ESCOLA DE GUERRA NAVAL

CC (FN) TIAGO CAMPOS DE SOUSA

OPERAÇÕES DE INFORMAÇÃO:
A Nova Guerra Invisível: O Papel das Operações de Informação e o Futuro da Doutrina Militar Brasileira

Rio de Janeiro

2025

CC (FN) TIAGO CAMPOS DE SOUSA

OPERAÇÕES DE INFORMAÇÃO:

A Nova Guerra Invisível: O Papel das Operações de Informação e o Futuro da Doutrina Militar Brasileira

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

Orientador: CMG (RM1) Jobim

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 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.

gov.br
Documento assinado digitalmente
TIAGO CAMPOS DE SOUSA
Data: 27/11/2025 12:08:18-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTO

Agradeço, em primeiro lugar, a Deus e à Nossa Senhora, por me concederem força, sabedoria e inspiração ao longo de toda esta caminhada.

Ao CMG (RM1) Jobim e ao CMG (RM1-FN) Mello, pelas valiosas e constantes orientações, que foram fundamentais durante todo o processo de pesquisa e escrita. Sua experiência e generosidade foram decisivas para a superação dos desafios encontrados.

Agradeço imensamente à minha prima, Gabrielly Graciano Gonçalves, por sua inestimável ajuda e apoio crucial na realização desta dissertação.

Aos meus pais, que sempre acreditaram em mim, apoiaram minha trajetória e elevaram preces silenciosas desde o início da minha carreira. A eles, minha eterna gratidão.

Por fim, agradeço à Escola de Guerra Naval, a seus oficiais e praças, por proporcionarem um ambiente inspirador, disciplinado e intelectualmente estimulante, que foi essencial para meu desenvolvimento profissional e acadêmico ao longo deste ano de estudos.

RESUMO

Esta dissertação se propõe a refletir sobre o papel crescente das Operações de Informação (OpInfo) no cenário dos conflitos contemporâneos e a compreender como as Forças Armadas Brasileiras podem aprimorar sua doutrina frente a esse novo e desafiador ambiente de atuação. Partindo de uma perspectiva histórica, o estudo mostra como a manipulação da informação sempre esteve presente nos embates humanos, desde os enganos táticos da antiguidade até as campanhas digitais sofisticadas dos tempos atuais. A pesquisa busca esclarecer os conceitos fundamentais que envolvem as OpInfo, explorando os manuais do Exército, Força Aérea e da Marinha do Brasil, e analisando como cada força compreende e aplica esses recursos na prática. Em paralelo, são examinadas doutrinas de países como Estados Unidos, Rússia, China e organizações como a OTAN, que têm feito da informação um instrumento central em suas estratégias militares. Mais do que um debate teórico, o trabalho mergulha em casos reais, como a guerra na Ucrânia, as tensões no Mar do Sul da China e os conflitos no Oriente Médio, para revelar como a guerra informacional molda narrativas, influencia decisões políticas e redefine o conceito de soberania. A partir dessas análises, propõe-se um conjunto de recomendações práticas para o contexto brasileiro, como a criação de estruturas especializadas, a formação de profissionais capacitados e o desenvolvimento de uma estratégia nacional de comunicação e defesa cognitiva. A conclusão é clara: em um mundo onde batalhas também se vencem com ideias, dados e percepções, é essencial que o Brasil invista com seriedade na modernização de sua doutrina de Operações de Informação. Somente assim poderá proteger seus interesses estratégicos e atuar com protagonismo em um cenário internacional cada vez mais orientado pelo poder da informação.

Palavras-chave: Operações de Informação. Ambiente Informacional. Capacidades Relacionadas à Informação. Forças Armadas Brasileiras.

ABSTRACT

The New Invisible War: The Role of Information Operations and the Future of Brazilian Military Doctrine

This dissertation aims to reflect on the growing role of Information Operations (OpInfo) in the context of contemporary conflicts and to understand how the Brazilian Armed Forces can enhance their doctrine in light of this new and challenging operational environment. Starting from a historical perspective, the study demonstrates how the manipulation of information has always been present in human conflicts, from tactical deception in antiquity to the sophisticated digital campaigns of modern times. The research seeks to clarify the fundamental concepts surrounding OpInfo by examining the Brazilian Army, Air Force and Navy manuals and analyzing how each branch understands and applies these resources in practice. In parallel, doctrines from countries such as the United States, Russia, China, and organizations like NATO are examined, highlighting how information has become a central instrument in their military strategies. More than a theoretical debate, this work dives into real-world cases, such as the war in Ukraine, the tensions in the South China Sea, and conflicts in the Middle East, to show how informational warfare shapes narratives, influences political decisions, and redefines the concept of sovereignty. Based on these analyses, a set of practical recommendations is proposed for the Brazilian context, such as the creation of specialized structures, the training of qualified professionals, and the development of a national strategy for communication and cognitive defense. The conclusion is clear: in a world where battles are also won with ideas, data, and perceptions, it is essential that Brazil seriously invests in the modernization of its Information Operations doctrine. Only then will it be able to protect its strategic interests and act with prominence in an international scenario increasingly driven by the power of information.

Keywords: Information Operations. Informational Environment. Information-Related Capabilities. Brazilian Armed Forces.

LISTA DE ABREVIATURAS E SIGLAS

BBC – British Broadcasting Corporation
CDC – Centers for Disease Control and Prevention
CDCiber – Centro de Defesa Cibernética
CIDOC – Comissão Interescolar de Doutrina de Operações Conjuntas
CRI – Capacidade Relacionada à Informação
EB – Exército Brasileiro
FAB – Força Aérea Brasileira
FN – Fuzileiros Navais
JFSC – Joint Forces Staff College
JP – Joint Publication
JCS – Joint Chiefs of Staff
MD – Ministério da Defesa
NATO – North Atlantic Treaty Organization (Organização do Tratado do Atlântico Norte)
ONG – Organização Não Governamental
OODA – Observar, Orientar, Decidir e Agir
OpInfo – Operações de Informação
OTAN – Organização do Tratado do Atlântico Norte
SCSPI – South China Sea Strategic Situation Probing Initiative
TI – Tecnologia da Informação
AIDS – Acquired Immunodeficiency Syndrome
CCRP – Command and Control Research Program
CGTN – China Global Television Network
CIA – Central Intelligence Agency
COMAER – Comando da Aeronáutica
DC – District of Columbia (comum em referências de Washington, D.C.)
EI – Estado Islâmico
EUA – Estados Unidos da América
FSB – Federal Security Service (Serviço Federal de Segurança da Rússia)
GRU – Main Intelligence Directorate (Diretório Principal de Inteligência da Rússia)
IA – Inteligência Artificial
JCOIE – Joint Concept for Operating in the Information Environment

KGB – Komitet Gosudarstvennoy Bezopasnosti (Comitê de Segurança do Estado da URSS)
ONU – Organização das Nações Unidas
PSYOP – Psychological Operations
RPC – República Popular da China
RT – Russia Today
RTO – Research and Technology Organization (da OTAN)
TR-SAS – Technical Report – Studies, Analysis and Simulation (da OTAN)

SUMÁRIO

1 INTRODUÇÃO

As operações de informação têm sido utilizadas ao longo da história como uma ferramenta estratégica essencial nos conflitos armados. Desde a antiguidade, exércitos compreendiam a importância da manipulação da informação para enganar inimigos e fortalecer suas próprias forças. Os gregos, por exemplo, utilizaram um dos mais icônicos estratagemas da história: o Cavalo de Troia, onde a falsa rendição e a ocultação de tropas permitiram a tomada da cidade inimiga. Séculos depois, o estrategista militar chinês Sun Tzu, em A Arte da Guerra, já defendia que a guerra deveria ser vencida antes mesmo do primeiro combate, por meio da informação e do engano.

No período medieval, as operações de informação desempenhavam um papel essencial na condução de campanhas militares. Antes das batalhas, exércitos espalhavam rumores sobre seu próprio tamanho e força para amedrontar adversários, enquanto mensagens falsas eram enviadas para desorientar comandantes inimigos. O uso de informações manipuladas desempenhou um papel crucial durante as Cruzadas, servindo como uma ferramenta poderosa para a construção de justificativas religiosas e políticas que impulsionaram esses conflitos. Através da disseminação estratégica de narrativas e boatos, os líderes da época conseguiram não apenas legitimar suas ambições territoriais e econômicas, mas também mobilizar um vasto número de combatentes sob a crença inabalável de que estavam lutando por uma causa divina.

Com o advento da imprensa no século XV, a disseminação de informações estratégicas passou a ser feita em larga escala. Durante a Guerra dos Trinta Anos (1618-1648), panfletos e discursos religiosos eram amplamente utilizados para convencer populações sobre a legitimidade de um conflito. Na Revolução Francesa, jornais e folhetins foram armas poderosas para moldar a percepção do público e instigar revoltas populares, demonstrando como a informação poderia ser usada para gerar mudanças sociais significativas.

Na Primeira (1914-1918) e Segunda (1939-1944) Guerras Mundiais, a propaganda tornou-se um componente essencial dos esforços de guerra. Países utilizavam meios de comunicação de massa para criar narrativas nacionalistas e

demonizar inimigos. O governo nazista[1], por exemplo, investiu pesadamente no uso da rádio e do cinema para manipular a percepção pública e fortalecer o regime de Hitler[2]. Já os Aliados, por sua vez, usaram campanhas de desinformação para confundir as tropas alemãs, como na Operação Fortitude[3], que enganou os nazistas sobre a verdadeira localização do desembarque do Dia D na Normandia.

A Guerra Fria transformou a maneira como as nações guerreavam, focando menos em conflitos armados diretos e mais em uma batalha de informações. Foi uma era de confronto ideológico e psicológico, onde a manipulação da informação se tornou fundamental.

Neste período, os Estados Unidos e União Soviética, os dois principais adversários, utilizaram a desinformação intensamente para enfraquecer governos e influenciar a opinião pública global. A CIA financiava secretamente jornais e campanhas políticas que apoiavam o bloco ocidental. Por outro lado, a KGB empregava as "Medidas Ativas", operações que criavam teorias da conspiração e disseminavam notícias falsas para desestabilizar os países oponentes. Esse período consolidou a informação como uma poderosa arma política, e essa abordagem continua a influenciar as estratégias de comunicação e segurança das nações até hoje.

Nos conflitos modernos, a guerra informacional atingiu um nível de sofisticação sem precedentes. Durante a Guerra do Iraque, a manipulação da informação foi decisiva, tanto para justificar a invasão quanto para sustentar a ocupação. Já na Guerra da Ucrânia, a disputa no campo de batalha foi acompanhada por uma intensa guerra de narrativas, onde vídeos, *fake news* e redes sociais foram usados para mobilizar o apoio internacional e enfraquecer a moral do inimigo. O conceito de guerra cognitiva tornou-se um dos pilares dos conflitos contemporâneos, explorando vulnerabilidades psicológicas e culturais para influenciar decisões e manipular percepções.

O Brasil, assim como outras nações, enfrenta desafios crescentes no ambiente informacional. Com a digitalização das comunicações e a ascensão das

---

1 Um nazista é um indivíduo que segue ou apoia o nazismo, uma ideologia política de extrema-direita, racista, nacionalista e totalitária que surgiu na Alemanha após a Primeira Guerra Mundial.

2 Adolf Hitler (1889-1945) foi um político austríaco que se tornou o ditador da Alemanha e o líder do Partido Nazista (Partido Nacional-Socialista dos Trabalhadores Alemães). Ele é amplamente reconhecido como a figura central por trás da Segunda Guerra Mundial na Europa e do Holocausto, um genocídio que resultou na morte de aproximadamente seis milhões de judeus, além de milhões de outras vítimas.

