ESCOLA DE GUERRA NAVAL

CMG KAYSEL COSTA RIBEIRO

O PAPEL DAS OPERAÇÕES DE INFORMAÇÃO NA EVOLUÇÃO DA GUERRA HÍBRIDA:

Como a Marinha do Brasil (MB) deverá se contrapor a essa nova ameaça.

RIO DE JANEIRO

2023

CMG KAYSEL COSTA RIBEIRO

O PAPEL DAS OPERAÇÕES DE INFORMAÇÃO NA EVOLUÇÃO DA GUERRA HÍBRIDA:

Como a Marinha do Brasil (MB) deverá se contrapor a essa nova ameaça.

Tese apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso de Política e Estratégia Marítimas 2023.
Orientador: CMG (RM1-FN) Jorge Luís de Araújo Mello.

RIO DE JANEIRO

2023

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.

ASSINATURA PELO GOV.BR
(LOCAL DA CHANCELA)

gov.br
Documento assinado digitalmente
KAYSEL COSTA RIBEIRO
Data: 01/12/2023 14:53:48-0300
Verifique em https://validar.iti.gov.br

AGRADECIMENTOS

À minha esposa, Maria Auxiliadora da Silva, pelo total apoio e incentivo, demonstrados durante o período no qual tive que me dedicar intensamente na elaboração deste trabalho. Seu companheirismo, sua amizade e seu amor é o que tenho de mais especial.

À minha mãe Sônia Rogeria Nunes Costa (*in memoriam*), à minha avó Imna Nunes Costa (*in memoriam*) e à minha tia Iza Nunes (*in memoriam*), que sempre souberam me educar da melhor forma possível, fazendo com que eu conseguisse cada vez mais buscar o crescimento intelectual e profissional.

Ao meu pai Francisco Ribeiro Filho (*in memoriam*), pelo apoio prestado durante a realização dos meus estudos.

Ao meu orientador, CMG (RM1-FN) Jorge Luís de Araújo Mello, pelas orientações seguras e precisas, pela transmissão de conhecimentos, pela paciência, pela dedicação, pela disponibilidade em sempre me atender, pela motivação, pelos conselhos, pelas correções realizadas no decorrer do trabalho e pela honestidade, que contribuíram de forma significativa para que eu conseguisse desenvolver a minha Tese.

Aos companheiros da turma do Curso de Política e Estratégia Marítimas do ano de 2023, com os quais tive a honra de compartilhar momentos de companheirismo e de aprendizado profissional.

E a todos os envolvidos direta ou indiretamente na sua contribuição para a elaboração desta Tese.

RESUMO

Devido aos diversos avanços tecnológicos ocorridos no final século XXI, tais como o advento da internet e das mídias sociais, a informação atingiu uma relevância e um protagonismo, conforme jamais visto no cenário mundial, principalmente devido à velocidade com que é transmitida, sendo empregada de forma contundente no contexto da Guerra Híbrida. Apesar de não possuir uma definição mundialmente aceita e uma clareza bem definida, a Guerra Híbrida vem sendo empregada em diversas partes do mundo e por diversos tipos de atores. Países e organismos importantes, como Estados Unidos da América (EUA), União Europeia (UE), Federação da Rússia e Organização do Tratado do Atlântico Norte (OTAN), têm se dedicado a estudar profundamente o assunto. Foram criados centros de excelência específicos para lidar com o tema, que é extremamente complexo e carece de estudos mais aprofundados. Entender a diferença entre as Ameaças Híbridas e a Guerra Híbrida torna-se um dos objetivos deste trabalho. A elaboração de metas estratégicas genéricas, que servem de modelo para que países que ainda não possuem as suas definidas consigam elaborar as mesmas é essencial. Conhecer a importância da comunicação estratégica e realizar um estudo aprofundado de como a desinformação é empregada nesse contexto, também são primordiais para lidar com esse novo tipo de ameaça. A análise da estratégia adotada pela OTAN para se preparar, dissuadir e defender contra as Ameaças Híbridas, observando o seu Plano de Ação de Prontidão (PAP) e a sua Força de Resposta (FR) é muito importante. O estudo sobre a Guerra Híbrida Marítima e as Ameaças Híbridas Marítimas adotadas pela República Popular da China, assim como os possíveis cenários para as Ameaças Híbridas Marítimas, elaborados pelo Centro de Excelência para Combater Ameaças Híbridas denominado como *Hybrid Coe*, localizado em Helsinque, na Finlândia, nos ajudam a vislumbrar medidas a serem implementadas na Marinha do Brasil (MB). Finalmente, após essas análises, será aplicado o DOPEMAI, constante no Guia de Planejamento Baseado em Capacidades (PBC) na Guerra Híbrida, de forma a verificar qual o nível de preparo que a MB possui atualmente para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida ofensiva perpetrada por um ator estatal ou não estatal externo. Serão contempladas algumas ações para elevar a capacidade de resposta da MB para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida de forma a reduzir a sua vulnerabilidade no tocante a essas novas ameaças.

