ESCOLA DE GUERRA NAVAL

CSUP2024

GUERRA HÍBRIDA

Rio de Janeiro

2024

CSUP2024

GUERRA HÍBRIDA

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

Orientador: CSUP2024

Rio de Janeiro

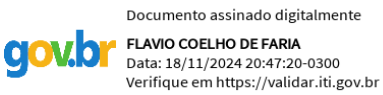
Escola de Guerra Naval

2024

DECLARAÇÃO DA NÃO EXISTÊNCIA DE APROPRIAÇÃO INTELECTUAL IRREGULAR

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.

Assinatura digital gov.br



DEDICATÓRIA

Dedico esse trabalho a minha família, em especial a minha esposa Andrea por trabalhar arduamente no lar e cuidas dos nossos filhos. Ao meu coordenador que dedicou seu tempo e esforço para acompanhar-me nesse projeto. E a toda EGN pela excelência na sua função.

AGRADECIMENTO

Primeiramente, a Deus por me dar saúde e força para superar os obstáculos. E a minha família por suportar as ausências. E aos amigos que me incentivaram nessa empreitada.

Não é preciso ter olhos abertos para ver o sol, nem é preciso ter ouvidos afiados para ouvir o trovão. Para ser vitorioso você precisa ver o que não está visível.

SUN-TZU

RESUMO

A Guerra Híbrida representa uma forma contemporânea de conflito que combina métodos tradicionais e não convencionais para alcançar objetivos estratégicos. Este trabalho explora as características e implicações da Guerra Híbrida, destacando seu uso de tecnologias avançadas, como ciberataques e campanhas de desinformação. Exemplos históricos e contemporâneos, como o conflito entre Rússia e Ucrânia e a interferência nas eleições presidenciais dos Estados Unidos em 2016, ilustram a complexidade e a eficácia dessa abordagem. Este estudo visa investigar o uso do lawfare no contexto da guerra marítima, justificando-se pela crescente importância dessa estratégia em disputas territoriais. A utilização de normas jurídicas como ferramentas estratégicas permite que os Estados evitem confrontos militares diretos, ao mesmo tempo em que avançam suas agendas políticas e territoriais. O objetivo é analisar como essas práticas influenciam a dinâmica internacional, destacando seus impactos éticos e legais. A metodologia inclui uma análise qualitativa baseada em revisão bibliográfica e estudo de casos específicos. Conclui-se que o lawfare é eficaz, porém apresenta desafios éticos significativos no cenário internacional.

Palavras-chave: Guerra Híbrida, cibersegurança, lawfare, desinformação.

ABSTRACT

Hybrid Warfare represents a contemporary form of conflict that combines traditional and unconventional methods to achieve strategic objectives. This scientific work explores the characteristics and implications of Hybrid Warfare, highlighting its use of advanced technologies such as cyberattacks and disinformation campaigns. Historical and contemporary examples, such as the conflict between Russia and Ukraine and the interference in the 2016 United States presidential elections, illustrate the complexity and effectiveness of this approach. This study aims to investigate the use of lawfare in the context of maritime warfare, justified by the growing importance of this strategy in territorial disputes. The use of legal norms as strategic tools allows States to avoid direct military confrontations, while advancing their political and territorial agendas. The objective is to analyze how these practices influence international dynamics, highlighting their ethical and legal impacts. The methodology includes a qualitative analysis based on a literature review and specific case studies. It is concluded that lawfare is effective, but presents significant ethical challenges in the international scenario.

Keywords: Hybrid War, cybersecurity, lawfare, disinformation.

SUMÁRIO

1 INTRODUÇÃO

A Guerra Híbrida é um conceito moderno e multifacetado que representa um desafio significativo para a segurança global e as relações internacionais contemporâneas. Diferentemente das guerras convencionais, a Guerra Híbrida combina uma variedade de técnicas de combate, que vão desde operações militares tradicionais até ciberataques, propaganda e influências econômicas. Essa forma de conflito, portanto, não se limita aos campos de batalha físicos, estendendo-se ao domínio cibernético e ao espaço da informação. A complexidade e a eficácia da Guerra Híbrida residem precisamente nessa capacidade de integrar múltiplas formas de agressão para atingir objetivos estratégicos, frequentemente sem uma declaração formal de guerra.

O termo "Guerra Híbrida" ganhou destaque significativo nas últimas décadas, especialmente com a intensificação das atividades militares e cibernéticas da Rússia. A anexação da Crimeia em 2014 é frequentemente citada como um exemplo clássico de Guerra Híbrida. Neste caso, a Rússia utilizou uma combinação de forças armadas regulares, tropas sem identificação (conhecidas como "homenzinhos verdes"), e uma campanha de desinformação sofisticada para assegurar o controle sobre a península. Além disso, a Rússia implementou bloqueios de comunicação e ciberataques para desestabilizar o governo ucraniano, criando confusão e dificultando uma resposta coordenada por parte de Kiev e seus aliados ocidentais (Galeotti, 2016).

Além da Crimeia, outros episódios de interferência russa em assuntos de Estados soberanos demonstram a extensão da Guerra Híbrida. A interferência nas eleições presidenciais dos Estados Unidos em 2016, por exemplo, é amplamente vista como uma forma de Guerra Híbrida. Por meio de uma combinação de ataques cibernéticos, campanhas de desinformação nas redes sociais e manipulação de dados, agentes russos tentaram influenciar o resultado eleitoral e semear desconfiança nas instituições democráticas americanas (Rid, 2020). Esses eventos sublinham a capacidade da Guerra Híbrida de alcançar impactos estratégicos significativos sem a necessidade de engajamento militar direto.

A Guerra Híbrida também não é um fenômeno novo. Embora o termo seja contemporâneo, as táticas associadas a esse tipo de conflito têm raízes históricas profundas. A Guerra do Vietnã, por exemplo, ilustra o uso de estratégias híbridas, em que as forças vietnamitas combinaram táticas de guerrilha com campanhas psicológicas e

políticas para minar a moral e a eficácia das forças americanas. Este conflito demonstrou como a integração de múltiplas formas de luta, incluindo ações não convencionais, pode superar até mesmo exércitos tecnologicamente superiores (Krepinevich, 1986).

No entanto, a natureza da Guerra Híbrida evoluiu consideravelmente com o avanço da tecnologia. Hoje, a cibersegurança tornou-se uma frente essencial no combate a essas ameaças. Estados e atores não estatais podem lançar ataques cibernéticos que comprometem infraestruturas críticas, roubam informações sensíveis e perturbam a ordem social e econômica. O ataque de 2007 contra a Estônia, atribuído a hackers russos, serve como um exemplo de como as operações cibernéticas podem paralisar um país, bloqueando sites governamentais, financeiros e de comunicação, e demonstrando a vulnerabilidade das nações modernas a esse tipo de guerra (Ottis, 2008).

A Guerra Híbrida tem implicações profundas para a segurança global e a política interna dos Estados. Em primeiro lugar, ela desafia as estratégias tradicionais de defesa, que muitas vezes se concentram em ameaças militares convencionais. As nações agora precisam desenvolver capacidades que integrem defesa cibernética, contrainformação e resiliência social para enfrentar esses desafios multifacetados. Em segundo lugar, a Guerra Híbrida pode ter consequências econômicas devastadoras. Ataques cibernéticos podem interromper cadeias de suprimentos, causar danos financeiros e desestabilizar mercados, enquanto a desinformação pode exacerbar tensões sociais e políticas internas.

Além disso, a Guerra Híbrida apresenta desafios únicos para a governança global. A natureza difusa e muitas vezes encoberta dessas operações dificulta a atribuição de responsabilidade e a formulação de respostas coordenadas por parte da comunidade internacional. Isso é exacerbado pelo fato de que muitos dos atores envolvidos, incluindo grupos insurgentes e hackers patrocinados por Estados, operam em uma zona cinzenta entre legalidade e ilegalidade. Portanto, a criação de políticas eficazes de prevenção e resposta requer uma cooperação internacional estreita e um entendimento compartilhado das ameaças e das melhores práticas de defesa.

A Guerra Híbrida sublinha a necessidade de inovação constante nas estratégias de segurança e defesa. À medida que as tecnologias evoluem, as táticas de Guerra Híbrida também se adaptam, explorando novas vulnerabilidades e oportunidades. A capacidade de antecipar essas mudanças e desenvolver respostas ágeis e

eficazes será muito importante para a proteção dos interesses nacionais e internacionais. Como observa Hoffman (2007), "a verdadeira força da Guerra Híbrida reside na sua flexibilidade e na capacidade de explorar as fraquezas do adversário por meio de uma combinação dinâmica de métodos convencionais e não convencionais."

