ESCOLA DE GUERRA NAVAL

CC (AFN) ARISTOTELES DE SÁ LEITÃO COSTA

GUERRA HÍBRIDA:
análise das características, impactos e estratégias de defesa no contexto contemporâneo

Rio de Janeiro

2024

CC (AFN) ARISTOTELES DE SÁ LEITÃO COSTA

GUERRA HÍBRIDA:
análise das características, impactos e estratégias de defesa no contexto contemporâneo

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

Orientador: CF Moreno de Queiroz Figueiredo

Rio de Janeiro
Escola de Guerra Naval
2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

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

Declaro também que tenho ciência de que a utilização de ideias ou palavras de autoria de outrem, sem a devida identificação da fonte, e o uso de recursos de inteligência artificial no processo de escrita constituem grave falta ética, moral, legal e disciplinar.

Ademais, assumo o compromisso de que este trabalho possa, a qualquer tempo, ser analisado para verificação de sua originalidade e ineditismo, por meio de ferramentas de detecção de similaridades ou por profissionais qualificados.

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

Assinatura digital gov.br

gov.br
Documento assinado digitalmente
ARISTOTELES DE SA LEITAO COSTA
Data: 09/11/2024 11:55:55-0300
Verifique em https://validar.iti.gov.br

DEDICATÓRIA

Dedico este projeto a todos os professores que me influenciaram na minha trajetória. Em especial ao meu orientador, com quem compartilhei minhas dúvidas e angústias a respeito do tema.

AGRADECIMENTOS

Agradeço a todos que contribuíram para a conclusão desse trabalho acadêmico.

À minha esposa, Maria, e minha filha, Juliana pelo apoio incondicional.

Aos meus Amigos e companheiros de trabalho do CPesFN pela compreensão e apoio nos momentos de ausência mesmo presente.

Por fim, agradeço a Escola de Guerra Naval, seus oficiais e praças, por me proporcionarem todo apoio necessário no crescimento profissional e intelectual.

Gratidão

A guerra é mais do que um verdadeiro camaleão que se adapta ligeiramente às características do caso dado.

Clausewitz, 1832, Da Guerra, I, 1, p. 101.

RESUMO

Este estudo analisa o conceito de guerra híbrida, destacando sua evolução histórica, características principais e os desafios que apresenta para a segurança nacional e global. A guerra híbrida combina táticas convencionais e não convencionais, como operações cibernéticas, propaganda, desinformação, forças irregulares e guerra econômica, para alcançar objetivos estratégicos complexos. A pesquisa discute os impactos significativos dessa forma de conflito nas infraestruturas críticas, na economia e na confiança pública, além de suas implicações para a sociedade, como a polarização social e o deslocamento populacional. Também são exploradas as respostas e contramedidas necessárias para mitigar essas ameaças, incluindo o desenvolvimento de capacidades cibernéticas, a promoção da conscientização pública e a cooperação internacional. A análise destaca a importância de uma abordagem integrada e adaptativa para enfrentar as ameaças híbridas, enfatizando a necessidade de constante adaptação das estratégias de defesa às mudanças tecnológicas e geopolíticas. Este trabalho contribui para a construção de conhecimentos no campo militar, oferecendo uma base sólida para futuros estudos e propondo estratégias eficazes de defesa nacional.

Palavras-chave: Guerra híbrida. Segurança nacional. Operações cibernéticas. Propaganda. Forças irregulares. Guerra economics.

ABSTRACT

Hybrid Warfare: analysis of characteristics, impacts and defense strategies in the contemporary context

This study analyzes the concept of hybrid warfare, highlighting its historical evolution, main characteristics, and the challenges it presents to national and global security. Hybrid warfare combines conventional and unconventional tactics, such as cyber operations, propaganda, disinformation, irregular forces, and economic warfare, to achieve complex strategic objectives. The research discusses the significant impacts of this form of conflict on critical infrastructures, the economy, and public trust, as well as its implications for society, such as social polarization and population displacement. The necessary responses and countermeasures to mitigate these threats are also explored, including the development of cyber capabilities, the promotion of public awareness, and international cooperation. The analysis underscores the importance of an integrated and adaptive approach to addressing hybrid threats, emphasizing the need for continuous adaptation of defense strategies to technological and geopolitical changes. This work contributes to the body of knowledge in the military field, providing a solid foundation for future studies and proposing effective national defense strategies.

Keywords: Hybrid warfare. National security. Cyber operations. Propaganda. Irregular forces. Economic warfare.

LISTA DE ABREVIATURAS E SIGLAS

AGCiber	-	Ações de Guerra Cibernética
DdoS	-	*Distributed Denial of Service*
Eciber	-	Espaço Cibernético
IA	-	Inteligência artificial
IBM	-	*International Business Machines Corporation*
IDS	-	*Intrusion Detection System*
IPS	-	*IPS Intrusion Prevention System*
MB	-	Marinha do Brasil
MCDC (CHW)	-	*Multinacional Capability Development Campaign Countering Hybrid Warfare*
OpCiber	-	Operações Cibernéticas
QDR	-	*Quadrennial Defense Review*
TEPT	-	Transtorno de estresse pós-traumático
TOR	-	*The Onion Router*
VPN	-	*Virtual Private Networks*
4GW	-	Guerra de quarta geração

SUMÁRIO

1 INTRODUÇÃO

O fim da Guerra Fria em 1991 reconfigurou a geopolítica global, com o colapso da União Soviética e o surgimento de novos Estados, resultando na reavaliação das alianças internacionais. Essa transformação alterou a forma dos conflitos, com um aumento de guerras civis e conflitos internos, por vezes envolvendo grupos não estatais, como insurgentes e milícias, em vez de confrontos diretos entre Estados, tornando os conflitos modernos complexos e desafiadores. Aliado a isso, o avanço tecnológico, especialmente nas áreas de comunicação, tecnologia da informação e inteligência artificial (IA), vem transformando a forma como as guerras são conduzidas e como as informações são disseminadas. Nesse cenário, surge o conceito de guerra híbrida caracterizado pela fusão de táticas convencionais e não convencionais, em que atores estatais e não estatais utilizam uma combinação de meios militares e não militares para alcançar objetivos estratégicos.

Essa forma de conflito representa um desafio significativo para as forças de segurança, exigindo a adaptação de estratégias para enfrentar novas ameaças. A dificuldade em detectar e combater essas ameaças, somada à evolução tecnológica e geopolítica, requer uma compreensão aprofundada e uma abordagem integrada para garantir a segurança nacional.

No contexto deste trabalho, a análise da guerra híbrida será focada em suas implicações para a segurança nacional, com ênfase no contexto marítimo. De forma geral, a guerra híbrida afeta várias dimensões da segurança, mas tem relevância particular para forças navais, que enfrentam ameaças múltiplas no mar e em zonas costeiras. Este estudo abordará como as forças de defesa podem adotar estratégias gerais para enfrentar operações cibernéticas, propaganda, desinformação, forças irregulares e guerra econômica. A ênfase será na identificação de vulnerabilidades e na proposição de contramedidas eficazes para fortalecer a defesa marítima e a segurança nacional em um cenário global cada vez mais complexo e interconectado.

Diante da crescente complexidade dos conflitos modernos, a guerra híbrida emerge como uma forma de guerra que desafia as noções tradicionais de combate, combinando operações cibernéticas, propaganda, desinformação, forças irregulares e guerra econômica para atingir objetivos estratégicos. A capacidade de atores estatais e não estatais de integrar essas táticas cria um ambiente de conflito altamente dinâmico e imprevisível, exigindo respostas adaptativas e inovadoras das forças de

defesa. As ameaças da guerra híbrida não se limitam a confrontos convencionais no mar, mas também incluem operações cibernéticas que podem comprometer infraestruturas críticas, campanhas de desinformação que minam a confiança pública, e a atuação de forças irregulares em zonas costeiras e marítimas. Portanto, é essencial compreender como essas ameaças se manifestam e identificar estratégias eficazes para mitigá-las no contexto da defesa marítima.

Com base nisso, o problema de pesquisa que este estudo busca responder é: de que forma a guerra híbrida representa uma ameaça significativa para a segurança nacional e como estratégias gerais podem ser adotadas para mitigar essas ameaças no contexto da defesa marítima? Essa questão orienta a análise das características, impactos e implicações da guerra híbrida, além de propor respostas e contramedidas que podem contribuir para o fortalecimento da defesa nacional, sem entrar em detalhes específicos sobre a adaptação de estratégias da Marinha do Brasil (MB).