Palavras-chave: Informação; Guerra Híbrida; Ameaça Híbrida.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ACISO	Ações Cívico-Sociais
AHM	Ameaça Híbrida Marítima
AJB	Águas Jurisdicionais Brasileiras
APEL	Aprestamento Eletrônico
CAN	Conselho do Atlântico Norte
CCSM	Centro de Comunicação Social da Marinha
CDDGN	Centro de Desenvolvimento Doutrinário de Guerra Naval
CDS	Conselho de Defesa Sul-Americano
CEMOI	Curso de Estado-Maior para Oficiais Intermediários
CEMOS	Curso de Estado-Maior para Oficiais Superiores
CFCA	Comando das Forças Conjuntas Aliadas
CGE	Capacidade de Guerra Eletrônica
CIAA	Centro de Instrução Almirante Alexandrino
CIABA	Centro de Instrução Almirante Braz de Aguiar
CIAGA	Centro de Instrução Graça Aranha
CIAW	Centro de instrução Almirante Wandenkolk
CIM	Centro de Inteligência da Marinha
CN	Colégio Naval
CINDACTA	Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo
CNUDM	Convenção das Nações Unidas sobre o Direito do Mar
COI	Capacidade Operacional Inicial
COM3°DN	Comando do 3° Distrito Naval
ComDiv-2	Comando da 2ª Divisão da Esquadra
COMPERJ	Complexo Petroquímico do Estado do Rio de Janeiro
ComSoc	Comunicação Social
CoNavOpEsp	Comando Naval de Operações Especiais
C-PEM	Curso de Política e Estratégia Marítimas

CRI	Capacidade Relacionada à Informação
DCIS	Divisão Conjunta de Inteligência e Segurança
DIH	Direito Internacional Humanitário
DM	Direito do Mar
DMI	Direito Marítimo Internacional
EB	Exército Brasileiro
EGN	Escola de Guerra Naval
EI	Estado Islâmico
EN	Escola Naval
END	Estratégia Nacional de Defesa
EUA	Estados Unidos da América
ex-URSS	ex-União das Repúblicas Socialistas Soviéticas
FA	Forças Armadas
FAA	Forças de Acompanhamento Aliadas
FAB	Força Aérea Brasileira
FAP	Forças de Alta Prontidão
FMM	Forças Marítimas Multinacionais
FN	Forças Navais
FNC	Forças Navais Chinesas
FNCH	Forças Navais Civis Híbridas
FNP	Forças Navais Permanentes
FopEsp	Forças de Operações Especiais
FR	Força de Resposta
FSM	Força de Segurança Marítima
FTCAP	Força-Tarefa Conjunta de Alta Prontidão
GALC	Grupo de Apoio Logístico Conjunto
GC	Guarda Costeira
GCC	Guarda Costeira Chinesa
GE	Guerra Eletrônica

GHM	Guerra Híbrida Marítima
GIFA	Grupo Inicial de Forças de Acompanhamento
GMP	Grupo Marítimo Permanente
GNL	Gás Natural Liquefeito
GPCM	Grupos Permanentes de Contramedidas de Minas
GT	Grupo de Trabalho
Hybrid CoE	Centro Europeu de Excelência para Combater Ameaças Híbridas
LBDN	Livro Branco de Defesa Nacional
MAE	Medidas de Ataque Eletrônico
MAGE	Medidas de Apoio a Guerra Eletrônica
MB	Marinha do Brasil
MD	Ministério da Defesa
MM	Milícia Marítima
MMC	Milícias Marítimas Chinesas
MPE	Medidas de Proteção Eletrônica
MRE	Ministério das Relações Exteriores
NBQR	Nuclear, Biológico, Químico e Radiológico
ONU	Organização das Nações Unidas
OpEsp	Operações Especiais
OpInfo	Operações de Informação
OpPsc	Operações Psicológicas
OTAN	Organização do Tratado do Atlântico Norte
PAP	Plano de Ação de Prontidão
PBC	Planejamento Baseado em Capacidades
PC	Plataforma Continental
PEM	Plano Estratégico da Marinha
PIB	Produto Interno Bruto
PM	Patrulhas Marítimas
PND	Política Nacional de Defesa

PRG	Plano de Resposta Graduada
PTD	Processo de Tomada de Decisão
QJN	Quadros Jurídicos Nacionais
RE	Regras de Engajamento
RETRON	Reconhecimento Eletrônico
RI	Relações Internacionais
RP	Relações Públicas
SisGAAz	Sistema de Gerenciamento da Amazônia Azul
SISFRON	Sistema Integrado de Monitoramento de Fronteiras
SISNC2	Sistema Naval de Comando e Controle
SIVAM	Sistema de Vigilância da Amazônia
TI	Tecnologia da Informação
TIC	Tecnologia de Informação e Comunicação
TTC	Trabalho de Conclusão de Curso
UE	União Europeia
UIF	Unidades de Integração de Forças
ZEE	Zona Econômica Exclusiva

SUMÁRIO

1 INTRODUÇÃO

A Guerra Cibernética e a Guerra de Informação são os principais mecanismos atualmente empregados no contexto da Guerra Híbrida, sendo a Ucrânia um verdadeiro laboratório para que a Federação da Rússia conseguisse comprovar a sua aplicação no campo de batalha. (POLYAKOVA *et al*., 2020).