A combinação de métodos de guerra convencionais e não convencionais, juntamente com o uso de tecnologias avançadas e estratégias de desinformação, cria um campo de batalha dinâmico e multifacetado.

A delimitação do problema deste trabalho centra-se na compreensão e análise da Guerra Híbrida, um fenômeno contemporâneo que combina métodos de guerra convencionais e não convencionais para alcançar objetivos estratégicos. Este tipo de conflito representa um desafio significativo para as nações modernas, devido à sua complexidade e capacidade de integrar operações militares tradicionais com ciberataques, desinformação, manipulação econômica e outras táticas irregulares. O problema é ainda agravado pela dificuldade em identificar e responder eficazmente a essas ameaças multifacetadas, que frequentemente operam abaixo do limiar de uma guerra declarada.

O objetivo deste trabalho é abranger as características e implicações da Guerra Híbrida, destacando a necessidade de políticas de defesa adaptativas e integradas. Especificamente, busca-se explorar as estratégias utilizadas na Guerra Híbrida, analisar exemplos históricos e contemporâneos, e identificar as melhores práticas para o desenvolvimento de políticas de defesa híbrida eficazes.

O trabalho está dividido em 4 capítulos, o primeiro trata-se da introdução , o segundo do referencial teórico que vai abordar definição de Guerra Híbrida ,Integração de Múltiplos Métodos De Guerra ,Conflito Rússia-Ucrânia ,Guerra do Vietnã dentre outros assuntos relacionados ao tema, o terceiro como pode se dar uma operação internacional, no quarto a elaboração de políticas de defesa e conclui-se o trabalho no quinto.

2 REFERENCIAL TEÓRICO

2.1 DEFINIÇÃO DE GUERRA HÍBRIDA

Este tipo de guerra integra operações militares tradicionais com táticas não militares, como ciberataques, campanhas de desinformação, sabotagem e influência política e econômica. A principal característica da Guerra Híbrida é a sua flexibilidade e capacidade de explorar as vulnerabilidades do adversário por meio de uma combinação dinâmica de métodos de ataque.

A origem do termo "Guerra Híbrida" é frequentemente atribuída a Frank G. Hoffman, que o utilizou para descrever a fusão de guerra regular e irregular, destacando que esses conflitos envolvem uma gama completa de modos de guerra, incluindo operações convencionais, insurgências e terrorismo. Segundo Hoffman (2007), a Guerra Híbrida é caracterizada pela fusão de táticas de guerra irregulares e convencionais, com elementos de apoio estatal e não estatal, gerando uma sinergia que potencializa o impacto estratégico.

A Guerra Híbrida se destaca pelo uso intensivo de tecnologias avançadas, especialmente no domínio cibernético. Os ciberataques são uma componente essencial desta forma de guerra, permitindo a sabotagem de infraestruturas críticas, o roubo de informações sensíveis e a manipulação de dados para desestabilizar o adversário (Ottis, 2008).

Além dos ciberataques, a desinformação desempenha um papel crucial na Guerra Híbrida. As campanhas de desinformação são projetadas para manipular a opinião pública, semear discórdia e minar a confiança nas instituições democráticas (Rid ,2020).

2.1.1 Lawfare Aplicado à Guerra Marítima

O *lawfare* aplicado à guerra marítima se refere ao uso estratégico de normas jurídicas para alcançar objetivos geopolíticos no domínio dos oceanos. Esse conceito tem se tornado cada vez mais relevante em disputas sobre soberania e direitos marítimos, particularmente à medida que as tensões em áreas como o Mar do Sul da China e o Ártico aumentam. O uso da lei como arma permite que estados manipulem as regras do direito internacional para obter vantagens estratégicas, sem a necessidade de recorrer ao confronto armado direto. Isso é especialmente verdadeiro no ambiente marítimo, onde a Convenção das Nações Unidas sobre o Direito do Mar (UNCLOS) define os direitos e deveres dos estados no uso dos oceanos, mas ao mesmo tempo permite diferentes interpretações que podem ser manipuladas

conforme os interesses de cada nação.

Um exemplo claro de *lawfare* marítimo é a disputa no Mar do Sul da China, onde a China tem utilizado uma combinação de reivindicações históricas e interpretações jurídicas seletivas para expandir seu controle sobre vastas áreas marítimas. Embora a UNCLOS limite as zonas econômicas exclusivas (ZEEs) a 200 milhas náuticas a partir da costa, a China reivindica a maior parte do Mar do Sul da China com base na chamada "linha de nove traços", um argumento que foi amplamente rejeitado pela comunidade internacional, incluindo uma decisão de 2016 do Tribunal Permanente de Arbitragem em Haia. Embora essa decisão tenha invalidado as reivindicações da China, o governo chinês continua a reforçar suas posições na região, construindo ilhas artificiais e militarizando-as, alegando direitos históricos que não são respaldados por normas internacionais. O uso de *lawfare* nesse caso permite que a China mantenha uma presença dominante sem recorrer à guerra aberta, enquanto desafia as normas jurídicas estabelecidas (Cheung, 2018).

Outro aspecto do *lawfare* marítimo é a criação e aplicação de regulamentos ambientais e de pesca para justificar o controle de áreas disputadas. Estados podem utilizar a proteção ambiental como uma justificativa legal para restringir o acesso de outras nações a determinados recursos marítimos. No Mar do Japão, por exemplo, disputas territoriais entre o Japão, a Coreia do Sul e a China têm levado a frequentes tensões sobre a exploração pesqueira e de recursos naturais. O Japão, utilizando a legislação ambiental, tem estabelecido zonas de proteção ecológica ao redor de áreas contestadas, restringindo as atividades de pesca estrangeira. Essas ações são justificadas por preocupações ambientais, mas também servem ao propósito estratégico de manter o controle sobre áreas economicamente vitais (Pardo, 2019).

No Ártico, o *lawfare* também tem desempenhado um papel importante à medida que o derretimento das calotas polares torna essa região mais acessível para exploração econômica e navegação. Países como Rússia, Canadá, Noruega e os Estados Unidos têm reivindicado extensões de sua plataforma continental no Ártico, buscando controlar os recursos minerais e as novas rotas comerciais que estão surgindo. A Rússia, em particular, tem sido ativa na utilização de *lawfare* para justificar suas reivindicações territoriais no Ártico. Por meio de uma série de submissões à Comissão das Nações Unidas sobre os Limites da Plataforma Continental, a Rússia procura expandir sua jurisdição sobre vastas áreas do fundo do mar, argumentando que essas áreas fazem parte de sua extensão natural. Ao utilizar processos jurídicos

internacionais para avançar suas reivindicações, a Rússia evita o confronto militar direto, ao mesmo tempo em que fortalece sua posição estratégica no Ártico (Byers, 2018).

A interceptação e inspeção de embarcações suspeitas em águas internacionais também são exemplos de *lawfare* na guerra marítima. Essas operações, muitas vezes justificadas por razões de segurança ou de prevenção de crimes como a pirataria e o tráfico de armas, podem ser usadas para afirmar controle sobre rotas marítimas estratégicas. A Operação Atalanta, da União Europeia, realizada no Golfo de Aden e nas águas ao largo da Somália, é um exemplo de como as leis internacionais podem ser utilizadas para justificar a interceptação de navios suspeitos de pirataria. Embora o objetivo principal da operação seja combater a pirataria, a presença prolongada de navios militares de várias nações na região também serve para afirmar o controle sobre uma das rotas marítimas mais importantes do mundo (Kraska, 2020).

Outro exemplo de *lawfare* no contexto marítimo é o bloqueio legal de portos e zonas costeiras sob o pretexto de imposição de sanções ou embargos. Estados podem recorrer ao direito internacional para justificar o bloqueio de rotas marítimas ou de portos de estados rivais. Um exemplo recente envolve as tensões entre os Estados Unidos e o Irã no Estreito de Ormuz, uma das vias navegáveis mais importantes para o comércio de petróleo. A imposição de sanções unilaterais pelos Estados Unidos ao Irã e a subsequente ameaça de impedir o tráfego de petróleo através do estreito mostram como o *lawfare* pode ser utilizado para atingir objetivos políticos e econômicos. Ao utilizar a lei para justificar essas ações, os Estados Unidos evitam o risco de confronto militar direto, ao mesmo tempo em que pressionam o governo iraniano de forma significativa (Gómez, 2019).

