Bloqueio de Sinais (*Jamming*)Tabela 27 – Valor da Atratividade para o Critério C₃ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,3	1,0	1,0	0,7

d) C₄ - Armas Antissatélites (ASAT)Tabela 28 – Valor da Atratividade para o Critério C₄ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,5	0,8	1,0	1,0

e) C₅ - Largura de BandaTabela 29 – Valor da Atratividade para o Critério C₅ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,9	1,0	0,5	0,1

f) C₆ - Controle NacionalTabela 30 – Valor da Atratividade para o Critério C₆ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,9	0,0	1,0	1,0

g) C₇ - LatênciaTabela 31 – Valor da Atratividade para o Critério C₇ - Segunda Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,3	0,9	1,0	1,0

5 TERCEIRA ENTREVISTA**5.1 QUALIFICAÇÃO RESUMIDA DO ENTREVISTADO**

- Posto, Especialidade e Nome do entrevistado: CMG (EN) Fábio Alexandre **LEAL** da Silva.

- Formação e Experiência do especialista:

- Engenheiro Eletrônico; e
- Mestre em Engenharia de Telecomunicações.

- Funções exercidas correlacionadas às Comunicações Militares Navais:

- Diretor do CTIM (atual);
- Superintendente de Telecomunicações da DCTIM;
- Chefe do Departamento Comunicações Navais da DCTIM; e
- Encarregado da Divisão de Comunicações Exteriores da DCTIM.

5.2 ATRIBUIÇÃO DE VALORES CARDINAIS – *MACBETH*

a) C₁ - Ataques Cibernéticos

Tabela 32 – Valor da Atratividade para o Critério C₁ - Terceira Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,5	0,8	1,0	0,9

b) C₂ - Interceptação

Tabela 33 – Valor da Atratividade para o Critério C₂ - Terceira Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,5	0,6	0,9	0,9

c) C₃ - Resiliência ao Bloqueio de Sinais (*Jamming*)

Tabela 34 – Valor da Atratividade para o Critério C₃ - Terceira Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,3	1,0	1,0	0,9

d) C₄ - Armas Antissatélites (ASAT)

Tabela 35 – Valor da Atratividade para o Critério C₄ - Terceira Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,2	1,0	1,0	1,0

e) C₅ - Largura de Banda

Tabela 36 – Valor da Atratividade para o Critério C₅ - Terceira Entrevista

A ₁ - Satélite GEO	A ₂ - Satélite LEO	A ₃ - WBHF	A ₄ - NBHF
0,9	1,0	0,7	0,3

f) C₆ - Controle NacionalTabela 37 – Valor da Atratividade para o Critério C₆ - Terceira Entrevista

A1 - Satélite GEO	A2 - Satélite LEO	A3 - WBHF	A4 - NBHF
0,9	0,0	1,0	1,0

g) C₇ - LatênciaTabela 38 – Valor da Atratividade para o Critério C₇ - Terceira Entrevista

A1 - Satélite GEO	A2 - Satélite LEO	A3 - WBHF	A4 - NBHF
0,1	0,8	1,0	1,0

APÊNDICE B – IMPLEMENTAÇÃO DA ANÁLISE MULTICRITÉRIO

% Limpa Todas as Variáveis da Memória do Matlab

clear;

%ANÁLISE MULTICRITÉRIO HÍBRIDA - AHP + MACBETH + TOPSIS

%Programa escrito como parte da Tese do C-PEM 2025

%=== ETAPA 1: MATRIZ DE COMPARAÇÃO AHP (par a par) ===

% Resolução, passo a passo, do problema completo de seleção de Infraestrutura ...

% Infraestrutura de Comunicações contingente à atual infraestrutura do SisNC²

% usando o método AHP + MACBETH + TOPSIS.

%===== Critério Elencados =====

% C1 - Ataques Cibernéticos

% C2 - Interceptação

% C3 - Bloqueio

% C4 - Armas Antissatélites

% C5 - Largura de Banda

% C6 - Controle Nacional

% C7 - Latência

%===== Alternativas =====

% A1 - Sistema Satelital Geoestacionário (GEO)

% A2 - Sistema Satelital de Baixa Órbita (LEO)

% A3 - Sistema de HF de Banda larga (WBHF)

% A4 - Sistema de HF de Banda Estreita (NBHF)

%=====

% Matriz de Comparação dos Critérios de Avaliação das Estruturas – Método AHP

% Escala Saaty (1 a 9)