3 A Operação Fortitude foi uma das mais importantes e bem-sucedidas operações de engano militar dos Aliados durante a Segunda Guerra Mundial, crucial para o sucesso do Dia D (Desembarques da Normandia) em 6 de junho de 1944.

redes sociais, a desinformação se tornou um problema crítico, afetando não apenas a opinião pública, mas também a segurança nacional. Campanhas de desinformação e ataques cibernéticos contra instituições governamentais são cada vez mais frequentes, o que torna essencial que as Forças Armadas desenvolvam capacidades mais avançadas de defesa informacional.

Assim, surge a seguinte questão: A Doutrina de Operações de Informação (OpInfo) das Forças Armadas Brasileiras atende efetivamente aos desafios dos conflitos modernos? Tendo esse objeto de pesquisa em vista, e considerando que toda área em constante aprimoramento exige avaliação, torna-se essencial questionar a solidez e a adaptabilidade da OpInfo nacional. Essa análise visa garantir o contínuo desenvolvimento doutrinário e identificar aspectos que possam ser aprimorados para lidar com a complexidade dos desafios atuais.

A evolução das estratégias militares em outras nações e a crescente importância da guerra cognitiva[4] indicam que o ambiente informacional pode ser tão decisivo quanto o poderio bélico convencional. Dessa forma, torna-se fundamental avaliar se a doutrina brasileira está alinhada com possíveis mudanças nas OpInfo dos conflitos modernos e quais possíveis adaptações, caso necessário, podem ser implementadas para fortalecer sua eficácia.

Para responder a essa questão, este trabalho de dissertação empregará uma metodologia de pesquisa qualitativa, com foco em uma abordagem exploratória e descritiva. A análise será fundamentada em revisão bibliográfica e análise documental nacionais e internacionais. A estrutura do trabalho se divide em seis capítulos: o Capítulo 2 investigará os conceitos fundamentais das OpInfo, buscando compreender o arcabouço teórico; o Capítulo 3 fará um estudo da estrutura da doutrina brasileira sobre o tema; o Capítulo 4 analisará a aplicação no contexto internacional, com foco em estudos de caso de nações como EUA, Rússia e OTAN; o Capítulo 5 avaliará os desafios dos conflitos contemporâneos, incluindo a guerra cibernética, a desinformação e o papel das redes sociais; e, por fim, o Capítulo 6 apresentará recomendações, caso necessário, para um possível aprimoramento da doutrina das Forças Armadas Brasileiras.

Por fim, com base nos resultados da pesquisa e na análise comparativa, este trabalho poderá apresentar recomendações para possíveis adaptações ou melhorias

4 A guerra cognitiva é uma forma avançada de conflito que tem como principal campo de batalha a mente humana. O objetivo não é apenas mudar o que as pessoas pensam, mas como elas pensam, influenciando suas percepções, crenças, valores e comportamentos.

na doutrina brasileira. Essas sugestões, que poderão ou não ser identificadas ao longo do estudo, visam aprimorar a capacidade das Forças Armadas Brasileiras de enfrentar os desafios informacionais, tanto em cenários de conflito quanto em tempos de paz. O objetivo é contribuir para que o país esteja mais preparado para os desafios futuros sobre o tema.

2 CONCEITO E DEFINIÇÕES SOBRE OPERAÇÕES DE INFORMAÇÃO

As OpInfo são um conjunto de ações estratégicas pensadas para influenciar, proteger e usar o ambiente informacional[5] tanto em situações militares quanto civis. Conforme o Manual de Campanha EB70-MC-10.213 do Exército Brasileiro (BRASIL, 2019), as OpInfo são cruciais para alcançar a superioridade informacional, pois elas buscam moldar a percepção do oponente e, ao mesmo tempo, salvaguardar os dados estratégicos das nossas próprias forças armadas.

2.1 Fundamentos das Operações de Informação

As OpInfo são baseadas na necessidade de controle e gerenciamento da informação em um ambiente operacional dinâmico. Desde a antiguidade, estratégias de guerra informacional foram utilizadas para enganar inimigos e obter vantagens estratégicas. Nos tempos modernos, o avanço tecnológico e a digitalização dos meios de comunicação elevaram a complexidade dessas operações, tornando-as um elemento central nos conflitos armados e na segurança nacional (SINGER; BROOKS, 2018).

De acordo com a Doutrina de OpInfo da Marinha do Brasil (BRASIL, 2020) não é uma capacidade isolada, mas sim um conjunto de ações interligadas que incluem guerra eletrônica, guerra psicológica, operações cibernéticas e ações de segurança da informação. Essas operações têm como principal objetivo modificar a tomada de decisão do adversário e influenciar a percepção da opinião pública.

O Exército Brasileiro define as OpInfo como "ações coordenadas para afetar a percepção, os processos de decisão e os sistemas informacionais de adversários e oponentes potenciais, protegendo, simultaneamente, as informações e infraestruturas próprias" (BRASIL, 2019). Complementando essa visão, a Marinha do Brasil destaca que as OpInfo são fundamentais para a condução das operações militares modernas, especialmente em cenários de guerra híbrida (BRASIL, 2020).

Essas definições revelam uma compreensão clara por parte das Forças Armadas Brasileiras sobre a natureza dual das OpInfo: não apenas buscam influenciar o inimigo, mas também garantir a segurança e integridade de suas

5 Um ambiente informacional é o conjunto de todos os elementos que influenciam como a informação é criada, organizada, armazenada, acessada, compartilhada e utilizada. Ele abrange não apenas as tecnologias, mas também as pessoas, os processos, as políticas, a cultura e o conteúdo informacional em si.

próprias capacidades informacionais. A ênfase da Marinha na guerra híbrida[6], por sua vez, ressalta a percepção de que as OpInfo são ferramentas essenciais para lidar com ameaças complexas que misturam táticas convencionais e não convencionais, indo além do combate físico. Essa sinergia entre as visões das forças demonstra um alinhamento estratégico crucial para a defesa nacional no ambiente informacional contemporâneo.

2.2 Principais Áreas de Atuação

As OpInfo englobam diversas capacidades inter-relacionadas, essenciais para atuação no ambiente informacional contemporâneo, conforme detalhado nos manuais das Forças Armadas Brasileiras e em conceitos internacionais.

A Guerra Eletrônica (GE), por exemplo, envolve a utilização estratégica do espectro eletromagnético. Seu propósito é tanto degradar as comunicações inimigas quanto salvaguardar as próprias transmissões, garantindo a fluidez informacional das forças amigas (BRASIL, 2019). Complementarmente, as Operações Psicológicas (OpPsc) empregam técnicas para influenciar diretamente a percepção, as emoções e o comportamento de alvos específicos, visando moldar o ambiente psicológico a favor dos objetivos nacionais (BRASIL, 2020).

No domínio digital, as Operações Cibernéticas abrangem ações ofensivas e defensivas. Elas incluem desde ataques direcionados a redes adversárias até a proteção robusta das infraestruturas informacionais próprias, um pilar fundamental da segurança na era digital (BRASIL, 2019). A Segurança da Informação reforça esse pilar, focando na proteção de dados sensíveis e na implementação de mecanismos eficazes para combater vazamentos informacionais, salvaguardando o conhecimento estratégico (BRASIL, 2020).

Um conceito emergente e de crescente importância é o da Guerra Cognitiva. Esta modalidade de guerra vai além da simples manipulação de informações, buscando influenciar a percepção humana por meio do uso sofisticado de inteligência artificial, redes sociais e algoritmos, visando impactar diretamente processos de decisão (NATO, 2022). Por fim, a Contrainteligência Informacional atua como uma linha de defesa crucial. Suas técnicas visam a proteção de

6 A guerra híbrida é uma estratégia militar complexa que combina uma variedade de táticas e métodos, tanto convencionais quanto não convencionais, para atingir objetivos políticos e estratégicos. O termo "híbrido" se refere à mescla de diferentes modos de conflito que operam simultaneamente e de forma adaptativa.

.

informações estratégicas, defendendo as forças contra ações de espionagem e campanhas de desinformação inimiga (BRASIL, 2019).

As OpInfo são multidimensionais, atuando nas camadas física, lógica e cognitiva do ambiente informacional, conforme abordagens doutrinárias como as da OTAN e das próprias Forças Armadas Brasileiras. A perspectiva física foca na infraestrutura tecnológica (redes de comunicação, satélites). A perspectiva lógica lida com os fluxos de informação e a segurança digital. Já a perspectiva cognitiva busca influenciar a tomada de decisão de líderes e do público. Essas três dimensões são interconectadas, e a eficácia das OpInfo reside na capacidade de coordenar ações em todas elas. Essa visão integrada é fundamental para as Forças Armadas Brasileiras enfrentarem os desafios de segurança atuais.

2.3 Impacto das Operações de Informação no Cenário Atual

As OpInfo passaram por uma grande evolução nas últimas décadas, acompanhando de perto os avanços tecnológicos e as novas estratégias de guerra. A história vem demonstrando a relevância das OpInfo, durante a Guerra Fria, por exemplo, tanto os Estados Unidos quanto a União Soviética utilizaram amplamente operações psicológicas e a manipulação da informação com o objetivo de influencias o domínio informacional. No cenário atual, conflitos como a Guerra na Ucrânia reforçam a importância crescente de campanhas de desinformação e da ampliação da utilização da guerra de narrativas. Essas táticas são usadas para influenciar a percepção pública e enfraquecer a vontade de lutar das forças inimigas, bem como, a opinião internacional do conflito (SINGER; BROOKS, 2018).

Com a ascensão da inteligência artificial (IA) e da análise de *big data*[7], as OpInfo ampliaram a importância da dimensão informacinal. O monitoramento de redes sociais, por exemplo, permite prever tendências e influenciar grandes grupos de pessoas antes mesmo do início de um conflito armado. A Primavera Árabe é um caso notório, onde movimentos de protesto foram amplificados pelo uso de plataformas digitais, evidenciando o impacto da informação no ambiente geopolítico global (THOMPSON, 2020).

7 Big Data refere-se a conjuntos de dados tão grandes e complexos que os métodos e ferramentas tradicionais de processamento de dados não conseguem armazená-los, processá-los ou analisá-los de forma eficiente. Não se trata apenas do volume de dados, mas também da sua diversidade e da velocidade com que são gerados. "híbrido" se refere à mescla de diferentes modos de conflito que operam simultaneamente e de forma adaptativa.

As OpInfo também desempenham um papel fundamental na segurança nacional, transcendendo as fronteiras do conflito armado. A disseminação de notícias falsas (*fake news*), ataques cibernéticos e a guerra psicológica tornaram-se ferramentas de combate tanto em tempos de paz quanto em cenários de conflito. Um exemplo recente é o uso de *deepfakes*[8] para espalhar desinformação e minar a credibilidade de líderes políticos e militares (NATO, 2022). Esse cenário sublinha a crescente relevância de estratégias híbridas que combinam elementos militares e não-militares no ambiente informacional.

As OpInfo, conforme delineado neste capítulo, vão muito além de uma simples estratégia militar, configurando-se como um elemento central na segurança e nos conflitos contemporâneos. Ao analisar as definições e as áreas de atuação, fica evidente que o sucesso das OpInfo depende da coordenação entre guerra eletrônica, psicológica e cibernética, além da contrainteligência. Essa abordagem integrada não só visa influenciar o adversário, mas também, e de forma crucial, proteger as próprias capacidades informacionais. Dessa forma, a compreensão das OpInfo torna-se indispensável para a defesa nacional e para o entendimento dos desafios da guerra híbrida e da desinformação na era digital.

8 Deepfake é um termo que surge da junção de "deep learning" (aprendizagem profunda) e "fake" (falso). Ele se refere a conteúdos sintéticos, como vídeos, áudios e imagens, que são criados ou alterados usando inteligência artificial (IA) generativa para parecerem autênticos. A característica mais marcante dos deepfakes é a capacidade de manipular a imagem e/ou a voz de uma pessoa, fazendo com que ela diga ou faça coisas que nunca disse ou fez na realidade.

