

ESCOLA DE GUERRA NAVAL

CC THALES CURIONI RAIA

**SOBERANIA MARÍTIMA E DEFESA MULTIDOMÍNIO:
Um Modelo Integrado de Resposta a Sistemas Não Tripulados**

Rio de Janeiro

2025

CC THALES CURIONI RAIA

**SOBERANIA MARÍTIMA E DEFESA MULTIDOMÍNIO:
Um Modelo Integrado de Resposta a Sistemas Não Tripulados**

Monografia apresentada à Escola de
Guerra Naval, como requisito parcial
para a conclusão do Curso Superior.

Orientador: CF Daniel Drumond Gama

Rio de Janeiro
Escola de Guerra Naval
2025

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

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

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

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

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

Assinatura digital gov.br

DEDICATÓRIA

Dedico este projeto a minha família, especialmente à minha esposa, Karina, por todo incentivo e compreensão durante o período deste Curso Superior. Ao meu orientador, CF Daniel Gama, que me auxiliou, sobremaneira para que minhas dúvidas fossem sanadas de forma mais breve possível, bem como para que o objetivo deste projeto fosse atingido. Aos oficiais e, antes de tudo, amigos do Centro de Guerra Eletrônica da Marinha (CGAEM) que compartilharam de seus conhecimentos na presente área de estudo e que possibilitaram que minha rotina semanal fosse compatível com as demandas apresentadas durante essa jornada.

O mar ensina que não há vitória sem respeito à natureza e que o poder repousa na inteligência, não na força.

Almirante Paulo Moreira da Silva

RESUMO

O presente trabalho analisa os desafios contemporâneos à soberania marítima brasileira diante do emprego crescente de Sistemas Remotamente Pilotados (SRPs) em diferentes domínios, propondo um modelo integrado de defesa multidomínio com ênfase em contramedidas não cinéticas. A pesquisa parte da constatação de que os SRPs apresentam vulnerabilidades que podem ser exploradas por medidas de guerra eletrônica, acústica e cibernética, possibilitando respostas eficazes sem recorrer ao emprego letal. A metodologia adotada foi qualitativa, com base em uma ampla revisão de doutrina nacional e internacional, documentos estratégicos como a Estratégia Nacional de Defesa e o PEM 2040, bem como em análises de casos recentes, como a guerra na Ucrânia, enfatizando a identificação de lacunas operacionais, a avaliação tecnológica e a proposição de diretrizes de integração. O modelo resultante articula sensores inteligentes, protocolos de decisão automatizados e efetores adaptativos, garantindo interoperabilidade entre os diversos domínios. Além disso, propõe a criação de centros de comando multidomínio e a capacitação contínua de operadores, alinhando-se às diretrizes da Marinha do Brasil e reforçando a concepção da Amazônia Azul como espaço de interesse vital. Os resultados indicam que a aplicação coordenada de contramedidas não cinéticas representa uma alternativa viável para ampliar a resiliência das Forças Navais, reduzir vulnerabilidades em cenários complexos e assegurar a soberania sobre áreas estratégicas. Ao final, conclui-se que a adoção de um modelo integrado multidomínio contribui não apenas para a modernização das capacidades de defesa, mas também para a consolidação de uma postura nacional proativa e dissuasória frente às ameaças emergentes.

Palavras-chave: Veículos Não tripulados. Sistemas Remotamente Pilotados. Contramedidas Não-cinéticas. Neutralização. Defesa Multidomínio. Guerra Eletrônica. Guerra Acústica. Guerra Cibernética. Modelo Integrado de Resposta

ABSTRACT

MARITIME SOVEREIGNTY AND MULTIDOMAIN DEFENSE:

An Integrated Response Model to Unmanned Systems

This study analyzes the contemporary challenges to Brazilian maritime sovereignty in light of the growing use of unmanned systems across multiple domains, proposing an integrated multidomain defense model with emphasis on non-kinetic countermeasures. The research is based on the premise that unmanned systems present vulnerabilities that can be exploited through electronic, acoustic, and cyber warfare measures, enabling effective responses without resorting to lethal means. A qualitative methodology was adopted, grounded in an extensive review of national and international doctrine, strategic documents such as the National Defense Strategy and Estrategic Plan for Brazilian Navy 2040, as well as case studies of recent conflicts, including the war in Ukraine. The focus was placed on identifying operational gaps, assessing technological capabilities, and proposing integration guidelines. The resulting model integrates intelligent sensors, automated decision-making protocols, and adaptive effectors, ensuring interoperability across different domains. Furthermore, it advocates the establishment of multidomain command centers and the continuous training of operators, aligning with the guidelines of the Brazilian Navy and reinforcing the concept of the Blue Amazon as a vital area of national interest. The findings indicate that the coordinated application of non-kinetic countermeasures represents a feasible alternative to enhance naval resilience, reduce vulnerabilities in complex scenarios, and safeguard sovereignty over strategic areas. Ultimately, the adoption of an integrated multidomain model contributes not only to the modernization of defense capabilities but also to the consolidation of a proactive and deterrent national posture against emerging threats.

Keywords: Unmanned Vehicles. Unmanned Systems. Soft Kill Coustermeasures. Neutralisation. Multidomain Defense. Electronic Warfare. Acoustic Warfare. Cybernetic Warfare. Integrated Response Model

LISTA DE ABREVIATURAS E SIGLAS

AIS	–	<i>Authomatic Identification System</i>
AJB	–	Águas Jurisdicionais Brasileiras
ANAC	–	Agência Nacional de Aviação Civil
ARP	–	Aeronave Remotamente Pilotada
BLOS	–	<i>Beyond Line of Sight</i>
C2	–	Comando e Controle
ComOpNav	–	Comando de Operações Navais
DARPA	–	<i>Defense Advanced Research Projects Agency</i>
DDoS	–	<i>Distributed Denial of Service</i>
DoD	–	<i>Department of Defense</i>
DoS	–	<i>Denial of Service</i>
DSSS	–	<i>Direct-Sequence Spread Spectrum</i>
ECR	–	Estação de Controle Remoto
EEM	–	Espectro Eletromagnético
END	–	Estratégia Nacional de Defesa
EO	–	Electro-optical
EUA	–	Estados Unidos da América
FHSS	–	<i>Frequency-Hopping Spread Spectrum</i>
FLIR	–	<i>Forward Looking InfraRed</i>
GA	–	Guerra Acústica
G Ciber	–	Guerra Cibernética
GE	–	Guerra Eletrônica
GNSS	–	<i>Global Navigation Satellite System</i>
GPS	–	<i>Global Positioning System</i>
IA	–	Inteligência Artificial
ID	–	Identificação
INS	–	<i>Inertial Navigation System</i>
IR	–	<i>InfraRed</i>
IVR	–	Inteligência, Vigilância e Reconhecimento
JAPCC	–	<i>Joint Air Power Competence Centre</i>
LOS	–	<i>Line of Sight</i>

MAE	–	Medidas de Ataque Eletrônico
MAGE	–	Medidas de Apoio à Guerra Eletrônica
MB	–	Marinha do Brasil
MD	–	Ministério da Defesa
MPE	–	Medidas de Proteção Eletrônica
ONR	–	<i>Office of Naval Research</i>
OTAN	–	Organização do Tratado do Atlântico Norte
PEM	–	Plano Estratégico da Marinha
RF	–	Radiofrequência
SARP	–	Sistema de Aeronave Remotamente Pilotada
SRP	–	Sistema Remotamente Pilotado
UAS	–	<i>Unmanned Aerial System</i>
UAV	–	<i>Unmanned Aerial Vehicle</i>
UHF	–	<i>Ultra High Frequency</i>
UUV	–	<i>Unmanned Underwater Vehicle</i>
VANT	–	Veículo Aéreo Não Tripulado
VHF	–	<i>Very High Frequency</i>
VNT	–	Veículo Não Tripulado
VRP	–	Veículo Remotamente Pilotado
VSNT	–	Veículo de Superfície Não Tripulado
VSOR	–	Veículo Submarino de Operação Remota
VSRP	–	Veículo de Superfície Remotamente Pilotado

SUMÁRIO

1	INTRODUÇÃO.....	12
2	FUNDAMENTAÇÃO TEÓRICA	14
2.1	VEÍCULOS NÃO TRIPULADOS: CONCEITOS E CLASSIFICAÇÃO.....	14
2.1.1	Sistemas Aéreos Remotamente Pilotados (SARP).....	15
2.1.2	Veículo de Superfície Remotamente Pilotado (VSRP).....	16
2.1.3	Veículo Submarino de Operação Remota (VSOR).....	18
2.2	A GUERRA ELETRÔNICA E SUA APLICAÇÃO CONTRA SISTEMAS REMOTAMENTE PILOTADOS.....	18
2.3	A GUERRA ACÚSTICA E SUA UTILIZAÇÃO EM AMBIENTES MARÍTIMOS E SUBMARINOS.....	19
2.4	A GUERRA CIBERNÉTICA E SUAS AÇÕES EM SISTEMAS REMOTAMENTE PILOTADOS.....	20
2.5	CONTRAMEDIDAS NÃO CINÉTICAS: CONCEITOS E CLASSIFICAÇÕES.....	21
3	TECNOLOGIAS E SOLUÇÕES DE DEFESA ATUAIS.....	21
3.1	CLASSIFICAÇÃO DAS TECNOLOGIAS DE DEFESA.....	21
3.1.1	Contramedidas Eletrônicas.....	22
3.1.1.1	<i>Interferência Eletromagnética (Jamming)</i>	22
3.1.1.2	<i>Simulação de Sinais (Spoofing)</i>	22
3.1.2	Contramedidas Acústicas.....	23
3.1.2.1	<i>Aplicações no Domínio Subaquático</i>	24
3.1.2.2	<i>Aplicações no Domínio Acima d'Água</i>	24
3.1.3	Contramedidas Cibernéticas.....	25
3.2	SOLUÇÕES INTEGRADAS ATUAIS.....	26
3.3	CENÁRIO OPERACIONAL.....	28
3.3.1	Estudo de Caso: Conflito entre Rússia e Ucrânia.....	28
4	PROPOSTA DE MODELO INTEGRADO DE DEFESA MULTIDOMÍNIO. 29	
4.1	PREMISSAS PARA INTEGRAÇÃO DE CONTRAMEDIDAS.....	29
4.2	ARQUITETURA CONCEITUAL DO MODELO.....	32
4.2.1	Deteção e Classificação.....	33

4.2.2	Tomada de Decisão.....	34
4.2.3	Neutralização Adaptativa.....	34
4.3	COMPARATIVO ENTRE TÉCNICAS E LACUNAS OBSERVADAS.....	36
4.4	CONDUTAS PARA IMPLEMENTAÇÃO.....	37
5	CONCLUSÃO.....	39
	REFERÊNCIAS	41

1 INTRODUÇÃO

Nas últimas duas décadas, os avanços tecnológicos impulsionaram uma transformação significativa no cenário de operações militares, especialmente com a crescente adoção de veículos não tripulados (VNT) (Matlack; Schwartz; Gill, 2025). Plataformas como Veículos Aéreos Não Tripulados¹ (VANT), Veículos de Superfície Não Tripulados² (VSNT) e Veículos Subaquáticos Não Tripulados³ passaram a desempenhar funções estratégicas em missões de Inteligência, Vigilância e Reconhecimento (IVR), Guerra Eletrônica (GA), coleta de dados sensíveis e até mesmo em ataques coordenados, muitas vezes com o apoio de Inteligência Artificial (IA), comprometendo significativamente a soberania e a prontidão operacional das Forças Navais (Slusher, 2025).