As disputas legais sobre o direito de passagem e a liberdade de navegação em zonas marítimas também são uma forma frequente de *lawfare*. Estados que controlam áreas marítimas estratégicas, como o Estreito de Malaca ou o Estreito de Bab el-Mandeb, podem utilizar a lei para regular o trânsito de embarcações civis e militares. Embora a UNCLOS garanta o direito de passagem inocente, a interpretação dessa norma pode ser manipulada para justificar a interceptação ou o monitoramento de navios, especialmente em regiões de interesse geopolítico. Por exemplo, a China frequentemente utiliza o argumento de segurança nacional para justificar a interceptação de navios estrangeiros que passam por suas águas territoriais no Mar do Sul da China, mesmo quando esses navios estão seguindo o princípio da

passagem inocente garantido pela UNCLOS (Bateman, 2020).

2.2 INTEGRAÇÃO DE MÚLTIPLOS MÉTODOS DE GUERRA

Essa abordagem multifacetada permite aos atores explorar as vulnerabilidades do adversário em diversas frentes simultaneamente, criando uma sinergia que potencializa o impacto das operações.

Um dos componentes principais da Guerra Híbrida é o uso de forças militares tradicionais em conjunto com táticas irregulares. As operações militares convencionais, que incluem o emprego de tropas regulares, tanques e aviação, são frequentemente usadas para criar uma presença física e intimidar o adversário. No entanto, essas operações são complementadas por táticas de guerrilha, sabotagem e ataques surpresa, que são típicos de conflitos assimétricos (Galeotti, 2016).

Além das operações militares, a Guerra Híbrida faz uso extensivo de operações cibernéticas para alcançar seus objetivos. Os ciberataques podem causar danos significativos a infraestruturas críticas, roubar informações sensíveis e desorganizar a sociedade civil (Ottis, 2008). Ciberataques também foram utilizados durante o conflito Rússia-Ucrânia, em que redes de comunicação e infraestrutura energética ucranianas foram alvo de ataques contínuos.

As campanhas de desinformação são outro pilar fundamental da Guerra Híbrida. Estas campanhas são projetadas para manipular a opinião pública, semear discórdia e minar a confiança nas instituições democráticas do adversário. Agentes russos utilizaram redes sociais e outros meios de comunicação para espalhar notícias falsas e teorias da conspiração, influenciando o eleitorado e criando divisões dentro da sociedade americana (Rid, 2020).

A guerra econômica também desempenha um papel na estratégia híbrida. Medidas como sanções econômicas, bloqueios comerciais e manipulação de mercados podem enfraquecer a economia do adversário, afetando sua capacidade de sustentar operações militares e mantendo a estabilidade interna (Marten, 2015).

As operações híbridas são frequentemente conduzidas de forma descentralizada, permitindo uma resposta rápida e adaptativa às mudanças no campo de batalha. Essa abordagem também dificulta a atribuição de responsabilidade, já que as

ações podem ser conduzidas por uma variedade de atores, incluindo forças regulares, grupos paramilitares, hackers e outros agentes clandestinos.

A eficácia da Guerra Híbrida depende da capacidade de integrar essas diversas formas de combate de maneira coesa e coordenada. Isso requer um planejamento estratégico detalhado e a capacidade de ajustar as operações conforme necessário para explorar as fraquezas do adversário.

2.2.1 Atribuição de responsabilidade

Atribuição de responsabilidade é um conceito fundamental no campo do Direito, que busca determinar quem deve ser legalmente responsável por uma ação ou omissão que causou um dano. Segundo Dunlap (2008), a responsabilidade implica tanto a obrigação de reparar os danos causados quanto a prestação de contas sobre as ações tomadas. No âmbito internacional, essa atribuição pode ser ainda mais complexa, pois envolve Estados, organizações internacionais e, em alguns casos, indivíduos.

No Direito Internacional, a atribuição de responsabilidade está vinculada à capacidade de um Estado ou organização em agir de acordo com as normas jurídicas internacionais. Koskenniemi (2011) argumenta que, em contextos de guerra ou conflito, a responsabilidade é atribuída com base na violação de princípios internacionais, como o respeito aos direitos humanos e à soberania dos Estados. No entanto, a aplicação dessas normas pode ser desafiada por questões políticas e pela própria manipulação do Direito, como no caso do uso do lawfare, em que a lei é utilizada como uma arma para atingir objetivos estratégicos.

Para a atribuição de responsabilidade ser efetiva, é necessário que haja mecanismos que garantam a prestação de contas. Schabas (2017) destaca que tribunais internacionais, como o Tribunal Penal Internacional, foram criados justamente para responsabilizar indivíduos por crimes graves, como genocídio e crimes de guerra. Contudo, o sucesso desses tribunais depende da cooperação dos Estados, que nem sempre é garantida, especialmente quando os interesses políticos estão em jogo.

A responsabilidade também pode ser compartilhada ou diluída, especialmente em casos de intervenções internacionais. Hehir (2013) sugere que, quando coalizões de Estados ou organizações internacionais realizam operações conjuntas, a atribuição de responsabilidade pode ser complexa, com dificuldades em identificar quais Estados

ou entidades são diretamente responsáveis por uma violação específica. Isso pode levar à falta de responsabilização efetiva e à impunidade.

Em última análise, a atribuição de responsabilidade é crucial para garantir a justiça e prevenir abusos no cenário internacional. No entanto, como apontam diversos autores, a politização desse processo e a falta de mecanismos robustos podem comprometer a eficácia da responsabilização no Direito Internacional.

2.3 CONFLITO RÚSSIA-UCRÂNIA

O conflito entre Rússia e Ucrânia, que começou em 2014 com a anexação da Crimeia pela Rússia, é um exemplo claro da aplicação de táticas de Guerra Híbrida.

A anexação da Crimeia pela Rússia, em março de 2014, foi um evento que surpreendeu a comunidade internacional pela sua rapidez e eficiência. Tropas russas, sem insígnias identificáveis, conhecidas como "homenzinhos verdes", foram enviadas para ocupar edifícios governamentais e instalações militares na Crimeia. Esta ação foi acompanhada por uma intensa campanha de desinformação que procurou justificar a intervenção russa sob o pretexto de proteger a população de etnia russa na região. A ausência de identificação nas tropas permitiu à Rússia negar formalmente a sua intervenção direta, criando confusão e dificultando uma resposta coordenada da Ucrânia e da comunidade internacional (Galeotti, 2016).

Além das operações terrestres, a Rússia utilizou extensivamente operações cibernéticas para desestabilizar a Ucrânia. Os ataques cibernéticos russos visaram infraestruturas críticas, incluindo redes de energia, comunicações e sistemas financeiros ucranianos. Um exemplo notável foi o ataque à rede elétrica da Ucrânia em dezembro de 2015, que resultou em apagões em várias regiões do país. O ataque demonstrou a capacidade da Rússia de usar o ciberespaço como um campo de batalha, causando danos significativos sem a necessidade de um confronto militar direto (Kovacs, 2016).

As campanhas de desinformação foram outra componente crucial da estratégia russa. Utilizando uma rede de meios de comunicação controlados pelo Estado, bem como bots e trolls [1] nas redes sociais, a Rússia espalhou notícias falsas e propaganda

[1] **Trolls**: São indivíduos que, intencionalmente, postam comentários ou mensagens provocativas, ofensivas ou enganosas para causar reações emocionais negativas, perturbar discussões ou gerar conflito em comunidades virtuais.

para semear discórdia e minar a confiança nas instituições ucranianas. Essas campanhas não se limitaram à Ucrânia; elas também visaram influenciar a opinião pública em países ocidentais, tentando enfraquecer o apoio internacional ao governo ucraniano. A eficácia dessas campanhas de desinformação pode ser vista na maneira como elas conseguiram criar narrativas alternativas que confundiram tanto o público quanto os formuladores de políticas (Pomerantsev & Weiss, 2014).

A guerra econômica também desempenhou um papel significativo no conflito Rússia-Ucrânia. A Rússia utilizou seu domínio sobre o fornecimento de gás natural à Ucrânia como uma ferramenta de pressão. Em várias ocasiões, a Rússia cortou o fornecimento de gás ou aumentou os preços, exacerbando as dificuldades econômicas da Ucrânia e tentando forçar concessões políticas. Este uso do fornecimento de energia como arma econômica é um exemplo clássico de como a guerra híbrida pode incluir elementos de pressão econômica para alcançar objetivos estratégicos (Marten, 2015).

Além disso, a Rússia apoiou militarmente e logisticamente grupos separatistas no leste da Ucrânia. Esses grupos, que declararam a independência das regiões de Donetsk e Luhansk, receberam armas, treinamento e apoio financeiro da Rússia. O conflito armado entre forças ucranianas e separatistas pró-russos resultou em milhares de mortos e milhões de deslocados, criando uma crise humanitária significativa. A intervenção russa, embora muitas vezes negada formalmente, foi essencial para a sustentação das operações separatistas (Hughes & Sasse, 2016).

