

ESCOLA DE GUERRA NAVAL

CC MANOEL JOSÉ MATTOS DOS SANTOS

**A ESTRUTURA VTS E O SEU RELACIONAMENTO COM A MARINHA
DO BRASIL POR MEIO DA INTEGRAÇÃO DOS CONCEITOS DE
C5IVR**

Rio de Janeiro

2024

CC MANOEL JOSÉ MATTOS DOS SANTOS

**A ESTRUTURA VTS E O SEU RELACIONAMENTO COM A MARINHA
DO BRASIL POR MEIO DA INTEGRAÇÃO DOS CONCEITOS DE
C5IVR**

Dissertação apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Estado-Maior para Oficiais Superiores.

Orientador: CF (RM1) Fabiano Rebello Cantarino.

Rio de Janeiro
Escola de Guerra Naval
2024

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.

DEDICATÓRIA

Dedico este projeto a todos os que se fazem ao mar, aos que labutam e extraem dos mares e rios o seu sustento. Aos homens e mulheres do mar.

AGRADECIMENTOS

Agradeço a Deus pelo dom da vida e por proporcionar-me ânimo e saúde para empreender esforços nesse trabalho especial. Agradeço à minha amada família: minha esposa Tatiana, que compreende minhas ausências e apoiou, como de costume, mais essa empreitada de grande vulto. Seu amor, carinho e dedicação foram essenciais para que eu pudesse dispender parcela de tempo expressiva na confecção dessa dissertação. Minhas filhas, Maria Eduarda e Laura, meus amores, que em meio às minhas ausências souberam aguardar e, com sua alegria e amor incondicionais, fortaleceram-me ao longo da jornada. Ao meu orientador, CF (RM1) Fabiano Rebello Cantarino, agradeço pela paciência, pela atenção meticulosa e por ter guiado-me, desde o início, por águas não antes navegadas, no oceano da imaginação e do conhecimento. Sempre disponível e acolhedor, sua orientação proporcionou-me a descoberta e o aprendizado de muitos aspectos da escrita acadêmica. Por fim, agradeço à Marinha do Brasil, por meio da Escola de Guerra Naval — instituição secular de relevância internacional — que nesse momento ímpar da minha carreira me deu a oportunidade de desenvolver-me intelectualmente, durante o Curso de Estado-Maior para Oficiais Superiores.

RESUMO

A presente dissertação investiga a integração das ferramentas C5IVR com o VTS (Serviço de Tráfego de Embarcações) e suas implicações para a Marinha do Brasil (MB). C5IVR, que representa Comando, Controle, Comunicações, Computação, Cibernética, Inteligência, Vigilância e Reconhecimento, é uma concepção essencial para aprimorar a eficácia militar através da coordenação eficiente de informações em tempo real, garantindo uma visão completa do campo de batalha. A pesquisa analisa o impacto dos sistemas VTS e VTMS (Sistema de Gerenciamento e Informações do Tráfego de Embarcações) nos portos de Açu e Vitória, destacando como esses sistemas podem ser utilizados para fornecer informações relevantes à inteligência operacional da MB. O provimento de conhecimentos dessa natureza visa aumentar a segurança e a eficiência da navegação, proteger o meio ambiente e proporcionar suporte crítico às operações militares. A análise aborda ainda os desafios e oportunidades da integração de aspectos do conceito C5IVR, enfatizando a necessidade de um equilíbrio entre aprimorar a inteligência operacional e preservar a função primordial de segurança da navegação aquaviária do VTS. As sugestões para futuras pesquisas incluem o aprimoramento de um arcabouço regulatório, análise de benefícios e desafios, investigação de tecnologias emergentes e capacitação de operadores e gestores. Conclui-se que a aplicação de recursos C5IVR com o sistema VTS tem o potencial de proporcionar uma gestão mais eficaz do tráfego marítimo e apoiar o processo de tomada de decisões da MB. A combinação dessas tecnologias e serviços permite uma abordagem holística e integrada para a segurança e defesa marítima, beneficiando não apenas a segurança do tráfego aquaviário, mas também as operações navais.

Palavras-chave: Serviço de Tráfego de Embarcações. C5IVR. NCW. Inteligência Operacional. Marinha do Brasil. Segurança Marítima. Navegação. Monitoramento. Operações Navais. Portos Brasileiros. Gestão de Tráfego Aquaviário.

ABSTRACT

The VTS structure and its relationship with the Brazilian Navy through the integration of C5ISR concepts

This dissertation investigates the integration of C5IVR tools with the Vessel Traffic Service (VTS) and its implications for the Brazilian Navy (BN). C5IVR, which stands for Command, Control, Communications, Computers, Cybernetics, Intelligence, Surveillance, and Reconnaissance, is an essential concept for enhancing military effectiveness through the efficient coordination of real-time information, ensuring a comprehensive view of the battlefield. The research analyzes the impact of the VTS and VTMS (Vessel Traffic Management and Information System) on the ports of Açú and Vitória, highlighting how these systems can be utilized to provide relevant information to the operational intelligence of the BN. The provision of such knowledge aims to increase the safety and efficiency of navigation, protect the environment, and provide critical support to military operations. The analysis also addresses the challenges and opportunities of integrating C5IVR concept aspects, emphasizing the need for a balance between enhancing operational intelligence and preserving the primary function of ensuring maritime navigation safety through the VTS. Suggestions for future research include the development of a regulatory framework, analysis of benefits and challenges, investigation of emerging technologies, and training for operators and managers. It is concluded that the application of C5IVR resources with the VTS system has the potential to provide more effective maritime traffic management and support the decision-making process of the MB. The combination of these technologies and services enables a holistic and integrated approach to maritime security and defense, benefiting not only the safety of waterway traffic but also naval operations.

Keywords: Vessel Traffic Service. C5ISR. NCW. Operational Intelligence. Brazilian Navy. Maritime Security. Navigation. Monitoring. Naval Operations. Brazilian Ports. Marine Traffic Management.

LISTA DE ILUSTRAÇÕES

FIGURA 1 – A Organização Militar como um Organismo Centrado em Rede.....	19
FIGURA 2 – Linha do tempo do desenvolvimento C5IVR.....	22
FIGURA 3 – Comparação entre LPS, VTS e VTMS.....	26
FIGURA 4 – Instalações do Centro VTS no Porto do Açú.....	34
FIGURA 5 – CCO do VTMS Vitória.....	35

LISTA DE TABELAS

TABELA 1 – Estrutura C5IVR.....	24
TABELA 2 – Ferramentas do VTS e VTMIS.....	37
TABELA 3 – Benefícios da integração.....	40

LISTA DE ABREVIATURAS E SIGLAS

AAM	—	Representante da Autoridade Marítima
AAW	—	<i>Anti-Aircraft Warfare</i>
AC	—	Autoridades Certificadoras
AES	—	<i>Advanced Encryption Standard</i>
AIS	—	<i>Automatic Identification System</i>
AM	—	Autoridade Marítima
AP	—	Autoridade Portuária
ARP	—	Aeronaves Remotamente Pilotadas
AtoN	—	<i>Aids to Navigation</i>
ATP	—	Associação de Terminais Portuários Privados
AWACS	—	<i>Airborne Warning and Control System</i>
BFT	—	<i>Blue Force Tracking</i>
C ²	—	Comando e Controle
C5IVR	—	Comando, Controle, Comunicações, Computação, Cibernética, Inteligência, Vigilância e Reconhecimento
CCO	—	Centro de Controle Operacional
CFTV	—	Circuito Fechado de Televisão
CIA	—	<i>Central Intelligence Agency</i>
CIM	—	Centro de Inteligência da Marinha
CME	—	Contramedidas Eletrônicas
CNUDM	—	Convenção das Nações Unidas sobre o Direito do Mar
ComOpNav	—	Comando de Operações Navais
COMPAAz	—	Comando de Operações Marítimas e Proteção da Amazônia Azul
COTS	—	<i>Commercial Off-The-Shelf</i>
CSM	—	Consciência Situacional Marítima
DGRM	—	Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos
DHN	—	Diretoria de Hidrografia e Navegação
DoD	—	<i>Department of Defense</i>
EGN	—	Escola de Guerra Naval

EOS	—	<i>Electro-Optical System</i>
ERGAF	—	Estação Radiogoniométrica de Alta Frequência
EUA	—	Estados Unidos da América
FA	—	Forças Armadas
GNR	—	Guarda Nacional Republicana
GPS	—	<i>Global Positioning System</i>
HAIGE	—	<i>High Assurance Internet Protocol Encryptor</i>
HF	—	<i>High Frequency</i>
IALA	—	International Association of Marine Aids to Navigation and Lighthouse Authorities
IBAMA	—	Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis
IEMA	—	Instituto Estadual de Meio Ambiente e Recursos Hídricos
IETF	—	<i>Internet Engineering Task Force</i>
IPSec	—	<i>Internet Protocol Security</i>
IMO	—	<i>International Maritime Organization</i>
ISPS Code	—	<i>International Ship and Port Facility Security Code</i>
LPS	—	<i>Local Port Service</i>
LRIT	—	<i>Long Range Identification and Tracking</i>
MB	—	Marinha do Brasil
MD	—	Ministério da Defesa
MDO	—	<i>Multi-Domain Operations</i>
MMSI	—	<i>Maritime Mobile Service Identity</i>
NCW	—	<i>Network Centric Warfare</i>
NORMAM	—	Normas da Autoridade Marítima
NSA	—	<i>National Security Agency</i>
OM	—	Organização Militar
OMI	—	Organização Marítima Internacional
OTAN	—	Organização do Tratado Atlântico Norte
PF	—	Polícia Federal
PGP	—	<i>Pretty Good Privacy</i>
PKI	—	<i>Public Key Infrastructure</i>
RADAR	—	<i>Radio Detection And Ranging</i>
SAGE	—	<i>Semi-Automatic Ground Environment</i>

SAIS	—	<i>Satellite Automatic Identification System</i>
SAR	—	<i>Search and Rescue</i>
Satellite SAR	—	<i>Synthetic-Aperture RADAR based on Satellite</i>
SIOP	—	<i>Sistema de Inteligência Operacional</i>
SisGAAz	—	<i>Sistema de Gerenciamento da Amazônia Azul</i>
SIVICC	—	<i>Sistema Integrado de Vigilância, Comando e Controle</i>
S/MIME	—	<i>Secure/Multipurpose Internet Mail Extensions</i>
SOLAS	—	<i>International Convention for the Safety of Life at Sea</i>
TDL A/B	—	<i>Tactical Data Link A/B</i>
TUP	—	<i>Terminal de Uso Privado</i>
USAF	—	<i>United States Air Force</i>
VPN	—	<i>Virtual Private Network</i>
VHF	—	<i>Very High Frequency</i>
VTMIS	—	<i>Vessel Traffic Management Information System</i>
VTS	—	<i>Vessel Traffic Service</i>
VTSO	—	<i>Vessel Traffic Service Operator</i>

SUMÁRIO

1	INTRODUÇÃO.....	14
2	CONCEITO DE C5IVR	17
2.1	GUERRA CENTRADA EM REDES.....	17
2.2	O DESENVOLVIMENTO DO C5IVR	20
2.3	ESTRUTURAÇÃO DO SISTEMA.....	22
3	FUNÇÃO PRIMORDIAL DO SISTEMA VTS E VTMS	25
3.1	OS SISTEMAS DE MONITORAMENTO DO TRÁFEGO MARÍTIMO.....	25
3.2	VTS.....	27
3.2.1	Elementos de um Sistema VTS.....	29
3.3	VTMS.....	31
3.3.1	Elementos de um VTMS.....	32
4	INTEGRAÇÃO DE FERRAMENTAS C5IVR COM O SISTEMA VTS.....	33
4.1	BREVE HISTÓRICO SOBRE A IMPLEMENTAÇÃO DO SISTEMA VTS E VTMS NO BRASIL.....	33
4.2	IDENTIFICAÇÃO DAS FERRAMENTAS DO VTS/VTMS E SUAS CONEXÕES COM C5IVR.....	36
4.3	APLICAÇÃO DOS CONCEITOS DE C5IVR E A INTEROPERABILIDADE	39
4.4	COMPARTILHAMENTO DE DADOS DE INTERESSE COM A MB	40
5	RELEVÂNCIA DOS DADOS PARA A INTELIGÊNCIA OPERACIONAL.....	44
5.1	AVALIAÇÃO DA RELEVÂNCIA DAS INFORMAÇÕES OBTIDAS PELA INTEGRAÇÃO DE FERRAMENTAS C5IVR PARA A INTELIGÊNCIA OPERACIONAL DA MB.....	44
5.2	REGULAMENTAÇÃO DO FLUXO DE DADOS	46
6	CONSIDERAÇÕES FINAIS.....	50
	REFERÊNCIAS.....	53

1 INTRODUÇÃO

O Serviço de Tráfego de Embarcações¹ é um conjunto de facilidades proporcionadas pela administração de um determinado porto organizado cujos objetivos são: aumentar a segurança e a eficiência da navegação, contribuir para a proteção da vida no mar e apoiar a preservação do meio ambiente. No Brasil, o serviço é regulamentado pela Diretoria de Hidrografia e Navegação (DHN), representante da Autoridade Marítima² (AM). A responsabilidade pela implantação, gestão, operação e coordenação do VTS, bem como a interação com as embarcações participantes e a prestação segura e eficaz do serviço, cabe ao Provedor de VTS, que no Brasil são as Autoridades Portuárias (AP) e os Operadores de Terminais de Uso Privado (TUP).

Após estabelecido, o VTS deve oferecer monitoramento ativo do tráfego aquaviário em uma área marítima designada (Área VTS), cuja visualização é apresentada em tempo real no Centro VTS. Dessa forma, o serviço pode interagir com o tráfego de embarcações e responder rapidamente a situações que ocorram no interior da área de interesse. A eficiência da operação marítima realizada em locais que fornecem segurança ao navegante, aliada ao correto controle do tráfego nas proximidades do porto organizado, agrega notável valor ao serviço portuário, fomentando o comércio e oferecendo condições propícias para o desenvolvimento e expansão das atividades. Este é o motivo pelo qual as companhias administradoras do VTS se empenham no desenvolvimento destes empreendimentos ao redor do mundo.