Esta tese tem como propósito analisar qual o papel das Operações de Informação (OpInfo) na evolução da Guerra Híbrida, servindo como base metodológica a estudos para que a Marinha do Brasil (MB) se contraponha à ameaça advinda dessa nova realidade.

Em virtude de ser um assunto novo e com poucas referências em âmbito nacional, o referencial teórico será sustentado por uma robusta base teórica pertinente, retirada de publicações estrangeiras, conceitos de Relações Internacionais (RI), doutrinas militares e em sites da União Europeia (UE) e da Organização do Tratado do Atlântico Norte (OTAN).

Além disso, será realizada uma fundamentação teórica amparada na teoria de Carl Von Clausewitz e no ciclo OODA de John Richard Boyd (BARBOZA; TEIXEIRA, 2020; CLAUSEWITZ, 2010).

A pesquisa científica será a metodologia empregada para a elaboração deste trabalho. O método escolhido será o dedutivo, realizado por meio da leitura de artigos acadêmicos internacionais e nacionais, livros, diversos sites da UE e OTAN. Será realizado um estudo descritivo amparando-se em referências bibliográficas existentes sobre o assunto em lide. Após o desenvolvimento desse estudo, será realizada uma conclusão, amparando-se nas conclusões parciais elaboradas ao final de cada capítulo, com o objetivo de obter-se embasamento para que a MB consiga se contrapor a essa nova ameaça.

Buscando-se entender a contextualização do assunto em questão e conforme o preconizado no EMA-335 (Doutrina de Operações de Informação da Marinha), podemos observar que os países mais poderosos do mundo têm sofrido grande influência em suas ações militares, principalmente devido a nova Era da Informação[1]. A ex-União das Repúblicas

1 A Era da Informação sucede a Era industrial e é proveniente de diversas mudanças tecnológicas e digitais ocorridas em todo o mundo, tendo seu início provavelmente entre o período de 1950 e 1970. A popularização da internet segue como sendo o seu marco principal. As diversas indústrias, tais como informática, robótica e genética, obtém grande relevância nessa conjuntura. A transição da Era Industrial para a Era da Informação foi marcada pela

Socialistas Soviéticas (ex-URSS) e os Estados Unidos da América (EUA), notaram a relevante importância da dimensão informacional no decorrer dos conflitos do Afeganistão (1979 – 1989) e do Vietnã (1955 – 1975), por ocasião do período da Guerra Fria (1947 – 1991). Devido ao fato dos seus oponentes possuírem habilidades para explorar o conflito em outros níveis, a ex-URSS e os EUA foram derrotados em suas campanhas militares e retiraram suas tropas, apesar de possuírem capacidades militares bastante superiores em comparação às capacidades dos seus oponentes (BRASIL, 2018).

Devido ao advento da evolução da informação e dos recentes conflitos ocorridos ao redor do mundo, surgiram novos conceitos denominados de Guerra Híbrida e Ameaças Híbridas. Apesar de atualmente não haver uma definição consensual de Guerra Híbrida, o assunto está sendo muito bem explorado pela UE, pela OTAN e pela Federação da Rússia, ainda que com denominações diversas, principalmente em face dos episódios ocorridos no leste da Ucrânia que resultaram na anexação da Crimeia em 2014. (LEAL, 2016). Observa-se ainda que a República Popular da China também se encontra bem evoluída no emprego de tal concepção.

Sendo assim, esta tese tem como objetivo pesquisar como a MB deverá empregar as Operações de Informação para se contrapor à Guerra Híbrida?

Ainda de acordo com o EMA-335, atualmente as Operações Militares encontram-se dentro de um ambiente onde a velocidade da informação e o seu alcance, principalmente devido à rápida evolução da internet e das mídias sociais, fazem com que elas tenham uma grande dependência da dimensão informacional do conflito (BRASIL, 2018).

Segundo o Centro Europeu de Excelência para Combater Ameaças Híbridas (*Hybrid CoE*), localizado em Helsinque na Finlândia, estamos atravessando atualmente uma "Era de Ameaças Híbridas", em que atores não estatais e estatais estão desafiando as instituições e países que eles enxergam como um potencial concorrente, oponente ou ameaça, contra seus objetivos e interesses. A quantidade de atividades e de métodos que se encontram à sua disposição é bastante diversificada, dentre as quais podemos citar como exemplos: chantagem comercial e econômica, obtida por meio de embargos; terrorismo; influenciar informações; minar as instituições internacionais ao tornar as suas regras ineficazes; explorar as

criação de computadores, microprocessadores e fibra ótica (ROCKCONTENT, 2019).

vulnerabilidades críticas tal como as deficiências logísticas, citando assim, os dutos de abastecimento de energia; etc. (HOFFMAN, 2007; NATO, 2023; WIELAND, 2022).