.

3 DOUTRINA BRASILEIRA DE OPERAÇÕES DE INFORMAÇÃO

A Doutrina Brasileira de OpInfo tem se desenvolvido para atender às exigências do ambiente operacional contemporâneo, marcado pela crescente complexidade do domínio informacional, conforme evidenciado pelos próprios manuais e diretrizes militares (BRASIL, 2019; BRASIL, 2020). As três Forças Armadas, Exército, Marinha e Força Aérea, possuem diretrizes que reconhecem a importância das OpInfo como instrumento estratégico de defesa e influência.

De forma integrada, a doutrina compreende as OpInfo como um conjunto de ações coordenadas destinadas à proteção de ativos estratégicos, à preservação da credibilidade institucional e à projeção de narrativas alinhadas aos interesses nacionais. Entre os elementos comuns destacam-se as Capacidades Relacionadas à Informação (CRI), a interoperabilidade entre as Forças, o respeito à legalidade e a integração com demais capacidades operacionais.

Como exemplo, a Marinha do Brasil estrutura sua doutrina em capítulos que abrangem desde os fundamentos conceituais até a aplicação prática no contexto naval, incorporando atividades como operações psicológicas, guerra eletrônica, ações de comunicação e defesa cibernética, todas articuladas com os meios convencionais de combate.

A doutrina brasileira, portanto, valoriza a informação como um recurso operacional essencial, integrando-a aos diversos níveis de planejamento e execução militar (BRASIL, 2019).

3.1 Estrutura e Diretrizes da Doutrina Brasileira

A doutrina brasileira de OpInfo está estruturada em documentos oficiais das Forças Armadas, com destaque para o Exército Brasileiro e a Marinha do Brasil, que estabeleceram normativas e orientações voltadas para o emprego dessas capacidades no contexto militar e estratégico nacional. A doutrina é composta por princípios, fundamentos e linhas de ação que visam garantir a efetividade das ações informacionais no ambiente operacional, especialmente diante da crescente complexidade do ambiente informacional contemporâneo.

A estrutura da doutrina brasileira de OpInfo se apoia em cinco pilares inter-relacionados, que garantem sua aplicação abrangente e coordenada. O primeiro

pilar são as Capacidades Relacionadas à Informação (CRI), que formam o cerne das OpInfo. Elas englobam um conjunto diversificado de atividades, como a guerra eletrônica, operações psicológicas, ações de comunicação, segurança da informação, operações cibernéticas e até a guerra de narrativas. A integração dessas capacidades é vital para influenciar comportamentos e proteger a infraestrutura informacional nacional (BRASIL, 2018) (BRASIL, 2019).

Em seguida, a doutrina é aplicada em diferentes Níveis de Emprego: tático, operacional e estratégico. Em cada um desses níveis, os objetivos e métodos variam, indo desde a disseminação de mensagens em ambientes locais até o planejamento de ações de grande escala com impacto internacional (BRASIL, 2018) (BRASIL, 2019).

A Interoperabilidade entre Forças também é um ponto importante na visão da doutrina brasileira de OpInfo, pois garante que as três Forças Singulares possam compartilhar informações em tempo real e coordenar ações de forma sinérgica, otimizando o emprego dos recursos no ambiente informacional. Embora esse processo ainda esteja em consolidação, a doutrina promove a integração entre o Exército, a Marinha e a Força Aérea, incentivando ações conjuntas e o intercâmbio de capacidades e tecnologias. As OpInfo são conduzidas por Atores e Organizações específicas, como o Centro de Comunicação Social do Exército (CCOMSEx), o Comando de Defesa Cibernética (ComDCiber) e órgãos correlatos nas outras Forças. Essas unidades são responsáveis por planejar, executar e avaliar as operações informacionais, embora sua atuação seja, por vezes, limitada na amplitude e na complexidade da dimensão informacional como um todo (BRASIL, 2018) (BRASIL, 2019).

Por fim, a doutrina enfatiza a Integração com a Defesa Cibernética. Essa convergência é crucial para a proteção de dados estratégicos, a resposta a ataques cibernéticos e o combate à desinformação, reconhecendo a estreita ligação entre o ambiente físico e o digital no contexto da guerra moderna (BRASIL, 2019).

A doutrina brasileira orienta o uso das OpInfo por meio de diretrizes claras que definem sua finalidade e método de aplicação. Dentre as principais, destaca-se a prevalência da legalidade e legitimidade, que exige que todas as ações estejam em conformidade com os princípios constitucionais e as normas legais nacionais e internacionais. Além disso, as OpInfo devem ter um alinhamento com os objetivos

políticos e estratégicos do país, apoiando diretamente os interesses nacionais (BRASIL, 2018) (BRASIL, 2019).

A doutrina também enfatiza a necessidade de um planejamento integrado, onde as ações informacionais são desenvolvidas em conjunto com outras operações militares, sejam elas convencionais ou não convencionais. Por fim, o acompanhamento contínuo é um elemento central, pois o ciclo das OpInfo prevê o monitoramento, a execução, a avaliação e a correção de rumo constante, com base em indicadores técnicos e de comportamento (BRASIL, 2018) (BRASIL, 2019).

A doutrina brasileira se baseia em diversos documentos oficiais, como o Manual de Campanha EB70-MC-10.213 (OpInfo) do Exército Brasileiro, os capítulos da Doutrina de OpInfo da Marinha do Brasil, as Diretrizes do Ministério da Defesa sobre CRI e Defesa Cibernética e as Normas Operacionais do ComDCiber. Esses textos cobrem desde os conceitos básicos até aspectos técnicos de planejamento, uso de recursos, coordenação entre setores e protocolos para atuação em operações conjuntas (BRASIL, 2018) (BRASIL, 2019).

Com base nessa estrutura, a doutrina brasileira de OpInfo tem avançado em sua consolidação, mas ainda enfrenta desafios quanto à sua aplicação integrada e à institucionalização plena dentro do planejamento militar. A expansão da formação de pessoal, o investimento em tecnologias e a criação de centros interforças de excelência figuram como os próximos passos para o fortalecimento dessa capacidade essencial à soberania e à segurança nacional.

3.2 Aplicação das Operações de Informação no Exército Brasileiro

A doutrina do Exército Brasileiro adota as OpInfo como parte integrante das operações militares. Conforme o Manual de Campanha EB70-MC-10.213, este documento orienta o emprego doutrinário das OpInfo no contexto terrestre, buscando influenciar comportamentos, proteger a força, apoiar decisões de comando e enfraquecer as capacidades do oponente no domínio informacional (BRASIL, 2019).

As OpInfo são tratadas como um conjunto de ações coordenadas que envolvem várias capacidades inter-relacionadas. Entre elas, destacam-se a guerra eletrônica, as ações de comunicação, as operações psicológicas, a segurança das comunicações e as operações cibernéticas. Essas capacidades são aplicadas de

forma integrada ao esforço operacional, visando ampliar os efeitos desejados no campo de batalha e no ambiente informacional (BRASIL, 2018) (BRASIL, 2019).

A aplicação das OpInfo é planejada e executada em todos os níveis da estrutura militar. No nível estratégico, as ações se alinham às diretrizes do Ministério da Defesa e às políticas de defesa nacionais. No nível operacional, são integradas ao planejamento das grandes unidades. Já no nível tático, as ações são executadas por tropas especializadas ou unidades subordinadas, com foco em operações específicas e no ambiente local de atuação (BRASIL, 2018) (BRASIL, 2019).

Essa abordagem é sustentada por estruturas específicas. O Centro de Comunicação Social do Exército (CCOMSEx), por exemplo, é responsável pela coordenação da comunicação institucional e de ações voltadas para a opinião pública. Além disso, o Comando de Defesa Cibernética (ComDCiber) desempenha um papel central na segurança da informação e na execução de ações cibernéticas, garantindo a proteção das redes e a capacidade de resposta a ameaças digitais (BRASIL, 2019).

O Exército também promove o constante aperfeiçoamento de sua doutrina por meio da Comissão de Doutrina de Operações de Informação (CIDOC OpInfo). Esta comissão é encarregada de consolidar conhecimentos, produzir manuais e padronizar procedimentos, garantindo a coerência e a aplicação efetiva das diretrizes por todas as unidades (BRASIL, 2019).

A doutrina do Exército, portanto, estabelece a integração das OpInfo aos demais meios de combate, especialmente em operações interagências, ambientes urbanos e cenários de guerra irregular. Essa abordagem promove a proteção da narrativa institucional, a antecipação de campanhas adversas e o apoio à decisão do comandante, considerados os pilares práticos da aplicação das OpInfo nas operações terrestres.

3.3 Aplicação das Operações de Informação na Marinha do Brasil

A Marinha do Brasil considera as OpInfo como um conjunto de ações coordenadas para influenciar o ambiente informacional, protegendo as suas próprias capacidades e explorando vulnerabilidades dos adversários. De acordo com a sua doutrina, as OpInfo desempenham um papel fundamental na segurança das comunicações navais, no monitoramento do tráfego marítimo estratégico e na

proteção das águas jurisdicionais brasileiras, especialmente na Amazônia Azul, área de grande importância geopolítica para o país (BRASIL, 2018).

A Marinha do Brasil categoriza as OpInfo em diversas áreas de atuação, todas interligadas e aplicadas conforme a necessidade estratégica. Uma das frentes principais é a Guerra Eletrônica (GE), que utiliza um conjunto de ações para detectar, identificar, interferir e neutralizar sinais eletromagnéticos adversários, garantindo a supremacia informacional no ambiente marítimo. Na dimensão cognitiva, as Operações Psicológicas (OpPsc) e o Gerenciamento da Percepção são utilizados para influenciar decisões de forças adversárias e da opinião pública, reforçando, por meio de campanhas de propaganda, a importância estratégica da Marinha para a soberania nacional (BRASIL, 2018).

No ambiente digital, as Operações Cibernéticas são essenciais, englobando tanto a defesa de infraestruturas críticas contra ameaças externas quanto a exploração de vulnerabilidades dos adversários. Essa proteção é reforçada pela Contra inteligência e Segurança da Informação, que atua para impedir a espionagem e o vazamento de dados sensíveis, além de focar na Proteção de Infraestruturas Críticas para assegurar a integridade dos sistemas navais e bases estratégicas (BRASIL, 2018).

A Marinha emprega as OpInfo em cenários operacionais para garantir a segurança da navegação e fortalecer sua posição estratégica. As principais aplicações incluem o monitoramento e controle do tráfego marítimo, utilizando inteligência informacional para identificar embarcações suspeitas de atividades ilícitas, como tráfico de drogas e pesca ilegal. Além disso, a guerra eletrônica em operações navais é usada para neutralizar radares inimigos e manter as comunicações seguras. A defesa cibernética de sistemas embarcados protege contra invasões digitais que possam comprometer sistemas de armamento e navegação. As OpInfo também são cruciais em missões de paz e assistência humanitária, coordenando operações de ajuda e controlando a narrativa durante crises. Por fim, são usadas na proteção contra fake news e manipulação de informação, neutralizando campanhas de desinformação que possam prejudicar a imagem da Marinha (BRASIL, 2018).

A Marinha do Brasil tem investido na modernização de suas capacidades informacionais, o que se evidencia em suas diretrizes estratégicas. Tais investimentos e prioridades estão dispostos em documentos como o Plano

Estratégico da Marinha (PEM) 2040 (MARINHA DO BRASIL, 2020), que direciona a aquisição de novas tecnologias de Comando e Controle e o aprimoramento da Defesa Cibernética. Essa iniciativa se manifesta no desenvolvimento de tecnologias e parcerias, onde a Marinha busca expandir sua infraestrutura de segurança digital e criar protocolos de defesa avançados, estabelecendo parcerias internacionais para troca de informações e aprimoramento de técnicas de guerra informacional. Além disso, a capacitação de pessoal é uma prioridade, com a implementação de cursos especializados para oficiais e praças, garantindo que o efetivo esteja preparado para as ameaças modernas. Com esses investimentos, a Marinha busca consolidar suas capacidades em OpInfo, fortalecendo sua posição como uma das principais forças navais do Atlântico Sul, e reforçando seu compromisso com a segurança digital, a proteção das comunicações e a defesa da soberania marítima do país (BRASIL, 2018).