A abordagem C5IVR refere-se à integração das capacidades de Comando, Controle, Comunicações, Computação, Cibernética, Inteligência, Vigilância e Reconhecimento. O conceito é fundamental para aprimorar a eficácia militar por meio da coordenação eficiente de informações em tempo real, proporcionando uma visão completa do campo de batalha. A estrutura promove a conectividade e interoperabilidade de sistemas, facilitando a rápida tomada de decisões e maximizando a consciência situacional e a adaptabilidade no emprego das Forças Armadas (FA).

¹ Tradução nossa para a sigla VTS—*Vessel Traffic Service*.

² No Brasil, a Lei Complementar n.º 97/1999 estabelece a atribuição subsidiária à Marinha de prover a segurança da navegação aquaviária e designa o Comandante da Marinha, no trato dos assuntos relacionados à atividade, como Autoridade Marítima.

Os elementos essenciais de um VTS assemelham-se, em determinados aspectos, à estrutura utilizada pela sistemática C5IVR para captação e manutenção do fluxo de dados de interesse. Logo, o processo analítico investiga uma alternativa relevante no campo das operações navais e das atribuições subsidiárias da Marinha do Brasil (MB). O emprego destes elementos tem o potencial de oferecer à MB uma opção aprimorada de coordenação estratégica, gestão de informações e resposta a ameaças em tempo real.

Este estudo visa explorar como as ferramentas disponíveis nos sistemas VTS e VTMIS podem ser aproveitadas para o provimento de informações à MB, alinhando-se aos princípios fundamentais C5IVR. A análise pretende demonstrar a viabilidade e os benefícios dessa integração, destacando a importância de uma abordagem consolidada para a eficácia das operações navais e a segurança marítima. Isto posto, pretende-se examinar a aderência que o VTS ou o Sistema de Gerenciamento e Informações do Tráfego de Embarcações³ apresentam em relação à teoria de C5IVR, que podem acarretar incremento expressivo nas estruturas de comando e processo decisório da MB.

A seguir, o capítulo 2 explora o desenvolvimento e a evolução do conceito de C5IVR, desde suas origens no Comando e Controle (C²) até a incorporação dos componentes Computação, Cibernética, Inteligência, Vigilância e Reconhecimento. O capítulo detalha a teoria de *Network Centric Warfare* (NCW) e sua aplicação prática em operações militares modernas.

No capítulo 3 serão examinados os sistemas de monitoramento do tráfego marítimo, incluindo o VTS e o VTMIS e discutidos os elementos essenciais de um sistema VTS, sua regulamentação e implementação no Brasil, e algumas informações acerca da evolução para o VTMIS.

Já o capítulo 4 enfoca a análise da integração das ferramentas C5IVR com os sistemas VTS e VTMIS, utilizando exemplos dos portos de Açu e Vitória. Descreve como essa integração pode melhorar a eficiência e segurança das operações portuárias, além de proporcionar dados valiosos para a inteligência operacional da MB.

Por fim, o capítulo 5 propõe-se a avaliar a relevância das informações obtidas do VTS/VTMIS por meio da integração das ferramentas C5IVR para a inteligência

³ Tradução nossa para a sigla VTMIS—*Vessel Traffic Management Information System*.

operacional da MB. São discutidos os benefícios do compartilhamento de dados, a importância da regulamentação adequada e os desafios associados à implementação de um fluxo contínuo e seguro de informações entre os sistemas.

2 CONCEITO DE C5IVR

O termo C5IVR é a abreviação de Comando, Controle, Comunicações, Computação, Cibernética, Inteligência, Vigilância e Reconhecimento. A teoria em pauta fundamenta-se no conceito de NCW – Guerra Centrada em Redes, tradução nossa – cuja abordagem extrapola a tecnologia empregada, tendo como cerne o comportamento humano e organizacional em um contexto militar. O escopo envolve a adoção de um novo paradigma, conhecido como pensamento centrado em rede, e sua aplicação nas operações militares (Alberts; Garstka; Stein, 2000).

2.1 GUERRA CENTRADA EM REDES

A característica central da NCW é a ênfase na capacidade de criar um alto nível de consciência compartilhada do espaço de batalha, mesmo entre forças geograficamente dispersas, por meio da eficaz vinculação ou conexão do combate, permitindo coordenação e colaboração mais eficientes. Como resultado, a iniciativa permite um aumento no ritmo das operações, maior responsividade, redução de riscos, custos mais baixos e maior eficácia no combate (Alberts; Garstka; Stein, 2000).

Um exemplo prático dessa abordagem é a Operação Tempestade no Deserto durante a Guerra do Golfo⁴ de 1991. As forças da coalizão utilizaram uma combinação de satélites, aeronaves AWACS⁵ e redes de comunicação para manter uma consciência situacional em tempo real, permitindo que os comandantes adaptassem rapidamente as estratégias de combate. Isso resultou em uma coordenação eficiente entre unidades aéreas, terrestres e navais, culminando em uma rápida vitória com mínimas baixas (Eddins, 2021).

Uma ilustração prática desta abordagem é a habilidade de diversas equipes militares trocarem informações em tempo real, possibilitando uma resposta mais ágil

⁴ A Guerra do Golfo (1990–1991) foi um conflito entre uma coalizão internacional liderada pelos EUA e o Iraque, após a invasão do Kuwait pelo Iraque em agosto de 1990. A operação Tempestade no Deserto, esforço principal da campanha, conduziu à rápida expulsão das forças iraquianas do Kuwait, destacando o emprego otimizado da estratégia terrestre e o uso intensivo de tecnologia militar avançada (Eddins, *op.cit.*).

⁵ *Airborne Warning and Control System*: aviões equipados com radares avançados para detectar e monitorar aeronaves, navios e veículos inimigos, proporcionando comando e controle em tempo real para operações militares. Essas aeronaves são essenciais para vigilância aérea e gerenciamento do espaço aéreo em combates (EUA, 2015).

e efetiva às mudanças no campo de batalha. A consciência coletiva do ambiente de combate é crucial para operações *autossincronizadas*⁶ e outras estratégias centradas em rede, que têm como função primordial alcançar os objetivos dos comandantes de forma mais precisa e eficaz (Alberts; Garstka; Stein, 2000).

Além disso, a NCW é adaptável a diferentes missões, tamanhos de força e cenários geográficos, o que a torna aplicável em uma variedade ampla de situações operacionais. Ela também tem o potencial de promover a integração entre os níveis tático, operacional e estratégico da guerra, proporcionando uma visão integrada e coordenada das operações militares em todos os níveis.

A NCW permite a dispersão geográfica das forças militares, superando as limitações históricas de comunicação e movimento. Isso possibilita uma transição de uma abordagem baseada na concentração de forças para uma baseada na concentração de efeitos. Com o aumento das capacidades de sensoriamento e armamentos, não é mais necessário concentrar fisicamente as forças para gerar um efeito concentrado (Alberts; Garstka; Stein, 2000).

Outrossim, a NCW enfatiza a importância do conhecimento das próprias forças, derivado de uma compreensão compartilhada do teatro de operações e da intenção dos comandantes. Uma força bem-informada pode se autossincronizar, ser mais discreta e ser mais eficaz quando operar autonomamente (Alberts; Garstka; Stein, 2000).

A eficácia da NCW depende da ligação entre as entidades no espaço de batalha, permitindo a geração de sinergias e a realocação dinâmica de responsabilidades. Isso requer uma infraestrutura de informação robusta e de alto desempenho, que forneça acesso a serviços de informação de alta qualidade para todos os elementos da empresa de combate (Alberts; Garstka; Stein, 2000).

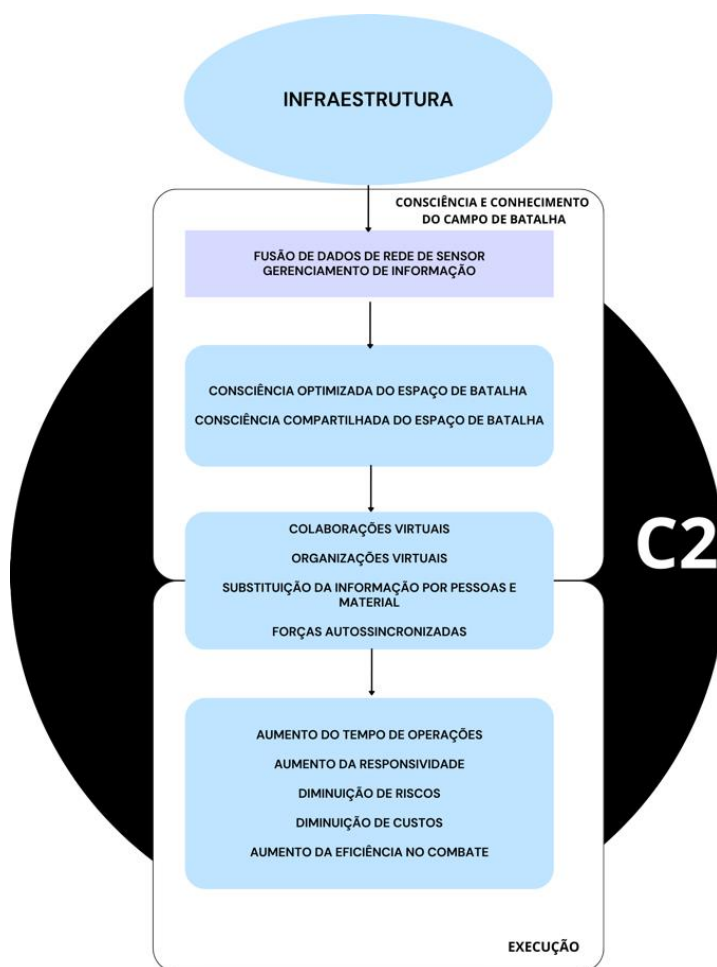
A Figura 1 a seguir representa a conexão entre os elementos fundamentais para a geração de poder de combate no modelo centrado em redes. O ponto de partida é a infraestrutura de informação⁷, que permite a criação de uma consciência

⁶ Operações *autossincronizadas* são aquelas as quais as unidades podem tomar decisões táticas e operacionais de forma autônoma, alinhando-se com os objetivos estratégicos gerais estabelecidos pelos comandos superiores, graças a um entendimento compartilhado da situação, objetivos claros e comunicação eficaz (Alberts; Garstka; Stein, *op.cit.*).

⁷ Conceito derivado do inglês *infostructure*, refere-se à capacidade de comunicações e computação de alto desempenho que fornece acesso a fontes de informação adequadas e permite interações contínuas entre entidades no campo de batalha, promovendo a consciência situacional e a colaboração. Ela é essencial para conectar entidades que desempenham funções de detecção, decisão e ação, contribuindo para a eficiência operacional (Alberts; Garstka; Stein, *op.cit.*).

e conhecimento compartilhados sobre o campo de batalha. Essa consciência e conhecimento são utilizados por novas abordagens adaptativas de comando e controle, além de forças *autossincronizadas* (Alberts; Garstka; Stein, 2000).

Figura 1 - A Organização Militar como um Organismo Centrado em Rede



Fonte: Elaborado pelo autor com base em Alberts; Garstka; Stein (2000).

Embora a NCW seja uma abordagem flexível e adequada para a era da informação, é importante notar que o termo pode ser mal interpretado como focado apenas em redes de comunicação, quando, na verdade, se trata de uma resposta militar mais abrangente baseada na fluidez das interações no espaço de batalha e no acesso a informações aprimoradas, valendo-se do poder da tecnologia e da colaboração para aprimorar a eficácia e a eficiência das operações militares (Alberts; Garstka; Stein, 2000).

2.2 O DESENVOLVIMENTO DO C²IVR

Os conceitos de C² foram desenvolvidos principalmente no contexto militar, especialmente durante e após a Segunda Guerra Mundial (1939–1945). Embora os princípios referentes ao assunto existam há séculos, a formalização e sistematização desses conceitos ocorreram ao longo do século 20, particularmente durante a Guerra Fria, em resposta à crescente complexidade dos conflitos e aos avanços tecnológicos em comunicação e informação.

Comando, em todos os níveis, é a arte de motivar e dirigir pessoas e organizações para a ação a fim de cumprir missões, e Controle é gerir e direcionar forças e funções consistentemente com a autoridade de comando de um comandante. O controle de forças e funções auxilia os comandantes e equipes a computar requisitos, alocar meios e integrar esforços. O comando de uma missão é o método preferido para o exercício de C² (EUA, 2017, p. I-18, tradução nossa).

Essas definições evoluíram ao longo do tempo, especialmente com a introdução de novas tecnologias e a necessidade de maior coordenação em operações militares complexas. A formalização desses conceitos é frequentemente associada ao desenvolvimento de doutrinas militares durante a Guerra Fria.

Diversas instituições e indivíduos contribuíram para o desenvolvimento dos conceitos de C². Nos Estados Unidos (EUA), o Departamento de Defesa (tradução nossa para *Department of Defense* – DoD) e as FA desempenharam papéis cruciais na refinação e implementação desses conceitos. Neste ínterim, ressalta-se a publicação, em 1941, do manual de campo do Exército dos EUA (FM 100–5), que detalhou as doutrinas de C². Esse manual, aliado a outros documentos doutrinários, contribuiu para a formalização e disseminação dos conceitos de C² (EUA, 1993).

Da mesma forma, o uso de sistemas de rádio e outras tecnologias de comunicação militar se tornou vital durante a Segunda Guerra Mundial. Um evento marcante foi o desenvolvimento e a utilização dos sistemas de criptografia Enigma pela Alemanha e sua subsequente ruptura pelos Aliados, o que destacou a importância das comunicações seguras e eficientes (Alberts; Hayes, 1995). A Comunicação, então, refere-se ao processo de transmissão e recepção de informações críticas entre diversas unidades e sistemas, proporcionando coordenação, consciência situacional e tomada de decisão eficaz em operações militares (EUA, 2017).