O principal objetivo deste trabalho é analisar o conceito de guerra híbrida, suas características, impactos e implicações, bem como as respostas e contramedidas necessárias para mitigar suas ameaças. Para isso, busca-se conceituar a guerra híbrida, destacando sua evolução histórica e principais características. Além disso, o estudo visa analisar as ferramentas utilizadas na guerra híbrida, incluindo operações cibernéticas, propaganda e desinformação, forças irregulares e guerra econômica. Outro objetivo é examinar os impactos da guerra híbrida na segurança nacional, com foco nas ameaças às infraestruturas críticas, desestabilização econômica e erosão da confiança pública. Este trabalho também explora as implicações da guerra híbrida para a sociedade, como a polarização social, o impacto psicológico e o deslocamento populacional. Finalmente, o estudo procura identificar e avaliar as respostas e contramedidas necessárias para enfrentar as ameaças híbridas, propondo estratégias gerais de adaptação às novas formas de conflito no contexto da segurança nacional e marítima

A guerra híbrida é um tema de extrema relevância no cenário atual devido à sua complexidade e ao impacto que pode ter na segurança nacional e global. A escolha deste tema foi motivada pela necessidade de entender como a combinação de táticas convencionais e não convencionais, incluindo operações cibernéticas, propaganda, desinformação, forças irregulares e guerra econômica, pode ser utilizada para alcançar objetivos estratégicos complexos. Esse tipo de conflito não apenas desafia as concepções tradicionais de guerra, mas também representa um desafio

significativo para as forças de segurança, exigindo novas abordagens e estratégias.

Compreender a guerra híbrida é primordial para a sociedade e para as forças de defesa, pois a crescente sofisticação das táticas utilizadas torna a detecção e o combate dessas ameaças extremamente difíceis. A importância deste estudo reside na capacidade de desenvolver estratégias eficazes de defesa que possam proteger infraestruturas críticas, garantir a estabilidade econômica e manter a confiança pública. A relevância para a comunidade científica é igualmente significativa, pois contribui para o avanço do conhecimento sobre formas modernas de conflito e suas implicações. Assim, justifica-se a necessidade de uma análise sobre a guerra híbrida para garantir a segurança nacional em um cenário global cada vez mais complexo e interconectado.

A abordagem metodológica utilizada nesta pesquisa é a revisão bibliográfica, que permite uma compreensão do conceito de guerra híbrida e a identificação dos principais desafios e implicações deste tipo de conflito. A coleta de dados foi realizada por meio da análise de diversos documentos e estudos acadêmicos relevantes, incluindo as obras de Hoffman (2007), Reichborn-Kjennerud e Cullen (2016), Yan (2020) e Thiele (2021).

Além da análise bibliográfica, a pesquisa beneficiou-se da análise de casos históricos e contemporâneos para ilustrar as táticas e estratégias empregadas na guerra híbrida. Esses casos proporcionaram exemplos práticos e concretos de como os conceitos teóricos são aplicados na prática, enriquecendo a compreensão do fenômeno. Para isso, foram analisados os estudos de caso descritos no *Multinational Capability Development Campaign (MCDC(CHW) Project*[1] .Em resumo, a metodologia adotada nesta pesquisa combinou uma revisão bibliográfica abrangente e uma análise qualitativa detalhada, proporcionando uma base para explorar o conceito de guerra híbrida, suas características, impactos e implicações, bem como as respostas e contramedidas necessárias para mitigar suas ameaças.

O trabalho está estruturado em quatro capítulos que analisam o conceito de guerra híbrida, seus impactos e as estratégias de defesa.

O Capítulo 2, denominado “Fundamentação Teórica”, apresenta a definição de

[1]Campanha de Desenvolvimento de Capacidades Multinacionais (tradução nossa). Projeto de Combate à Guerra Híbrida é uma iniciativa colaborativa que reúne várias nações e organizações internacionais com o objetivo de desenvolver e aprimorar capacidades de defesa e segurança em um contexto multinacional.

guerra híbrida, destacando sua evolução histórica e principais características. Este capítulo também analisa as ferramentas empregadas na guerra híbrida, incluindo operações cibernéticas, propaganda e desinformação, forças irregulares e guerra econômica. A fundamentação teórica fornece uma base para compreender as dinâmicas complexas desse tipo de conflito, destacando as estratégias e táticas empregadas pelos atores híbridos e como estas desafiam as concepções tradicionais de guerra.

No Capítulo 3, intitulado “Impactos e Implicações da Guerra Híbrida”, são explorados os impactos desse tipo de conflito na segurança nacional e suas implicações para a sociedade. Este capítulo discute como a guerra híbrida afeta infraestruturas críticas, desestabiliza a economia e mina a confiança pública. Além disso, são analisadas as consequências sociais, como a polarização, o impacto psicológico e o deslocamento populacional, ressaltando os desafios que esses impactos representam para a estabilidade e coesão social.

O Capítulo 4, “Desafios e Perspectivas Futuras”, examina os principais desafios na identificação e combate à guerra híbrida, bem como as tendências futuras deste tipo de conflito. Esta seção aborda as dificuldades na detecção e atribuição de ataques híbridos, a resiliência das forças irregulares e as inovações tecnológicas que estão moldando o futuro da guerra híbrida. Também é discutida a necessidade de adaptação contínua das estratégias de defesa para enfrentar essas ameaças emergentes, enfatizando a importância de uma abordagem proativa e inovadora.

A conclusão resume os principais pontos discutidos ao longo do estudo, refletindo sobre as implicações práticas das descobertas para o contexto da guerra híbrida e a segurança nacional. Embora o trabalho não explore detalhadamente áreas de pesquisa futura, ele enfatiza a necessidade de adaptação contínua às novas ameaças e sublinha a importância de uma abordagem integrada e flexível para enfrentar os desafios emergentes, reforçando o compromisso com a proteção da soberania e segurança global.

2 FUNDAMENTAÇÃO TEÓRICA

A guerra híbrida é um conceito que tem ganhado crescente atenção no estudo dos conflitos contemporâneos, especialmente devido à sua complexidade e capacidade de integrar múltiplos modos de guerra. Este capítulo tem como objetivo

fornecer uma base teórica sobre a guerra híbrida, abordando seu histórico, conceito, e as ferramentas que a constituem. Estabelecer uma compreensão clara da guerra híbrida é essencial para analisar as dinâmicas modernas de conflito e desenvolver estratégias adequadas e eficazes de defesa.

A análise histórica nos mostra que o conceito de guerra híbrida emergiu como resposta às transformações nas dinâmicas de conflito e nas táticas de combate do século 21, refletindo a complexidade dos conflitos modernos e a necessidade de revisar doutrinas militares tradicionais. Conflitos como a guerra no Iraque e o confronto entre Israel e Hezbollah em 2006 evidenciaram a combinação de táticas convencionais e irregulares, desafiando as categorias tradicionais de guerra. O avanço tecnológico permitiu que atores não estatais e estados menores adotassem táticas sofisticadas, enquanto mudanças geopolíticas, como a desestabilização de Estados e o surgimento de grupos terroristas, tornaram as fronteiras entre guerra, crime e política mais nebulosas, exigindo uma abordagem integrada.

As ferramentas empregadas na guerra híbrida são diversas e se interligam para produzirem efeitos sinérgicos. Operações cibernéticas, propaganda e desinformação, forças irregulares e guerra econômica são instrumentos essenciais que, quando combinados, criam um cenário de conflito altamente dinâmico e imprevisível. Cada um desses instrumentos será explorado detalhadamente ao longo do capítulo, destacando como contribuem para a complexidade da guerra híbrida e os desafios que representam para as forças de segurança.

2.1 HISTÓRICO DE GUERRA HÍBRIDA

A evolução do conceito de guerra híbrida é marcada por uma adaptação às novas realidades geopolíticas e tecnológicas, refletindo as mudanças na natureza dos conflitos ao longo das últimas décadas. Este subcapítulo apresenta uma revisão histórica do desenvolvimento da guerra híbrida, desde seus primeiros sinais até suas formas mais contemporâneas. Compreender essa evolução é essencial para analisar as dinâmicas modernas de conflito e desenvolver estratégias eficazes de defesa.

Para Solmaz (2022), o conceito de guerra híbrida é caracterizado como uma noção em contínua evolução e ampliação, que reflete a complexidade e a variedade das formas de conflito atuais. Segundo o autor, o conceito de guerra híbrida tem sido expandido e ajustado ao longo do tempo, muitas vezes incorporando novos elementos

e fenômenos que não faziam parte das definições iniciais.

A guerra híbrida emergiu como um conceito significativo nas discussões de segurança global após os ataques de 11 de setembro de 2001, que destacaram a complexidade e a natureza diversa dos conflitos contemporâneos. Este evento marcou o fim de uma era de guerra convencional e o início de um novo paradigma, onde a distinção entre guerra, terrorismo, crime organizado e violência política tornou-se cada vez mais tênue. Hoffman (2007), observa que essa transição foi fundamental para a compreensão da guerra híbrida como uma forma de conflito que integra múltiplos modos de guerra para alcançar objetivos estratégicos.