3.4 Aplicação das Operações de Informação na Força Aérea Brasileira

A Força Aérea Brasileira (FAB) integra as OpInfo em suas operações para garantir a segurança do espaço aéreo e a proteção das infraestruturas digitais associadas ao controle do tráfego aéreo e às missões estratégicas. Apesar de não possuir um manual específico exclusivo para OpInfo, a FAB segue diretrizes estabelecidas na Doutrina de Operações Conjuntas – MD30-M-01/Volumes 1 e 2 (2ª Edição/2020) (BRASIL, 2020).

A FAB também publicou o Manual de Conduta nas Mídias Sociais no Âmbito do COMAER, que estabelece diretrizes para o uso responsável de plataformas digitais pelos militares, prevenindo vazamentos de informações e fortalecendo a segurança institucional (BRASIL, 2021).

As principais aplicações das OpInfo na FAB incluem a Guerra Eletrônica Aérea para neutralizar radares e proteger aeronaves, a Segurança Cibernética de Sistemas de Defesa Aérea para proteger redes estratégicas, o Monitoramento do Espaço Aéreo para detectar ameaças em tempo real e as Operações Psicológicas e de Comunicação Estratégica para influenciar cenários de conflito e fortalecer a posição do Brasil (BRASIL, 2020).

3.5 Exemplos de Uso Real das Operações de Informação no Brasil

Os casos reais de aplicação de OpInfo no contexto da segurança nacional incluem o combate à desinformação eleitoral, uma prioridade formalizada pela Justiça Eleitoral por meio de ações preventivas voltadas à neutralização de *fake news* (TRIBUNAL SUPERIOR ELEITORAL, 2024).

Também se observa a proteção de infraestruturas críticas, com o fortalecimento da defesa cibernética em sistemas governamentais sensíveis diante de possíveis ataques estrangeiros (MINISTÉRIO DA DEFESA, 2024; FORÇA AÉREA BRASILEIRA, 2023). Nas operações de garantia da lei e da ordem (GLO) conduzidas pelas Forças Armadas brasileiras, ainda que não haja detalhamento público de todas as ferramentas específicas empregadas, são relatadas ações conjuntas de instituições militares e de segurança na prevenção e repressão de ilícitos, reforçando a integração entre defesa, segurança pública e inteligência institucional (FORÇA AÉREA BRASILEIRA, 2023).

Além disso, em operações de caráter humanitário, as OpInfo têm sido utilizadas para coordenar ações de resgate e resposta a desastres naturais, facilitando a comunicação entre órgãos envolvidos e a disseminação de informações confiáveis à população (MENEZES, 2024).

3.6 Desafios e Perspectivas para o Futuro

Apesar dos avanços na doutrina brasileira, ainda existem desafios a serem superados, especialmente no que tange à interoperabilidade. Freire (2021) aponta para a necessidade de maior integração das OpInfo entre as Forças Armadas e órgãos governamentais, citando desafios culturais e doutrinários. Adicionalmente, o cenário global exige um investimento contínuo em tecnologias emergentes, como a inteligência artificial e segurança cibernética, cuja relevância estratégica é crescente para a defesa de ativos nacionais (SIDI, 2025). Outro ponto crucial é o desenvolvimento de programas de capacitação para militares na área de guerra informacional. Para Souza (2018), a modernização constante da doutrina de OpInfo é fundamental para que o Brasil consiga enfrentar os desafios do cenário global contemporâneo, evitando o "fratricídio informacional" por meio de melhor coordenação.

No Brasil, as OpInfo estão sendo fortalecidas dentro da estrutura das Forças Armadas, mas ainda há desafios a serem superados. A proteção de infraestruturas críticas, como redes de telecomunicações e sistemas governamentais, é uma das prioridades, conforme estabelecido na Estratégia Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2020). Além disso, o combate à desinformação e as campanhas de manipulação de mídia social, consideradas ferramentas vitais nas OpInfo contemporâneas (SOUZA, 2024), exigem a criação de unidades especializadas em guerra cognitiva, dado o seu potencial de manipular o comportamento do público (NICHOLS, 2024).

As Forças Armadas brasileiras têm investido no aprimoramento das OpInfo por meio da criação de doutrinas específicas e capacitação de pessoal. No entanto, especialistas apontam que é necessário um maior alinhamento com as melhores práticas internacionais para que o país possa enfrentar ameaças cada vez mais sofisticadas no campo informacional (DUGGAN, 2018).

A doutrina brasileira de OpInfo se consolidou como um instrumento estratégico vital para as Forças Armadas, que adaptam suas diretrizes à complexidade do ambiente informacional. A doutrina é estruturada com pilares como as Capacidades Relacionadas à Informação, que incluem guerra eletrônica e operações cibernéticas, e busca a interoperabilidade entre Exército, Marinha e Força Aérea.

Apesar dos avanços, o país ainda enfrenta desafios, como a necessidade de maior integração entre as Forças e órgãos governamentais (BRASIL, 2017), o investimento em tecnologias emergentes (BRASIL, 2024) e a capacitação de pessoal para enfrentar ameaças modernas (SOUZA, 2018). A constante modernização da doutrina é crucial para que o Brasil se prepare para os desafios globais, garantindo a soberania e a segurança nacional no domínio informacional (BRASIL, 2017, 2024; SOUZA, 2018).

4 OPERAÇÕES DE INFORMAÇÃO NAS FORÇAS ARMADAS ESTRANGEIRAS

As OpInfo vêm sendo tratadas com crescente importância por diversas Forças Armadas estrangeiras, sobretudo diante da transformação do ambiente informacional em um verdadeiro campo de batalha. Países como os Estados Unidos, Rússia, China e os membros da OTAN têm desenvolvido doutrinas robustas que reconhecem o poder das OpInfo para moldar comportamentos, influenciar decisões políticas e obter vantagens estratégicas sem o uso direto da força. Este capítulo apresenta uma análise das doutrinas adotadas por essas potências militares, com exemplos reais de aplicação e referências aos documentos oficiais utilizados.

4.1 Doutrina dos Estados Unidos da América

Os Estados Unidos foram pioneiros no desenvolvimento das OpInfo como uma função militar essencial. A partir das experiências da Segunda Guerra Mundial e da Guerra Fria, as Forças Armadas americanas consolidaram uma doutrina altamente estruturada para integrar a guerra informacional às operações militares. Atualmente, essa doutrina está organizada sob o conceito de *Joint Concept for Operating in the Information Environment (JCOIE)* (JCS, 2018), que reconhece a informação como um fator crítico para a segurança nacional e o sucesso operacional.

A principal regulamentação para as OpInfo nos Estados Unidos está consolidada na Joint Publication 3-13 – Information Operations (JP 3-13), conforme a edição de 2014. Este documento define OpInfo, destacando seu caráter estratégico e integrado:

> O emprego integrado de capacidades relacionadas à informação, em conjunto com outras linhas de operação, para influenciar, interromper, corromper ou usurpar os processos decisórios de adversários, protegendo simultaneamente as decisões dos próprios comandos (JP 3-13, 2014, p. 3).

A doutrina dos EUA se divide em diversas áreas complementares. Elas incluem as Operações Psicológicas (PSYOP), criadas para influenciar a percepção e o comportamento de populações e adversários, e a Guerra Eletrônica, que visa controlar o espectro eletromagnético. No ambiente digital, as OpInfo abrangem a Defesa e Ataque Cibernético, enquanto a Segurança Operacional protege

informações sensíveis contraespionagem e vazamentos. Por fim, o Engajamento Militar e Diplomático coordena ações entre as forças armadas e organismos diplomáticos para influenciar decisões estratégicas globais (UNITED STATES, 2014).

Essa doutrina americana enfatiza o princípio da superioridade informacional, garantindo que as forças dos EUA possuam um maior controle sobre o ambiente informacional do que seus adversários. Esse princípio baseia-se na ideia de que quem detém a informação e sabe usá-la tem uma vantagem decisiva no campo de batalha.

A implementação da doutrina americana de OpInfo pode ser observada em diversas campanhas militares e políticas ao longo da história:

a) Segunda Guerra Mundial: As forças aliadas utilizaram propaganda extensiva, desinformação e guerra psicológica para enfraquecer o moral das tropas do Eixo. Exemplo disso foi a Operação Bodyguard[9], que envolveu a criação de unidades falsas e a disseminação de informações enganosas sobre o Dia D (JP 3-13, 2014).

b) Guerra Fria: Durante esse período, os EUA investiram maciçamente em campanhas de influência, como a Radio Free Europe[10] e a Voice of America[11], para espalhar propaganda anticomunista em países sob influência soviética. Além disso, a CIA utilizou operações secretas para desestabilizar governos alinhados com a União Soviética (JCS, 2018).

c) Guerra do Golfo (1991): Durante a Operação Tempestade no Deserto, os EUA distribuíram panfletos e usaram transmissões de rádio para persuadir soldados iraquianos a desertarem. Estima-se que mais de 100.000 militares iraquianos tenham se rendido sem resistência significativa devido ao impacto psicológico dessas operações (VERTULI; LOUDON, 2018).

d) Operação Iraqui Freedom (2003): No contexto da invasão do Iraque, os EUA utilizaram uma ampla gama de OpInfo, incluindo guerra cibernética, bloqueio de

9 A Operação Bodyguard foi um complexo e ambicioso plano de engano estratégico e desinformação elaborado pelos Aliados durante a Segunda Guerra Mundial. Seu principal objetivo era confundir o Alto Comando alemão sobre a data e o local exato da invasão aliada da Europa Ocidental, que culminaria no famoso Dia D (Operação Overlord) em 6 de junho de 1944.

10 A Radio Free Europe (RFE) é uma proeminente organização internacional de radiodifusão com uma rica história enraizada na Guerra Fria. Sua missão principal sempre foi fornece notícias e informações precisas e sem censura a audiências que vivem sob regimes onde a imprensa livre é suprimida ou inexistente.

11 A Voice of America (VOA), ou Voz da América em português, é a maior e mais antiga emissora internacional dos Estados Unidos. Fundada em 1942, durante a Segunda Guerra Mundial, sua missão principal é fornecer notícias e informações precisas, objetivas e abrangentes para audiências fora dos EUA, especialmente em regiões onde a imprensa livre é restrita ou inexistente.

.

transmissões hostis e campanhas psicológicas voltadas para a população civil e forças militares de Saddam Hussein (BEEHNER et al., 2018).

e) Interferência em Conflitos Modernos: A doutrina de OpInfo dos EUA tem sido aplicada recentemente em conflitos como a guerra na Síria, onde campanhas de desinformação foram implementadas para enfraquecer as operações de grupos extremistas e atores estatais adversários (NATO, 2006).

Os Estados Unidos estão constantemente aprimorando suas capacidades de guerra informacional, com foco em ciberespaço e redes sociais. Entre as iniciativas mais recentes, destaca-se o fortalecimento do Cyber Command (CYBERCOM), criado para coordenar a defesa e o ataque cibernético e garantir a soberania digital do país. Além disso, os EUA têm se empenhado no combate à desinformação estrangeira por meio de ações conjuntas com empresas de tecnologia para neutralizar campanhas de influência de adversários. Para aumentar a eficácia das OpInfo, o país também investe na modernização das capacidades de guerra eletrônica com o uso de inteligência artificial e aprendizado de máquina (ESTADOS UNIDOS, 2024).