A formalização da Inteligência como componente essencial das operações militares ocorreu durante a Guerra Fria. Um marco foi a criação da *Central Intelligence Agency* (CIA) em 1947, que sistematizou a coleta e análise de informações para apoiar a tomada de decisões estratégicas (Lowenthal, 2009). A Inteligência abrange a coleta, análise e disseminação de informações sobre o ambiente operacional e as atividades inimigas para apoiar a tomada de decisões e as operações (EUA, 2013).

A evolução do Reconhecimento começou com câmeras em aviões U-2 nos anos 1950, passando para satélites na era espacial, e incorporando imagens infravermelhas durante a Guerra do Vietnã. Reconhecimento é a obtenção e análise de informações sobre adversários, utilizando tecnologias como sensores de imagem, RADAR e inteligência de sinais. Visa fornecer dados precisos em tempo real para apoiar decisões estratégicas e operacionais, garantindo a superioridade informacional e o sucesso das missões militares (Demirtas; Turk; Ozer, 2014).

O sistema de Vigilância contínua se tornou crítico durante a Guerra Fria com a introdução de tecnologias avançadas. Um evento significativo foi o lançamento do primeiro satélite espião da série Corona pelos EUA em 1960, que permitiu a coleta de imagens de alta resolução de territórios inimigos (McCurdy, 1997). Entende-se por Vigilância como o monitoramento contínuo de áreas e atividades específicas para detectar e rastrear ameaças ou mudanças no ambiente operacional, fornecendo dados em tempo real para as forças militares (EUA, 1999).

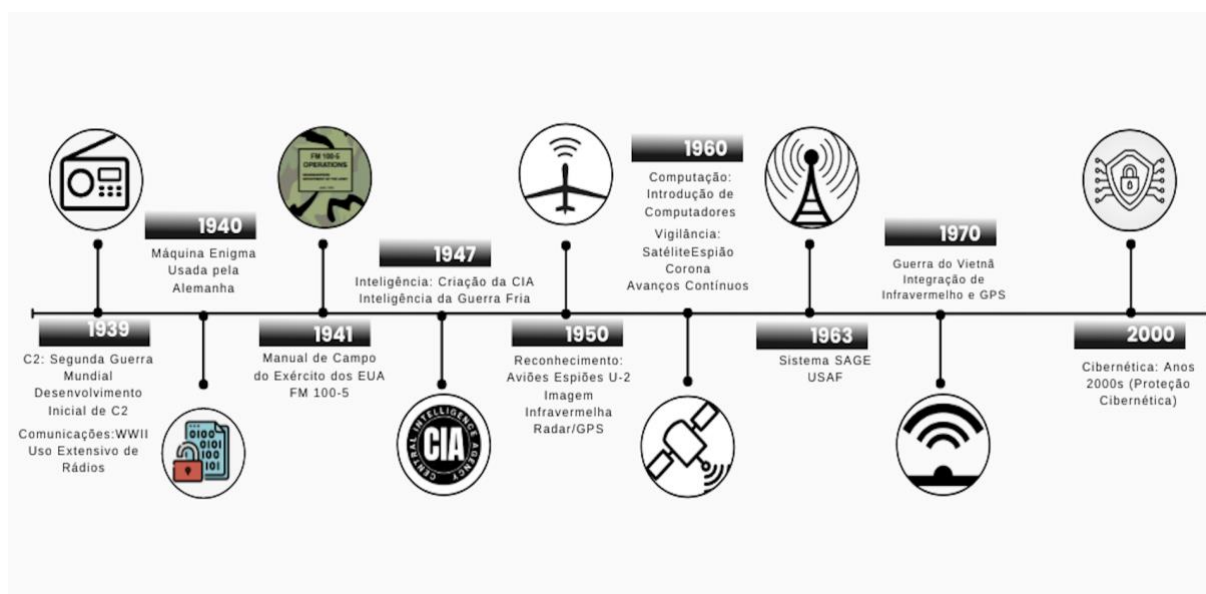
A integração da computação nas operações militares começou ainda na década de 1960. Um evento notável foi o desenvolvimento do Ambiente Terrestre Semiautomático (tradução nossa para *Semi-Automatic Ground Environment* – SAGE) pela Força Aérea dos Estados Unidos (USAF), operacional em 1963, que utilizou computadores para integrar dados de radares e coordenar a defesa aérea (Czerwinski, 1996). Nesse ínterim, Computação designa a infraestrutura tecnológica indispensável para o processamento, armazenamento e transmissão de informações críticas em operações de comando e controle. Este conjunto abrange servidores robustos, data centers e unidades de processamento tático, que asseguram a análise eficiente de dados e a disponibilização de informações em tempo real aos decisores (Alghamdi, 2009).

O conceito de Cibernética foi incorporado ao acrônimo no início dos anos 2000. Com o progresso das tecnologias de informação e comunicação, a proteção

das redes e dos sistemas de informação contra ameaças cibernéticas tornou-se imprescindível (Zubairi; Mahboob, 2012). A cibernética diz respeito ao estudo e aplicação de sistemas automatizados de controle e comunicação, integrando redes de informação visando aprimorar a eficiência e a segurança das operações (Alberts; Hayes, 2003).

Como resultado dessa evolução, o termo culminou em C5IVR e, na literatura moderna, admite alterações contínuas que extrapolam o escopo deste estudo, podendo resumir-se a C“n”IVR, conforme a perspectiva a ser adotada. Abaixo encontra-se uma linha do tempo simplificada a fim de ilustrar o aparecimento dos conceitos apresentados:

Figura 2 – Linha do tempo do desenvolvimento C5IVR



Fonte: Elaborado pelo autor.

2.3 ESTRUTURAÇÃO DO SISTEMA

A digitalização das FA representa o primeiro passo para a modernização de um sistema centrado em rede. Este conceito envolve a integração de soluções tecnológicas estabelecidas em um sistema de informações, de modo a compartilhar dados obtidos ao longo das diferentes fases de coleta e análise, maximizando o timing operacional. A digitalização também implica a unificação dos diferentes sistemas C² utilizados pelas FA e, sempre que possível, a consolidação dos diversos

meios empregados pela Marinha, Força Aérea e Exército, reunindo-os em uma única rede para disponibilizar informações ao vivo do teatro de operações (Laterza; Cabral, 2022).

Os sistemas de informações táticas em rede fornecem inteligência em tempo real, permitindo que as unidades na Área de Operações obtenham uma consciência situacional tática de seu entorno imediato. Este sistema capacita o comandante da unidade a tomar decisões informadas sobre o emprego dos recursos disponíveis. No Estado-Maior, o planejamento das operações é fundamentado em informações atualizadas, possibilitando um controle e coordenação eficazes das operações no campo de batalha. Essas ações podem ser realizadas em tempo presente com base nas informações fornecidas por diversos sistemas, aumentando a eficácia em combate e reduzindo as perdas (Laterza; Cabral, 2022). Um exemplo concreto é o uso do sistema *Blue Force Tracking* (BFT) pelos EUA no Afeganistão (2002) e no Iraque (2003). Esse sistema permitiu que os comandantes rastreassem a localização das tropas amigas durante as manobras, aperfeiçoando a coordenação e reduzindo incidentes de fogo amigo. Ademais, a integração com Aeronaves Remotamente Pilotadas (ARP) forneceu reconhecimento contínuo, permitindo uma resposta mais rápida às ameaças emergentes (Sweeney, 2008).

O termo “Operações de Vários Domínios” (tradução nossa para *Multi-Domain Operations* – MDO) emergiu recentemente para descrever a condução das batalhas nas cinco dimensões (ar, terra, mar, espaço e ciberespaço) operadas pelas forças militares. Tais operações são coordenadas simultaneamente a partir de um centro de comando que integra as capacidades de atuação em todos os domínios, como um único campo de batalha (Laterza; Cabral, 2022).

A agilidade da troca de dados informacionais, em tempo real, entre as diversas estruturas de comando e unidades de combate que operam no sistema MDO é essencial para o desempenho eficaz das unidades operativas. Este sistema representa o componente mais relevante e estratégico de toda a estrutura de comando de uma força. A garantia de sua eficácia pode ser obtida por meio da escolha de uma arquitetura de troca de dados ideal. Nesse contexto, é imperativo montar uma estrutura flexível de interação e gestão operacional, considerando que as operações serão realizadas em um ambiente dinâmico e com recursos limitados (Laterza; Cabral, 2022).

A fim de se contrapor às ameaças existentes e garantir a operacionalidade dos recursos supracitados, é de fundamental importância que o sistema C5IVR seja robusto, flexível, redundante e confiável. Os principais sensores empregados na estrutura do sistema estão simplificados na tabela 1 a seguir:

Tabela 1 - Estrutura C5IVR

COMPONENTE	DESCRIÇÃO	EXEMPLOS
Sensores de Imagem	Câmeras de alta resolução e sensores infravermelhos para coleta de imagens.	Câmeras de vigilância, drones de reconhecimento.
Sensores de Radar	Dispositivos que usam ondas de rádio para detectar e localizar objetos.	Radares de busca aérea, radares marítimos.
Sensores de Inteligência de Sinais (SIGINT)	Equipamentos que interceptam comunicações e sinais eletrônicos.	Sistemas SIGINT, receptores de comunicação.
Sensores Acústicos	Dispositivos que capturam sons submarinos e terrestres.	Hidrofones, sensores acústicos terrestres.
Sensores de Movimento	Detectores de movimento que monitoram atividades em uma área especificada.	Sensores infravermelhos, sistemas de vigilância perimetral.
Computadores	Infraestrutura para processar, armazenar e transmitir informações.	Servidores, data centers, unidades de processamento tático.
Redes de Comunicação	Meios de comunicação que permitem a troca de dados entre os componentes do sistema.	Redes de fibra óptica, satélites de comunicação, rádios estáticos.
Defesas Cibernéticas	Sistemas para proteger a infraestrutura de ciberataques.	Firewalls, sistemas de detecção e prevenção de intrusões (IDS/IPS), software antivírus.
Pessoal	Equipes que operam e mantêm o sistema.	Operadores de sistemas, analistas de inteligência, técnicos de manutenção.
Procedimentos	Normas e diretrizes que regulam as operações do sistema.	Protocolos de resposta a incidentes, manuais de operação, normas de segurança.
Sistemas de Comando e Controle	Plataformas que facilitam o comando e controle das operações.	Centros de Comando e Controle (C2), sistemas de gestão de batalha, consoles de operação.
Inteligência	Coleta e análise de informações para suporte à decisão.	Análise de sinais (SIGINT), análise de imagens (IMINT), análise de comunicações (COMINT).
Vigilância	Monitoramento contínuo de áreas de interesse.	Sistemas de vigilância por satélite, drones de vigilância aérea, sistemas de vigilância costeira.
Reconhecimento	Identificação e análise de objetos e atividades relevantes.	Drones de reconhecimento, veículos de reconhecimento terrestre, operações de patrulha.

Fonte: Elaborado pelo autor.

3 FUNÇÃO PRIMORDIAL DO SISTEMA VTS E VTMIS

Os sistemas de monitoramento do tráfego marítimo, bem como suas diretrizes e padrões, são estabelecidos pela *International Association of Marine Aids to Navigation and Lighthouse Authorities* (IALA) com o intuito de elevar a segurança e eficiência da navegação. O foco recai sobre os diferentes níveis de complexidade tecnológica desses sistemas, começando pelo Serviço Portuário Local (LPS) até os mais avançados, como o VTS e o VTMIS. Será analisado como essas tecnologias se inter-relacionam e evoluem para proporcionar uma gestão integrada e eficiente do tráfego marítimo, beneficiando as atividades econômicas portuárias e contribuindo para a segurança e proteção ambiental.

3.1 OS SISTEMAS DE MONITORAMENTO DO TRÁFEGO MARÍTIMO

A IALA⁸, autoridade internacional relacionada ao tema de “Informações de Auxílio à Navegação”, estabelece diretrizes e padrões para o desenvolvimento de dispositivos, sistemas e serviços que são externos às embarcações, projetados para melhorar a navegação segura e eficiente de embarcações individuais e do tráfego marítimo. Os sistemas de monitoramento de embarcações são empregados para a gestão de tráfego em áreas marítimas específicas, especialmente em portos, e têm o potencial de gerar vantagens significativas tanto para as atividades econômicas e produtivas desenvolvidas nos portos (Silva, 2023).

O LPS é o sistema de monitoramento de embarcações de menor complexidade tecnológica. Atua como recurso de coordenação dos serviços portuários, disseminando informações essenciais para a gestão das atividades do porto. Esse serviço representa o nível básico e fundamental dos sistemas de monitoramento de embarcações, sendo considerado a primeira etapa para que uma

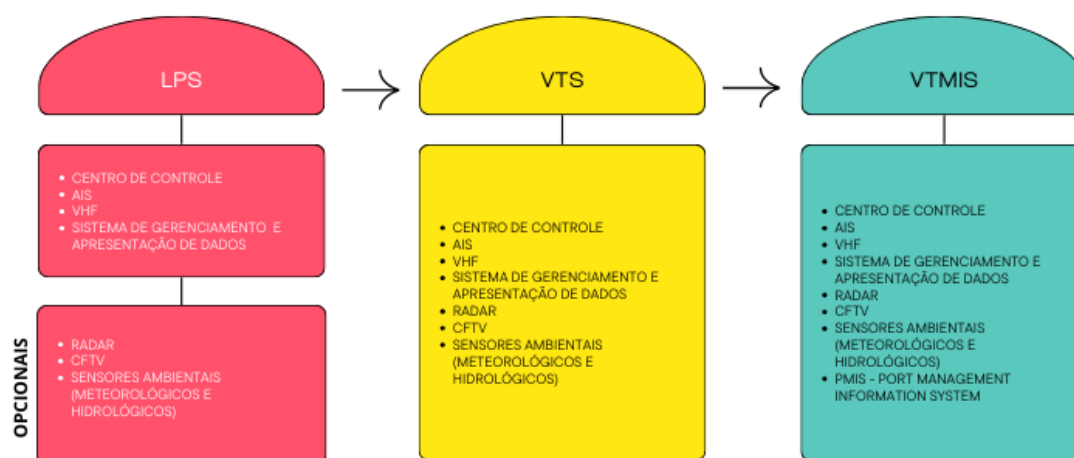
⁸ A IALA é uma associação técnica internacional sem fins lucrativos, fundada em 1957, que reúne autoridades de navegação, fabricantes, consultores e institutos de treinamento de todo o mundo para trocar experiências e harmonizar as ajudas à navegação marítima. Mediante comitês técnicos, a IALA desenvolve práticas recomendadas e padrões para garantir a segurança e eficácia do tráfego marítimo, contribuindo para a redução de acidentes e a proteção do meio ambiente. Além disso, promove a cooperação internacional para ajudar nações em desenvolvimento a estabelecer redes de navegação seguras (IALA, 2024b).