O emprego de VNTs transcende a mera substituição de meios convencionais, introduzindo uma nova lógica de operação baseada em conectividade em tempo real, modularidade e economia de recursos humanos e financeiros, o que demanda uma reformulação das arquiteturas tradicionais de defesa (Kunertova, 2024). No contexto marítimo, especificamente, os desafios se multiplicam, dada a tridimensionalidade do ambiente, a complexidade acústica subaquática e a necessidade de vigilância contínua em vastas áreas oceânicas.

A crescente acessibilidade dessas tecnologias por atores não estatais também amplia o escopo de risco. Grupos insurgentes, organizações criminosas transnacionais e mesmo empresas privadas com interesses estratégicos têm empregado VNTs para fins de monitoramento, contrabando, sabotagem ou ataques de precisão, muitas vezes utilizando artifícios de difícil rastreamento (Norman, 2019).

Este novo paradigma operacional apresenta desafios complexos para as Forças Armadas, uma vez que as capacidades defensivas tradicionais têm se mostrado insuficientes frente à agilidade, ao volume e à diversidade de ameaças que essas plataformas representam.

¹ De acordo com o Glossário das Forças Armadas, o *drone* aéreo, operado remotamente por um piloto ou de maneira autônoma é denominado Veículo Aéreo Não tripulado VANT (Brasil, 2015, p. 95 e p. 278).

² Não foi observado em doutrinas e manuais atuais a denominação oficial para um veículo de superfície não tripulado. Nos capítulos seguintes, este tipo de plataforma é designado pelo autor, de maneira conveniente para dar prosseguimento ao estudo realizado neste trabalho.

³ De acordo com o Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas, o veículo subaquático não tripulado, operado remotamente por um piloto, é denominado Veículo Submarino de Operação Remota – VSOR (Brasil, 2021, p. 158).

Nesse contexto, torna-se urgente o desenvolvimento de estratégias eficazes de neutralização, especialmente aquelas que não dependem de força cinética. Conforme apresentado em Wang, Liu e Song (2021), contramedidas baseadas em Guerra Eletrônica, Guerra Acústica (GA) e Guerra Cibernética (G Ciber) têm ganhado destaque como alternativas promissoras para a proteção de ativos sensíveis e infraestruturas críticas, tanto em ambientes terrestres quanto marítimos e subaquáticos. O desenvolvimento de contramedidas não cinéticas eficazes requer uma compreensão sistêmica das vulnerabilidades apresentadas por esses veículos. Tecnologias de interferência eletromagnética (*Jamming*), bloqueio aos sinais provenientes de Sistemas Globais de Navegação por Satélite (GNSS), engano (*Spoofing*), sequestro cibernético e armadilhas acústicas e térmicas são exemplos de recursos que, quando integrados a um sistema de Comando e Controle (C2) resiliente, podem ampliar significativamente a capacidade de resposta das Forças Navais (Kang *et al.*, 2020). A adoção de tais métodos se alinha aos princípios estabelecidos na Estratégia Nacional de Defesa (END) e no Plano Estratégico da Marinha (PEM), que destacam a importância do domínio tecnológico em áreas sensíveis e a defesa da Amazônia Azul (Brasil, 2020a; Brasil, 2020b).

Do ponto de vista doutrinário, observa-se uma crescente convergência entre os conceitos de GA, GE, G Ciber e operações de informação, o que reforça a necessidade de capacitação de recursos humanos, desenvolvimento de protocolos de interoperabilidade e investimentos em pesquisa *dual-use* (civil-militar). O domínio tecnológico, nesse contexto, passa a ser não apenas uma vantagem operacional, mas um requisito mínimo para garantir a defesa dos interesses nacionais em um ambiente geopolítico cada vez mais volátil.

Este trabalho tem como objetivo principal, descrever as principais tecnologias de neutralização não cinéticas atualmente disponíveis contra VNTs, sistematizando seus usos operacionais e propondo, conceitualmente, um modelo integrado de defesa multidomínio⁴. De maneira complementar, busca-se propor uma visão estratégica que possa orientar futuras atualizações doutrinárias e aquisições tecnológicas pela Marinha do Brasil (MB). Ao final, pretende-se oferecer subsídios que possam

⁴ Brasil (2018) cita os cinco domínios reconhecidos do conflito: naval, aéreo, terrestre, espacial e cibernético. Desta maneira, multidomínio é considerado o conjunto dos domínios em que o conflito pode ocorrer. As ações de Guerra Acústica, de Guerra Eletrônica e de Guerra Cibernética abordadas no trabalho, não se limitam a um único domínio, podendo ser aplicadas de maneira mais conveniente e eficaz.

contribuir para o fortalecimento das capacidades defensivas da MB diante das ameaças emergentes no século 21. Para tanto, será realizada uma revisão teórica fundamentada em doutrinas e manuais militares e na literatura científica dos últimos vinte anos, com foco em abordagens adaptativas e interoperáveis.

Neste ponto, é bastante importante entender as classificações apresentadas em doutrinas nacionais que definem as diferenças entre os tipos de sistemas e veículos não tripulados, seja por ambientes ou por seu modo de operação. Esta classificação é apresentada na Seção 2.1, e define o objeto de estudo abordado neste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo aborda os principais conceitos de sistemas não tripulados e as aplicações das ferramentas da Guerra Eletrônica, Acústica e Cibernética na mitigação e neutralização de veículos não tripulados.

2.1 VEÍCULOS NÃO TRIPULADOS: CONCEITOS E CLASSIFICAÇÃO

As doutrinas nacionais não contemplam a definição de veículo não tripulado. Além disso, não há uma definição doutrinária abrangente para os seus sistemas periféricos. O segmento da OTAN especializado em poder aéreo e espacial, com foco em doutrinas e conceitos, o *Joint Air Power Competence Centre* (JAPCC), define um Sistema Não Tripulado (SNT), em JAPCC (2021), como um conjunto integrado de componentes operacionais e sensoriais composto por, pelo menos um VNT e, por vezes, por um canal de C2 que permite a realização de missões sem a presença física de tripulantes a bordo do meio.

Veículos não tripulados são geralmente agrupados, de acordo com o ambiente em que operam, em três categorias principais: Veículos Aéreos Não Tripulados, Veículos de Superfície Não Tripulados e Veículos Subaquáticos Não Tripulados. Quanto ao modo de operação, se desdobram, essencialmente, em duas categorias: os Sistemas Remotamente Pilotados (SRPs), que dependem de um operador humano para sua condução em tempo real do veículo remotamente pilotado (VRP), e os sistemas autônomos, dotados de inteligência embarcada que lhes confere a capacidade de executar tarefas de forma independente, com base em programação

prévia ou em resposta a estímulos do domínio em que operam. Ambos os modelos têm ganhado crescente relevância nas operações militares modernas, no entanto este trabalho restringir-se-á aos Sistemas Remotamente Pilotados nos domínios aéreo, marítimo de superfície e subaquático⁵. A seguir, são apresentados os conceitos dos sistemas não tripulados⁶ selecionados neste estudo: o Sistema Aéreo Remotamente Pilotado (SARP), o Veículo de Superfície Remotamente Pilotado (VSRP) e, por fim, o Veículo Submarino de Operação Remota (VSOR).

2.1.1 Sistemas Aéreos Remotamente Pilotados (SARP)

Um Sistema Aéreo Remotamente Pilotado é composto, de acordo com JAPCC (2021), pelos seguintes elementos principais:

- a) Aeronave Remotamente Pilotada (ARP): é o próprio veículo aéreo, equipado com sensores, sistemas de navegação e carga útil (como câmeras, sensores eletro-ópticos (EO), radares, etc.). Pode ser de asa fixa, rotativa ou híbrida;
- b) Estação de Controle Remoto (ECR): é o local onde o operador humano pilota o sistema, podendo ser em solo, embarcada em navio ou até instalada em aeronaves-mãe. Permite o controle de voo, a recepção de dados e o envio de comandos à ARP;
- c) Enlaces de Comunicação: são os sistemas de transmissão de dados e comandos entre a ECR e a ARP, podendo ser via:
 - Rádio com linha de visada (LOS);
 - Satélite (BLOS); ou
 - Redes de dados seguras.
- d) Carga Útil de Missão: são os equipamentos ou armamentos transportados pela ARP, dependendo do tipo de missão: vigilância, reconhecimento, ataque, guerra eletrônica etc.

Os SARPs podem ser empregados, por exemplo, em missões de IVR, ataque de precisão e GE (Slusher, 2025). Sua flexibilidade operacional, aliada a baixos custos de produção e manutenção, tornou-os ferramentas centrais em operações militares e

⁵ Devido à existência de VNTs capazes de operar na superfície do mar ou de maneira subaquática, estes ambientes serão considerados aqui, pertencentes a domínios distintos.

⁶ Devido à carência de definições sobre os sistemas remotamente pilotados marítimos e subaquáticos, os VSRPs e VSORs serão considerados neste trabalho como sistemas, compreendendo todo o aparato que os faça operar de maneira remota.

em ações de grupos insurgentes (Norman, 2019).

As variadas aplicações e características dos SARP levaram à categorização desses vetores. A Agência Nacional de Aviação Civil (ANAC) leva em consideração, primordialmente, o peso da plataforma, assemelhando-se ao critério utilizado pela Organização de Tratado do Atlântico Norte (OTAN) (NATO, 2009). O Ministério da Defesa (MD) optou por categorizar os SARPs, com base no tipo de emprego do sistema (Tático, Operacional e Estratégico). Diante das diversas classificações correntes, a MB adotou a classificação para os SARPs com base na sua massa e nível de requisito operacional, conforme apresentado no quadro 1, que pode ser encontrada em Brasil (2022).

Quadro 1 – Categorias de SARP adotadas pela Marinha do Brasil

Requisito operacional	Categoria MB⁷	Massa
Requisito simples para operação em determinadas condições	0	< 2 kg
	1	Entre 2 kg e 25 kg
	2	Entre 25 kg e 150 kg.
	3	Entre 150 kg e 600 kg.
Requisitos mais elevados para operação	5	> 600 kg, até 45.000 pés.
	6	> 600 kg, > 45.000 pés.

Fonte: Brasil (2022)

Devido a parâmetros operacionais, como alcance, tipo de enlace de controle e emprego rotineiro, serão considerados para efeito de estudo, neste trabalho, somente os SARPs categoria 0 e 1, do referido quadro, reportados por serem comumente uma ameaça à segurança orgânica de uma Organização Militar, diante da possibilidade da prática de alguma das atividades citadas no capítulo introdutório.