% Igual importância | 1

% Importância moderada | 3

% Importância forte | 5

% Importância muito forte| 7

% Importância extrema | 9

% valores intermediários | 2, 4, 6, 8

```

% C1 vs C2 --> 3; % C1 vs C3 --> 5; % C1 vs C4 --> 7;
% C1 vs C5 --> 1; % C1 vs C6 --> 5; % C1 vs C7 --> 3;
% C2 vs C3 --> 3; % C2 vs C4 --> 5; % C2 vs C5 --> 1/3;
% C2 vs C6 --> 3; % C2 vs C7 --> 3; % C3 vs C4 --> 3;
% C3 vs C5 --> 1/3; % C3 vs C6 --> 3; % C3 vs C7 --> 3;
% C4 vs C5 --> 1/5; % C4 vs C6 --> 1; % C4 vs C7 --> 1;
% C5 vs C6 --> 3; % C5 vs C7 --> 3; % C6 vs C7 --> 3
%=====
V1=[3.0; 5.0; 7.0;1.0; 5.0; 3.0; 3.0; 5.0; 1/3; 3.0; 3.0; 3.0; 1/3; 3.0; 3.0; 1/5; 1.0; 1.0;
3.0; 3.0; 3.0];
AHP_mat=eye(n);
l0 = 1;
l1=n-1;
for cont=1:n-1
AHP_mat(cont,cont+1:n)= V1(l0:l1);
l0=l1+1;
l1=l1+n-(cont+2)+1;
AHP_mat(cont+1:n,cont)= 1./(AHP_mat(cont,cont+1:n));
end
% Cálculo dos Pesos usando autovetor normalizado da matriz
[vecs, vals] = eig(AHP_mat);
[~, idx] = max(diag(vals));
w = vecs(:, idx);
pesos = w / sum(w);
% Cálculo do Índice de Consistência
lambda_max = max(diag(vals));
IC = (lambda_max - n)/(n - 1);
% RI = [0 0 0.58 0.90 1.12 1.24 1.32];
RI = [0.00 0.00 0.58 0.90 1.12 1.24 1.32 1.41 1.45 1.49];
CR = IC / RI(n);
fprintf('\nPesos AHP:\n'); disp(pesos);
fprintf('CR = %.4f\n', CR);

```

%=== ETAPA 2: MATRIZES MACBETH POR CRITÉRIO ===

% MATRIZ DE VALORES CARDINALIZADOS: A1 - GEO, A2 - LEO, A3 - % WBHF,
A4 - NBHF

```
valores_cardinais = [
0.567 0.700 0.900 0.967; % C1 - Ataques Cibernéticos
0.567 0.633 0.800 0.800; % C2 - Interceptação
0.400 0.967 1.000 0.800; % C3 - Bloqueio
0.300 0.900 1.000 1.000; % C4 - Armas Antisatélite
0.900 1.000 0.600 0.200; % C5 - Largura de Banda
0.900 0.000 1.000 1.000; % C6 - Controle Nacional
0.200 0.833 1.000 1.000]; % C7 - Latência
```

```
valores_cardinais = valores_cardinais'; % Agora cada linha é uma alternativa
disp("Escalas MACBETH (matriz completa):");
disp(valores_cardinais);
```

%=== ETAPA 3: MATRIZ DE DECISÃO ===

A = valores_cardinais; % cada linha = critério, colunas = alternativas

%=== ETAPA 4: NORMALIZAÇÃO ===

```
[m, n] = size(valores_cardinais);
% A_norm = valores_cardinais ./ vecnorm(valores_cardinais);
A_norm = valores_cardinais ./ max(valores_cardinais);
```

%=== ETAPA 5: MATRIZ PONDERADA ===

```
pesos=pesos';
A_pond = A_norm .* pesos;
```

%=== ETAPA 6: TOPSIS ===

```
Ideal = max(A_pond);
Anti = min(A_pond);
Dplus = sqrt(sum((A_pond - Ideal).^2, 2));
Dminus = sqrt(sum((A_pond - Anti).^2, 2));
Ci = Dminus ./ (Dplus + Dminus);
```

```

%=== RESULTADOS ===
% A1 - Sistema Satelital Geoestacionário (GEO)
% A2 - Sistema Satelital de Baixa Órbita (LEO)
% A3 - Sistema de HF de Banda larga (WBHF)
% A4 - Sistema de HF de Banda Estreita (NBHF)
[~, ranking] = sort(Ci, 'descend');
Candidatos= ["A1 - Satélite GEO", "A2 - Satélite LEO", "A3 - WBHF", "A4 - NBHF" ];
Classificacao = ["1º - ", "2º - ", "3º - ", "4º - " ];
CI = ["1º", "2º", "3º", "4º" ];
Resultado=append(Classificacao,Candidatos(ranking));
fprintf("\nMatriz de Decisão Ponderada \n");
disp(A_pond);
fprintf("\nRanking final (Índice C_i):\n");
disp(Ci);
fprintf("Ranking das alternativas:\n\n");
% disp(Classificacao(1:end),Candidatos(ranking));
disp(Resultado(1,:));
Resultados_Finais=[Candidatos' ];
Primeira_Linha=["Infraestrutura", "Distância Ideal", "Distância Anti-ideal", "Índice C_i",
"Classificação"];
Resultados_Finais=[Primeira_Linha; Candidatos(ranking)' Dplus(ranking)
Dminus(ranking) Ci(ranking) CI'];
writematrix(Resultados_Finais,'Resultado_Simulacao.xlsx','Sheet','TOPSIS');
writematrix(resultado.A_pond,'Resultado_Simulacao.xlsx','Sheet','A_Ponderada');

```