Autoridade Portuária (AP)⁹ ou órgão responsável possa gerenciar navios, cargas e serviços portuários. A configuração e definição são realizadas pela AP conforme as necessidades e complexidade das operações do porto, não seguindo padrões e normas internacionais estabelecidos por autoridades competentes. Quando aprimorado com tecnologias adicionais que ampliam sua capacidade, o LPS evolui para uma nova categoria de sistemas, passando então a ser regulamentado por normativas internacionais (Silva, 2023).

Os dois tipos de sistemas de monitoramento de embarcações mais elaborados serão objeto de estudo do presente trabalho e explicitados detalhadamente mais a frente: VTS e o VTMISS, que possui a característica de ser uma ampliação do VTS (Silva, 2023).

As três estruturas apresentadas possuem uma relação progressiva entre si, significando que estão correlacionadas pelo grau de desenvolvimento dos elementos em seus respectivos escopos, como sistemas, equipamentos e funcionalidades. Sendo assim, um LPS, quando equipado com mais sistemas e capacidades, evolui para um VTS, que, ao ser ainda mais aprimorado, transforma-se em um VTMISS. A Figura 3, extraída de Villas-Bôas (2022), ilustra de forma prática esta progressão, resumindo o conjunto de equipamentos e tecnologias que caracterizam cada um dos três tipos de sistemas de monitoramento de embarcações discutidos: LPS, VTS e VTMISS (Silva, 2023).

Figura 3 – Comparação entre LPS, VTS e VTMISS



Fonte: Elaborado pelo autor com base em Villas-Bôas (2022).

⁹ Autoridade Portuária é a entidade competente local responsável pela gestão e coordenação de um determinado empreendimento portuário (Silva, *op.cit.*).

3.2 VTS

A Organização Marítima Internacional (OMI), ao regular o planejamento, a implementação e a operação dos VTS, tem a responsabilidade de fornecer orientações sobre sua criação, funcionamento, qualificação e treinamento. Tais atribuições envolvem liderar a criação de um fórum e uma estrutura para a cooperação entre Governos, visando a prestação uniforme e harmonizada dos VTS globalmente. A IALA é reconhecida como uma colaboradora significativa nas funções e responsabilidades da OMI em relação aos VTS (OMI, 2021).

Ao seguir tais Diretrizes, os Governos Contratantes devem considerar os instrumentos aplicáveis da OMI e consultar as orientações internacionais pertinentes elaboradas e publicadas por organizações internacionais competentes (OMI, 2021). No Brasil, a AM é a responsável por estabelecer todo o arcabouço regulatório para a implantação e operação do serviço conforme a legislação nacional e internacional, e a Diretoria de Hidrografia e Navegação (DHN), como sua representante, tem a delegação de licenciar a implantação e autorizar a operação, fiscalizando o cumprimento por parte das empresas aderentes (Marinha do Brasil, 2023).

Em virtude de sua habilidade para identificar, monitorar e auxiliar no planejamento das movimentações de embarcações, bem como na disseminação de informações e assistência aos navegantes, o Sistema VTS contribui significativamente para: a salvaguarda da vida humana no mar, a segurança da navegação, o aumento da eficiência do tráfego marítimo, a prevenção da poluição marítima e adoção de medidas de emergência antipoluição e a proteção das comunidades e infraestruturas contíguas à Área VTS¹⁰ (Marinha do Brasil, 2023, pp. 1-1 e 1-2).

Os VTS são enquadrados pela IALA como um Auxílio à Navegação, e disponibilizado para auxiliar na determinação da posição das embarcações, alertar sobre perigos que afetem a segurança ou fornecer informações que auxiliem na tomada de decisão a bordo (Marinha do Brasil, 2023, p. 1-2).

¹⁰ Área VTS é a área delimitada e formalmente declarada, na qual o Provedor de VTS está legalmente autorizado a prestar o serviço de tráfego de embarcações. Pode ser dividida em subáreas ou setores, limitados ao menor número possível, para não dificultar a compreensão do quadro geral do tráfego por parte do operador (Marinha do Brasil, *op.cit.*).

Por definição da Convenção Internacional das Nações Unidas sobre o Direito no Mar (CNUDM), o VTS somente ensejará o cumprimento obrigatório por parte do usuário em águas interiores (Nações Unidas, art. 2º e art. 21) e em seu mar territorial (Nações Unidas, art. 2º e art. 21). Todavia, se o Provedor de VTS¹¹ considerar que uma ampliação da área de cobertura para além dos limites do mar territorial contribuirá para o ordenamento do tráfego, segurança da navegação ou prevenção da poluição hídrica, encaminhará uma proposta justificada para análise da Autoridade Competente. Nesta hipótese, ainda que a proposta seja aprovada, a participação dos usuários na área marítima além do mar territorial será voluntária e, apenas sob essa condição, os navegantes deverão cumprir integralmente as instruções do VTS (Marinha do Brasil, 2023, p. 1-2).

Em uma área VTS, as embarcações participantes devem fornecer os relatórios ou informações solicitadas pelo serviço, considerar as informações e avisos emitidos, obedecer às instruções e requisitos do VTS, salvo razões de segurança ou proteção ambiental contrárias e reportar qualquer poluição ou perigo à navegação ao VTS. Navios não designados como participantes podem integrar-se ao VTS, caso atendam aos requisitos e orientações estabelecidos pelo provedor do sistema. Os comandantes podem ser interpelados sobre suas ações caso optem por desconsiderar qualquer instrução do VTS (OMI, 2021).

O provedor de VTS deve assegurar que o VTS esteja consoante as regulamentações estabelecidas pela autoridade competente, definir objetivos operacionais que promovam a segurança e a eficiência do tráfego marítimo, além da proteção ambiental, avaliando periodicamente esses objetivos para garantir seu alcance. Deve ainda garantir a disponibilização de equipamentos, sistemas e instalações adequados para a execução do VTS, certificar-se de que o VTS esteja adequadamente equipado com pessoal qualificado e devidamente treinado, e garantir que as informações sobre os requisitos e procedimentos do VTS, bem como as categorias de navios que devem participar, sejam disseminadas em publicações náuticas apropriadas. Cabe ressaltar que a responsabilidade última do comandante sobre todos os aspectos relativos à operação do navio, incluindo a responsabilidade pela navegação segura, permanece incólume (OMI, 2021).

¹¹ Provedor de VTS - Organização ou entidade responsável pela implantação, gestão, operação e coordenação das atividades do VTS, sua interação com os usuários e prestação segura e eficaz do serviço. No Brasil, tais atribuições são das AP ou Operadores de TUP que implantarem o serviço, mediante autorização da Autoridade Competente (Marinha do Brasil, *op.cit.*).

Um projeto de implantação de VTS pode ser desenvolvido por iniciativa da MB, da AP ou de Operador de TUP¹² isolado. É desejável que as orientações internacionais e nacionais relevantes sobre gerenciamento de projetos sejam consideradas para a confecção, execução e acompanhamento dos projetos de implantação de VTS (Marinha do Brasil, 2023).

A maioria dos incidentes de navegação são atribuídos a erro humano (IALA, 2024, p.10). Sendo assim, a utilização de serviços providos por um centro VTS pode ser de extrema valia, contribuindo para a prevenção de acidentes e no processo de tomada de decisão dos comandantes, como se prova em diversos portos do mundo (Escola de Guerra; Fundação Ezute, 2021).

Dessa forma, as benesses advindas da operação de um VTS contribuem sobremaneira com o desenvolvimento portuário e a sistematização do tráfego aquaviário nas adjacências do porto organizado. Essas características ensejam a expansão e a exploração dessa atividade ao redor do mundo, e em especial no Brasil, acarretando aumento da consciência situacional e da segurança da navegação.

3.2.1 Elementos de um Sistema VTS

Os elementos básicos de funcionamento de um VTS variam em função do volume e do tráfego na área de operação, como também dos perigos à navegação existentes e das condições geográficas, culminando com a delimitação da Área VTS. Necessidades específicas do sistema, como a cobertura de um setor por um RADAR serão objeto de uma avaliação holística da finalidade do serviço, em termos de expectativa dos usuários e nível de segurança almejado (Marinha do Brasil, 2023, p. 2-3).

A análise deve iniciar por meio de um levantamento das condições da área e dos locais disponíveis para encontrar a posição mais vantajosa tecnicamente. Estes aspectos irão definir os requisitos específicos de cada VTS instalado e determinar o seu desempenho final. Diretrizes gerais de alto nível podem ser estabelecidas para orientar os requisitos essenciais dos componentes de um VTS, podendo ser de grande utilidade na fase de implementação (Marinha do Brasil, 2023, p. 2-3).

¹² Terminal de Uso Privado (TUP): instalação portuária explorada mediante autorização e localizada fora da área do porto organizado (Brasil, 2013).

Os requisitos operacionais, estabelecidos a partir do processo de análise de necessidades que serão atendidas com a implantação de um VTS, constituem a base para todo o ciclo de vida do sistema e definição dos requisitos técnicos a serem adotados. Muitos aspectos são considerados neste processo, ressaltando-se a área de cobertura, os riscos à navegação, o compartilhamento de informações, a segurança cibernética, entre outros (Marinha do Brasil, 2023, p. C-1).

Após a realização de uma avaliação dos riscos, o Provedor de VTS estabelecerá metas para disponibilidade e confiabilidade do sistema que será implantado. De posse destas metas, pode-se enumerar os principais dispositivos que integram o VTS (IALA, 2022):

- a) RADAR: sensor ativo mais importante de um VTS. Deve operar simultaneamente para curtas e longas distâncias. Pode ser instalado em diferentes locais com superposição de cobertura em setores de uma Área VTS ou mais de um instalado em um mesmo local fim garantir redundância de sensores.
- b) Circuito Fechado de Televisão (CFTV): pode atuar como complemento aos sistemas de comunicação para localização e identificação dos alvos em locais onde existem restrições ao RADAR, como em vias fluviais. Outrossim, a instalação de câmeras corretamente posicionadas pode contribuir para a identificação e monitoramento a curto alcance.
- c) Sistemas de radiocomunicações (VHF e HF): toda a Área VTS deve estar coberta por, pelo menos, um dos sistemas de radiocomunicação disponíveis no Centro VTS¹³.
- d) Radiogoniômetro: equipamento utilizado para correlacionar a fonte de uma transmissão com um determinado alvo e, com isso, contribuir para a identificação de embarcações e operações SAR.
- e) Sistema de Identificação Automática (AIS)¹⁴: contribui para a identificação das embarcações, acompanhamento dos alvos, troca de mensagens e fornecimento de informações de interesse. Tem importância fundamental na

¹³ Centro VTS - local de operação do VTS, podendo ser dividido em sub-centros, caso julgado conveniente pelo Gerente do VTS (Marinha do Brasil, *op.cit.*).

¹⁴ O Sistema de Identificação Automática, tradução nossa da sigla AIS (*Automatic Identification System*), é um sistema de identificação de navios que, dentro do escopo do VTS, tem o propósito de contribuir para a identificação de embarcações, acompanhamento de alvos e simplificação da troca de informações, reduzindo os contatos por radiotelefonia e fornecendo dados básicos de navegação e outras informações de interesse (Marinha do Brasil, *op.cit.*).

compilação do quadro tático da Área VTS, ao proporcionar a solução para dois problemas do RADAR convencional: a identificação de embarcações ocultadas por curvas ou obstáculos, e a detecção de alvos desvanecidos em virtude de mar grosso ou chuva forte. Sua principal desvantagem é que algumas embarcações de pequeno porte e de lazer possuem a instalação facultativa deste equipamento (AIS classe B).

- f) Sistema Eletro-óptico (EOS): consistem em dispositivos de imagem, tais como câmeras de CCTV e infravermelhas. Pode auxiliar sobremaneira no aumento da consciência situacional do operador (VTSO) em tempo real, caso esteja integrado ao software de gerenciamento de dados do Centro VTS.
- g) Sensores ambientais: possuem importância primordial no monitoramento e controle das questões ambientais, tais como: detecção precoce de incidentes de poluição e coleta de dados meteorológicos.
- h) Sistemas de apresentação de dados: o sistema deve ser compatível com as Cartas Náuticas Eletrônicas oficiais.
- i) Sensores de longo alcance: além do RADAR HF pode ser utilizado o RADAR de abertura sintética baseado em satélite (tradução nossa para *Satellite SAR*).
- j) Sistemas: Satélite AIS (SAIS) e Identificação e Rastreamento de Longo Alcance (LRIT) (Marinha do Brasil, 2023).

3.3 VTMISS

O VTMISS é uma expansão do VTS, como um Sistema Integrado de Vigilância Marítima, que possibilita aos Serviços Aliados¹⁵ e a outros setores da empresa fornecedora do VTS o compartilhamento direto de dados ou o acesso a determinados subsistemas, com o fito de aumentar a efetividade das operações portuárias e das atividades marítimas em geral (Marinha do Brasil, 2023, p. 4-2).