2.1.2 Veículo de Superfície Remotamente Pilotado (VSRP)

O Glossário das Forças Armadas, em Brasil (2015), e o Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas do Ministério da Defesa em Brasil (2021), carecem da definição de um veículo não tripulado que realize ações em superfície de mares ou rios. A Marinha do Brasil, adota cotidianamente o termo Veículo de Superfície Não tripulado (VSNT) para este tipo de veículo, inclusive no que

⁷ Não foi observada, na publicação em lide, a categoria 4 para um SARP.

se refere ao sistema de controle como um todo. No entanto, há a carência de uma classificação para suas subcategorias, bem como uma definição quanto ao nível de autonomia de um VSNT. O quadro 2, apresenta uma compilação das classificações de VSNT, com base em estudos publicados pela OTAN em NATO (2014), e pelo americano *Office of Naval Research*, em *Congressional Research Service* (2024). É conveniente delimitar o escopo deste trabalho de maneira que as contramedidas apresentadas nas seções seguintes sejam coerentes em relação ao objeto de interesse. Desta maneira, um VSNT que possua modo de operação remota, por meio de um operador humano, mediante a transmissão de sinais, sejam eles radiofrequência por visada direta ou por meio de repetidoras de sinais intermediárias, será denominado neste trabalho Veículo de Superfície Remotamente Pilotado (VSRP).

Quadro 2 – Categorias de VSRP

Critério	Categoria	Descrição
Tamanho	Micro	Menor que 1 metro.
	Pequeno	Entre 1 e 7 metros.
	Médio	Entre 7 e 12 metros.
	Grande	Acima de 12 metros.
Grau de autonomia	Remotamente operado	Controlado em tempo real por operador via link de dados.
	Semiautônomo	Navegação e controle automatizado, com supervisão remota.
	Autônomo	Decide e executa missões com mínima intervenção humana.
Função operacional / Missão	IVR	Coleta de imagens, dados e monitoramento de áreas sensíveis.
	Guerra de minas	Localização e neutralização de minas navais.
	Guerra antissubmarino	Apoio à detecção de submarinos inimigos.
	Defesa de Porto / Força	Interceptação de ameaças e proteção de perímetros.
	Alvo naval / treinamento	Simulação de embarcações para exercícios navais.
Ambiente operacional	Fluvial	Operações em rios e ambientes interiores.
	Costeiro	Regiões litorâneas e zonas econômicas exclusivas.
	Oceânico	Missões em alto-mar e com grande autonomia.

Fonte: Adaptado de NATO (2014) e Congressional Research Service (2024).

A estrutura que compõe um VSRP é similar à de um SARP, distinguindo-se pelo veículo, neste caso, uma embarcação flutuante, com propulsão própria. Os VSRPs operam na superfície de mares ou rios e têm sido utilizados, em sua maioria, para patrulha naval, escolta, inteligência de sinais, guerra de minas e ataques a embarcações e infraestruturas. Seu emprego reduz a exposição de tripulações humanas em ambientes de alto risco.

2.1.3 Veículo Submarino de Operação Remota (VSOR)

Os Veículos Submarinos de Operação Remota (VSORs), conforme denominados em Brasil (2015), por sua vez, operam submersos e podem ser aplicados em tarefas como coleta de dados oceânicos, sabotagem de infraestruturas subaquáticas ou reconhecimento em áreas de interesse estratégico. Sua furtividade e capacidade de operar por longos períodos sem detecção os tornam uma ameaça crescente (Khawaja *et al.*, 2022).

Os VSOR são compostos por um casco resistente à pressão, que protege sua eletrônica embarcada, propulsores e lemes, que possibilitam manobras submersas em três dimensões, sensores de navegação, sonar e câmeras. Sua carga útil pode incluir sensores acústicos, espectrômetros, braços robóticos ou cargas para neutralização.

O enlace de comunicação entre um VSOR e sua ECR pode ser estabelecido tanto por cabo, como fibra ótica ou por ondas acústicas.

A classificação de um VSOR pode variar conforme a doutrina de cada país, mas há classificações amplamente aceitas em publicações da OTAN, do Departamento de Defesa (DoD) dos EUA e da comunidade científica e tecnológica. Não foram encontradas definição e classificação formais para este tipo de veículo nas doutrinas das Forças Armadas brasileiras.

2.2 A GUERRA ELETRÔNICA E SUA APLICAÇÃO CONTRA SISTEMAS REMOTAMENTE PILOTADOS

A Marinha do Brasil, por meio do Manual de Ações de Guerra Eletrônica, define o conceito de Guerra Eletrônica como:

O conjunto de ações que visam a:

- I. Explorar as emissões do inimigo, com a finalidade de conhecer a sua ordem de batalha, intenções e capacidades; e
- II. Utilizar medidas adequadas para prevenir o uso efetivo dos nossos sistemas. (Brasil, 2018, p. 17).

Este conceito é reforçado pela Política de Guerra Eletrônica de Defesa, que versa que:

As atividades de Guerra Eletrônica nas Forças Armadas são conduzidas de modo a assegurar o uso do espectro eletromagnético por nossas forças e impedir, reduzir ou prevenir seu uso contra os interesses do país; (Brasil, 2004, p. 13).

De maneira ampla, a GE tem se apresentado como um componente essencial das operações modernas. Ela surge como uma ferramenta de neutralização não cinética, com grande capacidade de comprometer a eficácia desses modernos e voláteis sistemas, seja em operações militares ou diante das ameaças corriqueiras à segurança de infraestruturas e meios navais, sem a necessidade de destruição física ou comprometimento da segurança do pessoal próximo.

As medidas de GE apresentadas em Brasil (2018) são amplamente conhecidas nas Forças Armadas, e podem ser aplicadas contra SRPs. São classificadas em três categorias principais: Medidas de Apoio Eletrônico (MAGE), Medidas de Proteção Eletrônica (MPE) e Medidas de Ataque Eletrônico (MAE). As Medidas de Apoio Eletrônico incluem a detecção, localização e rastreamento dos sinais emitidos pelos SRPs, como os enlaces de controle, vídeo, telemetria e sinais de navegação. Já as Medidas de Proteção Eletrônica visam resguardar os próprios sistemas contra ações de GE inimiga, como saltos de frequências, grandes larguras de bandas de canais e navegação inercial redundante. Por fim, as Medidas de Ataque Eletrônico consistem na interferência ativa nos sistemas do adversário, utilizando técnicas eletrônicas específicas para a interrupção dos sistemas e sensores embarcados.

Os métodos de GE aplicados a SRPs serão apresentados detalhadamente no Capítulo 3.

2.3 A GUERRA ACÚSTICA E SUA UTILIZAÇÃO EM AMBIENTES MARÍTIMOS E SUBMARINOS

A Guerra Acústica no Brasil é relativamente moderna quando comparada à

Guerra Eletrônica e carece de doutrina e manuais de procedimentos operativos. Os estudos aqui realizados foram realizados, majoritariamente, com base em doutrinas e manuais de Forças Armadas estrangeiras, disponíveis em fontes abertas.

A GA se baseia no uso estratégico das ondas sonoras, especialmente no ambiente marítimo. Em razão das limitações físicas da propagação de ondas eletromagnéticas na água — onde sinais de rádio e radar sofrem forte atenuação — o som torna-se o principal meio de comunicação, detecção e navegação abaixo d'água. United States (2010) define a Guerra Acústica como:

As ações que envolvem o uso de energia acústica subaquática para determinar, explorar, reduzir ou impedir o uso hostil do espectro acústico subaquático pelo oponente e, concomitantemente, as ações que garantem o uso do espectro acústico subaquático pela própria Força (United States, 2010, p. 2, tradução própria).

A GA representa uma ferramenta essencial para o controle do espaço subaquático, podendo integrar sensores e contramedidas voltadas à vigilância, dissuasão e neutralização de ameaças. Entre suas aplicações mais relevantes, abordadas em literaturas sobre o assunto, destaca-se o sensoriamento acústico, por meio de sonares ativos e passivos, utilizado para detectar, rastrear e classificar embarcações, torpedos, VSNTs e VSORs.

As contramedidas acústicas, conforme definidas em United States (2010) e Khawaja *et al.* (2022), podem ser definidas como o conjunto de técnicas e sistemas utilizados para enganar, bloquear ou saturar os sensores e sistemas de navegação acústica de Sistemas Remotamente Pilotados. O Capítulo 3 aborda as contramedidas mais comumente utilizadas a um SRP.

2.4 GUERRA CIBERNÉTICA E SUAS AÇÕES EM SISTEMAS REMOTAMENTE PILOTADOS

Como definida em Brasil (2015), a Guerra Cibernética refere-se diretamente “[...] ao uso de operações em ambiente digital, caracterizando-se pelo uso ofensivo e defensivo de tecnologias da informação e comunicação para comprometer, degradar, explorar ou controlar ativos digitais e sistemas computacionais de um adversário”. Diferentemente dos conflitos cinéticos, a G Ciber ocorre no domínio virtual, sendo conduzida por meio de *softwares* maliciosos, algoritmos autônomos e operações de

intrusão que visam vulnerabilidades específicas.

No contexto dos SRPs, as vulnerabilidades cibernéticas se multiplicam à medida que essas plataformas passam a incorporar tecnologias de IA, aprendizado de máquina e comunicações baseadas em rede, inclusive com dependência de sinais de navegação por satélite. Segundo Wang, Liu e Song (2021), a incorporação de IA e comunicação em rede nos SRPs modernos ampliou sua eficácia, mas também os tornou mais suscetíveis a ataques cibernéticos. A atuação cibernética pode permitir desde a coleta de dados até o desvio de rotas e a autodestruição da plataforma.

2.5 CONTRAMEDIDAS NÃO CINÉTICAS: CONCEITOS E CLASSIFICAÇÕES

As contramedidas para Sistemas Remotamente Pilotados dividem-se, genericamente, em cinéticas e não cinéticas, cotidianamente denominadas *hard kill* e *soft kill*, respectivamente. As primeiras envolvem a destruição física do alvo por projéteis, lasers ou sistemas capazes de gerar ondas eletromagnéticas de alta potência, por exemplo. Já as contramedidas não cinéticas têm como objetivo desabilitar, desorientar ou acessar e controlar os sistemas-alvo sem causar sua destruição, preservando, inclusive, a possibilidade de interceptação ou estudo da plataforma.

Dentre as técnicas de *soft kill*, apresentadas em Farlík e Gacho (2021), Khawaja *et al.* (2022) e Wang, Liu e Song (2021), destacam-se o bloqueio de sinal (*jamming*), o engano (*spoofing*), o ataque cibernético, a interferência e o engano acústico e a ilusão visual ou térmica (uso de dispositivos para confundir sensores ópticos ou infravermelhos, respectivamente).

A efetividade dessas contramedidas depende de fatores como o tipo e a robustez do sistema-alvo, o domínio (aéreo, marítimo, subaquático), e a capacidade de resposta da plataforma de defesa.

3 TECNOLOGIAS E SOLUÇÕES DE DEFESA ATUAIS

3.1 CLASSIFICAÇÃO DAS TECNOLOGIAS DE DEFESA

As tecnologias atuais voltadas à neutralização de sistemas remotamente pilotados são comumente classificadas com base no ambiente operacional em que

um efetor, isto é, um dispositivo de contramedida, atuará no sistema-alvo, assim como observado em Farlík e Gacho (2021), Khawaja *et al.* (2022) e Wang, Liu e Song (2021). Neste trabalho, serão adotadas três classificações principais de contramedidas não cinéticas: eletrônicas, acústicas e cibernéticas. Funcionalmente, cada uma atua de maneira distinta e independente, conforme demandadas pelas características operacionais da ameaça, seja ela um SARP, um VSRP ou um VSOR.