Apesar desses avanços, os EUA enfrentam desafios significativos, como a sofisticação crescente de campanhas de desinformação vindas de nações como Rússia e China. Além disso, precisam equilibrar ações de influência com os princípios democráticos de liberdade de informação. A experiência americana, no entanto, reforça a importância da integração entre operações militares e informacionais, mostrando que o controle da narrativa e da percepção é uma vantagem estratégica crucial nas guerras modernas.

4.2 Doutrina da Organização do Tratado do Atlântico Norte

A OTAN adota uma abordagem multidimensional para as OpInfo, integrando-as como um elemento central em suas operações conjuntas. O relatório *NATO RTO Technical Report TR-SAS-057* (2006) apresenta as ferramentas analíticas utilizadas para avaliar o impacto das ações informacionais e orienta a coordenação de capacidades como PSYOP, relações públicas, operações cibernéticas e influência civil-militar.

A Organização do Tratado do Atlântico Norte (OTAN) enxerga as OpInfo como parte de um esforço mais amplo de obtenção de "superioridade informacional",

empregando ações coordenadas para proteger suas próprias narrativas e influenciar os atores adversários. Tais ações são fortemente integradas ao planejamento e à avaliação de operações multinacionais (NATO, 2006). Um exemplo da aplicação histórica desse conceito remonta à Guerra Fria, quando a Aliança investiu amplamente em guerra psicológica e propaganda, utilizando meios de comunicação como a *Radio Free Europe*, com o objetivo de combater e neutralizar a influência ideológica da União Soviética na Europa.

Exemplo Contemporâneo: Em missões nos Bálcãs e no Afeganistão, a OTAN utilizou capacidades informacionais para neutralizar narrativas de grupos insurgentes e apoiar campanhas de reconstrução institucional com forte engajamento da população local (NATO, 2006).

4.3 Doutrina da Rússia

A Rússia considera as OpInfo um dos pilares fundamentais de sua doutrina militar moderna. Diferente das abordagens ocidentais, que focam na influência durante conflitos, a doutrina russa trata a guerra informacional como um campo de batalha contínuo, ativo tanto em tempos de paz quanto de guerra. Segundo a Doutrina Militar da Federação Russa (2014), as OpInfo são usadas para "desorganizar o funcionamento de órgãos estatais, minar a confiança na liderança política e militar adversária e manipular a percepção da população" (RÚSSIA, 2014).

A abordagem russa foi desenvolvida a partir das experiências da Guerra Fria, período em que a KGB e outras agências soviéticas já usavam a desinformação em grande escala. Hoje, a estratégia se baseia em três pilares principais. O primeiro é a desinformação estratégica, que manipula narrativas globais para criar confusão e enfraquecer adversários. Em seguida, a guerra cibernética utiliza ataques coordenados para desestabilizar sistemas governamentais e infraestruturas críticas. Por fim, as operações psicológicas têm como objetivo a influência direta sobre populações, usando mídias sociais e campanhas de influência (RÚSSIA, 2014).

A Rússia aplicou sua doutrina de OpInfo em diversos eventos históricos, moldando cenários políticos e militares sem a necessidade de conflitos diretos.

a) Guerra Fria: A KGB foi pioneira em operações de desinformação, utilizando agentes infiltrados para espalhar rumores e desestabilizar governos ocidentais. Um

exemplo clássico foi a operação InfeKtion[12], que disseminou a falsa informação de que o vírus HIV/AIDS havia sido criado pelos Estados Unidos como arma biológica (BEEHNER et al., 2018).

b) Guerra da Geórgia (2008): Durante o conflito entre a Rússia e a Geórgia, Moscou utilizou OpInfo para justificar a invasão da Ossétia do Sul. Os ataques cibernéticos coordenados desativaram sites do governo georgiano enquanto campanhas de mídia reforçavam a ideia de que a Geórgia era a agressora (VERTULI; LOUDON, 2018).

c) Anexação da Crimeia (2014): A Rússia combinou desinformação, guerra eletrônica e a presença de "tropas sem insígnia" para tomar a Crimeia sem grandes confrontos. A narrativa oficial apresentada à população russa e internacional foi de que a anexação era uma resposta ao desejo da população local, manipulando informações e censurando opositores (RÚSSIA, 2014).

d) Interferência Eleitoral nos EUA (2016): Grupos ligados ao governo russo foram acusados de realizar campanhas de desinformação para influenciar as eleições presidenciais americanas. Hackers russos invadiram servidores de partidos políticos, enquanto redes sociais foram utilizadas para disseminar notícias falsas e polarizar a opinião pública (NATO, 2006).

e) Guerra na Ucrânia (2022): A Rússia implementou uma vasta campanha informacional para justificar sua invasão da Ucrânia. O Kremlin[13] utilizou meios estatais para espalhar narrativas sobre "desnazificação", enquanto operações cibernéticas atacavam sistemas de comunicação ucranianos, dificultando a reação militar do país (BEEHNER et al., 2018).

A Rússia tem expandido suas capacidades de guerra informacional, investindo em novas tecnologias e métodos para manipular a opinião pública. Suas principais estratégias incluem a expansão das agências de inteligência GRU e FSB, que reforçaram suas unidades de guerra cibernética e de influência no Ocidente. Além disso, plataformas como RT (Russia Today) e Sputnik são usadas para disseminar propaganda e versões favoráveis ao Kremlin sobre eventos internacionais. A Rússia também utiliza ataques híbridos e cibernéticos, como

12 A Operação InfeKtion, também conhecida como Operação Denver, foi uma das mais ambiciosas e impactantes campanhas de desinformação conduzidas pela KGB, o principal serviço de inteligência da União Soviética, durante a Guerra Fria. O objetivo central dessa operação era propagar a falsa narrativa de que o vírus HIV/AIDS havia sido criado pelos Estados Unidos como parte de um projeto de pesquisa de armas biológicas em Fort Detrick, Maryland.

13 O Kremlin é um dos símbolos mais icônicos da Rússia e um complexo fortificado histórico localizado no coração de Moscou, a capital do país. A palavra "kremlin" em russo significa "fortaleza dentro de uma cidade", e embora existam outras fortalezas históricas chamadas kremlins em várias cidades russas, o de Moscou é, de longe, o mais famoso e o que é universalmente referido como "o Kremlin".

ataques coordenados a infraestruturas ocidentais e vazamento de informações sigilosas (ESTADOS UNIDOS. DEPARTAMENTO DE ESTADO, 2022).

A doutrina russa de OpInfo é um dos maiores desafios para os países ocidentais. Sua abordagem assimétrica e híbrida torna difícil identificar os responsáveis e dar uma resposta adequada. O sucesso dessas táticas em conflitos recentes mostra a importância da guerra informacional no século XXI e a necessidade de outras nações desenvolverem estratégias de defesa robustas.

4.4 Doutrina da China

A República Popular da China utiliza um conceito conhecido como Guerra de Informação Integrada, uma doutrina que prioriza o uso de OpInfo para obter vantagem estratégica antes que um conflito armado comece (JFSC, 2002). Entre as principais capacidades chinesas utilizadas nesse modelo, destacam-se ciberataques ofensivos, o controle rigoroso de mídias e redes sociais, a censura informacional e a manipulação de conteúdo digital, além de amplas campanhas de influência internacional (ESTADOS UNIDOS. DOD, 2024).

A história demonstra a aplicação dessa abordagem. Durante a Guerra da Coreia (1950-1953), por exemplo, a China utilizou táticas de guerra psicológica para abalar o moral as tropas da ONU, empregando rádios clandestinos e mensagens direcionadas aos soldados aliados (JFSC, 2002).

Em um contexto mais recente, durante a escalada das tensões no Mar do Sul da China, o país utilizou OpInfo para controlar a narrativa tanto em nível doméstico quanto internacional. Essa estratégia combinou censura e desinformação com diplomacia pública e coerção informacional para fortalecer sua posição (VERTULI; LOUDON, 2018).

4.5 Pensamentos Convergentes nas Doutrinas Estrangeiras

As experiências internacionais mostram que a informação deve ser tratada como um recurso estratégico desde o início das operações. A combinação de capacidades informacionais e militares tradicionais aumenta o impacto das ações, e a superioridade informacional é essencial para obter domínio cognitivo e tomar decisões favoráveis em conflitos modernos. A cooperação entre forças armadas,

setor civil e mídia também pode ser decisiva. Essas lições reforçam a necessidade de o Brasil ter uma doutrina mais integrada, proativa e tecnológica, pronta para os desafios do século XXI no domínio informacional.

O capítulo demonstrou que as OpInfo ocorrem em um ambiente de confronto determinante para potências globais, como EUA, OTAN, Rússia e China, que as utilizam para moldar comportamentos e obter vantagens estratégicas. A doutrina americana, por exemplo, foca na superioridade informacional, enquanto a russa adota uma abordagem assimétrica e híbrida, e a chinesa utiliza a Guerra de Informação Integrada. A partir dessas experiências, as lições aprendidas reforçam a necessidade de o Brasil desenvolver uma doutrina mais integrada, proativa e tecnológica, capaz de enfrentar os desafios do século XXI no domínio informacional.

5 AS DOUTRINAS DE OPERAÇÕES DE INFORMAÇÃO APLICADAS NOS CONFLITOS CONTEMPORÂNEOS

As OpInfo têm desempenhado um papel central nos conflitos contemporâneos, influenciando diretamente a percepção pública, o comportamento de adversários e a condução de operações militares. O ambiente informacional tornou-se um dos principais teatros de operação no século XXI, onde a manipulação de dados, narrativas, a guerra cibernética e a influência psicológica do adversário podem ter se tornado armas tão poderosas quanto os meios convencionais. A seguir, são analisadas algumas das principais frentes de aplicação das OpInfo em conflitos recentes e atuais.

5.1 Guerra Informacional no Conflito entre Rússia e Ucrânia

A guerra entre Rússia e Ucrânia, iniciada em 2014 com a anexação da Crimeia e intensificada em 2022 com a invasão em larga escala, representa um marco na aplicação de OpInfo em cenário de guerra híbrida. A utilização coordenada de desinformação, ataques cibernéticos e campanhas psicológicas foi planejada para enfraquecer a resistência ucraniana, confundir o público internacional e moldar o ambiente cognitivo em favor dos interesses russos (BARBOSA, 2020) (PARLAMENTO EUROPEU, 2025).

Antes mesmo do início formal do conflito, a Rússia já promovia uma intensa campanha de manipulação midiática, com o objetivo de justificar suas ações para o público doméstico e internacional. Essa campanha se destacou pela propagação da ideia de que a Ucrânia era governada por "nazistas" e que a invasão era necessária para proteger minorias russas, além de incluir a criação de conteúdos audiovisuais manipulados que retratavam atrocidades supostamente cometidas por forças ucranianas. A estratégia russa também se apoiou no financiamento e na disseminação de desinformação por meio de portais controlados, direta ou indiretamente, por Moscou (BARBOSA, 2020) (PARLAMENTO EUROPEU, 2025).

Durante a fase inicial da invasão em 2022, houve uma sincronia evidente entre as ações cinéticas e as ofensivas informacionais. Ataques cibernéticos contra a infraestrutura crítica da Ucrânia, como redes elétricas, bancos e meios de comunicação, antecederam e acompanharam as movimentações militares. Essas

ações não apenas dificultaram a resposta ucraniana, como também amplificaram o pânico social, elemento crucial para desestabilizar a resistência (NATO, 2006).

Paralelamente, a Ucrânia adotou uma abordagem inovadora de contrainformação. O presidente Volodymyr Zelenskyy se destacou por sua atuação direta nas redes sociais, fornecendo atualizações constantes em vídeo, rebatendo falsas alegações e promovendo uma imagem de coragem e liderança. Plataformas como Twitter, TikTok e Telegram foram amplamente utilizadas por civis e militares ucranianos para relatar ações do inimigo, divulgar desmentidos e mobilizar apoio global (REYNOLDS, 2022).