A resposta da comunidade internacional ao conflito incluiu sanções econômicas contra a Rússia e apoio financeiro e militar à Ucrânia. As sanções visaram setores-chave da economia russa, incluindo energia, defesa e finanças, com o objetivo de pressionar a Rússia a cessar suas atividades desestabilizadoras. No entanto, a eficácia das sanções tem sido um tema de debate, com alguns argumentando que elas não foram suficientes para deter a agressão russa (Connolly, 2018).

O conflito entre Rússia e Ucrânia exemplifica a aplicação abrangente de táticas de Guerra Híbrida. A combinação de operações militares convencionais e não convencionais, ciberataques, desinformação e guerra econômica permitiu à Rússia alcançar seus objetivos estratégicos de maneira eficaz e com custos relativamente baixos.

Bots: São programas automatizados que executam tarefas repetitivas na internet, incluindo interações em redes sociais. Alguns bots simulam comportamento humano, sendo usados para disseminar informações, aumentar o tráfego ou manipular debates online, especialmente em contextos políticos.

O conflito sublinha a necessidade de estratégias de defesa integradas e coordenadas que possam responder a ameaças multifacetadas de forma eficiente e adaptável.

2.4 GUERRA DO VIETNÃ

A Guerra do Vietnã, travada entre 1955 e 1975, é um exemplo emblemático de conflito que incorporou elementos de Guerra Híbrida, combinando operações militares convencionais com táticas irregulares e psicológicas. O conflito envolveu as forças da República do Vietnã (Vietnã do Sul), apoiadas pelos Estados Unidos e outras nações aliadas, contra o Vietnã do Norte e o Viet Cong, um grupo de guerrilheiros comunistas.

Uma característica marcante da Guerra do Vietnã foi o uso extensivo de táticas de guerrilha pelo Viet Cong e pelo Exército Popular do Vietnã (NVA). Esses grupos evitaram confrontos diretos com as forças americanas superiores em termos de tecnologia e poder de fogo, preferindo emboscadas, sabotagem e ataques surpresa. As táticas de guerrilha provaram ser extremamente eficazes em desgastar as forças americanas, tanto física quanto psicologicamente. Krepinevich (1986) observa que "as táticas de guerrilha do Viet Cong foram projetadas para explorar as fraquezas das forças americanas, especialmente sua dependência de grandes bases e linhas de suprimento".

Além das táticas militares irregulares, o Vietnã do Norte utilizou operações psicológicas e políticas para minar a moral das forças americanas e influenciar a opinião pública internacional. A Tet Offensive de 1968, por exemplo, foi uma campanha militar que teve um impacto psicológico profundo. Embora tenha sido militarmente custosa para o Viet Cong e o NVA, a ofensiva conseguiu desestabilizar a confiança do público americano na vitória e aumentar a pressão por uma retirada dos EUA. Como Herring (2002) aponta, "a Tet Offensive revelou a capacidade do Vietnã do Norte de lançar ataques coordenados em larga escala, desafiando a percepção de que a guerra estava sendo ganha pelos Estados Unidos".

A guerra psicológica também envolveu propaganda e esforços para ganhar o apoio da população rural vietnamita. O Viet Cong operou extensivamente em áreas rurais, fornecendo serviços sociais e prometendo reforma agrária, o que contrastava com o governo sul-vietnamita, amplamente visto como corrupto e inepto. Esse apoio popular foi crucial para a sustentação da insurgência comunista ao longo dos anos. A insurgência comunista também se beneficiou do apoio logístico e material da União

Soviética e da China, que forneciam armas, munições e treinamento, permitindo que as forças vietnamitas mantivessem a pressão sobre os americanos e seus aliados (Herring,2002).

O envolvimento dos Estados Unidos na Guerra do Vietnã também teve uma dimensão híbrida, combinando campanhas aéreas massivas e operações terrestres com esforços de "ganhar corações e mentes" por meio de programas de pacificação. No entanto, esses esforços muitas vezes falharam em contrabalançar a influência do Viet Cong nas áreas rurais. A incapacidade de assegurar a lealdade da população local e de derrotar a insurgência de guerrilha levou a um prolongamento do conflito e a uma crescente oposição pública à guerra nos Estados Unidos (Herring, 2002).

A Guerra do Vietnã exemplifica o uso de estratégias híbridas, em que operações militares convencionais são combinadas com táticas de guerrilha, operações psicológicas e apoio popular. Este conflito demonstrou como a integração de múltiplos métodos de guerra pode desafiar até mesmo as forças militares mais poderosas, ressaltando a importância de abordagens flexíveis e adaptativas em conflitos assimétricos (Krepinevich ,1986).

2.5 DESENVOLVIMENTO DE POLÍTICAS DE DEFESA HÍBRIDA

O desenvolvimento de políticas de defesa híbrida é essencial para enfrentar as ameaças complexas e multifacetadas representadas pela Guerra Híbrida.A criação de políticas eficazes envolve vários componentes, incluindo o fortalecimento da cibersegurança, a cooperação internacional, a resiliência social e a inovação contínua nas estratégias de defesa.

Primeiramente, o fortalecimento da cibersegurança é um pilar fundamental das políticas de defesa híbrida. À medida que os ataques cibernéticos se tornam mais sofisticados e frequentes, é essencial que os Estados desenvolvam capacidades robustas para proteger suas infraestruturas críticas. Isso inclui a proteção de redes de energia, sistemas de transporte, comunicação e instituições financeiras. A União Europeia, por exemplo, implementou a Diretiva NIS (Segurança das Redes e da Informação) para melhorar a segurança cibernética em todos os Estados membros, estabelecendo requisitos para a segurança das redes e sistemas de informação das infraestruturas críticas (European Commission, 2016).

Além da proteção de infraestruturas críticas, as políticas de cibersegurança devêm incluir a capacidade de detectar, responder e mitigar ciberataques. A criação de equipes de resposta a incidentes de segurança cibernética (CSIRTs) é essencial para lidar rapidamente com ameaças emergentes. Os Estados Unidos, por meio do Departamento de Segurança Interna (DHS), estabeleceram o Centro de Segurança Cibernética e Infraestrutura (CISA) para coordenar a resposta a incidentes cibernéticos e fornecer orientação sobre melhores práticas de segurança. O Centro de Segurança Cibernética e Infraestrutura (CISA) foi criado em 2018, como parte do Departamento de Segurança Interna dos Estados Unidos (DHS). (CISA, 2020).

A cooperação internacional também é crucial no desenvolvimento de políticas de defesa híbrida, A defesa híbrida refere-se a uma estratégia que combina diferentes métodos de defesa, englobando tanto táticas convencionais (como forças armadas e operações militares tradicionais) quanto meios não convencionais (incluindo guerra cibernética, campanhas de desinformação, operações encobertas e apoio a insurgências). As ameaças híbridas frequentemente transcendem as fronteiras nacionais, tornando necessária uma colaboração estreita entre os Estados para compartilhar informações e desenvolver respostas coordenadas. A Organização do Tratado do Atlântico Norte (OTAN) reconheceu a importância da defesa híbrida e estabeleceu um Centro de Excelência para a Defesa Contra Ameaças Híbridas em Helsinque, na Finlândia, para promover a cooperação e o intercâmbio de conhecimentos entre os países membros (OTAN, 2017).

Além disso, a resiliência social é um componente vital das políticas de defesa híbrida. A capacidade de uma sociedade resistir e recuperar-se de ataques híbridos depende em grande parte da confiança nas instituições e da coesão social. As campanhas de desinformação visam precisamente minar essa confiança, criando divisões e semeando desconfiança. Para combater isso, é necessário investir em programas de alfabetização midiática e digital que capacitem os cidadãos a reconhecer e resistir à desinformação. A Finlândia, por exemplo, implementou um programa abrangente de educação em mídia e informação nas escolas, que tem sido elogiado por sua eficácia em aumentar a resiliência contra a desinformação (Ministry of Education and Culture of Finland, 2019).

A inovação contínua nas estratégias de defesa é outro elemento importante. A natureza dinâmica da Guerra Híbrida significa que as táticas e tecnologias utilizadas pelos adversários estão em constante evolução. Os Estados devem, portanto, adotar

uma abordagem proativa na pesquisa e desenvolvimento de novas tecnologias e métodos de defesa. Isso inclui o investimento em inteligência artificial e machine learning para detectar padrões de ataque cibernético e prever ameaças potenciais. O uso de simulações e exercícios de guerra híbrida também pode ajudar a identificar vulnerabilidades e testar a eficácia das respostas planejadas.