3.1.1 Contramedidas Eletrônicas

3.1.1.1 *Interferência Eletromagnética (Jamming)*

A técnica de interferência eletromagnética, comumente chamada de *jamming*, baseia-se na emissão de sinais eletromagnéticos com o objetivo de sobrecarregar os receptores de comunicação, navegação, vídeo ou controle de um SRP. Essa interferência pode ser dirigida, por meio de feixes concentrados (diretivos), ou omnidirecional, dependendo do nível de precisão, descrição e alcance exigido pela operação.

O uso de *jammers* pode interromper a comunicação entre o operador e a plataforma (*link* C2), bloquear o recebimento de sinais GNSS ou prejudicar o fluxo de dados e vídeo de missão. No entanto, Curpen *et al.* (2018), mostra que sua eficácia está condicionada à potência do sinal, distância do alvo, largura de banda empregada e tipo bloqueio (ponto, barragem ou varredura). Esta técnica apresenta grande eficácia contra SARPs e VSRP, no entanto, SRPs providos com capacidades autônomas ou redundância de sistemas de navegação tendem a apresentar maior resistência a esse tipo de contramedida (Wang; Liu; Song, 2021).

3.1.1.2 *Simulação de Sinais (Spoofing)*

Ao contrário do *jamming*, o *spoofing* consiste na simulação de sinais de GNSS ou comunicação com o objetivo de enganar os sensores de um veículo remotamente pilotado. Por meio dessa técnica, é possível induzir a plataforma a alterar sua rota, pousar em área segura ou colidir de forma controlada (Kang *et al.*, 2020).

Essa abordagem mostra-se particularmente eficaz contra plataformas que dependem exclusivamente de navegação satelital (GNSS), sem validação cruzada

com sistemas inerciais. No entanto, sua implementação demanda conhecimento detalhado da arquitetura do sistema-alvo, o que restringe sua aplicação em cenários desconhecidos.

A eficácia de contramedidas de GE aplicadas a SRPs depende de diversos fatores, incluindo a distância, a potência dos transmissores, a arquitetura dos sistemas adversários, o nível de automação dos veículos e a existência de contramedidas. Sistemas mais autônomos, por exemplo, podem manter-se operacionais mesmo em ambientes de interferência intensa, utilizando sensores embarcados e rotinas de navegação independente. Ainda assim, a GE continua sendo uma opção estratégica atrativa por sua natureza não letal, de baixo custo relativo e elevada flexibilidade tática.

3.1.2 Contramedidas Acústicas

As contramedidas acústicas, segundo Khawaja *et al.* (2022) e United States (2010), se dividem em três categorias principais:

- a) Interferência Acústica (*Acoustic Jamming*): envolve a emissão de ruído ativo (*broadband* ou *narrowband*) com o objetivo de mascarar sinais reais ou saturar os receptores dos sensores acústicos dos veículos, comprometendo sua capacidade de navegação, detecção ou orientação;
- b) Simulação Acústica (*Acoustic Spoofing* ou *Decoying*): consiste na criação deliberada de ecos ou assinaturas falsas que simulam alvos inexistentes, desviando o veículo de sua rota original, atraindo-o para zonas controladas ou forçando-o a iniciar procedimentos de evasão ou autopreservação; e
- c) Isolamento Acústico (Silenciamento ou Camuflagem): refere-se a técnicas passivas empregadas para tornar as plataformas amigas indetectáveis aos sensores dos VSNTs e VSORs, reduzindo a assinatura sonora através de materiais anecóicos ou manobras acústicas discretas.

Além das plataformas navais tradicionais, estas contramedidas podem ser embarcadas em boias inteligentes e sistemas estáticos de vigilância subaquática, como redes de sensores distribuídos. O uso de transdutores acústicos direcionais ou sistemas de modulação de sinais acústicos digitais permite aumentar a eficácia das contramedidas, tornando possível interferir seletivamente em determinados tipos de sensores ou faixas de frequência (Fayaz; Parah; Qureshi, 2022).

A aplicação dessas técnicas, entretanto, demanda amplo conhecimento do comportamento acústico do ambiente marítimo, incluindo fatores como salinidade, temperatura, profundidade e topografia submarina, que afetam diretamente a propagação das ondas sonoras.

O emprego de contramedidas acústicas contra VSNTs e VSORs representa um componente tático relevante dentro da defesa multidomínio no ambiente marítimo, especialmente no contexto da proteção de áreas sensíveis, como portos, instalações *offshore*, rotas estratégicas e infraestruturas submarinas. A integração desses sistemas a redes de vigilância costeira pode ampliar significativamente a capacidade de dissuasão e resposta frente à crescente ameaça representada por veículos não tripulados em seu entorno estratégico.

3.1.2.1 Aplicações no Domínio Subaquático

No ambiente subaquático, onde veículos não tripulados operam com base em sensores acústicos e sistemas de navegação *doppler*, as contramedidas⁸ acústicas ganham destaque. Elas representam uma alternativa não cinética de proteção naval, permitindo a neutralização ou atraso de VSORs hostis sem o emprego de armas letais. Sua relevância tende a crescer no contexto da defesa multidomínio, sobretudo em áreas litorâneas e de interesse estratégico, onde a vigilância e a proteção de infraestruturas críticas demandam soluções inovadoras de dissuasão subaquática.

Plataformas como VSORs utilizam modems acústicos, sonares e sensores passivos. No contexto da Guerra Acústica, esses sistemas podem ser vulneráveis especificamente à interferência acústica e à simulação de alvos falsos (Khawaja *et al.*, 2022).

3.1.2.2 Aplicações no Domínio Acima d'Água

Devido a este tipo de sistema navegar na superfície de mares e rios, contramedidas como a interferência acústica, por meio de emissão contínua de ruído branco na água podem ser eficazes em dificultar a navegação acústica do VSRP se

⁸ O desenvolvimento lento de contramedidas acústicas submarinas decorre da alta complexidade física do ambiente aquático, da dificuldade técnica de gerar e controlar sinais acústicos eficazes, da falta de padronização internacional, do custo de pesquisa e testes e das dúvidas sobre sua eficácia operacional frente a novas ameaças autônomas.

ele for guiado por eco ou sensores sonares, ou reduzir sua capacidade de detecção por sensores passivos embarcados (Khawaja *et al.*, 2022). Alinhado a isto, o uso de *decoys* pode redirecionar o VSRP para uma localização falsa. No entanto, as possibilidades de emprego de contramedidas mais eficazes aos VSRPs, cabem aos artifícios de GE e G Ciber.

3.1.3 Contramedidas Cibernéticas

O avanço da digitalização e da conectividade dos sistemas de Comando e Controle de SRP amplia o espectro de atuação da Guerra Cibernética como ferramenta de neutralização. Nesse campo, as contramedidas buscam comprometer a operação do sistema-alvo por meio da exploração de vulnerabilidades em seus sistemas computacionais.

As técnicas mais empregadas incluem, de acordo com Dey *et al.* (2018), a injeção de *malware*, a manipulação de pacotes de dados, ataques de negação de serviço (DoS) e o sequestro remoto (*hijacking* ou *takeover*), no qual as vulnerabilidades nos canais de comunicação, sensores ou sistemas de navegação são exploradas até que o controle não autorizado do SRP seja assumido. Uma das vantagens dessa abordagem reside na possibilidade de executar ações discretas, reversíveis e de coleta de inteligência. No entanto, segundo Kang *et al.* (2020) a efetividade de tais ataques depende do acesso a informações prévias sobre o sistema-alvo, como suas redes e protocolos de comunicação.

As contramedidas cibernéticas⁹ direcionadas aos SRPs possibilitam a não interferência nos sensores presentes nas proximidades do sistema-alvo. Muitos sistemas atuais que possuem esta tecnologia, possuem a capacidade de seleção de alvos, permitindo, inclusive o cadastramento de modelos ou dispositivos singulares por meio de seus números de identificação (ID) individuais, durante a fase de planejamento da missão. No entanto, para a efetividade de um sistema cibernético anti-SRP, é necessário que haja, sempre, um banco de dados atualizado para a consulta, durante o período de operação.

⁹ As contramedidas cibernéticas aplicadas a SRPs diferem das medidas de guerra eletrônica tradicionais por atuarem diretamente na camada lógica dos sistemas, enquanto a GE atua na camada física do enlace entre o operador e o veículo.

O quadro 3 resume as contramedidas não cinéticas mais comumente utilizadas contra cada sistema, bem como seus respectivos efeitos esperados.

Quadro 3 – Contramedidas não cinéticas e seus respectivos efeitos esperados nos sistemas

Tipo de Ataque	Alvo Principal	Efeito Esperado
<i>Jamming</i>	Enlace de C2	Perda de comunicação com o sistema remoto
<i>Spoofing</i>	GPS ou sistemas de navegação	Desorientação, erro de posição ou desvio de rota
<i>Hijacking / Take over</i>	Sistema de controle embarcado	Assunção do controle por ator externo
<i>Malware</i>	Estação de controle, <i>firmware</i> ou rede	Comprometimento do sistema, vazamento ou dano aos dados
DoS/DDoS	Infraestrutura de controle ou rede	Saturação de recursos, travamento ou interrupção total
Injeção de Pacotes	Enlace de dados	Introdução de comandos falsos ou maliciosos
Interferência Acústica Direta	Sonar passivo ou sensores de navegação	Saturação sensorial, mascaramento de alvos ou erro de leitura
Ilusão Visual (<i>optical decoys</i>)	Câmeras visuais ou infravermelhas (EO/IR)	Engano na identificação de alvos, ocultação ou distração
Ilusão Térmica (IR <i>decoys</i>)	Sensores infravermelhos (FLIR)	Desvio de sensores de rastreamento, mascaramento de fontes reais
Ruído Acústico de Banda Larga	Sistemas de detecção subaquáticos (VSOR)	Não detecção sonar, perda de percepção situacional

Fonte: Compilado de Farlík e Gacho (2021), Khawaja *et al.* (2022) e Wang, Liu e Song (2021)