Com a finalidade de atingir o objetivo acima descrito, esta tese abordará além dessa introdução, a elaboração de mais 5 capítulos, sendo que no capítulo 2, será realizada uma análise sobre o conceito de Ameaça Híbrida e Guerra Híbrida com o intuito de entender a sua contextualização. Será apresentada a definição de metas estratégicas para combater a mesma. Será apresentando um modelo de *Framework* para combater a Guerra Híbrida. Será abordada a importância do emprego da comunicação estratégica contra Ameaças Híbridas e por último será dada ênfase para a "Desinformação", que é considerada uma das principais ferramentas da Guerra Híbrida.

Segundo Jonsson (2021), o local mais importante para a Guerra Híbrida está concentrado no domínio da informação. Atualmente a legitimidade, o poder e a forma como entendemos o mundo está regularizado pelas mídias sociais. Dessa forma, no capítulo 3, serão abordadas as OpInfo, para entendimento de sua dinâmica no contexto da Guerra Híbrida, assim como o seu papel na evolução da mesma.

No capítulo 4, será realizada uma análise com relação ao tipo de estratégia adotada pela OTAN para se preparar, dissuadir e defender contra Ameaças Híbridas, observando o seu Plano de Ação de Prontidão (PAP) e a sua Força de Resposta (FR) contra as Ameaças Híbridas.

O capítulo 5 abordará os aspectos intrínsecos da Guerra Híbrida Marítima (GHM) e as Ameaças Híbridas Marítimas (AHM), onde será estudada a questão atinente às "Milícias Marítimas Chinesas" (MMC), também intituladas como "Forças Navais Civis Híbridas" (FNCH) e serão analisados os possíveis cenários para as AHM, por meio de estudos realizados pelo *Hybrid CoE*.

No capítulo 6 será observado o DOPEMAI, constante no Guia de Planejamento Baseado em Capacidades (PBC), com o intuito de analisarmos qual o nível de preparo que a MB possui atualmente para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida ofensiva perpetrada por um ator estatal ou não estatal externo.

Serão ainda contempladas algumas ações para elevar a capacidade de resposta da MB para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida de forma a reduzir a sua vulnerabilidade no tocante a essas novas ameaças.

2 ENTENDENDO A GUERRA HÍBRIDA

O presente capítulo tem como objetivo realizar uma análise desse complexo fenômeno denominado Guerra Híbrida, que cada vez mais vem sendo adotado nos diversos conflitos modernos. Dessa forma, busca-se entender esse novo tipo de guerra, amparando-se na fundamentação teórica do general prussiano Carl Von Clausewitz, pois quando se realiza um estudo sobre temas intrinsecamente relacionados a guerra, não há como desassociá-lo desse grande estrategista militar.

Sendo assim, procuraremos compreender a definição de Guerra Híbrida e Ameaça Híbrida e a diferença entre ambas. Serão apresentadas as definições de metas estratégicas e um modelo de *Framework*[2] para combater a Guerra Híbrida.

Será abordada a importância do emprego da comunicação estratégica contra Ameaças Híbridas e, por último, será dada ênfase para a "Desinformação", que é considerada uma das principais ferramentas da Guerra Híbrida.

O advento da Tecnologia de Informação e Comunicação (TIC)[3] causou uma alteração na maneira como nos comunicamos, nos relacionamos e principalmente na maneira como nos informamos. A criação e a evolução da internet possibilitou que milhares de pessoas em todo o planeta pudessem acessar essa extraordinária fonte de informações, principalmente por meio de tablets, smartphones e notebooks (GIL, 2019).

A comunicação foi notoriamente uma das áreas onde a disseminação da internet teve maior impacto, tanto no conteúdo em si como no alcance ao público e na estrutura de mídia. Além de ter que se contrapor ao aparecimento de novos meios digitais, os meios tradicionais

---

2 O Framework no contexto da Guerra Híbrida tem como objetivo fornecer uma abordagem abrangente com a finalidade de melhorar o quadro de respostas frente aos desafios impostos pelas Ameaças Híbridas aos cidadãos, à segurança colectiva de uma comunidade e ao Estado. Ele engloba diversos instrumentos relevantes, políticas e vários integrantes com o intuito de mitigar e combater os impactos provocados pelas Ameaças Híbridas de uma maneira mais coordenada (COMISSÃO EUROPEIA, 2016).

3 TIC são os componentes e a infraestrutura que possibilitam a computação moderna, ou seja, são todos os aplicativos e sistemas, dispositivos, componentes de rede, que combinados possibilitam que organizações (ou seja, governos, agências sem fins lucrativos, empresas criminosas) e pessoas relacionem-se no mundo digital (PRATT, 2019).

tiveram que adequar a sua estrutura a uma demanda crescente de informações de seus leitores, assim como a sua organização a novos formatos (GIL, 2019).