A integração de forças armadas e civis é fundamental para uma abordagem eficaz de defesa híbrida. Isso envolve a coordenação entre militares, agências governamentais, setor privado e a sociedade civil para garantir uma resposta coesa e abrangente às ameaças híbridas. Em muitos países, essa integração é facilitada por meio da criação de comitês de segurança nacional e centros de comando unificados que reúnem representantes de diferentes setores para planejar e coordenar as respostas às crises (Bachmann & Gunneriusson, 2015).

Finalmente, a transparência e a comunicação clara por parte dos governos são essenciais para manter a confiança pública durante crises híbridas. A gestão eficaz da comunicação de crises pode ajudar a combater a desinformação e garantir que o público receba informações precisas e confiáveis. Isso é particularmente importante durante ataques híbridos, em que a confusão e o pânico podem ser explorados pelos adversários para amplificar o impacto das suas operações. A comunicação proativa e transparente pode, portanto, fortalecer a resiliência social e ajudar a manter a coesão durante períodos de crise (Linvill & Warren, 2018).

O desenvolvimento de políticas de defesa híbrida requer uma abordagem multifacetada que inclua o fortalecimento da cibersegurança, a cooperação internacional, a resiliência social, a inovação contínua e a integração de esforços militares e civis. Essas políticas devem ser adaptativas e capazes de responder à natureza dinâmica e evolutiva das ameaças híbridas. Somente por meio de uma abordagem integrada e coordenada será possível enfrentar eficazmente os desafios representados pela Guerra Híbrida e proteger a segurança e a estabilidade nacionais.

2.6 IMPLICAÇÕES DESSE ESTUDO PARA A MARINHA DO BRASIL OU MINISTÉRIO DA DEFESA

O estudo das características e implicações da Guerra Híbrida tem profundas implicações para a Marinha do Brasil e o Ministério da Defesa. Em um cenário global em que as ameaças híbridas se tornam cada vez mais prevalentes, entender e se

preparar para esses tipos de conflitos é essencial para a segurança nacional. A Guerra Híbrida, caracterizada pela combinação de operações militares convencionais com táticas irregulares como ciberataques, desinformação e guerra econômica, desafia as abordagens tradicionais de defesa e exige uma resposta integrada e adaptativa.

Para a Marinha do Brasil, uma das principais implicações deste estudo é a necessidade de fortalecer a cibersegurança. A proteção das redes de comunicação e dos sistemas de informação é fundamental para garantir a integridade das operações navais. A Marinha, como parte das Forças Armadas, deve investir em tecnologias avançadas de cibersegurança e desenvolver equipes especializadas em resposta a incidentes cibernéticos. Além disso, a criação de parcerias com outras agências governamentais e o setor privado é essencial para compartilhar informações e desenvolver uma defesa cibernética robusta. Como destaca o Departamento de Segurança Cibernética dos Estados Unidos (CISA, 2020), a colaboração entre diferentes setores é vital para proteger as infraestruturas críticas.

Outra implicação importante é a necessidade de adaptar as estratégias de defesa para incluir a guerra de informação e desinformação. A Marinha do Brasil deve estar preparada para enfrentar campanhas de desinformação que visem minar a confiança do público e semear divisões dentro da sociedade. Isso requer a implementação de programas de alfabetização midiática e digital para capacitar os membros da Marinha e a população em geral a reconhecer e resistir à desinformação. Além disso, a Marinha deve desenvolver capacidades de contra-propaganda para combater narrativas falsas e proteger a imagem das Forças Armadas. Como observado por Pomerantsev e Weiss (2014), a guerra de informação é uma ferramenta poderosa na Guerra Híbrida, e a capacidade de responder a ela é necessário para a defesa nacional.

A resiliência social é outro aspecto fundamental que o estudo destaca para a Marinha do Brasil e o Ministério da Defesa. A confiança nas instituições e a coesão social são essenciais para resistir a ataques híbridos. Investir em programas que promovam a coesão social e fortaleçam a confiança nas Forças Armadas é vital. Isso inclui iniciativas de comunicação transparente e eficaz durante crises, para garantir que o público receba informações precisas e confiáveis. A experiência da Finlândia em programas de educação em mídia e informação, que têm sido eficazes em aumentar a resiliência contra a desinformação (Ministry of Education and Culture of Finland, 2019), pode servir como um modelo para o Brasil.

A inovação contínua nas estratégias de defesa é fundamental para enfrentar as ameaças híbridas, que evoluem rapidamente (Dunlap, 2008). A Marinha do Brasil deve investir em inteligência artificial e machine learning para detectar e prever ataques, permitindo a identificação de vulnerabilidades e o teste da eficácia das respostas planejadas (Hehir, 2013). Isso assegura que a defesa se mantenha relevante diante de mudanças constantes (Koskenniemi, 2011).

A integração de esforços militares e civis também é crucial (Schmitt, 2012). A coordenação entre as Forças Armadas, agências governamentais e o setor privado garante uma resposta coesa às ameaças híbridas (Kraska, 2011). Comitês de segurança nacional e centros de comando unificados promovem a integração necessária para uma defesa robusta (Williams, 2013).

Além disso, o treinamento contínuo em todos os níveis é indispensável. Simulações de cenários de guerra híbrida garantem a preparação adequada para responder a uma variedade de ameaças (Guilfoyle, 2019). O constante desenvolvimento de conhecimentos e habilidades é essencial para a eficácia da defesa (Stiglitz, 2002).

Por fim, o Brasil deve participar ativamente de fóruns internacionais e buscar intercâmbio de conhecimento sobre defesa híbrida (Joyner, 2016). A cooperação com organizações como a OTAN pode trazer insights valiosos para aprimorar as estratégias nacionais (Schabas, 2017).

A análise das implicações da Guerra Híbrida destaca a necessidade de fortalecer a cibersegurança e promover a resiliência social (Beckman, 2017). O Brasil precisa se adaptar a essas ameaças para garantir sua defesa no cenário global (Held & McGrew, 2007).

2.7 FORTALECIMENTO DA CIBERSEGURANÇA

O fortalecimento da cibersegurança é uma componente crucial na defesa contra as ameaças híbridas, que combinam métodos tradicionais e não convencionais de guerra para alcançar objetivos estratégicos. No contexto da Guerra Híbrida, ciberataques são frequentemente utilizados para desestabilizar nações, afetar infraestruturas críticas e influenciar processos políticos e sociais. Portanto, desenvolver uma cibersegurança robusta é essencial para proteger a integridade nacional e garantir a resiliência contra essas ameaças multifacetadas.

A importância da cibersegurança é evidenciada por vários incidentes de alta visibilidade que demonstraram a vulnerabilidade das infraestruturas críticas a ataques cibernéticos. Por exemplo, o ataque cibernético contra a rede elétrica da Ucrânia em dezembro de 2015, atribuído a hackers russos, resultou em apagões significativos e destacou a capacidade dos ciberataques de causar danos físicos tangíveis (Kovacs, 2016). Este incidente sublinha a necessidade de sistemas de defesa cibernética que possam proteger infraestruturas críticas como redes elétricas, sistemas de transporte e instalações de comunicação.

Para fortalecer a cibersegurança, os Estados devem investir em tecnologias avançadas de detecção e mitigação de ameaças. Esses sistemas podem analisar grandes volumes de dados em tempo real, permitindo uma resposta rápida e eficaz a ataques cibernéticos. Além disso, a implementação de firewalls avançados, sistemas de criptografia e outras medidas de segurança pode dificultar a infiltração por agentes mal-intencionados (Conti, et al., 2018).

A criação de equipes de resposta a incidentes de segurança cibernética (CSIRTs[2]) é outra medida crucial para o fortalecimento da cibersegurança. Essas equipes são responsáveis por monitorar, identificar e responder a incidentes de segurança cibernética. Elas devem ser treinadas para lidar com uma ampla gama de ameaças, desde ataques de phishing, que é uma prática fraudulenta em que criminosos da computação se passam por entidades confiáveis para roubar informações pessoais e financeiras (Silva, 2021, p.45); até ataques de ransomware, tipo de programa maligno que criptografa dados do usuário, exigindo pagamento para restaurar o acesso (Silva, 2021, p.78); e ciberespionagem, que é o uso de técnicas digitais para obter informações confidenciais de governos ou empresas sem autorização (Silva, 2021, p.102). A capacidade de responder rapidamente a incidentes cibernéticos pode minimizar os danos e restaurar a funcionalidade dos sistemas afetados (Hausken, 2016).