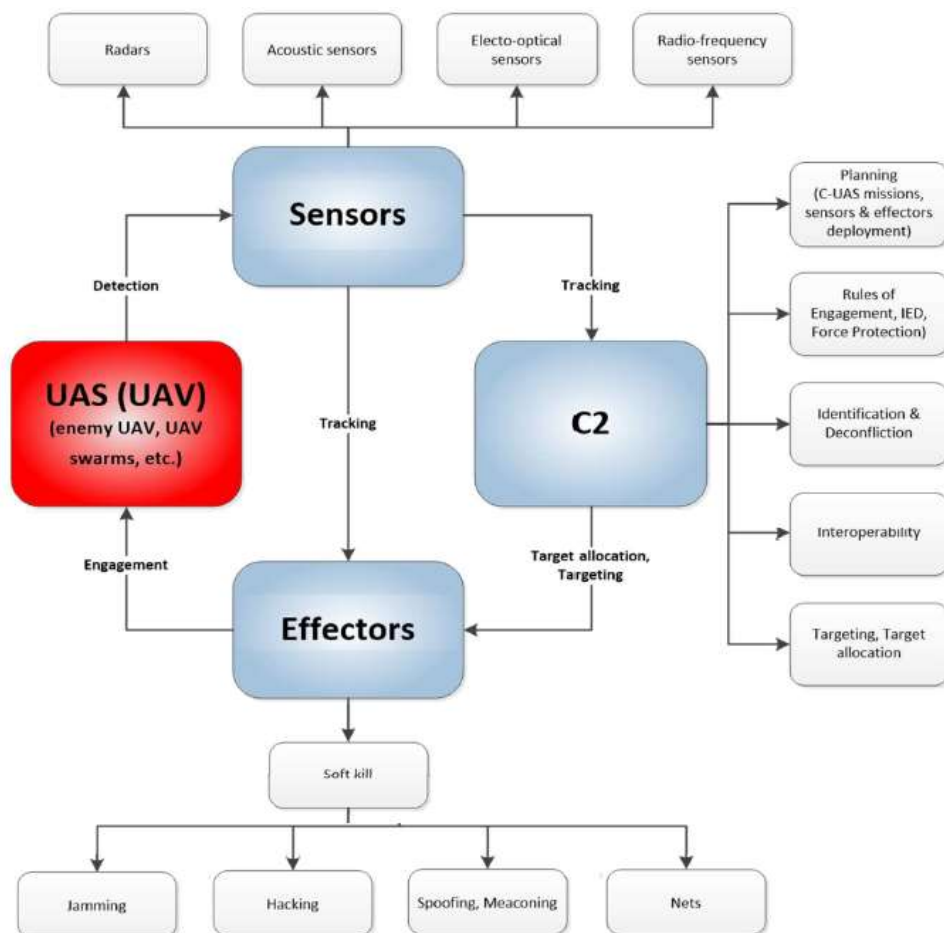
3.2 SOLUÇÕES INTEGRADAS ATUAIS

Atualmente as soluções de contraposição não cinética disponíveis no mercado, exclusivamente para SARP, contemplam a integração de muitas das contramedidas apresentadas nas seções anteriores, como radares, câmeras eletro-ópticas, infravermelhas e térmicas, além de receptores de radiofrequência e de áudio (Kang *et al.*, 2020). Esses sensores são combinados a mecanismos de identificação e classificação, culminando em um módulo de resposta que pode acionar *jammers*, *spoofers*, emissores acústicos ou sistemas de ataque cibernético, simultaneamente

ou não (Wang; Liu; Song, 2021). As características operacionais destes sistemas são efetivas, majoritariamente, contra SARPS de categoria 0 e 1, especificadas no quadro 1, devido, principalmente, ao alcance de seus sensores diante dos perfis de voo dos SARP incluídos nessa categoria. Não foi observado, durante a revisão bibliográfica realizada neste trabalho, soluções multidomínio, capazes de atuarem simultaneamente contra SARPs, VSNTs e VSORs. Uma busca de tecnologias anti-SRP comerciais, apresentou sistemas bem estruturados, providos de centrais de comando e controle, integração de sensores e efetores, dentre outras possibilidades contidas numa tecnologia robusta, porém sem integração entre os domínios aéreo e marítimo.

A figura 1 apresenta um exemplo de arquitetura de um sistema anti-SARP, conforme supracitado, que pode, com devidas adaptações, servir como base para uma arquitetura multidomínio.

Figura 1 – Arquitetura básica de um Sistema Anti-SRP



Fonte: Adaptado de Farlík e Gacho, 2021

A integração multidomínio pode se tornar um princípio essencial para a eficácia desses sistemas, pois permite uma resposta adaptativa frente à variedade de ameaças emergentes nos distintos domínios operacionais.

3.3 CENÁRIO OPERACIONAL

Como exemplo prático, pode-se considerar um meio naval submetido a um ataque coordenado por múltiplas plataformas: SARPs realizando vigilância e coleta de imagens, VSRPs equipados com explosivos de proximidade, e VSORs destinados à obtenção de parâmetros específicos de inteligência. Nesse contexto, a neutralização eficaz requer uma arquitetura integrada de sensores e contramedidas, para os distintos ambientes operacionais.

Um sistema multidomínio, com base em Farlík e Gacho (2021) e Kang *et al.* (2020), minimamente capaz de se contrapor as distintas ameaças, incluiria radares de baixa potência, câmeras EO/IR e receptores de radiofrequência (RF) para identificar e rastrear ameaças aéreas e de superfície, enquanto sensores acústicos passivos e ativos de resposta rápida, seriam utilizados para detectar veículos submersos. Em resposta às ameaças, sistemas anti-SRP, como *jammers*, protocolos automatizados de *spoofing*, mascaramento acústico e ataques cibernéticos poderiam ser acionados como primeira linha de defesa.

De acordo com a Estratégia Nacional de Defesa, a capacidade de resposta a ameaças assimétricas e o domínio de tecnologias críticas são elementos centrais para a soberania nacional, principalmente no contexto da proteção da Amazônia Azul e das infraestruturas críticas associadas (Brasil, 2020b).

3.3.1 Estudo de Caso: Conflito entre Rússia e Ucrânia

O conflito entre Rússia e Ucrânia tem sido um marco no uso militar de veículos não tripulados, com destaque para SARPs, VSRPs e dispositivos submersos. A Ucrânia empregou VNTs comerciais e sistemas como o turco Bayraktar TB2 para missões de inteligência e ataque (Ozberk, 2025). A Rússia, por sua vez, utilizou VNTs como o Orlan-10 e o iraniano Shahed-136, este último aplicado em ataques de saturação contra infraestrutura civil (SHAHED-136..., 2022).

Ambos os lados exploraram o uso de enxames, ataques noturnos e vetores autônomos. Em sua defesa, a Rússia utilizou sistemas de GE, como o Krasukha e o Repellent-1, para *jamming* e *spoofing*, enquanto a Ucrânia recorreu a defesas de curto alcance, barreiras físicas e respostas improvisadas.

Em outro aspecto, o conflito expôs a ausência de integração eficiente entre sensores e efetores em muitas unidades, o que resultou em tempo de resposta elevado e, em alguns casos, em fratricídios ou falhas na neutralização de ameaças. Em áreas costeiras e no Mar Negro, os ataques com VSRPs indicaram a necessidade de sistemas de detecção acústica distribuída, bem como de boias inteligentes e sonares portuários capazes de discriminar alvos pequenos e de baixa assinatura (Khomenko, 2024; RÚSSIA..., 2024).

As lições desse conflito reforçam os pilares do modelo proposto nesta monografia: necessidade de Centros de Comando Multidomínio, resposta automatizada, bancos de dados dinâmicos e integração entre domínios físicos e digitais.

Esse cenário real comprova que, diante de ameaças assimétricas e tecnológicas, somente sistemas integrados, autônomos e adaptativos são capazes de oferecer resposta eficaz e preservar a soberania nacional.

4 PROPOSTA DE MODELO INTEGRADO DE DEFESA MULTIDOMÍNIO

A defesa contra SRPs exige uma abordagem sistêmica, que ultrapasse soluções isoladas e considere o caráter multidomínio das ameaças. O presente capítulo traz uma proposta que visa a fornecer uma base conceitual para o desenvolvimento de um modelo integrado de defesa, adaptável, voltado à neutralização não cinética de sistemas não tripulados, que considera a atuação coordenada nos ambientes cibernético, eletromagnético e acústico em distintos domínios. Ainda que a validação do modelo seja teórica, sua arquitetura baseia-se em doutrinas vigentes, estudos técnicos e análise comparativa de soluções aplicadas.

4.1 PREMISSAS PARA INTEGRAÇÃO DE CONTRAMEDIDAS

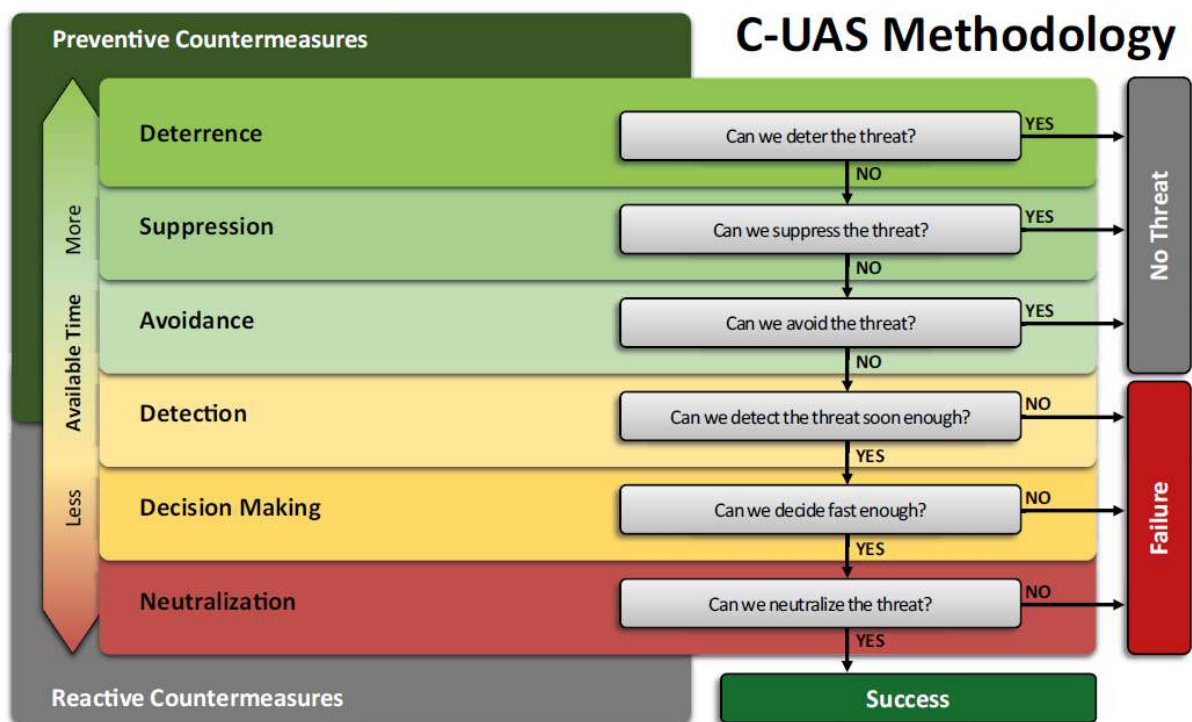
Esta proposta parte da constatação de que soluções isoladas, embora eficazes em contextos específicos, apresentam limitações quando aplicadas a cenários

assimétricos, saturados ou caracterizados pela atuação de enxames de SRP. Assim como apresentado em Farlík e Gacho (2021) e Kang *et al.* (2020), a crescente complexidade das ameaças remotamente pilotadas torna evidente a necessidade de uma abordagem integrada, capaz de combinar diferentes tecnologias e domínios de atuação.