O conceito de guerra de quarta geração (4GW) introduzido nos anos 1980 e 1990 ajudou a moldar a compreensão inicial das guerras híbridas. A 4GW enfatiza a difusão dos conflitos, onde as linhas entre guerra e paz, e entre combatentes e civis, são borradas. Essa teoria reconhece que o enfraquecimento do Estado como um mecanismo organizador leva ao surgimento de atores não estatais capazes de desafiar a legitimidade do Estado através de meios convencionais e não convencionais, como o terrorismo e a guerra de informação. Hoffman (2007) aponta que essa forma de guerra representa uma evolução significativa na maneira como os conflitos são conduzidos, desafiando as estruturas tradicionais de segurança e defesa.

Em seguida, nos anos 1990 e início dos anos 2000, surgiram várias teorias que exploravam a complexidade crescente dos conflitos. As guerras não-trinitárias e as guerras compostas são exemplos de conceitos que destacam a diversidade de atores e táticas envolvidas nos conflitos modernos. Essas teorias ajudaram a expandir a compreensão sobre como as guerras híbridas combinam elementos convencionais e irregulares para atingir objetivos estratégicos.

Nesse contexto, os conflitos no Iraque e no Afeganistão, bem como as operações militares em locais como Kosovo e Chechênia, forneceram exemplos de aplicação de táticas híbridas. Nessas regiões, as forças insurgentes utilizaram táticas de guerrilha, terrorismo, e operações cibernéticas para combater forças convencionais superiores. O uso de táticas de enxame[2] e combate urbano, por exemplo, demonstrou a eficácia das estratégias híbridas em ambientes complexos e densamente povoados. Esses exemplos ilustram a aplicação das teorias de guerra híbrida e sua relevância no cenário contemporâneo de segurança.

[2]Abordagem de combate ou de operações militares que se inspira no comportamento coletivo de grupos, como enxames de insetos (por exemplo, abelhas ou gafanhotos)

A globalização e o avanço das tecnologias de informação e comunicação desempenharam um papel fundamental na evolução das guerras híbridas. Esses fatores permitiram que atores estatais e não estatais explorassem vulnerabilidades em sociedades modernas de maneira mais eficaz, utilizando a internet para propaganda, recrutamento e coordenação de ataques. A capacidade de realizar operações cibernéticas e de desinformação tornou-se uma característica definidora dos conflitos híbridos, ampliando o alcance e a sofisticação das ameaças.

A resposta das forças militares e de segurança às ameaças híbridas evoluiu significativamente ao longo dos anos. O *Quadrennial Defense Review*[3] (QDR) de 2006, por exemplo, reconheceu a importância crescente dos desafios irregulares e destacou a necessidade de uma abordagem mais adaptativa e flexível para enfrentar esses conflitos. A evolução das estratégias de defesa para incluir uma gama mais ampla de ameaças e desafios expressa a resposta proativa às mudanças no ambiente de segurança global, demonstrando a necessidade de uma contínua adaptação das forças de segurança para lidar com o dinamismo e o hibridismo da guerra moderna.

Desde que foi popularizado por Hoffman (2007) em sua monografia *Conflict in the 21 Century: The Rise of Hybrid Wars*, o conceito de guerra híbrida passou por várias reformulações. Inicialmente, a Guerra Híbrida foi utilizada para descrever a complexidade e a sofisticação das táticas empregadas por atores não estatais, como grupos insurgentes ou terroristas. Exemplos incluem Hezbollah em conflitos no Oriente Médio, em que esses grupos combinavam táticas convencionais e não convencionais, como guerrilha, terrorismo e propaganda. Com o tempo, especialmente após eventos como a anexação da Crimeia pela Rússia em 2014, o foco do conceito de guerra híbrida começou a mudar. Em vez de se concentrar apenas em atores não estatais, a discussão se expandiu para incluir governos que utilizam táticas híbridas. A Rússia, em particular, se tornou um exemplo proeminente de como um estado pode empregar uma combinação de força militar, operações de informação, ciberataques e outras formas de coerção para alcançar seus objetivos políticos.

Além disso, o uso do conceito tem se estendido para descrever uma variedade de ações que vão além do campo de batalha tradicional, envolvendo meios militares e não militares como ciberataques, forças irregulares, campanhas de desinformação,

[3]Revisão Quadrienal de Defesa de 2006 é um documento estratégico elaborado pelo Departamento de Defesa dos EUA que avalia as ameaças à segurança nacional e estabelece diretrizes para a política de defesa do país.

manipulação política e coerção econômica, refletindo uma mudança na forma como os conflitos são conduzidos na era moderna, em que as linhas entre guerra e paz, militar e não militar, tornam-se cada vez mais borradas.

Assim, a história da guerra híbrida é marcada pela contínua adaptação às mudanças tecnológicas e geopolíticas. Desde a introdução da teoria da guerra de quarta geração até os conflitos contemporâneos no Oriente Médio, o conceito de guerra híbrida tem evoluído para refletir a complexidade e a heterogeneidade dos conflitos modernos. As forças militares e de segurança continuam a desenvolver novas estratégias e capacidades para enfrentar essas ameaças, ressaltando a importância de uma abordagem integrada e adaptativa para a segurança global.

2.2 CONCEITO DE GUERRA HÍBRIDA

Nesta seção, realizaremos uma análise das diferentes versões conceituais de guerra híbrida na literatura, que constantemente apresentam diferenças significativas e, por isso, contribuem para a ambiguidade e complexidade desse conceito.

Mormente a análise do conceito de guerra híbrida, partiremos da definição de ameaças híbridas publicada pela MB:

> Emprego sob medida, por ator oponente, de múltiplos instrumentos, militares ou não, como operações psicológicas, ataques cibernéticos, pirataria, ações terroristas, propaganda, contrapropaganda, desinformação, ações econômicas, crimes ambientais, interferências nas comunicações, ações de forças regulares e irregulares contra infraestruturas críticas, ataques nucleares, biológicos, químicos ou radiológicos, bem como outras atividades criminosas ou subversivas de naturezas diversas, combinando ações simétricas e assimétricas, com seu efeito sinérgico, podendo atuar em ambientes físicos ou não, particularmente o informacional, direcionados a vulnerabilidades específicas do alvo, visando a atingir os efeitos desejados pelo agressor e, normalmente, a partir de desestabilização, medo e incerteza gerados na sociedade como um todo ou em parte dela. (Brasil, 2020, p. 1)

Sob tal ótica, as ameaças híbridas referem-se ao uso estratégico de diversos instrumentos, militares e não militares, por um ator oponente, visando explorar vulnerabilidades específicas do alvo e gerar desestabilização, medo e incerteza na sociedade, por meio de ações simétricas e assimétricas.

Estudiosos como Hoffman (2007), Reichborn-Kjennerud e Cullen (2016), Yan (2020) e Thiele (2021) contribuíram para a definição e compreensão do conceito de guerra híbrida.

Em primeira análise, a guerra híbrida é um conceito que descreve um tipo de conflito que combina múltiplos modos de guerra para atingir objetivos estratégicos complexos. Incorpora elementos de guerra convencional, guerra irregular, terrorismo e crime organizado, tornando-se uma forma de conflito altamente complexa e interconectada (Hoffman, 2007).

Segundo Hoffman (2007), a guerra híbrida se caracteriza pela ausência de distinção clara entre soldados e civis, e entre violência organizada, terror, crime e guerra. Este tipo de conflito desafia as concepções tradicionais de guerra e representa um desafio significativo para as forças de segurança convencionais. A guerra híbrida visa explorar as vulnerabilidades das sociedades modernas através da combinação de diferentes táticas e estratégias, buscando desestabilizar o adversário de maneira eficaz e imprevisível. Essa falta de distinção clara entre combatentes e não combatentes, bem como entre diferentes tipos de violência, é um dos aspectos mais preocupantes da guerra híbrida. Como Hoffman (2007) aponta, essa característica torna a detecção e a resposta muito mais complicadas para as forças de segurança.

A transição dos conflitos interestatais tradicionais para as guerras híbridas demonstra uma adaptação às novas realidades geopolíticas e tecnológicas. A globalização e o avanço das tecnologias de informação e comunicação permitiram que atores estatais e não estatais explorassem vulnerabilidades em sociedades modernas de maneira mais eficaz. Como mencionado por Hoffman (2007), o paradigma emergente de conflito é exemplificado por indivíduos como Osama Bin Laden e pelos eventos no Afeganistão e no Iraque[4].

De acordo Reichborn-Kjennerud e Cullen (2016), a guerra híbrida é um conceito que envolve o uso sincronizado de diversos instrumentos de poder — militar, político, econômico, civil e informacional — adaptados às vulnerabilidades específicas de um alvo. Essa abordagem permite que atores estatais e não estatais combinem meios militares e não militares tais como forças irregulares, operações cibernéticas, propaganda e desinformação, além do uso de guerra econômica, entre outras estratégias para explorar fraquezas do adversário, na qual a diversidade de elementos torna a guerra híbrida difícil de combater, pois cada componente pode ser empregado

[4]Intervenções militares dos EUA no Afeganistão e no Iraque exemplificam as dificuldades enfrentadas pelas forças convencionais ao lidar com adversários irregulares. Essas experiências mostraram que a superioridade militar tradicional não é suficiente para garantir a segurança ou a estabilidade em contextos onde a insurgência e o terrorismo estão presentes.

de maneira coordenada para alcançar efeitos sinérgicos no campo de batalha. A integração dessas capacidades permite aos atores híbridos maximizar seu impacto e criar um ambiente de conflito altamente dinâmico e imprevisível.