A resistência digital ucraniana contou também com o apoio de especialistas em tecnologia e *hackers* voluntários, que formaram uma espécie de "exército cibernético civil" para defender as comunicações, promover campanhas pró-Ucrânia e atacar alvos informacionais russos. A utilização de drones, inteligência artificial e sistemas de mapeamento de alvos informacionais também demonstrou um elevado grau de sofisticação e adaptação tática (LYSENKO; GUNITSKY, 2025).

Outro aspecto relevante foi o apoio coordenado da comunidade internacional de tecnologia. Empresas como a Microsoft e o Google atuaram de forma decisiva para bloquear ameaças cibernéticas, apoiar a segurança dos sistemas do governo ucraniano e remover conteúdos enganosos em suas plataformas (MICROSOFT, 2023).

A guerra informacional na Ucrânia evidencia o novo paradigma dos conflitos contemporâneos: o domínio cognitivo tornou-se tão decisivo quanto os campos de batalha físicos. A disputa por narrativas, o controle da informação e a mobilização de atores digitais são hoje ferramentas cruciais para a vitória política e militar (GÓMEZ, 2023).

5.2 Estratégia de Operações de Informação na Disputa pelo Mar do Sul da China

O Mar do Sul da China[14] tornou-se um dos principais palcos da guerra informacional contemporânea, com ênfase nas estratégias de OpInfo utilizadas pela República Popular da China (RPC) para moldar a percepção internacional, silenciar

14 O Mar do Sul da China é um mar marginal do Oceano Pacífico Ocidental, localizado no sudeste da Ásia. É uma vasta extensão de água de aproximadamente 3,5 milhões de km², cercada por diversos países, incluindo China, Vietnã, Filipinas, Malásia, Brunei, Indonésia, Cingapura, Tailândia, Camboja e Taiwan.

críticas internas e legitimar suas reivindicações territoriais. A disputa sobre essa área estratégica é travada não apenas por meios diplomáticos ou militares, mas principalmente no domínio informacional, onde a influência sobre narrativas e o controle da opinião pública exercem papel central (ESTADOS UNIDOS. DOD, 2024).

A China emprega uma série de OpInfo. Um de seus métodos é a censura e a vigilância digital interna, onde o governo chinês bloqueia conteúdos críticos e monitora interações em plataformas como Weibo e WeChat para reforçar a narrativa estatal e reprimir informações que contrariem seus interesses. A China também realiza a amplificação da propaganda estatal internacional por meio de veículos como CGTN e Xinhua, que promovem uma imagem positiva do país no exterior, defendendo a "linha de nove traços" e retratando adversários como desestabilizadores. Outra estratégia é a chamada "diplomacia do lobo guerreiro"[15], uma postura agressiva de diplomatas chineses em redes sociais, que visa controlar o discurso global e projetar poder informacional. Além disso, a China produz e dissemina narrativas históricas seletivas, usando documentos manipulados como "provas" para justificar sua soberania em regiões disputadas (CHEVALARIAS; HORSBURGH, 2024).

Em contrapartida, os Estados Unidos e seus aliados usam OpInfo para contrabalançar a ofensiva chinesa com contranarrativas públicas estruturadas, contestando as alegações da China e promovendo a liberdade de navegação. Eles também monitoram a desinformação por meio de instituições como o South China Sea Strategic Situation Probing Initiative (SCSPI) e think tanks, que publicam análises críticas para neutralizar o impacto das ações chinesas. Por fim, promovem campanhas informacionais coordenadas para gerar um impacto favorável no Sudeste Asiático, defendendo a transparência, o multilateralismo e o respeito ao direito internacional como alternativa à opacidade chinesa (BOWLING; HODGE, 2024).

Dessa forma, a tensão no Mar do Sul da China configura-se como um exemplo emblemático da centralidade das OpInfo nos conflitos modernos. O uso coordenado de meios informacionais visa alcançar efeitos estratégicos duradouros, mesmo na ausência de confrontos militares diretos, reposicionando o domínio cognitivo como eixo central das disputas geopolíticas da atualidade.

15 A Diplomacia do Lobo Guerreiro (em inglês, Wolf Warrior Diplomacy) é um estilo de diplomacia agressiva e assertiva adotado por diplomatas chineses no século XXI, especialmente a partir da administração do líder Xi Jinping. O termo, que se popularizou durante a pandemia de COVID-19, é inspirado em uma série de filmes de ação chineses extremamente populares, como "Wolf Warrior 2", nos quais um herói chinês defende os interesses da China com força e coragem.

5.3 Uso de Operações de Informação em Conflitos no Oriente Médio

No Oriente Médio, as OpInfo são amplamente utilizadas em conflitos, como na guerra civil da Síria e no combate ao Estado Islâmico (EI). O EI, por exemplo, usou as redes sociais para recrutar e propagar sua ideologia extremista, produzindo vídeos em alta qualidade para causar impacto psicológico. Em resposta, as forças americanas e da coalizão desenvolveram campanhas para deslegitimar o grupo. Já o governo sírio e seus aliados russos utilizaram a desinformação para negar ataques a civis e gerar confusão na mídia internacional. Além disso, o Irã opera redes regionais de desinformação por meio de grupos como Hezbollah e Houthi. Em toda a região, regimes autoritários usam OpInfo para consolidar seu poder interno, manipulando eleições, censurando redes sociais e empregando bots para desviar o debate público, enquanto plataformas criptografadas como Telegram e Signal são usadas para distribuir propaganda e coordenar ações (DORAN; GULLEY, 2023).

5.4 O Papel das Operações de Informação em Atores Não-Estatais e Grupos Terroristas

Grupos terroristas, milícias armadas e organizações transnacionais têm adotado estratégias sofisticadas de OpInfo. Eles utilizam ferramentas de baixo custo com grande impacto, como a criação de canais criptografados em aplicativos de mensagens para espalhar propaganda. Também empregam *deepfakes*[16], *bots* e perfis falsos para manipular debates públicos e disseminar desinformação. Além de objetivos financeiros, ataques de *ransomware*[17] são usados para a destruição reputacional. Para evitar sistemas de monitoramento, esses grupos criam redes descentralizadas e utilizam plataformas como Reddit, 4chan e fóruns obscuros para disseminar ideologias extremistas e angariar apoio anônimo (IST, 2024).

Esse cenário exige uma resposta igualmente informacional, com estratégias de monitoramento em tempo real, combate à radicalização, desenvolvimento de

16 Os deepfakes são mídias sintéticas, vídeos, fotos ou gravações de áudio, que foram manipuladas com inteligência artificial (IA), especificamente aprendizagem profunda (deep learning), para parecerem reais. O termo em si é uma junção de "deep learning" e "fake" (falso em inglês).

17 Ransomware é um tipo de malware (software malicioso) que impede você de acessar seu dispositivo e os dados armazenados nele, geralmente criptografando seus arquivos. Um grupo criminoso então exige um resgate em troca da chave de descriptografia ou da restauração do acesso. O próprio computador pode ser bloqueado, ou os dados podem ser criptografados, roubados ou excluídos.

inteligência artificial para reconhecimento de padrões e cooperação internacional para rastrear e desmantelar redes informacionais hostis. Os exemplos mais recentes incluem o uso de canais no Telegram por grupos extremistas na Europa e no Oriente Médio, bem como a disseminação de *fake news* por grupos paramilitares em zonas de instabilidade na África. O crescente uso de inteligência artificial generativa para criação de conteúdos falsos em vídeo e áudio representa um novo desafio para a segurança internacional (ESTADOS UNIDOS. DOD, 2024).

O capítulo demonstrou que as OpInfo são um elemento central em conflitos contemporâneos. A guerra na Ucrânia, por exemplo, é um marco no uso de guerra híbrida, com a Rússia empregando desinformação e ataques cibernéticos, enquanto a Ucrânia se defende com uma abordagem inovadora nas redes sociais e o apoio de um "exército cibernético". A disputa no Mar do Sul da China também é um exemplo, mostrando como a China utiliza censura e propaganda para defender suas reivindicações. Além dos conflitos entre nações, as OpInfo são amplamente usadas por atores não estatais e grupos terroristas no Oriente Médio, que empregam mídias sociais, deepfakes e ataques de ransomware. Tais exemplos reforçam que o domínio cognitivo se tornou tão decisivo quanto o campo de batalha físico, fazendo com que a disputa por narrativas e o controle da informação sejam fatores críticos para o sucesso em conflitos do século XXI.

6 RECOMENDAÇÕES PARA A DOUTRINA DAS FORÇAS ARMADAS BRASILEIRAS

As OpInfo são cruciais no cenário de conflitos contemporâneos. Para combater eficazmente ameaças híbridas e fortalecer a soberania nacional, a doutrina militar brasileira precisa se adaptar a essa realidade. Este capítulo propõe aprimoramentos na doutrina das Forças Armadas Brasileiras (FAB) no âmbito das OpInfo, baseando-se em práticas bem-sucedidas de outros países e nas necessidades específicas do Brasil. As recomendações são apresentadas com o objetivo de que o leitor compreenda os desafios, as soluções propostas e os impactos esperados.

6.1 Fortalecimento da Estrutura de Comando e Controle das Operações de Informação

A criação de uma estrutura centralizada é essencial para a eficácia das OpInfo no Brasil. Atualmente, cada força militar atua de forma independente, o que gera redundância e falta de sinergia. Para resolver isso, propõe-se a criação de um Comando Conjunto de Operações de Informação, subordinado ao Ministério da Defesa, com a função de coordenar as ações de OpInfo em níveis estratégico e operacional. Esse comando também seria responsável por desenvolver doutrinas padronizadas para missões conjuntas, integrar a inteligência cibernética e o monitoramento informacional das três forças e criar um centro de análise de ameaças e de combate à desinformação (SILVA, 2024).

Além disso, sugere-se a implementação de centros regionais de inteligência operacional. Esses centros atuariam no nível tático, integrando unidades locais das Forças Armadas com órgãos de segurança pública e entidades civis (SILVA, 2024).

6.2 Desenvolvimento de Capacidades Cibernéticas para Defesa e Ataque

A guerra cibernética tem sido um dos pilares das OpInfo no século XXI, com países como China, EUA e Rússia investindo fortemente nesse setor. O Brasil deve expandir as capacidades do Centro de Defesa Cibernética (CDCiber), tornando-o um

pilar central na proteção de infraestruturas críticas e na condução de operações ofensivas e defensivas no ciberespaço.

Para enfrentar as ameaças no ambiente digital, as principais iniciativas recomendadas incluem o aprimoramento das defesas cibernéticas para proteger infraestruturas críticas, como redes elétricas e bancos de dados estratégicos. É crucial também o desenvolvimento de capacidades ofensivas, permitindo o monitoramento e a desativação de redes informacionais adversárias. Além disso, é essencial o treinamento especializado para militares e civis, formando especialistas em ciberdefesa e análise de inteligência digital. Por fim, a cooperação internacional com países aliados é fundamental para o intercâmbio de conhecimento acerca de ameaças informacionais (PEREIRA; SANTOS, 2023).

6.3 Modernização das Táticas de Guerra Psicológica e Campanha de Influência

A guerra psicológica e a manipulação informacional são amplamente utilizadas em conflitos modernos, como no caso da Ucrânia e das tensões no Mar do Sul da China (BEEHNER et al., 2018; JFSC, 2002). O Brasil deve investir em centros de análise comportamental e no treinamento de militares para a criação de narrativas eficazes que fortaleçam a imagem institucional das Forças Armadas e combatam a desinformação adversária (SANTOS; OLIVEIRA, 2024).