Os sistemas de gerenciamento dos portos, assim como sistemas dedicados à segurança portuária, apoio às operações da Polícia Marítima (repressão a ilícitos

¹⁵ Serviço Aliado: serviço existente nas áreas portuárias e envolvido na passagem segura e eficiente do navio pela Área VTS, podendo, a critério da AP ou Operador de TUP, receber e utilizar os dados produzidos pelo VTS para realizar de forma mais eficaz sua tarefa (Marinha do Brasil, *op.cit.*).

contra navios, contrabando, narcotráfico, entre outros) são alguns exemplos dos possíveis usuários dos dados compartilhados do VTS. No caso do VTMISS, a AM tem sua atuação direcionada apenas para o Auxílio à Navegação, representado pelo VTS, e os benefícios que poderá trazer ao navegante em termos de segurança da navegação, ordenamento do tráfego e proteção ao meio ambiente marinho. Neste escopo, os dados produzidos no VTS deverão ser disponibilizados com os Representantes da Autoridade Marítima (AAM) (Marinha do Brasil, 2023, p. 4-2).

No que diz respeito ao VTMISS, a definição dos Serviços Aliados e dos setores do porto que receberão e processarão os dados compartilhados provenientes do VTS é uma responsabilidade do provedor do serviço. A atuação da AM, que inclui a normatização, homologação e fiscalização do serviço, é limitada exclusivamente ao VTS (Marinha do Brasil, 2023, p. 4-3).

3.3.1 Elementos de um VTMISS

Segundo a NORMAM-602, a estrutura de um VTMISS assemelha-se à de um VTS, sendo composta por itens obrigatórios do sistema VTS, radares de diversas ordens, em especial, de vigilância marítima e *transponders* do AIS. Podem ainda ser adicionados sensores eletro-ópticos e câmeras, comunicações por voz e dados e redes de comunicações remotas, seguras e integradas (Marinha do Brasil, 2023).

Embora apresentado com possibilidades superiores nas publicações referenciadas acima, durante o processo de pesquisa desse trabalho não foi encontrada argumentação suficiente, na prática, que classifique esse sistema em um nível acima do VTS. Portanto, para efeito das análises e considerações subsequentes, será utilizado, preponderantemente, o VTS como modelo de estrutura padrão para o estudo de relevância das informações obtidas e as propostas de intercâmbio de dados com a MB.

4 INTEGRAÇÃO DE FERRAMENTAS C5IVR COM O SISTEMA VTS

Antes de discriminar os mecanismos que podem ser aplicados na interface entre aspectos do conceito C5IVR e o sistema VTS, serão examinados alguns aspectos do desenvolvimento e implantação dos serviços de tráfego de embarcações no país. O estabelecimento desses serviços no Brasil, especialmente nos portos de Açu e Vitória, destaca-se pela utilização de tecnologias avançadas que não apenas promovem a segurança da navegação, como também oferecem incremento significativo às operações portuárias. Possibilidades de integração, identificação de ferramentas de ambos os sistemas, sua aplicação e interoperabilidade, assim como meios de compartilhamento de dados de interesse com a MB são de suma importância para criticar a viabilidade da proposta desta dissertação e serão relacionados a seguir.

4.1 BREVE HISTÓRICO SOBRE A IMPLEMENTAÇÃO DO SISTEMA VTS E VTMS NO BRASIL

Ainda que alguns portos brasileiros tenham iniciado o processo de implementação do VTS e do VTMS, a presente dissertação abordará restritamente os ensinamentos obtidos com os portos de Açu e Vitória, pioneiros na homologação e utilização dos sistemas.

O Porto do Açu, situado ao norte do estado do Rio de Janeiro, obteve a licença de operação para o VTS em 3 de dezembro de 2015, obtendo significativos resultados com relação à eficiência e segurança na movimentação de embarcações. Os principais dispositivos da estrutura VTS naquele porto são: AIS, RADAR Terma Scantec 5102 (Banda-X), Sistemas de comunicação (transceptor VHF), Sistema meteorológico¹⁶, câmeras de monitoramento (circuito fechado de TV – CCTV e câmeras térmicas), boias, faróis e sistema de gerenciamento de tráfego “NAVI HARBOUR”¹⁷ (Gomes, 2024).

¹⁶ Compõem o referido sistema: 9 estações de monitoramento, um sistema de dados meteorológicos, um sistema de previsão meteorológica e sensores (Gomes, *op.cit.*).

¹⁷ O sistema, da empresa Wärtsilä, fornece uma visão integrada da situação do tráfego em qualquer área coberta pelo sistema de monitoramento VTS ou AIS existente. Isso ajuda a manter total consciência situacional, economizando tempo e custos (Wärtsilä, 2024, tradução nossa).

O VTS do Porto do Açú abrange uma área de monitoramento de 400 km², estendendo-se até 12 milhas náuticas da costa, permitindo o monitoramento contínuo do mar territorial adjacente ao do porto organizado. Cabe ressaltar que os sistemas e serviços de tráfego de embarcações já são amplamente utilizados por diversos portos ao redor do mundo, com estruturas e aparatos bem mais complexos e eficientes, acarretando incrementos significativos na eficácia da operação com benefícios diversos para a economia e para os próprios Estados (Silva, 2023).

A figura 4 ilustra as principais instalações do VTS do Porto do Açú:

Figura 4 - Instalações do Centro VTS no Porto do Açú



Fonte: DefenSea Consultoria (2016).

O Porto de Vitória, localizado na capital do estado do Espírito Santo, iniciou a operação do VTMS em 2017 (Vports, 2023). O sistema integra informações de diferentes fontes em um único programa, abrangendo tanto as embarcações quanto as instalações portuárias. Seus componentes incluem: RADAR, sensores meteoceanográficos (mareógrafos, correntômetros, medidores de ondas, boia AtoN¹⁸ e estações meteorológicas), AIS, câmeras de alta definição de médio alcance e térmicas de longo alcance e software de controle de tráfego Navi-Harbour 4.6 VTS 3D (Sopesp, 2021). A Figura 5 apresenta o Centro de Controle Operacional (CCO) do VTMS Vitória com suas câmeras e sensores em funcionamento:

¹⁸ *Aids to Navigation* (Auxílios à Navegação) – são dispositivos, sistemas ou serviços externos às embarcações, projetados e operados para promover a navegação segura e eficiente de navios e tráfego de embarcações (IALA, 2024, tradução nossa).

Figura 5 - CCO do VTMS Vitória



Fonte: Portal Portuario (2022).

A principal distinção entre o VTS e o VTMS reside no desenvolvimento e implantação de um Sistema Integrado de Vigilância Marítima, que possibilita o intercâmbio imediato dos dados de tráfego de embarcações e das condições ambientais, hidrológicas e meteorológicas na Área de Responsabilidade do VTMS com serviços aliados e outras agências interessadas. O objetivo é o incremento substancial das operações portuárias e das atividades marítimas em geral. No Brasil, os principais *stakeholders*¹⁹ incluem a AM e AP, a Polícia Federal, a Receita Federal, a ANVISA, o IBAMA, o IEMA, a Praticagem e os gestores de terminais privados, entre outros (Escola de Guerra Naval; Fundação Ezute, 2021).

Embora a ampla gama de possibilidades obtidas com o emprego da ferramenta C5IVR tenha sido concebida no âmbito do mundo militar, objetivando o cumprimento de missões em operações de guerra, cabe expandir a análise para o contexto do mundo globalizado, disruptivo e multifacetado. Não é difícil imaginar que plataformas altamente eficazes e conectadas em tempo real possam ser utilizadas em outros campos com resultados promissores.

As oportunidades de ganhos tangíveis e intangíveis da operação do VTS e VTMS também oferecem aptidão para beneficiar várias outras áreas relacionadas à

¹⁹ Partes interessadas envolvidas em projetos, processos ou organizações que têm interesse direto ou influência sobre o resultado destes (Silva, *op.cit.*).

atividade portuária, tais como: segurança, responsabilidade social, proteção ambiental marinha, prevenção da poluição por óleo, redução de acidentes e identificação de atividades criminosas, entre outras (Silva, 2023).

Os elementos essenciais de um VTS assemelham-se, em determinados aspectos, à estrutura utilizada pela estrutura C5IVR para captação e manutenção do fluxo de dados de interesse. Destarte, pretende-se analisar a aderência que o VTS ou o VTMIS apresentam em relação à teoria de C5IVR, e que pode acarretar incremento significativo de subsídios para a cadeia de comando e processo decisório da MB e contribuir para a obtenção, disseminação e consolidação de conhecimentos notáveis sobre áreas de interesse.

4.2 IDENTIFICAÇÃO DAS FERRAMENTAS DO VTS/VTMIS E SUAS CONEXÕES COM C5IVR

A análise das ferramentas disponíveis nos VTS e VTMIS dos portos de Açu e Vitória revela uma relação estreita com conceitos basilares da estrutura C5IVR. O emprego desses recursos à luz dessa doutrina pode proporcionar o fornecimento de dados significativos de inteligência para a MB. Os equipamentos, que incluem radares, AIS, câmeras de longo alcance e sensores meteoceanográficos, oferecem dados importantes para vigilância, rastreamento de alvos e análise de padrões. Integrar tais capacidades com a plataforma C5IVR pode intensificar a segurança e a eficiência das operações portuárias, como também apoiar a tomada de decisões estratégicas e a resposta a incidentes, servindo de importante fonte de conhecimento.

As informações provenientes do VTS/VTMIS podem ainda ser de grande valia para a elaboração de Planos de Inteligência Operacional, assim como as Estações Radiogoniométricas de Alta Frequência (ERGAF), dos meios de IVR da MB e de outras Forças, e órgãos (inclusive satelitais), informações interagências, órgãos e organizações internacionais (Marinha do Brasil, 2024).

A tabela 2 destaca os principais sensores dos dois portos identificados como relevantes para o início do processo de integração:

Tabela 2 - Ferramentas do VTS e VTMIS

FERRAMENTA VTS/VTMIS	FUNÇÃO	POTENCIAL PARA INTELIGÊNCIA OPERACIONAL
RADAR	Monitoramento contínuo do tráfego	Fornecimento de dados em tempo real sobre a posição e movimento das embarcações
AIS	Identificação automática de embarcações	Análise de padrões de tráfego e identificação de comportamentos suspeitos
Sensores Meteorológicos	Monitoramento de condições ambientais	Suporte a operações logísticas e planejamento estratégico com base em dados ambientais
Câmeras e Sistemas de Vigilância	Monitoramento contínuo das operações	Imagens e vídeos em tempo real para análise de segurança e vigilância
Sistemas de Comunicação	Comunicação entre o Centro VTS e as embarcações na Área VTS	Monitoramento e registro de comunicações e interceptação de comunicações de contatos de interesse
Sotware de integração de dados	Consolidação de dados de várias fontes	Ferramentas de análise de dados e apoio à decisão para operações navais
Segurança Cibernética	Proteção dos recursos computacionais críticos	Preservação da integridade e sigilo dos dados que serão compartilhados

Fonte: Elaborado pelo autor.

Em situações de normalidade, ou na evolução entre situações de crises, ou conflitos internacionais, a estrutura existente do VTS no Porto de Açu e do VTMIS no Porto de Vitória tem a capacidade de prover um fluxo contínuo de informações de interesse da força naval. A seguir, analisamos como essas estruturas podem ser utilizadas e os benefícios que podem ser obtidos, baseados nos conceitos de C5IVR.

Radares de superfície (Banda-X/S) – essenciais para o monitoramento contínuo do tráfego marítimo, acompanhando movimentos de embarcações em tempo real. Em situações de crise, os dados podem ser usados para rastrear a movimentação de embarcações hostis ou suspeitas, facilitando a coordenação de respostas navais.

AIS – transmite automaticamente dados como MMSI²⁰ (*Maritime Mobile Service Identity*), posição, rumo e velocidade das embarcações. A análise desses dados pode auxiliar na identificação de embarcações não autorizadas ou que estejam realizando manobras evasivas, permitindo uma resposta rápida e coordenada. Ressalta-se que, segundo a Regra 19 do capítulo V da Convenção Internacional para Salvaguarda da Vida Humana no Mar (SOLAS 74/88), a dotação do referido equipamento é de caráter obrigatório para os navios de arqueação bruta igual a 300 ou mais, empregados em viagens internacionais, todos os navios de

²⁰ MMSI - A Identidade no Serviço Móvel Marítimo (MMSI, na sigla em inglês) é um número, registrado na UIT, utilizado para individualizar as estações transmissoras nas faixas do SMM e permitir chamadas automáticas. Todo AIS necessita de um MMSI para se comunicar e isso é válido também para as estações-base e repetidoras, consideradas estações costeiras. Os MMSI serão atribuídos diretamente pela ANATEL e devem ser solicitados pelo Gerente (Marinha do Brasil, 2023).

carga de arqueação bruta igual a 500 ou mais, não empregados em viagens internacionais e todos os navios de passageiros, independente do seu porte (OMI, 1974, tradução nossa). A Resolução A.1106 (29) da OMI estabelece que o AIS deve estar sempre em operação quando os navios estiverem em trânsito ou fundeados, podendo ser desligado apenas se o comandante acreditar que sua operação contínua comprometa a segurança ou a proteção do navio, ou em caso de incidentes de segurança iminentes. Ou seja, a transmissão destes dados depende do navegante, durante o ajuste do equipamento, sendo necessário que tal obrigatoriedade e condições constem em instruções específicas da AM.

Câmeras de longo alcance – complementam os radares e o AIS, proporcionando vigilância visual detalhada das áreas portuárias e adjacentes, facilitando a coleta contínua de informações visuais críticas e a validação de dados obtidos por outros sensores. A vigilância contínua é crucial para a detecção de ameaças e para a resposta rápida a eventos críticos.