Devido à relevante importância dos meios de comunicação nas democracias consolidadas, a ávida procura por informação pode gerar dúvidas quanto à qualidade e à credibilidade da mesma, motivo de elevada preocupação. Atualmente a rapidez no fluxo de informações, seja por redes sociais, sites ou mídias, tem um elevado impacto na opinião pública. A constante necessidade pela produção de notícias condicionou a qualidade da informação, devido à grande volatilidade gerada (GIL, 2019).

Atualmente as novas tecnologias possibilitam conquistar objetivos estratégicos com efeitos cognitivos e não convencionais. Algumas formas de tecnologia, como a mídia social, possibilitam que um ator consiga atingir as principais infraestruturas e instituições de um Estado. Dessa forma, torna-se possível a invasão de um território sem o emprego de componentes militares convencionais, ou seja, apenas empregando meios não convencionais (DANIK; MALYARCHUK; BRIGGS, 2017).

Segundo Leal (2016), em virtude da evolução da informação e dos recentes conflitos observados ao redor do planeta, surgiu um novo conceito denominado de “Guerra Híbrida”. Apesar de atualmente não haver uma definição consensual de Guerra Híbrida, o assunto está sendo amplamente estudado pela União Europeia (UE), pela Organização do Tratado do Atlântico Norte (OTAN) e pela Federação da Rússia, ainda que com denominações diversas, especialmente em razão da anexação da Crimeia, ocorrida em 2014 (LEAL, 2016).

Podemos observar que a natureza dos conflitos pode permanecer a mesma, porém o “*modus operandi*” como eles são travados foi notoriamente alterado. Atualmente os conflitos são travados de maneiras novas, diferentes e inovadoras, usando-se cada vez menos a força cinética[4] ou letal (BILAL, 2021).

A partir do momento que os Estados começaram a empregar Tecnologia da Informação (TI) e atores não estatais, para subjugar seus oponentes durante um conflito

4 A Força cinética no contexto da Guerra Híbrida, refere-se a realização de um ataque físico a determinados tipos de alvos específicos, obtidos por meio do emprego de mísseis, aeronaves, veículos aéreos nao tripulados, ou por outros tipos de sistemas de armas (POMERLEAU, 2023).

armado direto ou na ausência desse, o conceito Guerra Híbrida ganhou importância e significativa relevância no contexto (BILAL, 2021).

2.1 Fundamentação teórica amparada na Teoria de Clausewitz

Como o escopo desta tese tem em sua essência o tema central “Guerra”, pode-se se basear no conceito de trindade paradoxal de Clausewitz para analisar a evolução da Guerra para a Guerra Híbrida.

Em sua obra “DA GUERRA”, Clausewitz (2010, p. 7) ressalta que “A guerra é, pois, um ato de violência destinado a forçar o adversário a submeter-se à nossa vontade”. Além disso, ele enfatiza que: “Não falta, portanto, senão o acaso para fazer da guerra um jogo, e é o que costuma acontecer na maioria dos casos” (CLAUSEWITZ, 2010, p. 24). Por último, ele descreve que: “A guerra é uma simples continuação da política por outros meios” (CLAUSEWITZ, 2010, p. 27).

Pode-se constatar a total subordinação da guerra à política, segundo a visão de Clausewitz. Em sua obra, ele descreve o motivo original da guerra como sendo o objetivo político, o qual será capaz de determinar a quantidade de esforços a ser empregada, assim como o objetivo militar a ser obtido (ČAJIĆ, 2016).

A teoria da Trindade de Clausewitz pode ser melhor compreendida por dois ângulos diferentes, a primeira formulada por componentes abstratos, tais como: o ódio, a animosidade e a escalada da violência; o acaso e o jogo das probabilidades; a sua subordinação à política, assim como a segunda formulada pelos atores: população; o comandante e o seu exército; e o governo legitimamente constituído (BASSFORD, 2007 *apud* MARENUCCI, 2021).

Segundo Clausewitz, a forma a ser empregada para que o inimigo faça a nossa vontade é utilizando a força, por meio da guerra. Apesar de no mundo atual os conflitos fazerem uso de diversos tipos de ameaças, tais como crime organizado, terrorismo e cartéis de drogas, pode-se observar que a definição de Clausewitz tem a sua relevância no contexto atual, mesmo que com algumas ressalvas (ČAJIĆ, 2016).

Devemos nos ater a um ponto crucial, pois a guerra realizada na época de Clausewitz era diferente da guerra realizada nos dias atuais, principalmente devido ao seu aspecto não cinético, como a Guerra de Informação[5]. O advento do desenvolvimento tecnológico e da globalização possibilita que os atores consigam enviar mensagens por meio de uma grande variedade de veículos de informação. A disseminação de informações atualmente tem um papel essencial para angariar corações e mentes, para obter vantagem na guerra (ČAJIĆ, 2016).