As recomendações para o aprimoramento das OpInfo incluem o monitoramento em tempo real de narrativas adversárias em redes sociais e mídias. Para isso, o uso de Inteligência Artificial (IA) e aprendizado de máquina é fundamental para detectar padrões de desinformação e analisar o comportamento do público-alvo. Também é sugerida a produção de conteúdos estratégicos para fortalecer a percepção sobre a atuação das Forças Armadas e neutralizar campanhas de desinformação contra o Brasil. Por fim, o treinamento de militares especialistas em informação é essencial para a atuação em operações psicológicas por meio digital e campanhas informacionais.

6.4 Integração das Operações de Informação ao Planejamento Estratégico Nacional

Para que as OpInfo sejam eficazes, elas precisam ser formalmente incorporadas ao planejamento estratégico nacional do Ministério da Defesa e de outros órgãos de segurança. Isso exige a criação de diretrizes oficiais e protocolos bem definidos para lidar com situações como ataques de desinformação em períodos eleitorais ou crises institucionais, além do monitoramento informacional em regiões estratégicas como a Amazônia e as fronteiras. Também é necessário estabelecer protocolos para o controle de campanhas de guerra híbrida conduzidas por atores estatais e não estatais contra o Brasil.

É recomendada, ainda, uma estreita cooperação entre as forças militares e a comunidade acadêmica. Essa colaboração promoveria estudos e publicações sobre OpInfo e sobre as ameaças emergentes no domínio informacional.

6.5 Capacitação de Pessoal Especializado

As forças militares que se destacam no uso de OpInfo possuem unidades altamente treinadas, como a *77th Brigade* do Exército Britânico e as unidades de guerra híbrida da Rússia (JP 3-13, 2014; NATO, 2006). Para que o Brasil se torne competitivo no campo das OpInfo, é essencial investir na capacitação contínua de militares e especialistas civis. As medidas necessárias para isso incluem a inclusão de disciplinas de OpInfo em cursos de formação militar, a criação de cursos de especialização em OpInfo e guerra cibernética avançada, o estabelecimento de parcerias com universidades para pesquisa e inovação tecnológica e a realização de exercícios conjuntos de guerra informacional que simulem cenários reais de ameaças (MACHADO; FERREIRA, 2024).

6.6 Criação de uma Estratégia Nacional de Comunicação Estratégica

A comunicação estratégica é essencial para fortalecer a resiliência da sociedade contra ameaças informacionais. Para isso, o desenvolvimento de um Plano Nacional de Comunicação Militar é sugerido. Esse plano deve incluir campanhas institucionais de conscientização pública sobre segurança digital e ameaças informacionais. Além disso, propõe-se a criação de canais de comunicação diretos entre as Forças Armadas e a população para promover a transparência e a confiança. O plano também deve prever a adoção de estratégias de

contrainformação para combater narrativas hostis à soberania nacional e o uso da diplomacia informacional para projetar as narrativas estratégicas do Brasil no cenário internacional.

6.7 Consolidação de Parcerias com Setores Tecnológicos e Acadêmicos

O desenvolvimento de capacidades em OpInfo no Brasil não pode acontecer de forma isolada. Para garantir competitividade e eficácia, é fundamental que o país invista em parcerias estratégicas com universidades, centros de pesquisa e indústrias de defesa. As ações recomendadas para isso incluem o financiamento de pesquisas acadêmicas em segurança da informação e OpInfo, a criação de programas de cooperação científica entre as Forças Armadas e instituições de ensino, e o estabelecimento de incubadoras militares para o desenvolvimento de novas tecnologias aplicadas às operações informacionais.

6.8 Impactos Esperados

A implementação dessas recomendações permitirá que as Forças Armadas Brasileiras se adaptem ao cenário global, garantindo maior eficiência na proteção da soberania nacional e defesa contra ameaças híbridas. Com a crescente digitalização das guerras e o aumento da relevância do domínio informacional, a modernização da doutrina brasileira nesse campo é essencial para sua posição estratégica no século XXI, conforme o modelo de integração doutrinária adotado pelas principais alianças militares ocidentais (NATO, 2006).

O capítulo propõe uma série de recomendações para aprimorar a doutrina brasileira de OpInfo, visando à maior eficácia contra ameaças híbridas e ao fortalecimento da soberania nacional. A principal sugestão é a criação de um Comando Conjunto de Operações de Informação, que centralizaria as ações das Forças Armadas para combater a redundância e promover sinergia operacional.

Além disso, são propostos o desenvolvimento de capacidades cibernéticas tanto defensivas quanto ofensivas, a modernização das táticas de guerra psicológica com o uso de IA e o treinamento de militares, e a formalização das OpInfo no planejamento estratégico nacional. O texto também ressalta a importância de capacitar militares e civis, criar uma estratégia de comunicação nacional e consolidar

parcerias com os setores tecnológico e acadêmico para promover inovação e pesquisa. Tais medidas são consideradas essenciais para garantir que o Brasil se adapte ao cenário global e proteja sua posição estratégica no século XXI.

7 CONSIDERAÇÕES FINAIS

Ao longo desta dissertação, a análise das OpInfo demonstrou que elas evoluíram de instrumentos complementares para se tornarem cruciais nos conflitos modernos. Esta pesquisa buscou analisar que o domínio informacional está cada vez mais consolidado como um campo de batalha decisivo, onde narrativas, percepções e o controle cognitivo podem influenciar os rumos de uma guerra, por vezes, antes mesmo do emprego de armamentos convencionais.

A análise de conflitos recentes, como a guerra entre Rússia e Ucrânia, a atuação da China no Mar do Sul da China e as dinâmicas do Oriente Médio, mostra que o uso coordenado de OpInfo é crucial para alcançar a vantagem estratégica. Esses exemplos indicam que uma Força Armada moderna precisa atuar não apenas em ambientes tradicionais como terra, mar e ar, mas também no ciberespaço e no domínio cognitivo do conflito.

Na Guerra da Ucrânia, a Rússia implementou campanhas massivas de desinformação, combinadas com ataques cibernéticos, guerra psicológica e controle de narrativas, visando desestabilizar o governo ucraniano e desmobilizar a opinião pública ocidental. Em resposta, a Ucrânia demonstrou que estratégias ágeis de contrainformação, comunicação direta com a população e engajamento em redes sociais podem ajudar a reverter os impactos de uma ofensiva informacional.

A partir da análise das doutrinas de Forças Armadas como as dos Estados Unidos, OTAN, Rússia e China, percebe-se uma convergência crescente sobre a necessidade de integrar as OpInfo a todos os níveis do planejamento estratégico militar. A doutrina americana e os conceitos da OTAN, por exemplo, reforçam a ideia de que a informação deve ser tratada como um recurso operacional de grande valor em um conflito e fora dele. Já no modelo russo, as OpInfo são utilizadas não apenas em tempos de guerra, mas também como instrumentos de dissuasão e controle sociopolítico em tempos de paz. A China, por sua vez, incorpora as OpInfo em uma estratégia mais ampla de guerra de informação integrada, buscando obter superioridade sem a necessidade de um confronto direto.

Diante da questão de pesquisa " A Doutrina de OpInfo das Forças Armadas Brasileiras atende efetivamente aos desafios dos conflitos modernos?", conclui-se que a doutrina atual, embora em evolução e com avanços notáveis em áreas como a defesa cibernética, apresenta oportunidades de melhoria para enfrentar a complexidade dos desafios informacionais contemporâneos. A análise desta dissertação indica que a falta de uma abordagem sistêmica que integre as OpInfo em todas as operações militares, a ausência de protocolos interforças bem definidos e a possível fragmentação das capacidades existentes são os principais desafios que limitam a consolidação de uma doutrina mais sólida.

Fundamentado nas experiências dos conflitos contemporâneos internacionais e nas necessidades da Defesa Nacional, o texto propõe recomendações doutrinárias visando o aumento da eficiência no emprego das OpInfo para o Brasil. A primeira é a criação de um Comando Conjunto de OpInfo, uma estrutura capaz de coordenar as ações de todas as Forças Armadas. O objetivo é padronizar doutrinas, promover a interoperabilidade e otimizar recursos humanos e tecnológicos.

Outro ponto importante é a integração plena da Defesa Cibernética às OpInfo. A recomendação é transformar o Centro de Defesa Cibernética (CDCiber) para que ele atue não apenas na proteção, mas também na ofensiva estratégica e na condução de campanhas informacionais. O desenvolvimento de capacidades de guerra psicológica e campanhas de influência também é visto como essencial, com a sugestão de investir na elaboração de campanhas que utilizem dados comportamentais e inteligência artificial para influenciar públicos-alvo.

No campo da capacitação, o texto propõe a formação e especialização militar em OpInfo, tornando a disciplina obrigatória nas academias e criando cursos focados em operações cognitivas, guerra cibernética e análise de narrativas. Para uma atuação mais ampla, é sugerida a criação de uma doutrina nacional de comunicação estratégica que envolva tanto as Forças Armadas quanto instituições civis, unificando discursos e combatendo a desinformação.

Por fim, o texto destaca a importância de parcerias civis-militares com universidades e empresas de tecnologia para promover a inovação, além da implementação de estruturas de resposta rápida para monitorar e combater ameaças cognitivas em tempo real.

Esta pesquisa buscou contribuir para a compreensão da importância e da complexidade das OpInfo no contexto brasileiro, à luz das experiências

internacionais. Contudo, reconhece-se que as limitações de tempo e recursos inerentes a um trabalho de mestrado impediram um aprofundamento em todas as nuances do tema. Espera-se que este estudo sirva como base e inspiração para pesquisas futuras, que possam avançar ainda mais na compreensão e no desenvolvimento da doutrina de Operações de Informação no Brasil, dada sua crescente relevância do tema para a segurança e defesa nacional.

REFERÊNCIAS

ALBERTS, David S.; GARSTKA, John J.; STEIN, Frederick P. **Network Centric Warfare: Developing and Leveraging Information Superiority**. Washington, DC: CCRP, 1999.

BEEHNER, Lionel et al. **Russian Information Warfare and the Hard Reality of Soft Power**. U.S. Army War College, 2018.

BRASIL. Marinha do Brasil. **Estado-Maior da Armada. EMA-335: Operações de Informação**. Brasília, 2018.

BRASIL. Exército Brasileiro. **Manual de Campanha: Operações de Informação**. C 100-5. Brasília, 2019.

BRASIL. Ministério da Defesa. **Doutrina de Operações de Informação**. MD-30-M-01. Brasília, 2020.

BRASIL. Ministério da Defesa. **Doutrina de Operações de Informação**. MD-30-M-01. Brasília, 2021.

BRASIL. Marinha do Brasil. **Plano Estratégico da Marinha (PEM) 2040**. Rio de Janeiro, RJ, 2020.

BRASIL. Comando da Aeronáutica. **DCA 1-1: Doutrina Básica da Força Aérea Brasileira**. Brasília, DF, 2020.

CHAUMONT, Jean-Baptiste. **La guerre cognitive: De la manipulation à l'influence. Paris**: Presses Universitaires de France, 2021.

CHINA DAILY. **China's Position on the South China Sea**. 2022.

COLBY, Elbridge A. **The Strategy of Denial: American Defense in an Age of Great Power Conflict.** New Haven: Yale University Press, 2021.

DUGGAN, Patrick. **Information Warfare and the Future of Conflict.** Washington, DC: National Defense University Press, 2018.

GERASIMOV, Valery. **The Role of Information in Modern Warfare.** Moscow: Military Thought Journal, 2013.

JOINT CHIEFS OF STAFF (JCS). **Joint Concept for Operating in the Information Environment (JCOIE).** Washington, D.C.: JCS, 2018.

JOINT CHIEFS OF STAFF (JCS). **Joint Publication 3-13 – Information Operations (JP 3-13).** Washington, D.C.: JCS, 2014.

JOINT FORCES STAFF COLLEGE (JFSC). **Information Operations: Warfare and the Hard Reality of Soft Power.** Norfolk, VA: National Defense University Press, 2002.