Sensores meteoceanográficos – monitoram as condições meteorológicas e oceânicas, fornecendo dados ambientais essenciais para a análise de padrões. Esses dados ajudam a prever condições que impactem a segurança da navegação e as operações portuárias, permitindo uma melhor preparação e mitigação de riscos.

Sistemas de Comunicação – os principais equipamentos são os transceptores de VHF ajustados em canais pré-determinados para contato com o Centro VTS. Em algumas situações podem ser disponibilizados dados de telefonia por IP (VOIP) para realizar ligações telefônicas, chamada telefônica para rádio, chamadas DSC²¹ (*Digital Selective Calling*), mensagem instantânea, transferência de arquivos e recursos para gravação de ligação.

Software de Integração de dados – softwares como o sistema de gerenciamento de tráfego NAVI HARBOUR monitoram o tráfego marítimo, planejam rotas otimizadas, facilitam a comunicação, integram-se com outros sistemas, geram relatórios e asseguram conformidade regulatória.

Segurança Cibernética – os principais equipamentos incluem *firewalls*, sistemas de detecção e prevenção de intrusões, antivírus, autenticação multifator

²¹ Padrão para transmissão de mensagens digitais predefinidas através dos sistemas de rádio marítimo, destinado para chamada automática de estação, alerta de socorro ou para transmissão de informações para a organização do tráfego (ANATEL, 2024).

(MFA), criptografia de dados, soluções de backup e monitoração contínua de rede. Eles asseguram a proteção contra acessos não autorizados e ataques maliciosos.

Ademais, as plataformas tecnológicas avançadas do VTMS consolidam dados de várias fontes, permitindo uma análise abrangente e suportando a coleta e o processamento de grandes volumes de dados críticos para a inteligência.

4.3 APLICAÇÃO DOS CONCEITOS DE C5IVR E A INTEROPERABILIDADE

A interoperabilidade²² refere-se à habilidade de sistemas, unidades ou forças em rede de intercambiar serviços de forma eficiente com outros sistemas, unidades ou forças. Essa capacidade é alcançada através da harmonização de procedimentos, regras e informações, permitindo que os elementos trabalhem de forma integrada, eficiente e contínua. Existe uma correlação entre interoperabilidade, custos e agilidade. Com o aumento da integração, há um maior controle ou dimensionamento da rede, o que pode comprometer sua agilidade. Assim, é necessário equilibrar o nível de interoperabilidade com os custos, tempo, controle e agilidade (Keller; Atkinson; Clarkson, 2008, p. 5).

A interoperabilidade entre os sistemas VTS e VTMS e os sistemas da MB, à luz do C5IVR, tem o potencial de incrementar, inicialmente, a Inteligência Operacional e, secundariamente, as capacidades de C², permitindo uma gestão mais eficiente dos recursos e a coordenação rápida de respostas a incidentes. A utilização de redes de comunicação seguras e dedicadas possibilita que as informações sejam disseminadas de maneira eficaz, essencial para a coordenação durante crises. Plataformas de computação em nuvem e sistemas de análise avançada de dados facilitam o processamento rápido e a análise de grandes volumes de informações, apoiando a tomada de decisões. A segurança cibernética é fundamental para proteger as infraestruturas de comunicação e dados contra ataques, assegurando a integridade da informação. Sistemas de vigilância, como radares e câmeras, assim como dados do AIS e sensores ambientais, proporcionam uma visão detalhada e contínua do ambiente operacional, crucial para a inteligência e o reconhecimento da Área de Operações.

²² O termo “interoperabilidade” utilizado no presente trabalho deriva do documento “*A New Chapter to the Strategic Defence Review*” do Ministério da Defesa do Reino Unido, publicado em 7 de maio de 2002 (tradução nossa).

Além de todas as potenciais vantagens, vislumbra-se ainda um benefício que, caso se concretize, pode contribuir substancialmente, em tempo e recursos: os esforços dispendidos pela Força Naval no monitoramento e vigilância nas áreas de responsabilidade dos portos que utilizam o VTS e o VTMS podem ser compartilhados com o Operador VTS. Faz-se necessária a análise da legislação vigente para a confirmação dessa premissa, a ser abordado no capítulo seguinte.

Como citado anteriormente, em situações de crises ou conflitos internacionais, as estruturas existentes no VTS do Porto de Açu e no VTMS do Porto de Vitória podem ser de grande valia para prover um fluxo contínuo de informações de interesse da AM. A tabela 3 resume como essas estruturas podem ser utilizadas e os benefícios que podem ser obtidos, com base nos conceitos de C5IVR.

Tabela 3 - Benefícios da integração

Ferramenta	Benefício	Conexão com C5IVR
Radares	Monitoramento contínuo do tráfego marítimo	Vigilância (V), Reconhecimento (R)
AIS	Identificação e rastreamento de embarcações	Rastreamento de alvos (I), Vigilância (V)
Sensores Meteoceanográficos	Monitoramento de condições ambientais	Análise de padrões (C5)
Câmeras e Sistemas de Vigilância	Vigilância visual contínua	Vigilância (V)
Software de integração de dados	Consolidação e análise de grandes volumes de dados	Análise de padrões (C5), Computação (C)
Sistemas de Comunicação	Disseminação rápida e eficiente de informações	Comunicações (C), Comando e Controle (C2)
Segurança Cibernética	Proteção das infraestruturas de comunicação e dados	Cibernética (C)

Fonte: Elaborado pelo autor.

4.4 COMPARTILHAMENTO DE DADOS DE INTERESSE COM A MB

Os diversos tipos de hardware e software que compõem o VTS e o VTMS incluem recursos de segurança integrados. Tais componentes são essenciais para garantir a segurança e a autenticidade dos dados transmitidos. Os sistemas operacionais, softwares e aplicativos de comunicação, como *e-mails* seguros e aplicativos de mensagens instantâneas, desempenham um papel crítico na proteção dos dados e na operação segura dos sistemas VTS e VTMS. Sendo assim, é de fundamental importância garantir a integração segura dessas plataformas, com eficiência e confidencialidade. Os principais métodos de compartilhamento que podem ser empregados incluem:

- a) Sistemas Operacionais (SO): a escolha do SO é essencial no desenvolvimento dos sistemas C5IVR. Inicialmente, os projetos de defesa utilizavam produtos próprios e exclusivos, mas devido ao alto custo, a atenção tem se voltado para soluções comerciais (COTS) e de código aberto. Os sistemas operacionais modernos são projetados com foco na segurança, incluindo controle de acesso, autenticação e uso de certificados digitais. Por exemplo, o Windows NT e seus sucessores, como o Windows Server, possuem recursos de segurança integrados primordiais para a operação segura dos sistemas VTS e VTMISS. Além disso, sistemas como o *Trusted Solaris*²³ e distribuições seguras de Linux, como *Openwall*²⁴ e *Immunix*²⁵, oferecem funcionalidades avançadas de segurança, como auditoria de tarefas, autenticação de complementos e criptografia de senhas (Zubairi; Mahboob, 2012, p. 241).
- b) Redes Privadas Virtuais (VPN): podem ser utilizadas para criar conexões seguras entre os centros de controle VTS/VTMISS e a MB. Elas garantem que os dados transmitidos sejam criptografados, protegendo-os contra interceptações e acessos não autorizados. Esta infraestrutura de comunicação é essencial para manter a segurança dos dados em trânsito e assegurar que apenas usuários autorizados acessem as informações (Zubairi; Mahboob, 2012, pp. 44 e 238).
- c) E-mail Seguro: para garantir a segurança das comunicações por e-mail, protocolos como o PGP (*Pretty Good Privacy*) e o S/MIME (*Secure/Multipurpose Internet Mail Extensions*) são utilizados. O PGP oferece criptografia e autenticação para e-mails, usando algoritmos para criptografia de chave pública. O S/MIME, desenvolvido pela IETF²⁶, é um padrão que integra certificados digitais X.509 e infraestrutura de chaves públicas (PKI),

²³ *Trusted Solaris* é uma segurança reforçada da versão do sistema operacional Solaris Unix, desenvolvido originalmente pela Sun Microsystems e, posteriormente, adquirido pela Oracle (Zubairi; Mahboob, *op.cit.*).

²⁴ Openwall é um projeto de segurança que desenvolve soluções para sistemas operacionais, como patches de segurança e ferramentas de criptografia (Zubairi; Mahboob, *op.cit.*).

²⁵ *Imunix* é um conjunto de ferramentas de segurança para sistemas Linux, projetadas para prevenir vulnerabilidades e ataques através da tecnologia de "imunização" do sistema (Zubairi; Mahboob, *op.cit.*).

²⁶ *Internet Engineering Task Force* é uma organização internacional de desenvolvedores, operadores e pesquisadores dedicados à evolução e ao bom funcionamento da internet. Fundada em 1986, a IETF desenvolve e promove padrões técnicos e boas práticas relacionadas aos protocolos e arquitetura da internet (IETF, 2024).

utilizando algoritmos para garantir a segurança das mensagens de e-mail. Tais tecnologias garantem o sigilo, autenticidade e integridade das mensagens transmitidas (Zubairi; Mahboob, 2012, p. 242).

- d) Criptografia de Dados e *High Assurance Internet Protocol Encryptor* (HAIGE): a criptografia de dados é vital para proteger a integridade e o sigilo das informações transmitidas pelos sistemas VTS e VTMS. Como exemplo, pode-se citar a criptografia AES (*Advanced Encryption Standard*), amplamente utilizada para proteger os dados durante a transmissão, e essencial para prevenir acessos não autorizados, garantindo que as informações sensíveis permaneçam seguras (Zubairi; Mahboob, 2012, p. 44). O HAIGE é um dispositivo de criptografia de alta segurança utilizado para a proteção dos dados transmitidos em redes inseguras ou de classificação inferior. Baseia-se principalmente no IPsec²⁷, com restrições e aprimoramentos adicionais, e é compatível com as especificações da *National Security Agency* (NSA)²⁸. Permite ainda que rede de computadores distintas transmitam e recebam dados seguramente mediante links não confiáveis, utilizando “Protocolos da Força-Tarefa” de Engenharia de Internet para o tráfego de dados (IETF), e garantindo que os dados transmitidos permaneçam seguros e protegidos (Zubairi; Mahboob, 2012, pp. 242–243).
- e) *Data Link*: empregado essencialmente para intercâmbio de informações sobre o quadro tático aéreo, de superfície e submarinos, além de dados de inteligência, guerra eletrônica e dados de C², assegurando a segurança e a eficiência na troca de informações críticas entre unidades militares e proporcionando uma infraestrutura de comunicação robusta. Embora a MB empregue alguns tipos de links nas operações internas da Força, serão citados alguns dos principais tipos de links, ao nível de análise, utilizados globalmente:
- *Link 11/Link 11B*: desenvolvido nas décadas de 1950 e 1960, também conhecido como TDL A/B (*Tactical Data Link A/B*). Funciona em alta

²⁷ IPsec (*Internet Protocol Security*) é um conjunto de protocolos para assegurar a comunicação segura e privada por meio de redes IP, utilizando criptografia e autenticação (Zubairi; Mahboob, *op.cit.*).

²⁸ A *National Security Agency* (NSA) é uma agência governamental dos EUA responsável pela inteligência de sinais, segurança da informação e atividades de cibersegurança (EUA, 2024).

frequência (HF) com baixas taxas de dados. É seguro, mas vulnerável a contramedidas eletrônicas (CME).

- *Link 16*: utilizado para guerra antiaérea (AAW), atende plenamente aos requisitos de controle de aeronaves. É o principal *link* de dados táticos adotado pelos EUA e pela OTAN destinado a detectar, rastrear, interceptar e destruir mísseis balísticos táticos ou de curto alcance em uma área de operações específica.
 - *Link 22*: criado para operações marítimas e também compatível com operações do *Link 16*. Possui uma arquitetura de sistemas abertos com interfaces bem definidas e uma pilha de comunicações em camadas. Sete países participaram de seu desenvolvimento: Alemanha, França, Itália, Canadá, Países Baixos, Reino Unido e EUA.
 - *Link Y Mk2*: desenvolvido pela Thales, faz parte da família dos *Links 11* e *16*, sendo utilizado por países não membros da OTAN. Oferece melhor desempenho que o *Link 11* e é um *link* confiável para transferência de dados entre forças navais via rede de rádio criptografada (Zubairi; Mahboob, 2012, p. 243).
- f) Infraestrutura de Chave Pública (PKI): é uma infraestrutura de TI que permite aos usuários de redes públicas inseguras trafegar dados de forma segura e privada, utilizando chaves públicas confiáveis distribuídas como parte de Certificados Digitais assinados por Autoridades Certificadoras (AC). Utiliza criptografia de chave pública e simétrica para garantir sigilo, integridade, autenticação (Zubairi; Mahboob, 2012, pp. 243–244).

5 RELEVÂNCIA DOS DADOS PARA A INTELIGÊNCIA OPERACIONAL

A Inteligência Operacional é uma atividade “[...] permanentemente exercida, com a finalidade de produzir e salvaguardar conhecimento requerido para planejar, conduzir e sustentar operações militares” (Ministério da Defesa, 2015, p. 149). Dado seu caráter contínuo e a importância de seus produtos para as operações, faz-se necessário que as fontes de inteligência operacional sejam tratadas no nível adequado à sua relevância no cenário nacional.

Um dos documentos de mais alto nível sobre a defesa nacional, o Livro Branco de Defesa Nacional, contribui nesse sentido, com diretrizes e criação de projetos de interesse a serem realizados em períodos de curto e longo prazo, considerados prioritários e estratégicos pela MB. Tais iniciativas abrangem: a ampliação da capacidade de Inteligência Operacional com foco no Poder Naval e a intensificação do intercâmbio com agências nacionais e internacionais, incluindo a compreensão e monitoramento das chamadas novas ameaças (Brasil, 2020, p. 139).