Baseado na análise das literaturas especializadas em sistemas de contramedidas a SARPs referenciadas neste trabalho, bem como nos atuais métodos singelos, mas eficazes contra VSRPs e VSORs, apresentados, por exemplo, em Fayaz, Parah e Qureshi (2022), o modelo integrado de defesa multidomínio proposto, parte de três premissas centrais que sustentam sua arquitetura conceitual:

- a) Integração entre sensores multidomínios e sistemas de resposta: a eficiência de uma rede de defesa contra SRPs depende da capacidade de fusão de dados provenientes de sensores heterogêneos — como radares, sonares, receptores RF e câmeras EO/IR — e de sua correlação em tempo real, como descrito em Kang *et al.* (2020) e Sander *et al.* (2018). A fusão de dados se faz suficiente em um sistema multidomínio do tipo *stand alone*, isto é, em uma arquitetura anti-SRP capaz de operar de forma autônoma, sem depender de integração contínua com outros sistemas ou redes externas para executar suas funções principais. Em utilizações que necessitem de dados provenientes de sensores remotos, presentes, por exemplo em outra plataforma, há a exigência de, não somente, conectividade segura e estável entre os sensores distribuídos, mas também protocolos padronizados e seguros que permitam a interoperabilidade entre estes e, numa maior escala, entre plataformas navais;
- b) Modularidade e escalabilidade das soluções conforme a ameaça: segundo JAPCC (2021), um sistema de defesa eficaz deve ser capaz de escalar suas respostas de acordo com a intensidade da ameaça. Para isso, é essencial que os módulos de neutralização sejam compatíveis com níveis distintos de risco e permitam o uso escalonado ou simultâneo de técnicas, desde alertas até ações de negação eletromagnética ou cibernética. Essa modularidade assegura que o sistema seja economicamente sustentável e operacionalmente viável, mesmo em ambientes com restrições de recursos. A figura 2, apresentada pela Joint Air Power Competence Centre em JAPCC (2021), ilustra um modelo escalável implementado na contraposição a SARPs, que pode respaldar, com os devidos ajustes, o modelo multidomínio aqui proposto.

Figura 2 – Modelo de metodologia de contraposição a Sistemas Remotamente Pilotados, por níveis



Fonte: JAPCC, 2021

c) Atuação simultânea em múltiplos domínios com base em protocolos automatizados: o sucesso na neutralização de SRPs, em especial em cenários de enxame, depende da capacidade de agir de forma coordenada nos ambientes cibernético, eletromagnético e acústico. Segundo o estudo realizado em Kang et al. (2020), que pode ser ajustada para esta proposta, a atuação simultânea deve ocorrer em ciclos de tempo reduzidos, com base em protocolos pré-configurados que permitam o disparo automático de contramedidas, conforme parâmetros de ameaça detectados. A automação, nesse contexto, não visa substituir o operador humano, mas ampliar sua capacidade de resposta frente à velocidade das ameaças modernas.

Além dessas três premissas principais, destaca-se a necessidade de resiliência do sistema frente a falhas ou ataques, o que demanda redundância nos meios de comunicação, protocolos de segurança cibernética embarcados e atualizações contínuas de banco de dados sobre ameaças emergentes. O conceito de “defesa em camadas” se fortalece ao se considerar que cada ambiente (eletrônico, acústico,

cibernético) possui pontos fortes e vulnerabilidades próprias, sendo sua combinação o elemento-chave para a dissuasão eficaz.

A concepção desse modelo está alinhada às diretrizes estabelecidas pela Estratégia Nacional de Defesa em Brasil (2020b) e pelo Plano Estratégico da Marinha do Brasil em Brasil (2020a), especialmente no que tange à proteção de infraestruturas críticas e defesa de áreas sensíveis em seus espaços jurisdicionais. O modelo busca, portanto, integrar as diretrizes estratégicas com soluções tecnológicas que respeitem a realidade logística e operacional das Força Naval brasileira.

4.2 ARQUITETURA CONCEITUAL DO MODELO

A arquitetura conceitual proposta neste trabalho se ancora em uma estrutura modular em camadas, no qual o modelo de defesa básico seja capaz de se contrapor a ameaças nos três domínios operacionais – aéreo, marítimo e subaquático, sendo organizada de forma cíclica e iterativa, composta por três eixos principais: detecção e classificação, tomada de decisão e neutralização adaptativa. Esta segmentação das ações alinha-se aos esquemas propostos nas literaturas precursoras dos estudos na área, como em Arteché *et al.* (2017) e Kilian *et al.* (2015) e às tecnologias atuais consolidadas no mercado.

Essas camadas são concebidas para operar em ciclos curtos, com constante realimentação de dados (*feedback*), de modo a permitir ajustes táticos em tempo real, com base na análise dos efeitos gerados por cada contramedida aplicada. Esse modelo cíclico se mostra particularmente eficaz em cenários dinâmicos, nos quais múltiplas ameaças podem surgir de forma simultânea, exigindo flexibilidade, velocidade e precisão (Kang *et al.*, 2020). Além disso, a escalabilidade da arquitetura permite sua aplicação tanto em ambientes de baixa quanto alta complexidade. Outro aspecto central é a resiliência cibernética da arquitetura, garantida por camadas de proteção contra sabotagens, ataques remotos e interferência intencional. A arquitetura contempla redundância de enlaces de dados, mecanismos de verificação cruzada entre sensores e criptografia *end-to-end* nos canais de comunicação (Rodday; Schmidt; Pras, 2016). Isso assegura que o sistema continue operando mesmo sob tentativas de bloqueio, *spoofing* ou degradação de sinais, especialmente em operações de longa duração em áreas de baixa conectividade (Huang; Wang, 2018).

A integração entre os ambientes eletrônico, acústico e cibernético é realizada por meio de uma camada intermediária de coordenação lógica, similar ao modelo apresentado por Wang, Liu e Song (2021) para medidas anti-SARP, que pode ser baseada em IA embarcada. Essa camada é responsável por processar dados em tempo real, correlacionar informações provenientes de sensores diversos e gerar comandos para efetores específicos, conforme as regras de engajamento predefinidas. Isso confere ao sistema capacidade adaptativa, minimizando a dependência de operadores humanos e reduzindo o tempo entre detecção e reação.

4.2.1 Detecção e Classificação

A etapa de detecção e classificação constitui o primeiro elo da cadeia de resposta do modelo integrado de defesa multidomínio, sendo decisiva para o sucesso das ações subsequentes de tomada de decisão e neutralização. Trata-se da fase em que o sistema detecta, rastreia e classifica potenciais ameaças com base em suas assinaturas eletromagnéticas, térmicas, acústicas, cibernéticas ou comportamentais, discriminando alvos hostis de plataformas legítimas ou elementos do ambiente.

Nesta camada, atuam diversos tipos de sensores heterogêneos e complementares, cujo funcionamento é ajustado de acordo com o domínio operacional e a natureza do veículo a ser detectado. Em ambientes aéreos, por exemplo, predominam sensores radar de curto e médio alcance, receptores de RF, câmeras eletro-ópticas e sensores infravermelhos, capazes de detectar SARPs de pequeno porte e voo baixo. Já no domínio marítimo de superfície, o sistema pode empregar AIS passivo (*Automatic Identification System*), receptores de RF, boias de escuta ou radares de navegação ou de busca de superfície. No domínio subaquático, destacam-se sonares ativos e passivos, modems acústicos de escuta e redes de sensores de fundo (Christnacher *et al.* 2016; Basak; Scheer, 2018; Fayaz; Parah; Qureshi, 2022; Jian; Lu; Chen, 2018).

A fusão desses dados multissensoriais permite ao sistema estabelecer uma imagem tática integrada do espaço protegido, estabelecendo padrões típicos de comportamento associados a SRPs hostis, reduzindo o número de falsos positivos e aumentando a confiabilidade na identificação de ameaças reais.

Além da detecção, essa camada é responsável por classificar automaticamente o tipo de vetor (SARP, VSRP ou VSOR), sua trajetória, velocidade, altitude ou

profundidade, assinatura espectral e nível de ameaça estimado. Para isso, o sistema deve se apoiar em bancos de dados dinâmicos contendo perfis conhecidos de ameaças, históricos de incursões anteriores, características técnicas de SRPs comerciais e militares, além de parâmetros configuráveis de acordo com o Teatro de Operações.

Por fim, cabe ressaltar que o nível de automação da classificação deve ser ajustável, conforme as regras de engajamento e o perfil da missão.

4.2.2 Tomada de Decisão

A etapa de tomada de decisão é o centro lógico do modelo proposto. Em Kang *et al.* (2020), essa camada é apresentada como a responsável por interpretar os dados coletados, avaliar o grau de ameaça e definir a contramedida mais adequada, com base em protocolos pré-configurados e critérios operacionais. Essa resposta é determinada considerando fatores como o tipo de vetor (SARP, VSRP, VSOR), proximidade do alvo, trajetória, ambiente de operação e riscos colaterais.

Kang *et al.* (2020) também explica que a seleção da resposta ocorre a partir de um repositório de protocolos automatizados, permitindo ações escalonadas — desde alertas até interferências eletromagnéticas, acústicas ou cibernéticas. O processo pode ser automatizado, semiautomatizado ou manual com suporte do sistema, dependendo do nível de criticidade e da política de engajamento definida.

Para isso, o sistema deve operar com lógica distribuída e interoperável. O uso de IA e aprendizado supervisionado contribui para o aprimoramento contínuo do processo decisório, com base em simulações, registros de operação e retroalimentação.

4.2.3 Neutralização Adaptativa

A etapa de neutralização adaptativa constitui a camada final e executiva da arquitetura multidomínio, responsável por aplicar, de forma precisa e ajustável, as contramedidas selecionadas durante o processo decisório. Diferente de sistemas tradicionais, onde a resposta tende a ser fixa ou reativa, a neutralização adaptativa permite escalar a resposta de acordo com o comportamento do alvo, atualizando os protocolos à medida que novos dados são recebidos (JAPCC, 2021).

A atuação adaptativa depende da disponibilidade de efetores modulares, capazes de operar em ambientes eletrônico, acústico e cibernético, com variações de intensidade, alcance e tempo de atuação. De acordo com a estrutura desejada, esses efetores podem estar embarcados em plataformas navais, serem fixos em áreas críticas ou mesmo acoplados a sensores móveis (boias e SRPs). Kang *et al.* (2020) apresenta uma estrutura de neutralização adaptativa subdividida em contramedidas para ameaças presentes em solo ou no ar. A inserção de sensores acústicos naquele modelo garantiria, com algumas adaptações, sua aplicação nos domínios de interesse neste trabalho.

Unindo à Kang *et al.* (2020) os modelos apresentados em Farlík e Gacho (2021) e Wang, Liu e Song (2021), é possível definir o início das ações de neutralização multidomínio a partir de gatilhos, como aproximação a uma zona sensível, mudança abrupta de trajetória, perda de comunicação com centro de comando, entre outros. A partir disso, são aplicadas contramedidas específicas para o tipo de vetor detectado:

- a) SARP: *jamming* direcionado no canal C2, *spoofing* de sinais GNSS e, em situações críticas, ataque cibernético ao *link* de dados ou à estação de controle;
- b) VSRP: *jamming* de sinais rádio em *Very High Frequency* (VHF) e *Ultra High Frequency* (UHF), indução de falha em sensores de proximidade, inserção de *malware* no sistema de navegação embarcado; e
- c) VSOR: emissão de ruídos acústicos de saturação, simulação de alvos sonoros falsos e interferência em modems acústicos.