Analisando a trindade de Clausewitz, Forças Armadas (FA), governo e povo, observa-se que as pessoas são extremamente sensíveis no que diz respeito ao apoio à guerra, e com relação a esse aspecto pode-se concluir que sem o apoio público, torna-se bastante complexo conduzir uma guerra com sucesso (ČAJIĆ, 2016).

Atualmente a sociedade é vista como um alvo extremamente valioso para agressores externos, devido ao aumento de sua importância no esforço de guerra. Os objetivos do esforço de guerra poderão ser melhor obtidos se o Estado conseguir dominar as mentes das pessoas na sociedade do Estado-alvo. Dessa forma, o Estado agressor pode utilizar a sociedade do Estado-alvo como uma ferramenta à sua disposição (DUMLUPINAR; EROL, 2020).

Outrossim, pode-se observar que, apesar do avanço tecnológico, do aparecimento de diversos tipos de atores e da globalização, não houve mudanças significativas na essência da guerra, uma vez que seus objetivos continuam visando a questão política, sendo assim pode-se constatar que os componentes clássicos da estratégia militar têm a sua validade confirmada para o emprego nos conflitos contemporâneos (MAHNKEN, 2010 *apud* MARENUCCI, 2021).

Realizando-se uma análise mais aprofundada da obra de Clausewitz, pode-se observar que ele faz uma comparação da guerra com um camaleão, uma vez que ela se

5 A Guerra de Informação visa salvaguardar o acesso à própria informação, controlando o próprio espaço informacional, enquanto adquire e utiliza a informação do oponente, interrompendo o fluxo de informação e destruindo seus sistemas de informação, de forma a obter uma vantagem de informação sobre o oponente. Ela utiliza-se de elementos inovadores, como o advento do desenvolvimento tecnológico, que resulta na disseminação de informações em maior escala e de forma mais rápida. Disponível em: <https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4- information-warfare.pdf>. Acesso em: 19 abr. 2023.

manifesta de formas variadas e se adapta a diferentes situações porém devido à sua essência intrínseca, ela mantêm suas próprias características. O camelão, apesar de possuir a capacidade de poder alterar a sua cor, conforme o tipo de ambiente em que se encontra, continua sendo um camaleão. Fato semelhante ocorre na guerra, pois apesar do surgimento de inúmeras inovações tecnológicas, a guerra não perdeu a sua essência e suas características constantes na trindade de Clausewitz (ARON, 1986 *apud* MARENUCCI, 2021).

2.2 Definindo a Guerra Híbrida e a Ameaça Híbrida

A origem do termo Guerra Híbrida é um pouco confusa e não há um consenso. Estudos apontam que, para alguns autores, o General estadunidense Robert Walker foi o criador do termo, apresentando-o em sua dissertação de mestrado, em 1998. Outros relatam que a origem ocorreu em 2002, como tentativa de explicar as ações de natureza tática desencadeadas na Guerra da Chechênia (1994 – 1996). O conceito adquiriu conteúdo teórico e se tornou popular a partir de 2005, com a publicação do artigo Future Warfare: The Rise of Hybrid Warfare, do General James N. Mattis e do Tenente-Coronel Frank G. Hoffman. E mais tarde, em 2007, com a publicação do Livro Conflict in the 21st Century: The Rise of Hybrid Wars, de autoria do Tenente-Coronel Frank G. Hoffman (GIL, 2019).

Como forma de melhor compreender o assunto que está sendo estudado, descrevem-se alguns conceitos atinentes aos termos Guerra Híbrida e Ameaça Híbrida. A definição de Frank G. Hoffman é a mais empregada por estudiosos do assunto e ela ressalta que:

> As Guerras Híbridas podem ser conduzidas por Estados e por uma variedade de atores não estatais. As Guerras Híbridas incorporam uma variedade de diferentes modos de guerra, incluindo capacidades convencionais, táticas e formações irregulares, atos terroristas, incluindo violência e coerção indiscriminada e desordem criminal. Essas atividades multimodais podem ser conduzidas por unidades separadas, ou mesmo pela mesma unidade, mas são geralmente operacional e taticamente dirigidas e coordenadas dentro do campo de batalha principal para alcançar efeitos sinérgicos. (HOFFMAN, 2007, p.14, tradução nossa).

Segundo Rodrigues (2021), conforme acima conceituado por Frank G. Hoffman, diversificadas formas de conflitos, entre o uso de tecnologias e os combatentes, caracterizam a guerra. Podem ser empregados uma variedade de tipos de força, no mesmo momento por oponentes sofisticados e flexíveis. Ele sugere ainda que os conflitos futuramente poderão incluir organizações híbridas, empregando um diversificado conjunto de habilidades, como a empregada pelo Hezbollah[6] contra o Estado de Israel no ano de 2006 (RODRIGUES, 2021).