No nível operacional, a atividade de inteligência é amplificada pela integração dos conhecimentos disponíveis no Sistema de Inteligência Operacional (SIOP). O SIOP agrega as ações de planejamento e execução da atividade de Inteligência Operacional, visando manter atualizado, desde o tempo de paz, um banco de dados que sirva de base para o planejamento dos Comandos Operacionais, durante a deflagração das operações. O sistema é composto pelos órgãos de Inteligência das FA responsáveis pela atividade, bem como pela Subchefia de Inteligência de Defesa do Ministério da Defesa (MD) e pela respectiva Seção do Estado-Maior Conjunto, quando ativado. Na MB, a responsabilidade pela Inteligência Operacional é atribuição do Centro de Inteligência da Marinha (CIM) (Ministério da Defesa, 2020, p. 23 e pp. 89–90).

5.1 AVALIAÇÃO DA RELEVÂNCIA DAS INFORMAÇÕES OBTIDAS PELA INTEGRAÇÃO DE FERRAMENTAS C5IVR PARA A INTELIGÊNCIA OPERACIONAL DA MB

Como apresentado no capítulo anterior, a operação dos serviços de tráfego de embarcações traz consigo inúmeras contribuições como o aumento e velocidade

das operações portuária seguras e coordenadas, redução de acidentes, otimização do emprego de recursos, fiscalização ambiental e elevação significativa nos níveis de monitoramento. Essas melhorias aplicam-se aos portos organizados, à região adjacente que será beneficiada e, em última análise, ao próprio país.

Todavia, vislumbra-se que as vantagens obtidas podem ser ainda maiores do que as apresentadas, como é possível destacar no âmbito internacional. Conforme a Direção-Geral de Recursos Naturais, Segurança e Serviços Marítimos (DGRM) de Portugal, além do monitoramento e acompanhamento, o sistema e serviço VTS possui uma série de outras capacidades, sendo as informações relacionadas com a segurança, proteção e vigilância marítima compartilhadas com o Sistema Integrado de Vigilância, Comando e Controle (SIVICC) da Guarda Nacional Republicana (GNR) (DGRM, 2018).

Outro exemplo relevante é o do Porto de Zhoushan, no leste da China, que, após a implementação do VTS, apresentou redução de 11% nos custos de vigilância, como a patrulha costeira, o que resultou em economia de recursos humanos e materiais. Os resultados foram detalhados em um estudo que abrangeu um espaço temporal de dez anos, tendo sido conduzido pela Universidade de Tecnologia da China e publicado no *International Journal of e-Navigation and Maritime Economy*²⁹ (MOU et al., 2015).

Extrapolando a esfera dos eventos reais citados acima, é possível vislumbrar o desenvolvimento e aplicação do modelo de intercâmbio de informações entre o VTS e a MB para obtenção de conhecimento no âmbito do emprego militar, como, por exemplo, em um cenário de resposta à crise. Com base nas informações apresentadas até o momento, há a viabilidade da utilização da tecnologia disponível atualmente para coletar, processar e analisar dados em tempo real, incluindo informações de VTS/VTMIS, para apoiar o planejamento e a execução das operações navais. Os dados coletados podem ser integrados a uma rede de sensores e sistemas de vigilância para fornecer uma visão holística e atualizada da situação operacional, permitindo uma resposta rápida e eficaz a incidentes e ameaças aos quais as forças militares podem ser expostas.

²⁹ Revista acadêmica semestral dedicada a pesquisas teóricas e empíricas nas áreas de tecnologia de navegação e economia marítima. Focada em temas como tecnologia, sistemas de informação, engenharia de tráfego, gestão e legislação, é patrocinada pela *International Association of e-Navigation and Ocean Economy* e pelo *Korea Institute of Aids to Navigation*, com incentivo da GMT Co., Ltd. (e-Nav, 2018).

5.2 REGULAMENTAÇÃO DO FLUXO DE DADOS

Como mencionado no capítulo 3, a IALA publica normas que norteiam o emprego do VTS/VTMIS no âmbito internacional. Para o presente estudo, as seguintes publicações fornecem uma abordagem ampla para o entendimento do processo de desenvolvimento e implantação do sistema VTS:

- a) IALA *Guideline G1111 (On Preparation of Operational and Technical Performance Requirements for VTS Systems)* que provê informações detalhadas para auxiliar os Provedores de VTS na definição, especificação, estabelecimento, operação e atualizações do serviço, estabelecendo os requisitos operacionais e técnicos de desempenho do sistema VTS e como eles influenciam a arquitetura do sistema e os requisitos dos subsistemas projetados; e
- b) IALA *Guideline G1089 (Provision of VTS types of service)* que fornece aos Provedores de VTS informações detalhadas para auxiliar na elaboração de normas internas e externas para a operação do VTS.

No Brasil, a sistemática acerca das especificidades do VTS/VTMIS encontra amparo na legislação vigente, com ressalvas à recente inclusão do tema na pauta da administração portuária nacional. A seguir serão relacionadas algumas normas em vigor de importância para o tema, no âmbito nacional:

- a) Lei Complementar n.º 97/1999 – Normas gerais para a organização, o preparo e o emprego das Forças Armadas: estabelece a atribuição subsidiária à Marinha de prover a segurança da navegação aquaviária e designa o Comandante da Marinha, no trato dos assuntos relacionados à atividade, como Autoridade Marítima.
- b) Lei n.º 9.537/1997 – Lei de Segurança do Tráfego Aquaviário (LESTA): trata sobre a elaboração de normas para o tráfego e permanência das embarcações nas águas sob jurisdição nacional, bem como sua entrada e saída de portos, atracadouros, fundeadouros e marinas e o estabelecimento e funcionamento de sinais e auxílios à navegação.
- c) Lei n.º 13.874/2019 – Declaração dos Direitos de Liberdade Econômica: estabelece os procedimentos para o processo de concessão da Licença de Implantação das atividades econômicas.

- d) Lei n.º 12.815/2013 – Nova Lei dos Portos: estabelece diretrizes para a exploração direta e indireta dos portos e instalações portuárias pela União, bem como para as atividades dos operadores portuários.
- e) NORMAM-602 – Normas da Autoridade Marítima para Serviço de Tráfego de Embarcações (VTS): estabelece normas e procedimentos para o licenciamento, implantação e autorização para operação de um Serviço de Tráfego de Embarcações (VTS) no Brasil.

Para que o Poder Naval brasileiro possa se beneficiar do fluxo de dados fornecido pelo Centro VTS, faz-se necessário que esse intercâmbio de informações esteja normatizado, com orientações específicas e responsabilidades bem definidas. A NORMAM-602, no capítulo 3, estabelece que o VTS deverá possuir a capacidade de: “[...] fornecer informações oportunas e relevantes sobre os fatores que possam influenciar a movimentação das embarcações” (Marinha do Brasil, 2023, p. 3–1). Tais informações englobam relatórios e detalhes do *ISPS Code*³⁰, apoio e cooperação com os Serviços Aliados. Outrossim, o VTS deve ser capaz de controlar e gerenciar o tráfego de navios e embarcações, incluindo a contribuição com os AAM locais para avaliação de impactos da carga transportada no ecossistema marinho, segurança das comunidades e infraestruturas adjacentes à Área VTS (Marinha do Brasil, 2023).

Nesse íterim, o desafio encontrado é a definição precisa de como, quando e por quais canais essa troca de informações deve ser conduzida, assim como a obrigatoriedade da manutenção da comunicação e os responsáveis por ela. Sem o devido cuidado com a terminologia empregada para a disseminação de assuntos de natureza sensível, não é possível afirmar que os dados estarão disponíveis e acurados quando a necessidade se fizer imperativa. Partindo-se do pressuposto da existência de informações de relevância operacional para a MB nos portos nacionais e suas cercanias, e que a transmissão desses dados necessite ser contínua a fim de alimentar as estruturas do sistema militar em questão, não há como garantir a ininterruptibilidade do fluxo pelo Provedor VTS com base estrita nas normas atuais.

Um exemplo ilustrativo da aplicação normativa como recurso compulsório à obtenção de um efeito no campo marítimo é o da SOLAS 74/88, que, no Capítulo IV,

³⁰ Código Internacional de Segurança para Navios e Instalações Portuárias (tradução nossa) é o conjunto de medidas para aumentar a segurança marítima, implementado após os ataques de 11 de setembro de 2001, visando prevenir atos ilícitos e garantir a proteção de navios e portos internacionais (Kantharia, 2024).

impõe requisitos funcionais para os navios com arqueação bruta igual ou acima de 300:

Todo navio, estando no mar, deve ser capaz de [...] exceto como determinado nas Regras 8.1.1 e 10.1.4.3, de transmitir avisos de socorro do navio para terra, por pelo menos dois meios separados e independentes, cada um usando um serviço diferente de radiocomunicação [...] (OMI, 1974, p.333, tradução nossa).

Ou ainda:

1. Cada navio deverá ser dotado de instalação rádio capaz de cumprir integralmente com os requisitos funcionais prescritos pela Regra 4 durante toda sua viagem pretendida e, a menos que tenha sido dispensado de acordo com a Regra 3, capaz de cumprir com os requisitos da Regra 7 e, como for apropriado para a área ou áreas marítimas pelas quais passará durante sua viagem pretendida, de cumprir com os requisitos de quaisquer das Regras 8, 9, 10 ou 11. (OMI, 1974, p.335, tradução nossa).

Uma explicação plausível para o hiato encontrado na legislação atual no tocante à obrigatoriedade e definições da transferência contínua de dados da AP para a AM encontra amparo na própria natureza de concepção do VTS/VTMIS. Conforme apresentado no capítulo 3, o sistema de monitoramento de embarcações deriva da necessidade de otimizar a segurança e a eficiência da navegação, ou seja, emerge no campo dos Auxílios à Navegação. Conforme a SOLAS 74/88 e a Resolução A.1158(32) da IMO, o VTS é estabelecido por uma Autoridade Competente visando aumentar a segurança³¹ e eficiência da navegação, contribuir para a proteção da vida humana no mar e auxiliar a preservação do meio ambiente (Marinha do Brasil, 2023).

Não obstante muitos países adotarem o VTS há décadas, como um recurso indispensável à navegação nas proximidades do porto organizado, tal realidade se encontra bem diferente no Brasil, cuja implementação ao longo dos inúmeros e importantes portos da costa ainda não recebeu a atenção e as iniciativas devidas.

As conclusões advindas das análises dos capítulos anteriores sugerem que, caso haja alteração de percepção de ambos os atores: AP e AM (principalmente), sobre o emprego do VTS/VTMIS para o provimento de informações de relevância para a Força Naval, e seja vislumbrado o potencial de contribuir para o incremento da proteção marítima (*security*³²) ao invés de restringir-se apenas aos benefícios

³¹ Cabe ressaltar que o caráter impositivo adotado pela SOLAS 74/88 aos países signatários da Convenção deriva do foco primordial relacionado à segurança, traduzido na necessidade de proteção de vidas humanas a bordo de embarcações.

³² Divisão relacionada aos conceitos internacionalmente consagrados e denominados, em inglês, *Security* e *Safety*. Dessa forma, a MB adota a conceituação Proteção Marítima (*Security*) e Segurança da Navegação Aquaviária (*Safety*).

relacionados à segurança da navegação (*safety*), seria de suma importância que tal mudança de postura fosse refletida nas normas que tratam do assunto, com as redações adequadas fim garantir o cumprimento e manutenção do fluxo de dados de interesse.

O arcabouço legal que trata do tema em questão no Brasil carece de aprimoramento, com ênfase em detalhamento e divulgação. É provável que, com a aderência de mais portos aos sistemas no decorrer do tempo, aliada à disseminação dos benefícios e vantagens provenientes tanto operacionalmente quanto em segurança, a legislação amplie o seu escopo, refletindo as especificidades adequadas para a atividade ser desenvolvida em seu pleno potencial, com vantagem tanto para a iniciativa privada quanto para a estrutura de defesa brasileira.

6 CONSIDERAÇÕES FINAIS

A incorporação de ferramentas C5IVR ao sistema VTS representa tanto um desafio quanto uma oportunidade para a MB. Um dos principais desafios está na complexidade de harmonizar diferentes sistemas e tecnologias a fim de garantir um fluxo de informações seguro e eficiente. A implementação bem-sucedida desses recursos exige uma infraestrutura robusta e coordenação estreita entre todas as partes envolvidas, incluindo as autoridades portuárias, operadores de terminais e a própria MB.

Por outro lado, a integração também oferece vastas oportunidades. A combinação das capacidades de monitoramento e controle do VTS com as avançadas funcionalidades C5IVR tem o potencial efetivo de atuar como uma fonte de conhecimentos importante para a inteligência operacional da MB. A capacidade de coletar, processar e analisar dados em tempo real pode incrementar substancialmente o planejamento e condução das operações militares. Este conhecimento tem a capacidade de contribuir para a melhoria da consciência situacional, permitindo respostas mais rápidas e eficazes a ameaças e emergências.

Outrossim, é fundamental encontrar um equilíbrio entre aprimorar a inteligência operacional e preservar a função primordial de segurança do VTS. Embora a introdução de tecnologias C5IVR possa trazer melhorias, é imperativo que o foco na segurança da navegação e na proteção ambiental não seja comprometido. O VTS deve continuar a proporcionar um serviço seguro e eficiente, garantindo que as operações portuárias e marítimas ocorram sem interrupções.

Por meio da compilação da fundamentação teórica e do histórico da implementação dos sistemas VTS e VTMS nos portos de Açu e Vitória foi evidenciado que a eficiência das operações marítimas, associada à segurança e ao controle do tráfego nas proximidades dos portos, é de suma importância para fomentar o comércio e o desenvolvimento das atividades portuárias. A análise dos dados históricos e das regulamentações vigentes demonstrou que a implementação de sistemas VTS é um processo complexo, mas essencial para a modernização e segurança dos portos brasileiros.

A consolidação e o emprego coordenado das vertentes Comando, Controle, Comunicações, Computação, Cibernética, Inteligência, Vigilância e Reconhecimento é primordial para o aprimoramento das operações militares. A interoperabilidade de

sistemas e a conectividade contínua são aspectos críticos que permitem a coleta e análise de dados *online*, proporcionando uma visão completa do teatro de operações. A aplicação dessas perspectivas no contexto marítimo destaca a importância de uma infraestrutura robusta e segura para a gestão eficiente do tráfego de embarcações e para o suporte às operações militares.