A adaptabilidade está associada a ciclos curtos de análise e realimentação, nos quais o sistema avalia a eficácia da ação aplicada. Se o vetor permanecer ativo após a aplicação inicial, novas contramedidas podem ser ativadas automaticamente ou sob autorização do operador. Isso confere ao sistema maior flexibilidade, especialmente diante de ataques simultâneos ou coordenados por múltiplas plataformas.

A eficácia da neutralização também depende da capacidade de predição de comportamento, baseada em algoritmos que analisam padrões históricos e ajustam a resposta de forma preemptiva. Além disso, a presença de sensores de verificação pode permitir confirmar o efeito desejado (perda de sinal, desvio de rota, imobilização), evitando redundância de ação e sobrecarga nos sistemas.

Por fim, essa camada deve operar com redundância de efetores e protocolos de segurança embarcados, para garantir a continuidade da resposta mesmo sob

interferência hostil. A neutralização adaptativa, portanto, não é apenas uma ação terminal, mas parte integrante de um ciclo dinâmico de defesa, que deve atuar continuamente até a cessação da ameaça.

4.3 COMPARATIVO ENTRE TÉCNICAS E LACUNAS OBSERVADAS

A adoção de um modelo integrado de defesa multidomínio exige a avaliação crítica das principais técnicas de neutralização atualmente disponíveis para enfrentamento de ameaças representadas por sistemas remotamente pilotados. Neste contexto, torna-se essencial comparar os meios cibernéticos, eletromagnéticos e acústicos, considerando critérios como aplicabilidade, reversibilidade, custo e resiliência operacional.

No ambiente eletrônico, as técnicas mais consolidadas incluem o *jamming* de sinais de C2, o *spoofing* de GNSS e a interferência radar. Tais métodos têm se mostrado eficazes contra SRPs aéreos e de superfície que dependem de *links* ativos para navegação e operação. No entanto, sua eficácia pode ser limitada por contramedidas adversárias, como saltos de frequência (dos tipos FHSS ou DSSS), criptografia de sinais ou navegação inercial. Além disso, há riscos de efeitos colaterais sobre sistemas amigáveis, especialmente em ambientes urbanos ou com infraestrutura crítica próxima.

No campo cibernético, destaca-se o uso de *malware* embarcado, interceptação de pacotes de dados e *takeover* remoto. Estas ações têm a vantagem de poderem ser furtivas, persistentes e reversíveis, além de oferecerem acesso a informações sensíveis da ameaça. Contudo, sua execução exige elevado grau de inteligência prévia sobre o alvo e tempo de preparação, o que reduz sua aplicabilidade em respostas imediatas.

Já no ambiente acústico, as técnicas utilizadas contra VSRPs e VSORs envolvem saturação sonar, ruído branco e iscas acústicas. Embora eficazes em ambientes marítimos e subaquáticos, essas técnicas têm alcance limitado, são altamente dependentes das condições ambientais (salinidade, temperatura, profundidade, ruído ambiente) e ainda carecem de maior padronização doutrinária, especialmente no contexto da MB.

A análise comparativa dessas técnicas revela uma lacuna importante: a baixa integração entre os domínios, tanto em termos de operação coordenada quanto de

interoperabilidade entre sistemas. Muitas soluções atuais ainda operam de forma isolada, sem troca de dados entre sensores, algoritmos de apoio à decisão ou efetores combinados. Essa fragmentação pode reduzir a eficiência do sistema e o tempo de resposta.

Outra lacuna crítica observada refere-se à ausência de protocolos automatizados para resposta escalonada, o que implica grande dependência da decisão humana em tempo real. Isso contrasta com o ritmo acelerado dos ataques baseados em veículos autônomos, especialmente quando empregados em enxames. A ausência de regras bem definidas para o uso combinado de contramedidas não letais, sobretudo em zonas costeiras ou áreas civis, também impõe desafios operacionais e jurídicos relevantes.

Além disso, há limitações tecnológicas e logísticas para a adoção em larga escala dessas soluções: sensores subaquáticos de longo alcance são caros e exigem manutenção constante; sistemas de GE direcionada requerem treinamento especializado; e ataques cibernéticos dependem de estruturas robustas de inteligência.

Portanto, o comparativo evidencia a necessidade de desenvolver um modelo integrado, adaptável e automatizado, capaz de atuar de forma coordenada nos três domínios, com base em protocolos dinâmicos e interfaces interoperáveis. Somente assim será possível responder com eficácia às ameaças não convencionais que se projetam no horizonte estratégico da defesa marítima brasileira.

4.4 CONDUTAS PARA A IMPLEMENTAÇÃO

Com base nas referências apresentadas neste estudo, observa-se que para viabilizar a aplicação prática do modelo proposto de defesa multidomínio em cenários operacionais reais, especialmente no contexto brasileiro, algumas condutas estruturantes devem ser adotadas. Estas diretrizes contemplam desde a adaptação de estruturas de comando até a capacitação de pessoal e o desenvolvimento de capacidades tecnológicas específicas. A seguir, são detalhadas cinco orientações fundamentais, baseadas, principalmente em Farlík e Gacho (2021), Kang *et al.* (2020), Khawaja *et al.* (2022), JAPCC (2021) e Wang, Liu e Song (2021):

- a) Desenvolvimento de Centros de Comando Multidomínio: consiste na criação ou adaptação de Centros de Comando e Controle Multidomínio locais ou de área, de

acordo com a necessidade, com infraestrutura adequada para o monitoramento e controle simultâneo de sensores e efetores distribuídos nos distintos domínios operacionais. Esses centros devem ser capazes de integrar dados oriundos de sensores acústicos, eletromagnéticos e cibernéticos, realizando a fusão dessas informações em tempo real e coordenando respostas automatizadas ou humanas conforme os protocolos definidos. A arquitetura desses centros pode ser adaptada para operar de maneira embarcada (em navios de maior porte), em terra, ou integrada, numa estrutura maior de interesse. Todas com redundância de enlaces e proteção cibernética;

- b) Capacitação Técnica de Operadores: a operação segura e eficaz de sistemas integrados de contramedidas requer a formação de operadores multidisciplinares, com domínio das ferramentas de guerras eletrônica, cibernética e acústica. Essa capacitação deve ser incorporada aos currículos de formação e aperfeiçoamento nas escolas e centros especializados, com ênfase na interpretação de assinaturas espectrais, análise de tráfego de rede e manipulação de efetores inteligentes. A criação de simuladores táticos e exercícios pode acelerar a formação e promover a familiarização dos operadores com as decisões rápidas e coordenadas exigidas por ameaças híbridas e assimétricas;
- c) Integração com Plataformas Existentes: para garantir economicidade e agilidade na implementação, pode ser realizada a integração dos módulos do sistema às plataformas já em uso, incluindo navios de superfície e instalações de vigilância. Essa integração deve prever a instalação de sensores de escuta passiva, receptores e emissores de RF, enlaces seguros de dados e, quando possível, sistemas de neutralização cibernética e acústica;
- d) Criação de Bancos de Dados Dinâmicos: a eficácia da detecção e da resposta automatizada depende da disponibilidade de um banco de dados robusto e constantemente atualizado com assinaturas espectrais, padrões de tráfego de rede e configurações comportamentais típicas de SRPs. Esses bancos devem incluir dados de inteligência, telemetria, incidentes anteriores, dentre outros, alimentados por plataformas nacionais e compartilhados com outras Forças. A atualização contínua desses dados é essencial para a identificação antecipada de ameaças e para a evolução do sistema frente a novas táticas adversárias; e
- e) Realização de Exercícios Conjuntos: a última orientação trata da realização periódica de exercícios táticos e operacionais, com ênfase em cenários que

simulem o emprego de SRPs em ataques coordenados. O objetivo é avaliar a interoperabilidade entre sistemas, testar a eficiência das contramedidas, identificar vulnerabilidades e consolidar a doutrina. Os aprendizados desses exercícios devem retroalimentar os protocolos automatizados e orientar o aprimoramento do modelo proposto.

Essas orientações, em conjunto, estruturam o caminho para a possível implementação de um modelo de defesa multidomínio, compatível com os desafios estratégicos da Amazônia Azul, com a evolução das ameaças tecnológicas e com a necessidade crescente de atuação integrada entre domínios e plataformas.

5 CONCLUSÃO

O presente trabalho propôs um modelo integrado de resposta multidomínio, com ênfase em contramedidas não cinéticas eletrônicas, acústicas e cibernéticas, aplicados a veículos remotamente pilotados, no que tange à proteção do espaço estratégico brasileiro.

Partindo de uma revisão abrangente da literatura técnica, das doutrinas militares e de um estudo de caso relevante capaz de identificar os principais desafios operacionais e tecnológicos que permeiam estas plataformas, foi possível realizar a análise das suas vulnerabilidades, identificando-se a necessidade de um sistema que articule sensores heterogêneos, protocolos de decisão automatizados e efetores adaptativos. O modelo proposto busca preencher lacunas operacionais hoje existentes, como a fragmentação entre domínios, a ausência de resposta automatizada e a limitação de doutrina quanto ao emprego de meios não letais em ambientes sensíveis.

A arquitetura conceitual desenvolvida oferece uma estrutura modular, escalável e interoperável, capaz de ser aplicada tanto em plataformas navais existentes quanto em ambientes fixos de interesse estratégico. As diretrizes apresentadas para sua implementação futura contemplam aspectos técnicos, humanos, normativos e doutrinários, promovendo a viabilidade do sistema em médio prazo, desde que inserido em uma política de defesa alinhada com a inovação, pesquisa e a atuação proativa frente às ameaças tecnológicas emergentes.

Ao propor a integração entre sensores inteligentes, centros de comando multidomínio, capacitação de operadores e atualização contínua de bancos de dados,

o modelo responde não apenas a desafios táticos imediatos, mas contribui com uma perspectiva estratégica para a modernização das capacidades de defesa marítima do Brasil. Alinha-se, assim, aos fundamentos estabelecidos pela Estratégia Nacional de Defesa e ao escopo transformador previsto pelo Planejamento Estratégico da Marinha para 2040.

Por fim, ressalta-se que a implementação do modelo aqui proposto requer esforços conjuntos entre a Marinha do Brasil, a Base Industrial de Defesa, instituições de pesquisa e agências de segurança, de modo a consolidar uma capacidade nacional autônoma e resiliente no enfrentamento aos riscos crescentes impostos pela proliferação de veículos remotamente pilotados. A dissuasão eficaz e a proteção da soberania marítima dependerão, cada vez mais, da habilidade de operar simultaneamente nos domínios físico e virtual, de forma coordenada, inteligente e contínua.

REFERÊNCIAS

ARTECHE, D.; CHIVERS, K.; HOWARD, B.; LONG, T. **Drone defense system architecture for U.S. Navy strategic facilities**. Monterey, CA: Naval Postgraduate School, 2017. Technical Report AAT-0704-0188. Disponível em: <http://hdl.handle.net/10945/56172>. Acesso em: 7 ago. 2025.

BASAK, S.; SCHEERS, B. Passive radio system for realtime drone detection and DoA estimation. **International Conference on Military Communications and Information Systems**, 2018. Anais [...]. IEEE, maio 2018. p. 1–6. Disponível em: <https://doi.org/10.1109/ICMCIS.2018.8398721> Acesso em: 8 ago. 2025.