Frank G. Hoffman estabelece a seguinte definição de Ameaça Híbrida em seu artigo "Hybrid vs. Compound War. The Janus choice: Defining today's multifaceted conflict".

> A Ameaça Híbrida é definida como qualquer adversário que emprega simultaneamente e de forma adaptativa uma mistura fundida de armas convencionais, táticas irregulares, terrorismo e comportamento criminoso no espaço de batalha para obter seus objetivos políticos (HOFFMAN, 2009, p.2, tradução nossa).

Segundo o Centro de Excelência para Combater Ameaças Híbridas, denominado como *Hybrid Coe*, localizado em Helsinque na Finlândia, a definição de Ameaça Híbrida refere-se a uma ação praticada por atores não estatais ou estatais, com a finalidade de prejudicar ou minar um determinado alvo, atuando diretamente na sua tomada de decisão no nível institucional, estadual, local ou regional (HYBRID COE, 2023).

Essas ações são sincronizadas e coordenadas, tendo como finalidade atingir as vulnerabilidades das instituições e dos Estados democráticos legitimamente constituídos. As atividades podem ser realizadas nos domínios militar, econômico, civil, político ou de informação. Elas são realizadas empregando-se uma grande quantidade de meios e planejadas de forma que seja difícil de se atribuir a responsabilidade ao real autor, tornando complexa a sua detecção (HYBRID COE, 2023).

---

6 O Hezbollah foi fundado no ano de 1982 em resposta às ações israelenses no Líbano, sendo considerado uma forte milícia xiita com diversas aspirações políticas. Essa milícia é apoiada por aliados anti-israelenses, como o Irã e a Síria, os quais têm disponibilizado para o mesmo treinamento, financiamento e equipamentos (MCCULLOH; JOHNSON, 2013).

A ação híbrida tem como característica a ambiguidade[7], uma vez que os atores híbridos fazem com que as fronteiras da política internacional se tornem obscuras, operando assim nas interfaces entre ilegal e legal, paz e guerra, interno e externo. A ambiguidade é gerada pela combinação de meios não convencionais e convencionais, tais como: operações cibernéticas, desinformação, diferentes formas de atividades criminosas, distúrbios ou ataques a infraestruturas críticas, uso assimétrico de meios militares e de guerra e interferência no debate político ou nas eleições (HYBRID COE, 2023).

Analisando a UE, observa-se que o seu Quadro Conjunto de 2016 descreve o conceito de Ameaça Híbrida alertando que, embora as definições de Ameaças Híbridas necessitem manterem-se flexíveis de forma a responder à sua natureza em evolução e devido a sua variação, o conceito em si tem como objetivo deter o conjunto de atividades subversivas e coercitivas, métodos não convencionais e convencionais (ou seja, tecnológicos, militares, econômicos e diplomáticos), os quais podem ser empregados de forma coordenada por atores não estatais ou estatais para obterem objetivos específicos, mantendo-se abaixo da fronteira da guerra declarada formalmente (WEISSMANN *et al.*, 2021).

Normalmente existe uma ênfase em gerar ambiguidade e em explorar as vulnerabilidades do alvo, de forma a dificultar os processos de tomada de decisão. A utilização de mídias sociais, com o intuito de obter o controle da narrativa política, recrutar, radicalizar e direcionar atores substitutos, e o emprego de grandes campanhas de desinformação podem ser meios a serem explorados pelas Ameaças Híbridas (WEISSMANN *et al.*, 2021).

Segundo Weissmann *et al.* (2021), a OTAN define Guerra Híbrida como sendo o local onde uma ampla gama de medidas civis, paramilitares e militares, encobertas e abertas, são empregadas em um projeto altamente integrado, onde o oponente busca influenciar importantes tomadores de decisão e influentes formuladores de políticas, combinando

7 A ambiguidade nesse contexto pode ser entendida como o conjunto de ações hostis em que o Estado encontra dificuldades para atribuir, identificar ou definir o emprego coercitivo da força. O processo de tomada de decisão do adversário fica comprometido com o emprego da ambiguidade. Ele dificulta a implementação de uma reposta política ou militar. Analisando o enfoque militar, pode-se observar que a ambiguidade tem como meta a deslegitimização da capacidade de efetuar uma resposta pelo emprego da força militar, ou seja, ela visa tornar tal ato politicamente irracional. Analisando o enfoque estratégico, a Guerra Híbrida estatal é planejada para evitar que ocorra a guerra convencional (REICHBORN-KJENNERUD; CULLEN, 2017).

esforço subversivo com operações cinéticas. Como forma de evitar retribuição ou imputação, o agressor na maioria das vezes recorre a ações clandestinas.

Métodos híbridos de guerra, como sabotagem, dissimulação, propaganda e diversas outras táticas não militares, são empregados a bastante tempo, como forma de desestabilizar os adversários. O que podemos observar nos ataques realizados nos últimos anos é sua intensidade, velocidade e escala, facilitadas pela interconectividade global e pela rápida mudança tecnológica (WEISSMANN *et al.*, 2021).