A formação e o treinamento contínuos são essenciais para manter a eficácia das defesas cibernéticas. A evolução constante das ameaças cibernéticas requer que profissionais de segurança estejam atualizados com as últimas tendências e tecnologias. Programas de treinamento que simulam cenários de ataque cibernético podem ajudar a preparar as equipes de resposta para situações reais, permitindo-lhes praticar e refinar suas habilidades em um ambiente controlado. Além disso, a educação em

[2] CSIRTs (Computer Security Incident Response Teams) são equipes especializadas responsáveis por gerenciar e responder a incidentes de segurança cibernética

cibersegurança deve ser promovida em todos os níveis da sociedade, desde escolas até instituições governamentais e empresariais, para criar uma cultura de segurança que envolva todos os cidadãos (Von Solms & Van Niekerk, 2013).

Além das medidas técnicas, é urgente desenvolver políticas e regulamentações robustas de cibersegurança. Essas políticas devem definir claramente as responsabilidades de todos os atores envolvidos na proteção cibernética, desde governos até empresas privadas e indivíduos. Regulamentações rigorosas podem garantir que as empresas adotem práticas de segurança adequadas e que haja consequências legais para negligência em cibersegurança. A implementação de normas e padrões de segurança pode uniformizar as práticas de cibersegurança e garantir um nível básico de proteção em todas as áreas críticas (Bada, et al., 2015).

A resiliência cibernética é outro aspecto importante do fortalecimento da cibersegurança. A capacidade de uma nação se recuperar rapidamente de um ataque cibernético é tão importante quanto a prevenção do ataque em si. Isso envolve a criação de planos de contingência, redundâncias de sistemas e a realização de exercícios regulares de recuperação de desastres. A resiliência cibernética garante que os serviços essenciais possam continuar operando mesmo sob ataque, minimizando a interrupção e os danos causados por ciberincidentes (Linkov, et al., 2013).

A cibersegurança deve ser vista como um esforço contínuo e dinâmico, exigindo adaptação constante às novas ameaças e tecnologias. A colaboração entre o setor público e privado é fundamental, dado que muitas infraestruturas críticas são operadas por empresas privadas. O estabelecimento de parcerias público-privadas pode facilitar o compartilhamento de informações sobre ameaças e a implementação de medidas de segurança mais eficazes. Além disso, a pesquisa e o desenvolvimento em cibersegurança devem ser incentivados para criar novas soluções tecnológicas que possam enfrentar as ameaças emergentes (Humphreys, 2010).

O fortalecimento da cibersegurança é vital para proteger as nações contra as ameaças híbridas contemporâneas. Investir em tecnologias avançadas, criar equipes de resposta a incidentes, promover a cooperação internacional, desenvolver políticas robustas e fomentar a resiliência cibernética são passos essenciais para garantir a segurança cibernética. A capacidade de antecipar, detectar e responder a ataques cibernéticos de maneira eficaz é necessário para a defesa nacional e internacional no século XXI.

3 COOPERAÇÃO INTERNACIONAL

A cooperação internacional é um elemento crucial no combate às ameaças híbridas contemporâneas, que combinam métodos de guerra convencionais e não convencionais, como ciberataques, desinformação e manipulação econômica. A natureza transnacional dessas ameaças requer uma abordagem coordenada e colaborativa entre os Estados para garantir uma defesa eficaz. Nesse contexto, a cooperação internacional pode ser vista através de vários prismas, incluindo a troca de informações, a harmonização de políticas, a formação de alianças estratégicas e a participação em organizações internacionais.

A troca de informações é uma pedra angular da cooperação internacional na defesa contra ameaças híbridas. As ameaças cibernéticas, por exemplo, frequentemente transcendem fronteiras, e a troca rápida de informações sobre incidentes de segurança cibernética pode ajudar os países a se defenderem de ataques iminentes. Um exemplo de sucesso é o Fórum Europeu para a Resposta a Incidentes e Equipes de Segurança (FIRST), que facilita a cooperação entre equipes de resposta a incidentes de segurança cibernética (CSIRTs) em todo o mundo. A colaboração dentro do FIRST permite que os membros compartilhem informações sobre vulnerabilidades, técnicas de ataque e melhores práticas de defesa, fortalecendo a resiliência coletiva contra ciberameaças (Hausken, 2016).

A formação de alianças estratégicas é outra dimensão vital da cooperação internacional. A Organização do Tratado do Atlântico Norte (OTAN) exemplifica a importância das alianças na defesa contra ameaças híbridas. Em resposta ao crescente uso de táticas híbridas, a OTAN estabeleceu o Centro de Excelência para a Defesa Contra Ameaças Híbridas em Helsinque, na Finlândia. O centro serve como um hub para a pesquisa, a formação e o desenvolvimento de estratégias para combater ameaças híbridas, promovendo a colaboração entre os membros da OTAN e parceiros internacionais (OTAN, 2017). Além disso, a OTAN tem integrado considerações de cibersegurança em suas operações militares, reconhecendo que o domínio cibernético é tão importante quanto os domínios terrestre, marítimo e aéreo.

A participação em organizações internacionais também facilita a cooperação e a coordenação na defesa contra ameaças híbridas. A Organização das Nações Unidas (ONU), por meio de seu Grupo de Trabalho sobre Segurança da Informação, tem

promovido o diálogo entre Estados para desenvolver normas e princípios que governem o comportamento no ciberespaço. Essas discussões são necessárias para estabelecer um consenso internacional sobre a conduta aceitável e para desenvolver medidas de confiança que possam prevenir conflitos cibernéticos (United Nations, 2015).

A cooperação internacional também se estende ao desenvolvimento e à implementação de capacidades de defesa conjuntas. Exercícios multinacionais, como os realizados pela OTAN, são fundamentais para testar e aprimorar as capacidades de resposta a ameaças híbridas. Esses exercícios permitem que os participantes pratiquem a coordenação de operações militares, cibernéticas e de informação em cenários complexos e realistas. Por meio desses treinamentos, os aliados podem identificar lacunas em suas defesas e desenvolver estratégias mais eficazes para enfrentar ameaças híbridas (OTAN, 2019).

A resiliência cibernética, um componente essencial da defesa contra ameaças híbridas, também se beneficia da cooperação internacional. A iniciativa Global Forum on Cyber Expertise (GFCE) reúne governos, organizações internacionais e o setor privado para promover o desenvolvimento de capacidades cibernéticas em todo o mundo. O GFCE facilita o compartilhamento de conhecimentos e recursos, ajudando os países a fortalecerem suas defesas cibernéticas e a recuperarem-se rapidamente de ciberataques (GFCE, 2017).

A cooperação internacional é igualmente importante no combate à desinformação, uma tática chave da Guerra Híbrida. As campanhas de desinformação podem influenciar eleições, semear discórdia social e minar a confiança nas instituições democráticas. Para enfrentar essa ameaça, a UE criou o East StratCom Task Force, que monitora e combate a desinformação proveniente de fontes externas. Este grupo trabalha em estreita colaboração com Estados membros e parceiros internacionais para identificar e expor campanhas de desinformação, além de promover a alfabetização midiática entre os cidadãos (European External Action Service, 2018).

A colaboração entre o setor público e privado também é vital na defesa contra ameaças híbridas. Muitas infraestruturas críticas são operadas por entidades privadas, e a segurança dessas infraestruturas depende de uma parceria eficaz entre os governos e o setor privado. Iniciativas como o Fórum Econômico Mundial (WEF) em cibersegurança promovem a colaboração entre líderes governamentais e empresariais para fortalecer a segurança cibernética global. Por meio dessas parcerias, as melhores práticas de segurança podem ser compartilhadas e implementadas em uma

escala mais ampla, aumentando a resiliência geral contra ciberameaças (World Economic Forum, 2018).

A cooperação internacional é indispensável na defesa contra ameaças híbridas. A troca de informações, a harmonização de políticas, a formação de alianças estratégicas e a participação em organizações internacionais são todos componentes essenciais dessa cooperação. Além disso, a colaboração com o setor privado e o desenvolvimento de capacidades de defesa conjuntas são fundamentais para fortalecer a resiliência cibernética e combater a desinformação.

4 DESENVOLVIMENTO DE POLÍTICAS DE DEFESA HÍBRIDA

O desenvolvimento de políticas de defesa híbrida é essencial para enfrentar as ameaças complexas e multifacetadas representadas pela Guerra Híbrida. Esse tipo de conflito combina operações militares convencionais com ciberataques, desinformação, manipulação econômica e outras táticas não convencionais. Para enfrentar essas ameaças de maneira eficaz, os Estados precisam de uma abordagem integrada e adaptativa, que inclua o fortalecimento da cibersegurança, a cooperação internacional, a resiliência social e a inovação contínua nas estratégias de defesa.