BRASIL. Marinha do Brasil. **COMOPNAV-220**: Manual de Guerra Eletrônica da Marinha. Rio de Janeiro, 2018. Classificação: reservado. Não disponível para consulta pública.

BRASIL. Marinha do Brasil. **Plano Estratégico da Marinha (PEM 2040)**. Brasília, DF: Estado-Maior da Armada, 2020. Disponível em: <https://www.marinha.mil.br/pem2040>. Acesso em: 05 abr. 2025.

BRASIL. Marinha do Brasil. **Portaria nº 213/DGMM**. Rio de Janeiro, RJ: Marinha do Brasil, 12 dez. 2022. Assunto: Normas para a Operação e Emprego de Sistemas de Aeronaves Remotamente Pilotadas (SARP) na MB.

BRASIL. Ministério da Defesa. **MD32-P-01**: Política de Guerra Eletrônica de Defesa. 1. ed. Brasília, 2004. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/publicacoes/md32a_pa_01a_polguerraeletrdefa_1a_a_eda_2004.pdf/view. Acesso em: 09 abr. 2025.

BRASIL. Ministério da Defesa. **MD33-M-02**: Manual de Abreviaturas, Siglas, Símbolos e Convenções Cartográficas das Forças Armadas. 4. ed. Brasília, 2021. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/File/legislacao/emcfa/publicacoes/manual-md33-m-02-manual-de-abreviaturas-siglas-simbolos-e-convencoes-cartograficas.pdf/view>. Acesso em: 27 jun. 2025.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. 5. ed. Brasília, 2015. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/ajuste-01/legislacao/emcfa/publicacoes/doutrina/md35-G-01-glossario-das-forcas-armadas-5-ed-2015-com-alteracoes.pdf>. Acesso em: 27 jun. 2025.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, DF: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 10 abr. 2025.

CHRISTNACHER, F. et al. Optical and acoustical UAV detection. **Electro-Optical Remote Sensing X**, 2016, Bellingham, WA. Proceedings [...]. Bellingham: SPIE,

2016. v. 9988, Art. no. 99880B. Disponível em: <https://doi.org/10.1117/12.2240752>. Acesso em: 8 ago. 2025.

CONGRESSIONAL RESEARCH SERVICE. **Navy Large Unmanned Surface and Undersea Vehicles**. [s.n.], 2024. Disponível em: <https://crsreports.congress.gov/product/pdf/R/R45757>. Acesso em: 4 ago. 2025.

CURPEN, R.; BĂLAN, T.; MICLOȘ, I. A.; COMĂNICI, I. Assessment of signal jamming efficiency against LTE UAVs. **IEEE International Conference on Communications (ICC)**, 2018. Proceedings... IEEE, jun. 2018. p. 367–370. Disponível em: <https://doi.org/10.1109/ICComm.2018.8484746>. Acesso em: 17 maio 2025.

DEY, V.; PUDI, V.; CHATTOPADHYAY, A.; ELOVICI, Y. Security vulnerabilities of unmanned aerial vehicles and countermeasures: an experimental study. **31st International Conference on VLSI Design and 17th International Conference on Embedded Systems (VLSID)**, Pune, Índia, 6 a 10 de jan. de 2018. Proceedings... Pune: IEEE, Jan. 2018. p. 398–403. Disponível em: <https://doi.org/10.1109/VLSID.2018.97>. Acesso: 8 ago. 2025.

FARLÍK, J.; GACHO, L. Researching UAV threat – new challenges. **International Conference on Military Technologies**, Brno, República Tcheca. Anais [...] p. 1-6. 2021. Disponível em: <https://ieeexplore.ieee.org/document/9502759>. Acesso em: 23 mar. 2025.

FAYAZ, S.; PARAHA, S. A.; QURESHI, G. J. Underwater object detection: architectures and algorithms – a comprehensive review. **Multimedia Tools and Applications**, v. 81, n. 15, p. 20871–20916, jun. 2022. Disponível em: https://www.researchgate.net/publication/359195058_Underwater_object_detection_architectures_and_algorithms_-_a_comprehensive_review. Acesso em: 6 ago. 2025.

HUANG, K.; WANG, H. Combating the control signal spoofing attack in UAV systems. **IEEE Transactions on Vehicular Technology**, v. 67, n. 8, p. 7769–7773, ago. 2018. DOI: <https://doi.org/10.1109/TVT.2018.2832080>. Disponível em: <https://ieeexplore.ieee.org/document/8350330>. Acesso em: 5 ago. 2025.

JIAN, M.; LU, Z.; CHEN, V. C. Drone detection and tracking based on phase-interferometric Doppler radar. **IEEE Radar Conference**, 2018. Anais [...]. IEEE, abr. 2018. p. 1146–1149. Disponível em: <https://ieeexplore.ieee.org/document/8378723>. Acesso em: 08 ago. 2025.

JOINT AIR POWER COMPETENCE CENTRE (JAPCC). **A comprehensive approach to countering unmanned aircraft systems**. Kalkar, DEU: Joint Air Power Competence Centre, 2021. Disponível em: <https://www.japcc.org/books/a-comprehensive-approach-to-countering-unmanned-aircraft-systems/>. Acesso em: 08 maio 2025.

Kang, H.; Joung, J.; Kim, J.; Kang, J.; Cho, Y. S. Protect Your Sky: A Survey of Counter Unmanned Aerial Vehicle Systems, **IEEE Access**, vol. 8, pp. 168671–

168710, 2020, doi: 10.1109/ACCESS.2020.3023473. Disponível em: <https://ieeexplore.ieee.org/document/9194729/>. Acesso em: 12 jun. 2025.

KHAWAJA, W.; SEMKIN, V.; RATYAL, N. I.; YAQOOB, Q.; GUL, J.; GUVENC, I. Threats from and counter-measures for unmanned aerial and underwater vehicles. **Sensors**, v. 22, n. 10, p. 3896, 2022. Disponível em: <https://www.mdpi.com/1424-8220/22/10/3896>. Acesso em: 12 abr. 2025.

KHOMENKO, Ivan. Russia forced to develop specialized buoys to detect Ukrainian maritime drones. **United24 Media**, 28 out. 2024. Disponível em: <https://united24media.com/latest-news/russia-forced-to-developed-specialized-buoys-to-detect-ukrainian-maritime-drones-3327>. Acesso em: 4 ago. 2025.

KILIAN, J. C.; WEGENER, B. J.; WHARTON, E.; GAVELEK, D. R. **Counter-unmanned aerial vehicle system and method**. U.S. Patent n. 9 085 362, 21 jul. 2015. Disponível em: <https://patents.google.com/patent/US9085362B1/en>. Acesso em: 11 ago. 2025.

KUNERTOVA, Dominika. **Learning from the Ukrainian Battlefield: Tomorrow's Drone Warfare, Today's Innovation Challenge**. Zurich: Center for Security Studies (CSS), ETH Zürich, ago. 2024. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS_Study_2024_Learning_from%20the_Ukrainian_Battlefield.pdf. Acesso em: 16 ago. 2025.

MATLACK, David; SCHWARTZ, Shoshana; GILL, Ilya. Ukraine's Drone Ecosystem and the Defence of Europe. London: **LSE IDEAS**, abr. 2025. Disponível em: <https://www.lse.ac.uk/ideas/Assets/Documents/2025-04-05-DRONES-MatlackSchwartzGill-FINAL-WEB-03.pdf>. Acesso em: 16 ago. 2025.

NATO. **Guidance for Developing Maritime Unmanned Systems (MUS)**. NATO Allied Maritime Command. 2014. Disponível em: <https://publicintelligence.net/cjoscoe-mus/>. Acesso em: 8 jun. 2025.

NATO. **Joint Capability Group Unmanned Aircraft Systems**. 2009. Disponível em: https://www.nato.int/cps/en/natolive/topics_82779.htm. Acesso em: 7 jun. 2025.

NORMAN, G. **Border patrol spots drone trying to help migrants illegally enter America**. Fox News, 1 abr. 2019. Disponível em: <https://www.foxnews.com/us/border-patrol-foils-drone-trying-to-help-migrants-illegally-enter-america>. Acesso em: 16 ago. 2025.

OZBERK, Tayfun. Return of the Bayraktar: TB2 Drone Strikes Again in Ukraine. **Naval News**, 24 jun. 2025. Disponível em: <https://www.navalnews.com/naval-news/2025/06/return-of-the-bayraktar-tb2-drone-strikes-again-in-ukraine/>. Acesso em: 4 ago. 2025.

PHAM, Minh; XIONG, Kaiqi. A survey on security attacks and defense techniques for connected and autonomous vehicles. **Computers & Security**, v. 109, 2021. Disponível em: <https://arxiv.org/pdf/2007.08041>. Acesso em: 12 abr. 2025.

RODDAY, N. M.; SCHMIDT, R. D. O.; PRAS, A. Exploring security vulnerabilities of unmanned aerial vehicles. **IEEE/IFIP Network Operations and Management Symposium**, 2016, Anais [...]. IEEE, abr. 2016. p. 993–994. Disponível em: <https://ieeexplore.ieee.org/document/7502939>. Acesso em: 8 ago. 2025.

RUSSIA CREATES AQUA BUOYS TO DETECT KAMIKAZE BOATS, PLANS TESTING IN THE BLACK SEA. **Defense Express**, 27 out. 2024. Disponível em: https://en.defence-ua.com/weapon_and_tech/russia_creates_aqua_buoys_to_detect_kamikaze_boats_plans_testing_in_the_black_sea-12332.html. Acesso em: 4 ago. 2025.

SANDER, J.; KUWERTZ, A.; MUHLENBERG, D.; MULLER, W. High-level data fusion component for drone classification and decision support in counter UAV. **Open Architecture/ Open Business Model Net-Centric Systems and Defense Transformation**, Bellingham, WA, v. 10651, Art. no. 106510F, 2018. Disponível em: <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10651/106510F/High-level-data-fusion-component-for-drone-classification-and-decision/10.1117/12.2306148.short?>. Acesso em: 08 ago. 2025.

SHAHED-136 AND LOITERING MUNITIONS IN UKRAINE. **Prevail Partners**, 28 out. 2022. Disponível em: <https://prevail-group.prezly.com/shahed-136-and-loitering-munitions-in-ukraine>. Acesso em: 14 ago. 2025

SLUSHER, M. N. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience. **Center for Strategic and International Studies (CSIS)**, Washington, DC, jun. 2025. Disponível em: <https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience>. Acesso em: 19 abr. 2025.

UNITED STATES. Department of Defense. **Joint Publication 1-02**: Department of Defense Dictionary of Military and Associated Terms (Amended Through April 2010). Washington, D.C.: Department of Defense, 2010. Disponível em: https://archive.org/details/bub_gb_Ap_En_k7r9AC/mode/2up. Acesso em: 2 ago. 2025.

WANG, Jian; LIU, Yongxin; SONG, Houbing. Counter-Unmanned Aircraft System(s) (C-UAS): State of the art, challenges, and future trends. **IEEE Aerospace and Electronic Systems Magazine**, v. 36, n. 3, p. 4-29, 1 mar. 2021. Disponível em: <https://ieeexplore.ieee.org/document/9374654>. Acesso em: 27 mar. 2025.