Na visão de Yan (2020), a guerra híbrida combina diferentes formas de luta, utilizando uma mistura de tecnologias novas e estilos de combate, tanto por atores estatais quanto não estatais, sendo caracterizada por operações que buscam alcançar objetivos políticos sem desencadear uma resposta militar convencional, muitas vezes operando abaixo do limiar da guerra.

Para Thiele, (2021) a guerra híbrida é uma manifestação criativa de poder que integra uma vasta gama de instrumentos, tanto militares quanto não militares, e diferentes vetores de influência, atuando em um amplo espaço de batalha que abrange múltiplos domínios. Ela opera de maneira ambígua nas zonas cinzentas de interfaces complexas, especialmente nas transições entre guerra e paz, amigo e inimigo, e nas esferas de segurança interna e externa. O objetivo principal é alcançar uma decisão favorável em um confronto, focando em centros de gravidade[5] que não são exclusivamente militares, enquanto evita ser derrotada militarmente ou forçada a agir pelo adversário.

Portanto, fica claro que a ênfase de Hoffman (2007) está na incorporação de vários “modos de guerra” por atores estatais e não estatais, sendo a característica saliente a combinação de capacidades convencionais com táticas irregulares e até atos de terrorismo. Já Reichborn-Kjennerud e Cullen (2016), sublinham a combinação de meios militares e não militares, que são empregados de forma coordenada e sincronizada para criar efeitos sinérgicos, enquanto Yan (2020) destaca o uso de tecnologias disruptivas como IA, que podem surpreender o adversário e mudar a dinâmica do conflito. Thiele (2021), por sua vez, ressalta a ampliação do campo de batalha, utilizando uma variedade de domínios e dimensões, como política, diplomacia, informação, economia, tecnologia, e sociedade, focando em centros de gravidade não militares.

A análise dos conceitos apresentados por Hoffman (2007), Reichborn-Kjennerud e Cullen (2016), Yan (2020) e Thiele (2021) revela uma compreensão abrangente da guerra híbrida, que se caracteriza pela fusão de diferentes modos de combate e pela utilização de uma ampla gama de recursos. A guerra híbrida não se

[5]Conceito estratégico que se refere a pontos ou elementos críticos que, se afetados, podem influenciar significativamente o resultado de um conflito ou operação.

limita a confrontos convencionais, mas integra táticas irregulares, atos de terrorismo e a combinação de meios militares e não militares de forma coordenada para maximizar a eficácia. A introdução de tecnologias disruptivas, como a IA, acrescenta uma nova dimensão ao conflito, permitindo surpresas estratégicas e mudanças na dinâmica das operações. Além disso, a ampliação do campo de batalha para incluir domínios como política, diplomacia, informação, economia, tecnologia, e sociedade destaca a complexidade e o dinamismo da guerra moderna.

2.3 FERRAMENTAS DA GUERRA HÍBRIDA

A guerra híbrida visa explorar as vulnerabilidades dos adversários de maneira coordenada e eficaz, empregando uma combinação de operações cibernéticas, propaganda e desinformação, forças irregulares e guerra econômica. Este subcapítulo apresentará uma análise detalhada das principais ferramentas utilizadas na guerra híbrida.

CHIVVIS (2017), relaciona campanhas de propaganda e desinformação, operações cibernéticas, influência econômica, ações clandestinas como ferramentas de guerra híbrida empregadas pela Rússia. Essas ferramentas são utilizadas de forma coordenada para criar um ambiente de instabilidade e incerteza, permitindo que a Rússia alcance seus objetivos estratégicos sem recorrer a uma guerra convencional aberta.

Yan (2020) enfatiza que a guerra híbrida busca explorar as fragilidades das sociedades contemporâneas, empregando táticas que vão desde ataques cibernéticos avançados até operações psicológicas e ações paramilitares. A coordenação dessas atividades é essencial para criar efeitos sinérgicos, em que as ações combinadas produzem impactos mais significativos do que cada elemento isoladamente. Esse enfoque multidimensional permite que os atores da guerra híbrida desestabilizem e enfraqueçam seus adversários de maneira eficaz, ao mesmo tempo em que evitam a confrontação direta com forças convencionais superiores.

2.3.1 Operações Cibernéticas

Os avanços significativos na tecnologia da informação têm transformado a configuração da guerra híbrida, especialmente com a crescente utilização de ataques

cibernéticos.

As operações cibernéticas são um componente essencial da guerra híbrida, permitindo que os atores realizem ataques que podem desestabilizar infraestruturas críticas, roubar informações sensíveis, e espalhar desinformação. Essas operações são caracterizadas pela utilização de tecnologias da informação para realizar ataques direcionados que podem ter efeitos devastadores sem a necessidade de confronto físico. Exemplos incluem ataques a redes elétricas, sistemas financeiros, e redes de comunicação. Brasil (2021, p. B-8), descreve infraestruturas críticas como: “instalações, serviços, bens e sistemas que, se tiverem seu desempenho degradado, ou se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional ou à segurança do Estado e da sociedade”. No Brasil, os setores considerados críticos incluem: energético, telecomunicações, nuclear, financeiro, transportes e águas (Brasil, 2021).

Para Thiele (2021), os ataques cibernéticos, quando combinados com tecnologias emergentes e disruptivas, como IA e sistemas autônomos, conferem à guerra híbrida uma nova dimensão.

Segundo Yan (2020), as operações cibernéticas são ações coordenadas que utilizam redes de computadores e a internet para atingir objetivos estratégicos e táticos. Estas operações podem incluir ataques de negação de serviço[6] (DDoS), invasões para roubo de dados, inserção de *malware*[7] e campanhas de desinformação através de plataformas digitais. A importância das operações cibernéticas na guerra híbrida encontra-se na sua capacidade de atingir alvos críticos com precisão e causar danos desproporcionais aos recursos investidos.

Essa capacidade de realizar ataques precisos sem a necessidade de confronto físico direto torna as operações cibernéticas uma ferramenta poderosa na guerra híbrida. No entanto, a complexidade técnica envolvida na execução desses ataques requer habilidades e recursos avançados. A defesa contra operações cibernéticas exige investimentos significativos em cibersegurança, incluindo a proteção de sistemas críticos, a educação e treinamento de pessoal, e a criação de políticas e procedimentos de resposta a incidentes.

---

[6]A negação de serviço distribuída (DDoS, do inglês *Distributed Denial of Service*) é um tipo de ataque cibernético que visa tornar um serviço, servidor ou rede indisponível para os usuários legítimos.

[7]Abreviação de *malicious software* (software malicioso), refere-se a qualquer tipo de software projetado para causar danos, explorar ou comprometer sistemas, redes ou dispositivos.

De acordo com Brasil (2021), as operações Cibernéticas (OpCiber)[8] envolvem a utilização da capacidade cibernética, com o objetivo principal de alcançar metas no ou por meio do Espaço Cibernético (ECiber). Essas operações se combinam com outras capacidades para garantir e sustentar uma vantagem operacional, além de colocar as forças adversárias em desvantagem.

A MB desempenha papel fundamental nas operações cibernéticas, protegendo seus sistemas e atacando os do inimigo por meio de OpCiber e Ações de Guerra Cibernética[9] (AGCiber) (Brasil, 2021). Dado que o espaço de batalha no ECiber abrange múltiplos domínios, a MB destaca-se como a Força Singular mais apta a operar nesse ambiente operacional. Isso se deve à sua capacidade de realizar operações em diferentes áreas: no domínio terrestre, por meio dos Fuzileiros Navais; no aéreo, com suas unidades Aeronavais; e no marítimo, com suas Forças Navais de superfície e submarinas. A Força possui uma vantagem particular no domínio marítimo, onde opera em um subambiente que outras forças não conseguem alcançar. Portanto, para a MB é fundamental construir capacidades cibernéticas robustas e confiáveis de forma que possa contribuir para segurança e defesa nacional contra AGCiber.

2.3.2 Propaganda e Desinformação

A propaganda e a desinformação são ferramentas centrais da guerra híbrida, empregadas para manipular a percepção pública, desestabilizar governos, e influenciar a opinião pública. Essas táticas envolvem a disseminação de informações falsas ou enganosas por meio de diversos meios de comunicação, incluindo mídias sociais, notícias falsas e campanhas de influência. A eficácia dessas táticas está na sua capacidade de criar confusão, semear desconfiança e polarizar sociedades, tornando-as ferramentas poderosas para alcançar objetivos estratégicos sem a necessidade de confronto físico direto.