O fortalecimento da cibersegurança é um pilar fundamental das políticas de defesa híbrida. Os ciberataques são uma das ferramentas mais utilizadas na Guerra Híbrida, permitindo que os adversários causem danos significativos a infraestruturas críticas, roubem informações sensíveis e desorganizem a sociedade civil. A criação de capacidades robustas de cibersegurança, incluindo sistemas avançados de detecção e mitigação de ameaças, é essencial para proteger as redes e sistemas de informação. Além disso, a implementação de firewalls avançados, sistemas de criptografia e outras medidas de segurança pode dificultar a infiltração por agentes mal-intencionados (Conti, et al., 2018). A formação de equipes de resposta a incidentes de segurança cibernética (CSIRTs) é crucial para monitorar, identificar e responder a incidentes de segurança cibernética. Essas equipes devem ser treinadas para lidar com uma ampla gama de ameaças, desde ataques de phishing até ataques de ransomware e ciberespionagem.

A cooperação internacional é outro componente vital no desenvolvimento de políticas de defesa híbrida. As ameaças híbridas frequentemente transcendem as fronteiras nacionais, tornando necessária uma colaboração estreita entre os Estados

para compartilhar informações e desenvolver respostas coordenadas. A União Europeia (UE) e a Organização do Tratado do Atlântico Norte (OTAN) são exemplos de organizações que promovem a cooperação cibernética. A Diretiva NIS (Segurança das Redes e da Informação) da UE estabelece requisitos de segurança para operadores de infraestruturas críticas em todos os Estados membros, garantindo um nível básico de segurança cibernética (European Commission, 2016).

As campanhas de desinformação visam minar essa confiança, criando divisões e semeando desconfiança. Investir em programas de alfabetização midiática e digital é vital para capacitar os cidadãos a reconhecer e resistir à desinformação. Além disso, a comunicação transparente e eficaz por parte dos governos durante crises é vital para manter a confiança pública e prevenir o pânico e a confusão que os adversários podem explorar.

A inovação contínua nas estratégias de defesa é essencial para enfrentar as ameaças híbridas em constante evolução. A natureza dinâmica da Guerra Híbrida significa que as táticas e tecnologias utilizadas pelos adversários estão em constante mudança. Os Estados devem adotar uma abordagem proativa na pesquisa e desenvolvimento de novas tecnologias e métodos de defesa. O uso de simulações e exercícios de guerra híbrida pode ajudar a identificar vulnerabilidades e testar a eficácia das respostas planejadas. O investimento em pesquisa e desenvolvimento deve ser uma prioridade para garantir que as forças de defesa estejam equipadas com as tecnologias mais avançadas e eficazes para enfrentar as ameaças futuras.

A integração de esforços militares e civis é fundamental para uma abordagem eficaz de defesa híbrida. Isso envolve a coordenação entre militares, agências governamentais, setor privado e a sociedade civil para garantir uma resposta coesa e abrangente às ameaças híbridas (Bachmann & Gunneriusson, 2015). A colaboração interinstitucional é essencial para garantir que todos os aspectos da defesa – desde a cibersegurança até a resiliência social – sejam abordados de maneira integrada e coordenada.

Além disso, a preparação para a Guerra Híbrida deve incluir a formação e treinamento contínuo de pessoal em todos os níveis. Isso envolve não apenas as forças armadas, mas também as agências de segurança, o setor privado e a sociedade civil. A educação contínua e a atualização de conhecimentos são essenciais para garantir que as capacidades de defesa permaneçam relevantes e eficazes diante de ameaças em constante mudança.

A transparência e a comunicação clara por parte dos governos são essenciais para manter a confiança pública durante crises híbridas. A gestão eficaz da comunicação de crises pode ajudar a combater a desinformação e garantir que o público receba informações precisas e confiáveis. Isso é particularmente importante durante ataques híbridos, em que a confusão e o pânico podem ser explorados pelos adversários para amplificar o impacto das suas operações. A comunicação proativa e transparente pode, portanto, fortalecer a resiliência social e ajudar a manter a coesão durante períodos de crise (Linvill & Warren, 2018).

Em conclusão, o desenvolvimento de políticas de defesa híbrida requer uma abordagem multifacetada que inclua o fortalecimento da cibersegurança, a cooperação internacional, a resiliência social, a inovação contínua e a integração de esforços militares e civis. Essas políticas devem ser adaptativas e capazes de responder à natureza dinâmica e evolutiva das ameaças híbridas.

5 CONCLUSÃO

A Guerra Híbrida emergiu como uma forma de conflito altamente complexa e multifacetada, desafiando as noções tradicionais de guerra e defesa. A crescente prevalência da Guerra Híbrida sublinha a necessidade urgente de os Estados desenvolverem políticas de defesa híbrida que sejam abrangentes, adaptativas e capazes de responder às ameaças dinâmicas e evolutivas que caracterizam esse tipo de conflito.

O fortalecimento da cibersegurança é um componente fundamental dessas políticas. Os ciberataques são uma das ferramentas mais utilizadas na Guerra Híbrida, permitindo que os adversários causem danos significativos a infraestruturas críticas, roubem informações sensíveis e desorganizem a sociedade civil sem recorrer a confrontos militares diretos.

A cooperação internacional também desempenha um papel crucial na defesa contra ameaças híbridas. A natureza transnacional dessas ameaças torna necessária uma colaboração estreita entre os Estados para compartilhar informações, desenvolver respostas coordenadas e estabelecer normas e padrões comuns de segurança. Organizações internacionais, como a OTAN e a União Europeia, têm um papel vital na promoção dessa cooperação, facilitando o intercâmbio de conhecimentos e a coordenação de políticas entre os seus membros. A criação de centros de excelência e

fóruns de cooperação, onde os Estados podem compartilhar melhores práticas e desenvolver estratégias conjuntas, é um passo importante na construção de uma defesa coletiva eficaz contra a Guerra Híbrida.

A promoção da coesão social e da confiança nas instituições também é crucial, pois uma sociedade unida e bem informada é menos suscetível a ser manipulada por campanhas de desinformação. Além disso, a comunicação transparente e eficaz por parte dos governos durante crises é vital para manter a confiança pública e prevenir o pânico e a confusão que os adversários podem explorar.

A realização de simulações e exercícios de guerra híbrida pode ajudar a identificar vulnerabilidades e testar a eficácia das respostas planejadas, garantindo que as estratégias de defesa sejam robustas e adaptáveis. O investimento em pesquisa e desenvolvimento deve ser uma prioridade para garantir que as forças de defesa estejam equipadas com as tecnologias mais avançadas e eficazes para enfrentar as ameaças futuras.

A integração de esforços militares e civis é fundamental para uma abordagem eficaz de defesa híbrida. A coordenação entre forças armadas, agências governamentais, setor privado e sociedade civil é necessária para garantir uma resposta coesa e abrangente às ameaças híbridas. Essa integração pode ser facilitada por meio da criação de comitês de segurança nacional e centros de comando unificados que reúnam representantes de diferentes setores para planejar e coordenar as respostas às crises. A colaboração interinstitucional é essencial para garantir que todos os aspectos da defesa – desde a cibersegurança até a resiliência social – sejam abordados de maneira integrada e coordenada.

Além disso, a preparação para a Guerra Híbrida deve incluir a formação e treinamento contínuo de pessoal em todos os níveis. Isso envolve não apenas as forças armadas, mas também as agências de segurança, o setor privado e a sociedade civil. Programas de treinamento que simulem cenários de guerra híbrida podem ajudar a preparar melhor todos os envolvidos para responder de maneira eficaz a uma ampla gama de ameaças. A educação contínua e a atualização de conhecimentos são essenciais para garantir que as capacidades de defesa permaneçam relevantes e eficazes diante de ameaças em constante mudança.

Em conclusão, a Guerra Híbrida representa um dos desafios mais complexos e urgentes para a segurança global contemporânea. A combinação de métodos de

guerra convencionais e não convencionais, ciberataques, desinformação e manipulação econômica cria um campo de batalha dinâmico e multifacetado. Para enfrentar essa ameaça, é necessária uma abordagem integrada e coordenada que inclua o fortalecimento da cibersegurança, a cooperação internacional, a resiliência social, a inovação contínua e a integração de esforços militares e civis. Somente por meio de uma abordagem abrangente e adaptativa será possível proteger os interesses nacionais e internacionais e garantir a segurança e a estabilidade diante das ameaças representadas pela Guerra Híbrida. A capacidade de antecipar, responder e se adaptar a essas ameaças será crucial para a defesa nacional e a segurança global no século XXI.

A combinação de métodos de guerra convencionais e não convencionais, como ciberataques, desinformação, sabotagem econômica e operações militares irregulares, cria um cenário de conflito dinâmico e multifacetado. Essa complexidade exige uma compreensão profunda das diversas táticas empregadas e uma capacidade de resposta rápida e eficaz para proteger a integridade e a soberania dos Estados.