MICROSOFT. **Defending Ukraine: Early Lessons from the Cyber War.** Microsoft Digital Threat Analysis Center, 2022.

NATO. **Cognitive Warfare: The Battle for the Human Mind.** Brussels, 2022.

NATO. **NATO RTO Technical Report TR-SAS-057: Analysis of NATO Information Operations Tools and Capabilities.** Brussels: NATO, 2006.

RÚSSIA. **Doutrina Militar da Federação Russa.** Moscou, 2014.

SINGER, P. W.; BROOKS, Emerson T. **LikeWar: The Weaponization of Social Media.** New York: Houghton Mifflin Harcourt, 2018.

SOUTH CHINA SEA STRATEGIC SITUATION PROBING INITIATIVE (SCSPI). **Reports and Briefings**, 2021–2023.

SUN TZU. **A Arte da Guerra**. Tradução de André Bueno. São Paulo: Edipro, 2015.

THOMPSON, Mark. **Psychological Warfare and Cyber Conflict in the 21st Century**. London: Routledge, 2020.

U.S. DEPARTMENT OF DEFENSE. **Annual Report to Congress: Military and Security Developments Involving the People's Republic of China**. 2022.

VERTULI, Robert; LOUDON, David. **Perceptions Are Reality: Historical Case Studies of Information Operations in Large-Scale Combat Operations.** U.S. Army War College, 2018.

VERTULI, A.; LOUDON, J. **Propaganda do Estado Islâmico: técnicas e objetivos. Journal of Security Studies,** v. 45, n. 2, p. 215-235, 2018.

ZELENSKYY, Volodymyr. **Official Statements and Social Media Broadcasts**, 2022.

https://www.tse.jus.br/comunicacao/noticias/2024/Maio/gestao-alexandre-de-moraes-combate-as-fake-news-e-milicias-digitais-reforcaram-confiabilidade-do-processo-eleitoral

FORÇA AÉREA BRASILEIRA. **Comandante de Operações Aeroespaciais visita Exercício Guardião Cibernético 6.0**. Brasília, 17 nov. 2023. Disponível em: https://www.fab.mil.br/noticias/mostra/43283. Acesso em: 27 out. 2025.

MENEZES, Hélio Sancler Santos de. **O papel das Forças Armadas nas ações humanitárias: catástrofes e epidemias: as normas do setor operativo da Marinha do Brasil atendem as necessidades das ações de resposta a catástrofes naturais em apoio à Defesa Civil?** 2024. Monografia (Curso Superior) – Escola de Guerra Naval, Rio de Janeiro, 2024. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/cctsancler%20-

%20O%20PAPEL%20DAS%20FOR%C3%87AS%20ARMADAS%20NAS%20A%C3%87%C3%95ES%20HUMANIT%C3%81RIAS.

BARBOSA, Alexandre Henrique Batista. **A desinformação como ferramenta da guerra híbrida**. 2020. 85 f. Monografia (Curso de Política e Estratégia Marítimas) – Escola de Guerra Naval, Rio de Janeiro, 2020. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/C-PEM010%20-%20CMG%20%28FN%29%20ALEXANDRE%20HENRIQUE%20BATISTA%20BARBOSA%20-%20A%20DESINFORMA%C3%87%C3%83O%20COMO%20FERRAMENTA%20DA%20GUERRA%20H%C3%8DBRIDA.pdf

PARLAMENTO EUROPEU. **Resolução do Parlamento Europeu, de 23 de janeiro de 2025, sobre a desinformação e falsificação histórica por parte da Rússia para justificar a sua guerra de agressão contra a Ucrânia (2024/2988(RSP)).** [S. l.]: Parlamento Europeu, 2025. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:C_202502147.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas. MD30-M-01: Doutrina de Operações Conjuntas. 2. ed**. Brasília, DF, 2020. v. 1 e 2.

FREIRE, Maria Eduarda Laryssa Silva. **A interoperabilidade entre as Forças Armadas Brasileiras: uma análise da Operação Ágata**. 2021. Monografia (Trabalho de Conclusão de Curso) – Universidade Federal da Paraíba, João Pessoa, 2021. Disponível em: https://repositorio.ufpb.br/jspui/handle/123456789/13942.

SIDI. **Cibersegurança na era da Inteligência Artificial: desafios e soluções**. SiDi, [S. l.], 4 set. 2025. Disponível em: https://www.sidi.org.br/pt-br/blog/ciberseguranca-na-era-da-inteligencia-artificial-desafios-e-solucoes.

SOUZA, João Cláudio Ramos de. **Operações de Informação (OpInfo). Âncora & Fuzis: Revista de Estudos Navais**, Rio de Janeiro, n. 43, p. 119-138, 2018. Disponível em: https://portaldeperiodicos.marinha.mil.br/index.php/ancorasefuzis/article/download/2287/2300.

BRASIL. Presidência da República. **Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Brasília, DF: Presidência da República**, 2020. Disponível em: https://www.planalto.gov.br/cCivil_03/_Ato2019-2022/2020/Decreto/D10569.htm.

SOUZA, Diego Resende Miranda de. **Operações de Informação: análise das capacidades relacionadas à informação (CRI) na Doutrina da Marinha do Brasil**. 2024. Monografia (Curso de Altos Estudos de Política e Estratégia) – Escola de Guerra Naval, Rio de Janeiro, 2024. Disponível em: https://www.repositorio.mar.mil.br/bitstream/ripcmb/847544/1/C-EMOS2024_CC_MIRANDADESOUZA.pdf.

NICHOLS, Giselli Christina Leal. **Guerra cognitiva nas redes sociais: análise das ameaças e propostas para políticas públicas do Ministério da Defesa**. 2024. Relatório Técnico (Doutorado Profissional em Estudos Marítimos) – Escola de Guerra Naval, Rio de Janeiro, 2024. Disponível em:

https://www.marinha.mil.br/ppgem/sites/www.marinha.mil.br.ppgem/files/TCD%20Final%20Giselli%20Nichols.pdf.

BRASIL. Ministério da Defesa. **Estado-Maior Conjunto das Forças Armadas. MD33-M-12: Operações Interagências (2ª Edição)**. Brasília, DF: Ministério da Defesa, 2017. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/operacoes/md33a_ma_12a_opa_interagenciasa_2a_eda_2017.pdf.

BRASIL. **Ministério do Desenvolvimento, Indústria, Comércio e Serviços. Missão 6 da Nova Indústria Brasil: Rumo à Soberania Tecnológica.** Brasília, DF: MDIC, 2024. Disponível em: https://www.gov.br/mdic/pt-br/noticias/2024/janeiro/missao-6-da-nova-industria-brasil-rumo-a-soberania-tecnologica.

ESTADOS UNIDOS. **Department of Defense. 2023 Department of Defense Cyber Strategy. Washington, D.C.: U.S. Department of Defense**, 2023. Disponível em: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf

ESTADOS UNIDOS. **Department of State. Gabinete do Porta-Voz. As cinco principais narrativas persistentes de desinformação da Rússia. Washington, D.C.: U.S. Department of State**, 2022. Disponível em: https://2021-2025.state.gov/translations/portuguese/as-cinco-principais-narrativas-persistentes-de-desinformacao-da-russia/

ESTADOS UNIDOS. **Department of Defense. Military and Security Developments Involving the People's Republic of China 2024: Annual Report to Congress. Washington, D.C.: U.S. Department of Defense**, 2024. Disponível em: https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF.

REYNOLDS, Jefferson. Volodymyr Zelenskyy's **New Rules for Information Warfare. Atlantic Council, Washington, D.C.**, 20 set. 2022. Disponível em: https://www.atlanticcouncil.org/blogs/new-atlanticist/volodymyr-zelenskyys-new-rules-for-information-warfare/.

LYSENKO, Anna; GUNITSKY, Seva. **The invisible front: Ukraine's IT army and the evolution of cyber resistance. [S.l.: s.n.]**, 2025. Disponível em: https://www.researchgate.net/publication/391793477_The_invisible_front_Ukraine's_it_army_and_the_evolution_of_cyber_resistance.

MICROSOFT. **Threat Intelligence Center (MSTIC). Defending Ukraine: Early Lessons from the Cyber War. Redmond, WA: Microsoft**, 2023. Disponível em: https://www.microsoft.com/en-us/security/business/content-hub/defending-ukraine-early-lessons-from-the-cyber-war.

GÓMEZ, Ricardo. **The cognitive domain: The new battleground for influence and control. Revista de Relações Internacionais, v. 15, n. 2, p. 45-62**, 2023. Disponível em: https://journal.scientificsociety.net/index.php/sobre/jornal-academico.

CHEVALARIAS, Laura; HORSBURGH, Michael. **China's Coercive Statecraft: How Beijing Uses Digital Surveillance, Data Flows, and Economic Tools to Control the Narrative. Atlantic Council, Washington, D.C., 20 mar.** 2024. Disponível em: https://www.atlanticcouncil.org/in-depth-research-reports/report/chinas-coercive-statecraft/.

BOWLING, Shannon; HODGE, Joshua. **The US and China Are Fighting an Information War over the South China Sea. Here's How to Win It. Center for Strategic and International Studies (CSIS), Washington, D.C.**, 20 maio 2024. Disponível em: https://www.csis.org/analysis/us-and-china-are-fighting-information-war-over-south-china-sea-heres-how-win-it.

DORAN, Michael; GULLEY, Chris. **The New Information War in the Middle East: Cyber, Cognitive, and Cross-Platform Conflict. Middle East Institute (MEI), Washington, D.C.**, 2023. Disponível em: https://www.mei.edu/publications/new-information-war-middle-east-cyber-cognitive-and-cross-platform-conflict.

INSTITUTE FOR SECURITY AND TECHNOLOGY (IST). Trends in the Use of Advanced Technology by Extremist and Criminal Organizations. [S.l.]: IST, 2024. Disponível em: https://www.securityandtechnology.org/report/advanced-technology-trends/.

ESTADOS UNIDOS. **Department of Defense. DOD's Strategy on Enhancing Resilience in the Defense Industrial Base Through Artificial Intelligence. Washington, D.C.: U.S. Department of Defense**, 2024. Disponível em: https://media.defense.gov/2024/Mar/26/2003417757/-1/-1/1/DODS-STRATEGY-ON-ENHANCING-RESILIENCE-IN-THE-DEFENSE-INDUSTRIAL-BASE-THROUGH-ARTIFICIAL-INTELLIGENCE.PDF.

SILVA, João P. **A Centralização do Comando no Ciberespaço: Proposta de Estrutura Conjunta para as Operações de Informação no Brasil**. 2024.

PEREIRA, Carlos A.; SANTOS, Renato B. **Ciberguerra e soberania digital: a expansão das capacidades do CDCiber frente ao cenário global de OpInfo. Revista Brasileira de Estudos de Defesa, v. 10, n. 3, p. 115-135**, 2023. Disponível em: https://journal.scientificsociety.net/index.php/sobre/jornal-academico.

SANTOS, Lucas V.; OLIVEIRA, Maria A.. **A Guerra Cognitiva e o Elemento Humano: a necessidade de análise comportamental na Defesa Nacional. Revista da Escola Superior de Guerra, v. 39, n. 1, p. 77-98**, 2024. Disponível em: https://www-science-org.ez129.periodicos.capes.gov.br/.

MACHADO, Roberto; FERREIRA, Ana L. **O Desafio da Capacitação: Formando Especialistas em Operações de Informação para a Defesa Brasileira. Cadernos de Defesa Nacional, [Local da Revista], v. 22, n. 3, p. 45-65**, 2024. Disponível em: https://revista.esg.br/.

NORTH ATLANTIC TREATY ORGANIZATION (NATO). RESEARCH AND TECHNOLOGY ORGANISATION (RTO). **Information Operations: Analysis Support and Capability Requirements: Final Report of RTO Task Group SAS-057.** [S.l.]: NATO, 2006.