De acordo com Yan (2020), a propaganda é definida como a disseminação

[8] Espaço virtual, composto por um conjunto de canais de comunicação da internet e outras redes de comunicação que garantam a interconexão de dispositivos de Tecnologia da Informação e Comunicações e que engloba todas as formas de atividades digitais em rede, incluindo o armazenamento, processamento e compartilhamento de conteúdo, além de todas as ações, humanas ou automatizadas, conduzidas através desse ambiente (Portaria nº 93/GSI/PR/2021).

[9] Envolvem o emprego de ferramentas disponíveis no campo da Tecnologia da Informação e Comunicações para desestabilizar os ativos de informação do inimigo e, também, para possibilitar a proteção dos ativos de informação de interesse (Brasil, 2021, p. B-1).

sistemática de informações, especialmente de natureza tendenciosa ou enganosa, com o objetivo de promover uma causa política ou ponto de vista. A desinformação, por sua vez, refere-se à propagação deliberada de informações falsas para enganar e manipular a audiência. Essas técnicas são utilizadas na guerra híbrida para enfraquecer a moral do adversário, influenciar a opinião pública e criar divisões internas.

Durante as eleições presidenciais dos EUA em 2016, por exemplo, foram identificadas campanhas de desinformação que utilizavam plataformas como *Facebook* e *Twitter* para influenciar eleitores e semear desconfiança no processo eleitoral (MCDC, 2019). A capacidade de influenciar a percepção pública e moldar narrativas pode ser tão poderosa quanto o uso da força física, permitindo que os atores da guerra híbrida alcancem seus objetivos estratégicos de maneira eficaz e furtiva.

Reichborn-Kjennerud e Cullen (2016) destacam que a propaganda e a desinformação são utilizadas em conjunto com outras formas de guerra híbrida, como operações cibernéticas e ações militares, para maximizar seu impacto. Essa coordenação de atividades é essencial para criar efeitos sinérgicos, onde as ações combinadas produzem impactos mais significativos do que cada elemento isoladamente.

2.3.3 Forças Irregulares

As forças irregulares são um componente vital na guerra híbrida, operando de maneira furtiva e adaptável para realizar ataques de guerrilha, sabotagem, e outras ações de baixo nível que podem ter um impacto significativo. Essas forças podem incluir grupos paramilitares, insurgentes, terroristas e outros atores não estatais que utilizam táticas não convencionais para alcançar seus objetivos. Sua capacidade de operar em terrenos complexos e de se misturar com a população civil torna-as difíceis de detectar e neutralizar, representando um desafio significativo para as forças de segurança convencionais.

Forças irregulares são grupos armados que não fazem parte das forças armadas regulares de um Estado e que operam fora das normas e convenções da guerra tradicional. Elas podem ser compostas por milícias, insurgentes, terroristas, mercenários, ou outros grupos que utilizam táticas de guerra não convencionais. De

acordo com Hoffman (2007), as forças irregulares são capazes de explorar as fraquezas dos exércitos convencionais, utilizando táticas de guerrilha e operações assimétricas para alcançar vantagens estratégicas.

Reichborn-Kjennerud e Cullen (2016) observam que a utilização de forças irregulares na guerra híbrida permite que os atores híbridos causem danos significativos sem a necessidade de confronto direto com forças convencionais superiores. A capacidade de se misturar com a população civil e operar em terrenos complexos torna as forças irregulares especialmente eficazes em conflitos híbridos. Essa abordagem tática cria desafios adicionais para as forças de segurança, que devem desenvolver novas estratégias para identificar e neutralizar esses grupos.

2.3.4 Guerra Econômica

A guerra econômica é uma ferramenta da guerra híbrida, empregada para enfraquecer e desestabilizar o adversário através de medidas econômicas e financeiras. Essas medidas podem incluir sanções, bloqueios comerciais, manipulação de mercados financeiros, e outras ações destinadas a causar dano econômico. A guerra econômica complementa outras ferramentas de guerra híbrida, criando pressão adicional sobre o adversário e dificultando sua capacidade de responder efetivamente às ameaças.

A guerra econômica é definida como o uso de ferramentas econômicas e financeiras para atingir objetivos estratégicos. Segundo Yan (2020), a guerra econômica visa minar a estabilidade econômica de um adversário, reduzir sua capacidade de financiar operações militares e enfraquecer seu governo e sociedade. A guerra econômica é importante na guerra híbrida por sua capacidade de causar danos consideráveis sem o uso direto da força militar, tornando-se uma ferramenta poderosa para atores estatais e não estatais.

Reichborn-Kjennerud e Cullen (2017) destacam que as medidas econômicas podem ser implementadas de maneira relativamente rápida e têm o potencial de afetar amplamente a economia e a sociedade do adversário. No entanto, a eficácia das sanções e outras medidas econômicas pode ser limitada se o alvo encontrar maneiras de contornar as restrições. Além disso, a guerra econômica pode levar a retaliações que afetam negativamente a economia do ator que implementa as sanções.

A Rússia tem utilizado sua posição como um grande fornecedor de energia,

especialmente gás natural, para exercer influência sobre países europeus. Um exemplo claro disso ocorreu quando Moscou cortou o fornecimento de gás natural para a Ucrânia durante o inverno de 2006 e 2009. Essas ações foram vistas como tentativas explícitas de coagir a Ucrânia a aceitar condições favoráveis em negociações sobre preços de gás. Interrompendo o fornecimento de um recurso vital, a Rússia buscou pressionar a Ucrânia a alinhar-se com seus interesses (CHIVVIS, 2017).

Dado o exposto, a análise das ferramentas da guerra híbrida revela uma intersecção complexa entre táticas convencionais e não convencionais, criando um ambiente de conflito dinâmico. Operações cibernéticas visam desestabilizar infraestruturas críticas e influenciar a percepção pública, enquanto propaganda e desinformação manipulam narrativas e polarizam sociedades. A utilização de forças irregulares e guerra econômica permitem que atores híbridos explorem vulnerabilidades estatais, minando a segurança nacional de forma sutil.

Essas ferramentas se reforçam mutuamente, criando um ciclo de retroalimentação que potencializa seus efeitos. Por exemplo, a desinformação pode facilitar operações cibernéticas, e a guerra econômica pode justificar intervenções militares. Portanto, a compreensão das ferramentas da guerra híbrida deve considerar suas inter-relações, sendo essencial para o desenvolvimento de estratégias de defesa eficazes.

3 IMPACTOS E IMPLICAÇÕES DA GUERRA HÍBRIDA

A guerra híbrida, com sua combinação de táticas convencionais e não convencionais, tem impactos significativos na segurança nacional, nas sociedades e nas estratégias de defesa dos Estados. A capacidade de atores estatais e não estatais de integrar operações cibernéticas, propaganda, desinformação, forças irregulares e guerra econômica torna este tipo de conflito especialmente desafiador. Este capítulo explora os diversos impactos e implicações da guerra híbrida, destacando como ela afeta a segurança nacional, suas consequências para a sociedade, e as respostas e contramedidas que podem ser implementadas para mitigar suas ameaças.

3.1 IMPACTOS NA SEGURANÇA NACIONAL

Infraestruturas críticas, como redes de comunicação e sistemas financeiros, são frequentemente alvos em operações híbridas, causando interrupções significativas e prejudicando a capacidade de resposta dos estados. Segundo Yan (2020), os ataques cibernéticos contra estas infraestruturas podem causar interrupções significativas e prejudicar a capacidade de um Estado de responder a crises de forma eficaz. Esses ataques são projetados para criar caos, paralisar serviços essenciais e enfraquecer a moral pública. Por exemplo, o ataque cibernético contra a rede elétrica da Ucrânia em 2015, que deixou centenas de milhares de pessoas sem eletricidade, demonstra a vulnerabilidade das infraestruturas críticas a operações cibernéticas (MCDC, 2019). Além disso, forças irregulares podem realizar atos de sabotagem física, como ataques a oleodutos, instalações de energia, ou sistemas de transporte, para interromper serviços essenciais e causar danos econômicos e psicológicos.

A guerra econômica é uma ferramenta poderosa na guerra híbrida, usada para enfraquecer a economia de um adversário e reduzir sua capacidade de financiar operações militares e manter a estabilidade interna. Reichborn-Kjennerud e Cullen (2016) destacam que medidas como sanções, bloqueios comerciais, e manipulação de mercados financeiros podem ter impactos devastadores na economia de um país, prejudicando sua capacidade de operar efetivamente em um ambiente de segurança complexo. Por exemplo, as sanções econômicas podem restringir o acesso de um país a mercados internacionais, tecnologia e capitais, como visto nas sanções impostas à Rússia após a anexação da Crimeia em 2014, que contribuíram para uma recessão econômica significativa (MCDC, 2019). Além disso, bloqueios e embargos podem isolar economicamente um país, como os bloqueios navais impostos durante conflitos para impedir a entrada de suprimentos críticos. A manipulação de mercados financeiros pode causar volatilidade econômica, afetando negativamente os mercados de ações e aumentando os custos de financiamento para o adversário.