Além disso, a natureza assimétrica dessas ameaças, que frequentemente operam abaixo do limiar de uma guerra aberta, desafia as estruturas tradicionais de defesa e segurança.

Diante desse cenário, a adaptação e a inovação nas estratégias de defesa são de suma importância. As políticas de defesa devem ser flexíveis e capazes de evoluir rapidamente para responder a ameaças em constante mudança. A inovação tecnológica desempenha um papel crucial nesse contexto, com o desenvolvimento de novas ferramentas e metodologias para a detecção e mitigação de ciberataques, bem como para a análise e combate à desinformação.

Além da inovação tecnológica, é essencial fomentar a cooperação internacional para enfrentar a natureza transnacional das ameaças híbridas. A colaboração entre Estados, organizações internacionais e o setor privado facilita a troca de informações, o desenvolvimento de normas comuns e a implementação de estratégias conjuntas de defesa. A integração de esforços militares e civis também é vital para garantir uma resposta coordenada e abrangente, que envolva todos os setores da sociedade.

A complexidade da Guerra Híbrida exige uma abordagem multidimensional que combine inovação tecnológica, cooperação internacional, resiliência social e integração de esforços militares e civis. Somente por meio de uma adaptação constante e da

implementação de estratégias de defesa inovadoras será possível enfrentar eficazmente as ameaças representadas por essa forma de conflito. A capacidade de antecipar, responder e se adaptar a essas ameaças será crucial para a segurança e a estabilidade das nações no século XXI.

REFERÊNCIAS

ARENQUE, G. C. Guerra mais longa da América: Estados Unidos e Vietnã, 1950-1975. São Paulo: McGraw-Hill, 2022.

BACHMANN, S. & GUNNERIUSSON, H. Hybrid Wars*: The 21st-century's new threats to global peace and security*. Abingdon: Routledge, 2015.

BACHMANN, S. D., & GUNNERIUSSON, H. Guerras Híbridas: As Novas Ameaças do Século 21 à Paz e Segurança Globais. Jornal Sul-Africano de Estudos Militares , ed. 21, 2015.

BADA, M., et al. *Cyber Security Awareness Campaigns: Why Do They Fail to Change Behaviour?*. *Computers & Security*, v.53, p.94-104, 2015.

BATEMAN, S.Liberdade de navegação e direito de passagem no Mar do Sul da China. *Asian Geopolitical Review*, v.18, n.1, p.67-83, 2020.

BYERS, M. A geopolítica do Ártico e as reivindicações territoriais russas." *Polar Studies Review*, v.37, n.1, p.12-28, 2018.

CHEUNG, T. A disputa no Mar do Sul da China e o uso estratégico de lawfare." *sian Maritime Review*, v.24, n3, p.45-58, 2018.

CISA. (2020). "Agência de Segurança Cibernética e Infraestrutura." Departamento de Segurança Interna. Disponível em: https://www.cisa.gov. Acesso: em 21 ago. 2024.

COMISSÃO EUROPEIA. (2016). "Diretiva sobre segurança de redes e sistemas de informação (Diretiva NIS)." Comissão Europeia. Disponível em: https://eur-lex.europa.eu. Acesso: em 21 ago, 2024.

CONNOLLY, R. A resposta da Rússia às sanções: como a política econômica ocidental está remodelando a economia política na Rússia. *Cambridge Review of International Affairs*, v.31, n.2, p.125-141, 2018.

CONTI, G., et al. *Countering Cyber Threats: The Evolution of Security Measures*. 2018. Springer.

GALEOTTI, M. Híbrido, ambíguo e não linear? Quão novo é o 'novo modo de guerra' da Rússia? *Pequenas Guerras e Insurgências*, v.27, n.2, p.282-301, 2016.

GÓMEZ, A. "Sanções e bloqueios no Estreito de Ormuz: uma análise jurídica." *International Law Journal*, v.21, n.4, p.77-93, 2019.

GUILFOYLE, D. *Interdição de Navegação e o Direito do Mar*. 2019. Imprensa da Universidade de Cambridge.

HAUSKEN, K. (2016). *Cybersecurity in Critical Infrastructure: A Risk-Based Approach*. 2016. Springer.

HEHIR, A. A permanência da inconsistência: a Líbia, o Conselho de Segurança e a responsabilidade de proteger. *Segurança Internacional*, v.38, n.1, p. 137-159, 2013.

HELD, D. & MCGREW, A. *Globalization/Anti-Globalization: Beyond the Great Divide*. 2007. Polity Press.

HERRING, G. C. *America's Longest War: The United States and Vietnam,* p*. 1950-1975*. 2002. McGraw-Hill.

HUGHES, J., & SASSE, G. Ideias de Poder e Conflito: Forças Ideacionais nas Fronteiras Russas e Ucranianas. *Política e Sociedades do Leste Europeu*, v.30, n.3, p.471-491, 2016.

HUGHES, J., & SASSE, G. *Conflict in Ukraine: A Comparative Perspective*. Cambridge University Press, 2016.

JOYNER, C. C. *International Law in the 21st Century: Rules for Global Governance*. Rowman & Littlefield, 2016.

KOSKENNIEMI, M. A Política do Direito Internacional. *Revista Europeia de Direito Internacional*, v. 20, n.1, p. 7-19, 2011.

KOVACS, E. (2016). Ucrânia: Novos ataques cibernéticos causam queda de energia. Semana de Segurança.Disponível em: (https:// https://www.securityweek.com/source-code-carberp-trojan-sale-cybercrime-underground/). Acessado em: 19 ago. 2024.

KRASKA, J. Operações de segurança marítima e o uso de lawfare no Golfo de Aden. *Naval Review*, v.55, n.2, p. 33-50, 2020.

KREPINEVICH, A. F. *O Exército e o Vietnã*. Imprensa da Universidade Johns Hopkins, 1986.

KREPINEVICH, A. F. *The Army and Vietnam*. Johns Hopkins University Press, 1986.

LINKOV, I., et al. Resilience Metrics for Cyber Systems. *Environment Systems and Decisions*, v. 33, n.4, p.471-476, 2013.

LINVILL, D. L. & WARREN, P. L. Troll Factories*: The Internet Research Agency and State-Sponsored Agenda Building. Computers in Human Behavior*, v.84, p.282-290, 2018.

LINVILL, D. L., & WARREN, P. L. Fábricas de trolls: a agência de pesquisa da Internet e a construção da agenda patrocinada pelo Estado. Revisão de Relações Públicas, v.44, n. 3, 2018.

MARTA, K. As escolhas de Putin: explicando a política externa russa e a intervenção na Ucrânia. *Washington Quarterly* , v.38, n.2, p.189-204, 2015.

MARTEN, K. Rússia, OTAN e segurança do Mar Negro: um novo ponto crítico para o conflito? PND. *Washington Trimestral*, v.38, n.2, p.133-148, 2015.

MINISTÉRIO DA EDUCAÇÃO E CULTURA DA FINLÂNDIA. (2019). Alfabetização midiática na Finlândia. Disponível em: https://www.minedu.fi. Acesso em: 20 ago, 2024.

OTAN. (2017). CdE Híbrido: Centro Europeu de Excelência para Combater Ameaças Híbridas. Disponível em: https://www.hybridcoe.fi. Acesso em: 20 ago, 2024.

OTTIS, R. Análise dos ataques cibernéticos de 2007 contra a Estônia da perspectiva da guerra de informação. Anais da 7ª Conferência Europeia sobre Guerra de Informação, 2008.

PARDO, R. Conflitos pesqueiros e a aplicação de regulamentos ambientais no Mar do Japão. *Environmental Policy Journal*, v.14, n.2, p. 89-105, 2019.

POMERANTSEV, P., & WEISS, M. (2014). A ameaça da irrealidade: como o Kremlin transforma a informação, a cultura e o dinheiro em armas.O intérprete. Disponível em: https://www.interpretermag.com. Acesso em: 20 ago, 2024.

POMERANTSEV, P., & WEISS, M. *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, 2014.

RID, T. *Medidas Ativas: A História Secreta da Desinformação e da Guerra Política*. New York: Farrar, Straus e Giroux. 2020.

SCHABAS, W. A. *Uma introdução ao Tribunal Penal Internacional*. Imprensa da Universidade de Cambridge, 2017.

SILVA, J. Segurança da informação: Protegendo Dados no Mundo Digital. São Paulo: Editora TeckPress, 2021.

VON SOLMS, R. & VAN NIEKERK, J. From Information Security to Cyber Security. *Computers & Security*, v.38, p.97-102, 2013.