A apresentação de estudos de caso e exemplos de como os dados coletados pelos sistemas VTS podem ser utilizados para viabilizar e sustentar a operacionalidade desta iniciativa. O estudo do Porto de Zhoushan, na China, exemplificou como a associação de tecnologias de monitoramento e controle pode transformar dados brutos em informações valiosas para a tomada de decisões. A capacidade de monitorar o tráfego marítimo em tempo real e de responder prontamente a incidentes é crucial para garantir a segurança e a eficiência das operações portuárias e navais. Tais exemplos demonstram que a aplicação prática dos conceitos de C5IVR na sistemática VTS é viável e pode trazer benefícios significativos para a MB.

Algumas direções futuras e as correspondentes políticas para facilitar a integração de C5IVR no VTS fazem-se necessárias. A regulamentação do fluxo de dados, a definição de protocolos de segurança e a responsabilidade das entidades envolvidas foram identificadas como aspectos críticos para o sucesso desse empreendimento. Para futuras pesquisas, sugere-se o exame detalhado das políticas e regulamentações necessárias para viabilizar a integração completa do C5IVR no VTS. Isso inclui a definição clara dos protocolos de segurança, os mecanismos de compartilhamento de dados e a responsabilidade de cada entidade envolvida. A criação de um *framework* regulatório sólido é essencial para garantir que a troca de informações entre o VTS e a MB seja contínua, segura e eficaz. Além disso, a análise dos benefícios e desafios específicos de cada porto pode fornecer opiniões valiosas para a implementação de melhorias contínuas nos sistemas de monitoramento marítimo.

Ademais, a pesquisa e o desenvolvimento de tecnologias emergentes que possam ser integradas aos sistemas VTS e VTMS aumentará significativamente a capacidade de coleta e análise de dados, aprimorando a inteligência operacional. Finalmente, o desenvolvimento de programas de capacitação e treinamento para operadores e gestores dos sistemas VTS e VTMS e do pessoal da MB que lidará com essas informações é essencial, proporcionando a utilização eficiente e segura

dos recursos C5IVR. Esses programas devem focar não apenas no uso técnico, mas também nas melhores práticas de integração e gestão da informação, assegurando que todos os envolvidos estejam preparados para maximizar os benefícios dessas tecnologias avançadas.

Em síntese, as opções apresentadas representam uma alternativa viável para otimizar a inteligência operacional da MB no âmbito costeiro e portuário. Entretanto, tal proposta deve ser realizada sob uma perspectiva fundamentada e responsável, garantindo que os benefícios potenciais sejam plenamente realizados sem comprometer a função primordial do VTS de garantir a segurança da navegação e a proteção ambiental, como um caminho promissor para a evolução das operações navais e a segurança marítima no Brasil.

REFERÊNCIAS

- AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (ANATEL). **Glossário de Termos da Anatel**, 2024. Disponível em: <<https://informacoes.anatel.gov.br/legislacao/component/fsf/?view=faq&catid=3&faqid=3714>>. Acesso em: 11 nov. 2024.
- ALBERTS, D. S.; GARSTKA, J. J.; STEIN, P. F. **Network Centric Warfare: Developing and leveraging information superiority**. 2. Ed (Revised). Washington, D.C.: The Command and Control Research Program (CCRP), 2000. p. 284.
- ALBERTS, D. S.; HAYES, R. E. **Command Arrangements for Peace Operations**. Washington D.C.: National Defense University Press, 1995.
- ALBERTS, D. S.; HAYES, R. E. **Power to the Edge: Command and Control in the Information Age**. Washington, D.C.: CCRP Publication Series, 2003. p. 303.
- ALGHAMDI, A. S. Evaluating Defense Architecture Frameworks for C4I System Using Analytic Hierarchy Process. **Journal of Computer Science**, Riyadh, 2009. Disponível em: <<https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=8a6ceecb13e4cf4976db842370edefddeb74095>>. Acesso em: 22 abr. 2024.
- BRASIL. Ministério da Defesa. **Glossário das Forças Armadas**. 5. ed. Brasília: MD, 2015.
- BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília: MD, 2020.
- BRASIL. Presidência da República. **LEI N.º 12.815, DE 5 DE JUNHO DE 2013**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12815.htm. Acesso em: 11 nov. 2024.
- CZERWINSK, T. J. **Command and Control at the Crossroads**. The US Army War College Quarterly: Parameters, 1996, p. 121–132. Disponível em: <https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1788&context=parameters>. Acesso em: 7 jun. 2024.
- DEFENSEA CONSULTORIA. **O Serviço de Tráfego de Embarcações (VTS – Vessel Traffic Service) No Brasil e no Mundo**. 2016. Disponível em: <<https://www.defensea.com.br/breve-historico-vts>>. Acesso em: 2 jun. 2024.
- DEMIRTAS, U.; TURK, Y. Z.; OZER, M. The Role Of Intelligence, Surveillance, And Reconnaissance In Disaster And Public Health Emergency. **Prehospital And Disaster Medicine**, Cambridge, v. 29, n. 5, 2014. Disponível em: <<https://doi.org/10.1017/S1049023X14001009>>. Acesso em: 25 abr. 2024.
- DIREÇÃO-GERAL DE RECURSOS NATURAIS, SEGURANÇA E SERVIÇOS MARÍTIMOS (DGRM). **VTS System**, 2018. Disponível em: <<https://www.dgrm.pt/en/sistema-vts>>. Acesso em: 29 mai. 2024.
- EDDINS JR. J.M. Preparing For A Storm. **Airman Magazine**, 2021. Disponível em: <<https://www.airmanmagazine.af.mil/Features/Display/Article/2604080/preparing-for-a-storm/>>. Acesso em: 12 abr. 2024.

E-NAV. **International Journal of e-Navigation and Maritime Economy**, 2018. Disponível em: <<http://www.e-navi.kr/sub602.asp>>. Acesso em: 11 nov. 2024.

ESCOLA DE GUERRA NAVAL; FUNDAÇÃO EZUTE. **Relatório de Pesquisa: Logística Marítima e a Importância do VTMIS**. Escola de Guerra Naval: Rio de Janeiro, 2021, p.55.

ESTADOS UNIDOS DA AMÉRICA (EUA). Departamento do Exército. **FIELD MANUAL (FM) 100-5 OPERATIONS**. Washington, D. C., 1993.

ESTADOS UNIDOS DA AMÉRICA (EUA). Departamento de Defesa. **Joint Publication 2-0 Joint Intelligence**. Revised Edition. Washington, D. C., 2013.

ESTADOS UNIDOS DA AMÉRICA (EUA). Departamento de Defesa. **Joint Publication 3-01: Countering Air and Missile Threats**. Washington, D.C., 1999.

ESTADOS UNIDOS DA AMÉRICA (EUA). Departamento de Defesa. **Joint Publication 6-0: Joint Communications System**. Washington, D.C., 2017.

ESTADOS UNIDOS DA AMÉRICA (EUA). Força Aérea. **E-3 Sentry (AWACS)**, 2015. Disponível em: <<https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104504/e-3-sentry-awacs/>>. Acesso em: 11 nov. 2024.

ESTADOS UNIDOS DA AMÉRICA (EUA). National Security Agency. **About NSA/CSS**, 2024. Disponível em: <<https://www.nsa.gov/about/>>. Acesso em: 11 nov. 2024.

GOMES, A. Centro VTS Porto do Açú. [**Apresentação (PowerPoint) à Delegação de Angola**]. Porto do Açú, 2024.

IETF. **Introduction to the IETF**, 2024. Disponível em: <<https://www.ietf.org/about/introduction/>>. Acesso em: 11 nov. 2024.

INTERNATIONAL ASSOCIATION OF MARINE AIDS TO NAVIGATION AND LIGHTHOUSE AUTHORITIES (IALA). **IALA Guideline G-1111-1 Producing Requirements for the Core VTS System**. Edition 1.0. France: IALA, 2022.

INTERNATIONAL ASSOCIATION OF MARINE AIDS TO NAVIGATION AND LIGHTHOUSE AUTHORITIES (IALA). **International Dictionary of Marine Aids to Navigation**, 2024. Disponível em: <https://www.iala.int/wiki/dictionary/index.php/Aid_to_Navigation>. Acesso em: 11 nov. 2024.

INTERNATIONAL ASSOCIATION OF MARINE AIDS TO NAVIGATION AND LIGHTHOUSE AUTHORITIES (IALA). **About The Organization**, 2024b. Disponível em: <<https://www.iala.int/about-iala/>>. Acesso em: 11 nov. 2024.

INTERNATIONAL ASSOCIATION OF MARINE AIDS TO NAVIGATION AND LIGHTHOUSE AUTHORITIES (IALA). **Vessel Traffic Services Manual**. 8.3. Ed. France: IALA, 2024. Disponível em: <<https://www.iala-aism.org/product/m0002/>>. Acesso em: 26 mai. 2024.

KANTHARIA, RAUNEK. The Ultimate Guide to the ISPS Code for Ships – Enhancing Maritime Security. **Marine Insight**, 2024. Disponível em: <<https://www.marineinsight.com/maritime-law/the-isps-code-for-ships-a-quick-guide/>>. Acesso em: 11 nov. 2024.

KELLER, R.; ATKINSON, S. R.; CLARKSON, P. J. **Network enabled capability as a challenge for design: a change management view**. DS 48: Proceedings DESIGN 2008, the 10th International Design Conference. Dubrovnik: The Design Society, 2008, p. 943 - 950.

LATERZA R. Q.; CABRAL R. A importância dos sistemas C4ISR na Guerra da Ucrânia. **Forças Terrestres**, 2022. Disponível em: <<https://www.forte.jor.br/2022/11/29/a-importancia-dos-sistemas-c4isr-na-guerra-da-ucrania/>>. Acesso em: 10 mai. 2024.

LOWENTHAL, M. **Intelligence: from secrets to policy**. Washington, D.C.: CQ Press, 2009. p. 692.

MARINHA DO BRASIL. Diretoria de Hidrografia e Navegação. **Normas da Autoridade Marítima para Serviço de Tráfego de Embarcações (NORMAM-602/DHN)**. Rio de Janeiro, 2023.

MCCURDY, H. E. **Space and the American Imagination**. [S.l.]: Smithsonian Institution Press, 1997.

MINISTÉRIO DA DEFESA. Estado-Maior Conjunto das Forças Armadas. **Doutrina de Operações Conjuntas – MD30-M-01**. Volumes 1 e 2. 2. ed. Brasília: MD, 2020.

MOU, J.; ZHOU C.; DU Y., TANG W. M. Evaluate VTS benefits: A case study of Zhoushan Port. **International Journal of E-Navigation and Maritime Economy**. Volume 3. Zhejiang, 2015. Disponível em: <<https://www.sciencedirect.com/science/article/pii/S240553521500073X>>. Acesso em: 6 jun. 2024.

NAÇÕES UNIDAS. **Convenção das Nações Unidas sobre o Direito do Mar**. Montego Bay, 1982.

ORGANIZAÇÃO MARÍTIMA INTERNACIONAL (OMI). **Consolidated text of the International Convention for the Safety of Life at Sea, 1974, and its Protocol of 1988: articles, annexes and certificates (SOLAS 1974/1988)**. 7. Ed. London: IMO, 2020.

ORGANIZAÇÃO MARÍTIMA INTERNACIONAL (OMI). **Resolution A.1158(32) on Guidelines for Vessel Traffic Services**. London: IMO, 2021.

PORTAL PORTUARIO. **VTMIS completa cinco anos com eficiência e segurança**. 2022. Disponível em: <<https://portalportuario.cl/vtmis-completa-cinco-anos-con-eficiencia-e-seguranca/>>. Acesso em: 19 mar. 2024.

REINO UNIDO. House of Commons. Defence Committee. **A New Chapter to the Strategic Defence Review**. Sixth Report of Session 2002–03. Volume I: Report. London: The Stationery Office Limited, 2003. Disponível em: <<https://publications.parliament.uk/pa/cm200203/cmselect/cmdfence/93/93.pdf>>. Acesso em: 5 jul. 2024.

SILVA, Jéssica Germano de Lima. **Uma inovação tecnológica no ambiente portuário brasileiro e suas interfaces com a defesa: o caso do Porto do Rio de Janeiro na implementação do e-Navigation**. 175 f. Relatório Técnico (Doutorado Profissional em Estudos Marítimos) - Escola de Guerra Naval, Programa de Pós-Graduação em Estudos Marítimos, Rio de Janeiro, 2023.

SOPESP. Porto de Vitória – **VTMIS: quatro anos de eficiência e segurança**. 2021. Disponível em: <<https://sopesp.com.br/2021/09/17/porto-de-vitoria-vtmis-quatro-anos-de-eficiencia-e-seguranca/>>. Acesso em: 17 mai. 2024.

SWEENEY, M. M. **Blue Force Tracking: Building a Joint Capability**. Carlisle Barracks: U.S. Army War College, 2008.

VILLAS-BÔAS, Marcelo Santiago. **A CIA DOCAS do Rio de Janeiro e o uso de tecnologia de ponta em seus portos**. Companhia Docas do Rio de Janeiro. Rio de Janeiro, 2022.

VPORTS. **VTMIS**. 2023. Disponível em: <<https://vports.com.br/vtmis/>>. Acesso em: 12 mai. 2024.

WÄRTSILÄ. **Wärtsilä Navi-Harbour Web VTS**, 2024. Disponível em: <<https://www.wartsila.com/marine/products/port-optimisation/webvts>>. Acesso em: 11 nov. 2024.

ZUBAIRI, J. A.; MAHBOOB, A. **Cyber Security Standards, Practices and Industrial Applications: Systems and Methodologies**. Hershey: Information Science Reference, 2012. p. 337.