A complexidade e diversidade das ameaças da guerra híbrida exige que os Estados desenvolvam respostas adaptativas e integradas para mitigar seus impactos. Yan (2020) destaca que a adaptação das estratégias de defesa é fundamental para enfrentar a guerra híbrida, exigindo uma abordagem que combine capacidades militares tradicionais com novas tecnologias e métodos de combate. Desenvolver capacidades cibernéticas, fortalecer a resiliência econômica, promover a conscientização pública e cooperar internacionalmente são passos essenciais para

mitigar as ameaças representadas pela guerra híbrida.

3.2 IMPLICAÇÕES PARA A SOCIEDADE

As implicações da guerra híbrida para a sociedade são profundas e abrangentes. As táticas empregadas na guerra híbrida não apenas visam capacidades militares e infraestruturas, mas também têm como objetivo influenciar e manipular a opinião pública. Hoffman (2007) argumenta que a guerra híbrida desfoca as linhas entre combatentes e civis, criando um ambiente em que a população civil é eventualmente uma vítima direta ou indireta dos conflitos.

A manipulação da informação por meio de desinformação e propaganda tem o poder de polarizar sociedades e desestabilizar governos, exacerbando tensões internas. Durante as eleições presidenciais dos EUA em 2016, campanhas de desinformação atribuídas a atores estrangeiros foram utilizadas para influenciar eleitores e semear desconfiança no processo eleitoral (MCDC, 2019). Essas campanhas exacerbaram divisões políticas e criaram um ambiente de polarização intensa. Além disso, grupos extremistas utilizam a propaganda para recrutar membros e radicalizar indivíduos, promovendo ideologias divisivas que fragmentam a sociedade. O Estado Islâmico[10], por exemplo, utilizou propaganda sofisticada para atrair jovens de diversas partes do mundo, incitando violência e polarização.

Dada a complexidade e a gravidade das implicações da guerra híbrida para a sociedade, é essencial que os Estados desenvolvam estratégias abrangentes para mitigar seus impactos e fortalecer a resiliência social. Yan (2020) enfatiza a importância de uma abordagem integrada que combine medidas de segurança com esforços de educação e conscientização pública.

Nesse sentido, para mitigar os impactos da desinformação, é essencial promover a alfabetização midiática e campanhas de conscientização. Como afirma Barbosa (2020), promover a educação midiática e digital, além de aumentar a conscientização sobre a desinformação, capacitará as pessoas a avaliarem as informações de forma crítica. A educação sobre como verificar a veracidade das informações e entender as táticas de manipulação pode reduzir a eficácia das campanhas de desinformação. Dessa forma, para mitigar esses impactos é preciso

[10]Grupo jihadista extremista que ganhou notoriedade mundial a partir de 2014, quando proclamou um califado em partes do Iraque e da Síria.

promover iniciativas que fortaleçam a coesão social e reduzam as divisões dentro da sociedade. Além disso, programas de diálogo intercomunitário, inclusão social e participação cidadã podem ajudar a construir resiliência contra a polarização e a desinformação.

A guerra híbrida pode ter um impacto psicológico significativo na população civil, causando medo, ansiedade e trauma. Ataques cibernéticos, campanhas de desinformação e atos de violência cometidos por forças irregulares podem criar um ambiente de incerteza e insegurança. Yan (2020) argumenta que o uso de táticas de terror e ataques cibernéticos na guerra híbrida visa não apenas causar danos físicos, mas também desestabilizar a psique da população, minando a moral pública e a confiança nas instituições. Ataques cibernéticos a infraestruturas críticas, como redes elétricas e sistemas de comunicação, podem causar medo e ansiedade generalizada. A população pode se sentir vulnerável e desprotegida, especialmente se esses ataques forem repetidos e imprevisíveis. Atos de violência cometidos por forças irregulares, como ataques terroristas e sabotagem, podem causar trauma psicológico significativo. As vítimas diretas e indiretas desses ataques podem sofrer de transtorno de estresse pós-traumático (TEPT)[11] e outras condições de saúde mental.

A guerra híbrida pode levar ao deslocamento forçado de populações, resultando em crises humanitárias e fluxo de refugiados. Conflitos envolvendo forças irregulares e violência extrema por vezes resultam em deslocamento populacional, à medida que civis fogem da violência e buscam segurança em outras regiões ou países. Reichborn-Kjennerud e Cullen (2017) destacam que o deslocamento populacional é uma consequência significativa da guerra híbrida, com implicações profundas para a estabilidade regional e a segurança global.

O deslocamento forçado de grandes populações pode levar a crises humanitárias, com falta de abrigo, alimentos, água e assistência médica. As populações deslocadas enfrentam riscos elevados de doenças, desnutrição e violência. Os fluxos de refugiados podem desestabilizar regiões inteiras, criando tensões entre os países de origem e os países de acolhimento. A chegada de grandes números de refugiados pode sobrecarregar os recursos dos países de acolhimento e causar conflitos sociais e políticos. Além disso, o deslocamento populacional pode

[11]Condição de saúde mental que pode se desenvolver após a exposição a um evento traumático, como um acidente grave, combate militar, abuso físico ou sexual, desastres naturais, ou qualquer situação que cause medo intenso, impotência ou horror.

resultar na desintegração de comunidades, separando famílias e rompendo laços sociais. A perda de redes de apoio social e comunitário pode ter efeitos duradouros sobre a coesão social e a capacidade de recuperação das comunidades afetadas (MCDC, 2019).

3.3 RESPOSTAS E CONTRAMEDIDAS

Os desafios complexos e em constante mudança apresentados pela guerra híbrida exigem respostas e contramedidas integradas e adaptativas. Os Estados precisam desenvolver estratégias abrangentes que combinem capacidades tradicionais de defesa com novas abordagens tecnológicas e metodológicas para enfrentar as diversas ameaças associadas à guerra híbrida. Esta seção examina as principais respostas e contramedidas que podem ser adotadas para mitigar os impactos da guerra híbrida, destacando o desenvolvimento de capacidades cibernéticas, o fortalecimento da resiliência econômica, as campanhas de conscientização e educação, e a cooperação internacional.

A proteção das infraestruturas críticas contra ataques cibernéticos é uma prioridade fundamental na resposta à guerra híbrida. Yan (2020) destaca a necessidade de investir em cibersegurança para desenvolver capacidades ofensivas e defensivas no domínio cibernético. Para tal fim, faz-se necessário implementar sistemas avançados de detecção e prevenção de intrusões[12] (IDS/IPS), *firewalls*[13] e software antivírus para proteger as redes de computadores contra ataques. Além disso, é imperioso promover o treinamento contínuo de profissionais de cibersegurança e a capacitação de pessoal militar e civil para identificar e responder a ameaças cibernéticas. Outra medida é fomentar a colaboração entre o setor público e privado para compartilhar informações sobre ameaças cibernéticas e desenvolver soluções conjuntas para proteger infraestruturas críticas. Ademais, desenvolver capacidades ofensivas no domínio cibernético para dissuadir e retaliar contra atacantes demonstra a capacidade de infligir danos significativos em resposta a ataques cibernéticos (MCDC, 2019).

[12]Componentes críticos na segurança da informação, projetados para monitorar redes e sistemas em busca de atividades maliciosas ou violações de políticas de segurança.
[13]Componentes fundamentais na segurança de redes, projetados para monitorar e controlar o tráfego de entrada e saída com base em regras de segurança predefinidas.

A guerra econômica é uma ferramenta poderosa na guerra híbrida, usada para enfraquecer a economia de um adversário e reduzir sua capacidade de manter a estabilidade interna. Reichborn-Kjennerud e Cullen (2017) destacam que sanções, bloqueios comerciais e manipulação de mercados financeiros podem ter impactos devastadores na economia de um país. Para mitigar esses impactos, os Estados devem diversificar a economia, criar reservas estratégicas, implementar reformas econômicas e promover a inovação tecnológica para fortalecer a resiliência econômica e a competitividade global.

A desinformação e a propaganda são ferramentas significativas na guerra híbrida, utilizadas para manipular a opinião pública e criar divisões dentro da sociedade. Para mitigar os impactos da desinformação é essencial promover a conscientização pública e a alfabetização midiática nas escolas e comunidades para ensinar as pessoas a identificar e avaliar criticamente informações falsas ou enganosas. Outras respostas e contramedidas incluem: Realizar campanhas públicas de conscientização para informar a população sobre as táticas de desinformação utilizadas na guerra híbrida e como se proteger contra elas; Trabalhar em conjunto com veículos de mídia para promover práticas jornalísticas responsáveis e garantir a disseminação de informações precisas e verificadas; e Estabelecer unidades dedicadas ao monitoramento de desinformação para identificar e desmascarar campanhas de desinformação em tempo real para ajudar a aumentar a resiliência contra essas ameaças (MCDC, 2019).

A guerra híbrida não é um fenômeno isolado, mas sim uma realidade global que requer uma compreensão abrangente e uma abordagem colaborativa para a segurança e a defesa em um mundo interconectado. Yan (2020) enfatiza a importância da cooperação internacional para enfrentar as ameaças híbridas de maneira eficaz. Para esse propósito, a adoção de algumas medidas são imprescindíveis: Estabelecer mecanismos de compartilhamento de informações entre países aliados para trocar dados sobre ameaças e vulnerabilidades cibernéticas, econômicas e de desinformação; Realizar exercícios conjuntos de defesa cibernética e resposta a crises para melhorar a coordenação e a interoperabilidade entre as forças armadas e agências de segurança dos países aliados; Desenvolver acordos de apoio mútuo para fornecer assistência econômica, humanitária e militar em caso de ataques híbridos significativos pode fortalecer a resposta coletiva; e Colaborar na criação de normas e regulamentos internacionais para combater a guerra híbrida, incluindo tratados de

cibersegurança e acordos sobre sanções econômicas para uma abordagem integrada e eficaz (MCDC, 2019).

Em conclusão, os impactos e implicações da guerra híbrida são vastos e multifacetados, afetando a segurança nacional, a sociedade e as estratégias de defesa dos Estados. A capacidade de adaptação e a implementação de respostas e contramedidas integradas são indispensáveis para proteger a segurança nacional e garantir a estabilidade social em face desse tipo de conflito complexo e dinâmico.

4 DESAFIOS E PERSPECTIVAS FUTURAS

A guerra híbrida, com sua combinação de táticas convencionais e não convencionais, apresenta desafios significativos para a segurança global e exige uma constante adaptação das estratégias de defesa. À medida que a tecnologia avança e as táticas de guerra evoluem, os Estados enfrentam novos obstáculos na identificação e combate às ameaças híbridas. Além disso, as perspectivas futuras da guerra híbrida indicam um cenário de segurança cada vez mais complexo e imprevisível. Este capítulo examinará os principais desafios na identificação e combate à guerra híbrida e explora as tendências e inovações que moldarão o futuro deste tipo de conflito.

4.1 DESAFIOS NA IDENTIFICAÇÃO E COMBATE À GUERRA HÍBRIDA

A identificação e o combate à guerra híbrida apresentam desafios relevantes devido à sua complexidade e à diversidade de táticas empregadas. A ambiguidade entre guerra e paz dificulta a classificação de ações que não se encaixam nas definições tradicionais de conflito, enquanto a presença de atores não estatais, como grupos terroristas, complica ainda mais a identificação de ameaças. Nesse contexto, a capacidade de atores estatais e não estatais de integrar operações cibernéticas, propaganda, desinformação, forças irregulares e guerra econômica torna a detecção e a resposta a essas ameaças especialmente difíceis. Yan (2020), destaca que a guerra híbrida desfoca as linhas entre guerra e paz, combatentes e civis, criando um ambiente em que as ameaças são difíceis de identificar e neutralizar.

Uma das características definidoras da guerra híbrida é a ambiguidade tática, que dificulta a distinção entre ações militares e civis. Segundo Yan (2020), a capacidade dos atores híbridos de mesclar operações militares com atividades civis e

comerciais complica a identificação das verdadeiras intenções e capacidades dos adversários. Isso cria um ambiente onde as ações hostis podem ser facilmente disfarçadas como atividades legítimas, tornando difícil para os Estados responderem de maneira apropriada. Por exemplo, atores estatais e não estatais podem utilizar empresas de fachada para conduzir operações cibernéticas ou de espionagem, disfarçando suas atividades como transações comerciais legítimas. Além disso, forças irregulares podem envolver-se em atividades criminosas, como tráfico de drogas ou armas, para financiar suas operações, dificultando a distinção entre atividades criminosas e operações militares.

A atribuição de ataques, especialmente cibernéticos, é um dos desafios mais significativos na guerra híbrida. Como destaca Reichborn-Kjennerud e Cullen (2016), a dificuldade em identificar os perpetradores de ataques cibernéticos deve-se à utilização de *proxies* [14], técnicas de camuflagem, bem como o anonimato do ciberespaço. A ausência de evidências claras e diretas complica a responsabilização dos atores, permitindo que eles operem com um certo grau de impunidade. É comum Atores híbridos utilizarem intermediários para conduzir ataques, ocultando sua identidade e dificultando a rastreabilidade. Ferramentas como *Virtual Private Networks* (VPN)[15], *The Onion Router* (TOR)[16] e outras tecnologias de anonimato complicam a identificação das origens dos ataques.

Esses fatores combinados tornam a atribuição de ataques cibernéticos um processo complexo e muitas vezes incerto, exigindo uma abordagem técnica e colaborativa entre nações e organizações para melhorar a detecção, a resposta e a prevenção de futuras ameaças cibernéticas.

As forças irregulares, incluindo insurgentes, milícias e grupos terroristas, são extremamente resilientes e adaptáveis, o que representa um desafio significativo para as forças convencionais. Hoffman (2007) argumenta que a capacidade dessas forças de operar em terrenos complexos e de se misturar com a população civil torna a detecção e a neutralização especialmente difíceis. Além disso, as forças irregulares usualmente empregam táticas de guerrilha e ataques de baixo nível, que são difíceis

[14]Intermediários que atuam entre um cliente e um servidor, facilitando a comunicação e oferecendo uma variedade de funcionalidades, incluindo segurança, anonimato e controle de acesso.
[15]Tecnologia que cria uma conexão segura e criptografada entre o dispositivo do usuário e um servidor VPN.
[16]Rede de anonimato que permite que os usuários naveguem na internet de forma anônima. Ele faz isso roteando o tráfego através de uma série de servidores (nós) operados por voluntários, tornando difícil rastrear a origem do tráfego.

de prever e combater. O uso de táticas de guerrilha em áreas urbanas densamente povoadas dificulta a resposta das forças convencionais, que precisam equilibrar a necessidade de segurança com a proteção de civis. Ataques de baixo nível, como emboscadas, sabotagem e assassinatos seletivos, mantêm a pressão sobre as forças governamentais e criam um ambiente de constante insegurança. A capacidade de se misturar com a população civil permite que as forças irregulares evitem a detecção e a retaliação direta, complicando as operações de contrainsurgência.

A guerra híbrida utiliza desinformação e propaganda para manipular a opinião pública e desestabilizar governos. Yan (2020) destaca que a disseminação de informações falsas através de mídias sociais visa semear desconfiança e confusão. A rápida propagação das informações falsas dificulta a verificação e neutralização, permitindo que as narrativas falsas ganhem força. Campanhas de desinformação bem-sucedidas podem polarizar a sociedade, criar um ambiente de desconfiança e dificultar a comunicação eficaz e a governança.

A guerra híbrida exige uma resposta integrada que combine capacidades militares, cibernéticas, econômicas e de informação. Reichborn-Kjennerud e Cullen (2016) enfatizam a necessidade de coordenação eficaz entre diferentes agências governamentais e setores privados para enfrentar as ameaças híbridas de maneira holística. No entanto, a integração de capacidades e a coordenação interagências apresentam seus próprios desafios, incluindo questões de jurisdição, comunicação e compartilhamento de informações. Diferentes agências e setores podem ter responsabilidades e jurisdições sobrepostas, criando conflitos e ineficiências na resposta às ameaças híbridas. Barreiras de comunicação e a falta de protocolos claros para o compartilhamento de informações podem dificultar a coordenação eficaz entre agências. Além disso, as diferenças nas capacidades e nos recursos disponíveis entre agências podem criar desequilíbrios e lacunas na resposta às ameaças híbridas.

4.2 FUTURO DA GUERRA HÍBRIDA

O futuro da guerra híbrida será moldado por uma série de fatores, incluindo avanços tecnológicos, mudanças geopolíticas e a evolução contínua das táticas de combate. À medida que os atores estatais e não estatais adaptam suas estratégias para explorar novas vulnerabilidades e maximizar o impacto de suas operações, as características da guerra híbrida continuarão a se transformar. Esta seção examina as

tendências e inovações que provavelmente definirão o futuro da guerra híbrida, destacando a crescente sofisticação das operações cibernéticas, o uso ampliado de IA para desinformação, e a integração de tecnologias emergentes em táticas de guerra irregulares.

As operações cibernéticas já são um componente central da guerra híbrida, e sua importância só tende a crescer. Segundo Yan (2020), a proliferação de tecnologias de informação e comunicação proporcionará novas oportunidades para ataques cibernéticos mais sofisticados e integrados. Os Estados e atores não estatais investirão cada vez mais em capacidades cibernéticas para conduzir espionagem, sabotagem e desinformação com maior precisão e impacto. O uso de IA para automatizar ataques cibernéticos permitirá a execução de campanhas mais complexas e coordenadas com menos intervenção humana. Tecnologias de *hacking*[17] mais sofisticadas permitirão a coleta de informações sensíveis de maneira mais furtiva, dificultando a detecção e a prevenção. A combinação de ataques cibernéticos com operações físicas, como sabotagem e espionagem, ampliará o impacto geral das operações híbridas. De acordo com Thiele (2021), a IA será fundamental para a coleta, processamento e exploração de informações, proporcionando uma vantagem decisiva em conflitos híbridos através da aceleração dos processos de tomada de decisão e do aprimoramento da consciência situacional em múltiplos domínios.

A IA desempenhará um papel de destaque no futuro da guerra híbrida, especialmente na área de desinformação. Yan (2020) destaca que a capacidade de criar e disseminar informações falsas de maneira convincente será significativamente ampliada com o uso de IA. Tecnologias como *deepfakes*[18], algoritmos de geração de texto e *bots* sociais[19] tornarão a desinformação mais difícil de detectar e combater. A criação de vídeos falsos altamente realistas permitirá a disseminação de desinformação visual convincente, usada para difamar indivíduos, manipular eventos e incitar violência. Algoritmos avançados de IA serão usados para gerar grandes volumes de conteúdo falso, como notícias, postagens em redes sociais e comentários, amplificando campanhas de desinformação. *Bots* programados para interagir de

[17]Ferramentas, técnicas e métodos utilizados por hackers para explorar vulnerabilidades em sistemas, redes e aplicativos.
[18]Tecnologia de IA que permite a criação de vídeos, áudios ou imagens falsificadas que parecem autênticos.
[19]Programas de software projetados para interagir com usuários em plataformas de redes sociais e outros ambientes online.

maneira convincente nas redes sociais poderão manipular discussões online, criar divisões sociais e influenciar a opinião pública em escala massiva.

O futuro da guerra híbrida será marcado pela integração de uma variedade de tecnologias emergentes, que proporcionarão novas capacidades e táticas para os atores híbridos. Yan (2020) sugere que tecnologias como drones, robótica, e sistemas de armas autônomas desempenharão um papel crescente nas operações híbridas. O uso de drones para vigilância, reconhecimento e ataques precisos proporcionará uma vantagem significativa em operações híbridas, permitindo ações furtivas e de baixo custo. Sistemas de robótica avançada e armas autônomas permitirão a condução de operações sem a necessidade de intervenção humana direta, reduzindo o risco para os operadores e aumentando a eficácia das missões. Além disso, o desenvolvimento de tecnologias de comunicação segura, como criptografia avançada e redes descentralizadas, permitirá a coordenação e execução de operações híbridas de maneira mais eficaz e resiliente.

Os Estados precisarão adaptar suas estruturas de defesa e segurança para enfrentar os desafios e oportunidades apresentados pelo futuro da guerra híbrida. Yan (2020) enfatiza a necessidade de uma abordagem integrada que combine capacidades militares tradicionais com novas tecnologias e métodos de combate. Para esse fim, será essencial melhorar a coordenação entre diferentes agências governamentais e setores privados para enfrentar as ameaças híbridas de maneira holística. Também será importante estabelecer unidades de resposta rápida capazes de identificar e neutralizar ameaças híbridas de maneira eficiente e eficaz. Além disso, implementar estratégias de defesa que antecipem e previnam ataques híbridos, em vez de apenas reagir a eles, fortalecerá a resiliência nacional contra ameaças emergentes.

O futuro da guerra híbrida será definido por avanços tecnológicos, mudanças geopolíticas e a evolução das táticas de combate. A crescente sofisticação das operações cibernéticas, o uso ampliado de IA para desinformação e a integração de tecnologias emergentes representarão desafios significativos para os Estados. Para enfrentar essas ameaças, será necessário desenvolver respostas inovadoras e integradas, adaptando as estruturas de defesa e segurança para proteger a segurança nacional e global.

5 CONCLUSÃO

A análise da guerra híbrida, conforme discutido nesta monografia, destaca a complexidade e a variabilidade dos conflitos contemporâneos, apresentando desafios significativos para a segurança nacional. Conclui-se que uma abordagem integrada e adaptativa é essencial para lidar com as ameaças da guerra híbrida, especialmente no contexto da defesa marítima, e que o fortalecimento das capacidades cibernéticas e de combate à desinformação são cruciais para a segurança nacional.

É fundamental investir em capacidades cibernéticas robustas, dado que as operações cibernéticas são uma das principais ferramentas empregadas em conflitos híbridos. Isso envolve não apenas o aprimoramento da tecnologia e infraestrutura digital, mas também a capacitação contínua dos profissionais de segurança para que possam responder de maneira eficaz às ameaças digitais. A conscientização sobre segurança cibernética também deve ser promovida amplamente, envolvendo tanto as forças de defesa quanto a sociedade em geral.

Adicionalmente, as estratégias de defesa devem integrar operações convencionais e não convencionais, reconhecendo a importância de forças irregulares e o impacto de táticas de propaganda e desinformação. A coordenação com outras forças de segurança e a cooperação internacional são fundamentais para criar uma resposta eficiente e coordenada contra as ameaças híbridas, especialmente em um cenário global interconectado.

A pesquisa ressaltou ainda a necessidade de adaptação contínua das estratégias de defesa, considerando as rápidas inovações tecnológicas e as dinâmicas geopolíticas em constante mudança. Tecnologias emergentes, como a IA, devem ser exploradas para garantir que as capacidades defensivas permaneçam eficazes e atualizadas frente as novas formas de conflito.

Por fim, a construção de resiliência social e a manutenção da confiança pública são fundamentais para fortalecer a segurança nacional. A promoção da transparência e da comunicação eficaz sobre as ações e estratégias de defesa é essencial para mitigar os efeitos da desinformação e da polarização social, e para garantir o apoio da sociedade às medidas de defesa.

Em suma, a guerra híbrida representa uma ameaça significativa para a segurança nacional, especialmente no contexto da defesa marítima. A adoção de estratégias gerais, como o fortalecimento das capacidades cibernéticas, a integração de tecnologias emergentes e a promoção de cooperação internacional, pode mitigar

essas ameaças de maneira eficaz. Além disso, a construção de resiliência social e a manutenção da confiança pública são essenciais para garantir que a defesa marítima esteja preparada para enfrentar os desafios impostos pelas táticas híbridas em um cenário global cada vez mais complexo.

REFERÊNCIAS

BARBOSA, Alexandre Henrique Batista. **A DESINFORMAÇÃO COMO FERRAMENTA DA GUERRA HÍBRIDA.** 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. Acesso em: 26 ago.2024.

BRASIL. Marinha do Brasil. Comando de Operações Navais. COMOPNAVINST 30-01- **Definição da expressão "Ameaças Híbridas".** Rio de Janeiro, 2020.

BRASIL. Marinha do Brasil. Estado-Maior da Armada. EMA-419 - **DOUTRINA CIBERNÉTICA DA MARINHA.** Brasília, 2021.

CHIVVIS, Christopher S. **Understanding Russian 'Hybrid Warfare' And What Can Be Done About it.** RAND Corporation. Santa Monica, 2017. Disponível em: https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf. Acesso em: 24 ago 2024.

HOFFMAN, Frank G. **Conflict in the 21º Century: the rise of hybrid war.** Potomac Institute for Policy Studies. Arlington, 2007. Disponível em: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. Acesso em: 31 mar. 2024.

MULTINATIONAL CAPABILITY DEVELOPMENT CAMPAIGN. **MCDC Countering Hybrid Warfare Project: Countering Hybrid Warfare**. 2019. Disponível em: https://assets.publishing.service.gov.uk/media/5c8141e2e5274a2a51ac0b34/concepts_mcdc_countering_hybrid_warfare.pdf. Acesso em: 24 ago. 2024.

REICHBORN-KJENNERUD, Erik; CULLEN, Patrick J. **Understanding Hybrid Warfare**. Norwegian Institute of International Affairs. Oslo, 2016. Disponível em: https://nupi.brage.unit.no/nupi-xmlui/bitstream/handle/11250/2380867/NUPI_Policy_Brief_1_Reichborn_Kjennerud_Cullen.pdf. Acesso em: 24 fev. 2024.

REICHBORN-KJENNERUD, Erik; CULLEN, Patrick J. **MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare.** Multinational Capability Development Campaign (MCDC). Reino Unido, 2017. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf. Acesso em: 07 set. 2024.

SOLMAZ, Tarik. **"Hybrid Warfare": One Term, Many Meanings**. Small Wars Journal. Bethesda, 2022. Disponível em: https://smallwarsjournal.com/jrnl/art /hybrid-warfare-one-term-many-meaning. Acesso em: 16 jun. 2024.

THIELE, Ralph (ed.). **Hybrid Warfare Future and Technologies**. 1. ed. Nickenich: Springer VS, 2021. E-book.

YAN, Guilong (ed.). **The impact of Artificial Intelligence on hybrid warfare**. Small Wars & Insurgencies, Londres, 2020. Disponível em: https://doi.org/10.1080/09592318.2019.1682908. Acesso em: 31 mar. 2024.