Conforme Weissmann *et al.* (2021), podem-se observar que, em virtude das diversas definições de Guerra Híbrida e Ameaça Híbrida descritas, algumas características centrais são compartilhadas para as ações híbridas, pois elas: exploram a fronteira entre a paz e a guerra; são multidimensionais; são sincronizadas e coordenadas; fazem parte de uma campanha integrada com um objetivo estratégico e são enganosas.

No ano de 2015, a OTAN adotou uma estratégia nova para se contrapor a Ameaças Híbridas com foco em 3 elementos: preparação, dissuasão e defesa contra Ameaças Híbridas. As lideranças da OTAN, em 2018, criaram equipes de apoio para combater Ameaças Híbridas, denominadas de “Equipes contra-híbridas”[8] (WEISSMANN *et al.*, 2021).

Existe uma unidade na Divisão Conjunta de Inteligência e Segurança (DCIS) da OTAN que tem como atribuição analisar e combater ameaças híbridas, além de disponibilizar apoio aos Estados membros e atuar também em operações de informação e propaganda (WEISSMANN *et al.*, 2021).

Para as FA Ocidentais e a UE, a guerra convencional não será mais a característica dos conflitos futuros. Os oponentes serão dotados de habilidades para empregar combinação de métodos irregulares, disruptivos e tradicionais, para alcançar objetivos estratégicos e operacionais. As Ameaças Híbridas e o terrorismo passaram a constar em um Quadro regulamentar elaborado para lidar com esses tipos de ameça, a partir de uma decisão da

8 As lideranças da OTAN, criaram em julho de 2018, equipes que disponibilizam assistência direcionada para os seus países membros, no auxílio para a resposta e preparação contra Ameaças Híbridas, sendo as mesmas classificadas como “Equipes contra-híbridas” (NATO, 2023). Essas equipes são compostas principalmente por especialistas civis e os seus integrantes possuem ampla experiência em áreas específicas, como proteção de infraestruturas críticas, tanto físicas quanto cibernéticas, além de contra espionagem (RÜHLE, 2021a).

Comissão Europeia de 2016. Essa estrutura tem como objetivo ajudar a responder e fortalecer a resiliência[9] às Ameaças Híbridas, por meio de uma série de medidas propostas com a finalidade de ajudar a UE, seus Estados membros e parceiros (WEISSMANN *et al.*, 2021).

Essa proposta também contempla diversas medidas para identificar e proteger infraestruturas importantes em diversos setores considerados estratégicos, como sistema financeiro, abastecimento de energia, espaço e transporte. Além disso, também são propostas medidas para proteger a saúde, a segurança alimentar, a produção de energia, a indústria, assim como medidas no domínio da cibersegurança. A UE também elaborou algumas para o setor de defesa, de forma a fortalecer as capacidades para enfrentar as Ameaças Híbridas, sendo que essas propostas são abrangidas pela Agenda de Segurança Europeia, com ênfase na abordagem da prevenção do extremismo e da radicalização (WEISSMANN *et al.*, 2021).

Pode-se observar que, conforme descrito, os termos "Guerra Híbrida" e "Ameaça Híbrida" estão cercados de confusão conceitual. Os respectivos termos são muitas vezes empregados de forma intercambiável, sendo que o próprio conceito de "Guerra Híbrida" por si só já é um conceito contestado. Devemos nos ater se o uso da força ou a ameaça estão incluídos na atividade ou não (SØRENSEN; NYEMANN, 2019).

As Ameaças Híbridas são ambíguas por design estratégico com ênfase em instrumentos não cinéticos de poder e operam na chamada "zona cinzenta"[10] entre a paz e a guerra. Devido ao fato de uma gama de ações coercitivas ser perpetrada contra nós e ocorrer em domínios que são

9 A resiliência tem como definição a habilidade de um determinado organismo ou sistema de manter suas funções vitais básicas operando, mesmo após ter sido atingido por danos graves. No contexto da segurança nacional significa que um Estado pode assimilar um ataque cibernético, um atentado terrorista, um ataque militar ou uma sequência de ações de escala de menor magnitude em todo o espectro da Guerra Híbrida e continuar a funcionar normalmente, tanto quanto for possível (GAREIS, 2017).

10 O conjunto de atividades que ocorrem entre a guerra ou conflito armado e a paz é definido como zona cinzenta. Várias atividades enquadram-se nesse termo obscuro, tais como: campanhas de desinformação; operações mercenárias; operações de influência; ataques cibernéticos; assassinatos; atividades econômicas nefastas. Essas atividades permanecem abaixo do limiar do conflito armado e são enquadradas como campanhas que aumentam ou diminuem a gradação, sendo desencadeadas por atores não estatais e estatais, combinando diversos tipos de feramentas não militares e quase militares (STARLING, 2022).

considerados como fora do domínio da guerra, as Ameaças Híbridas desafiam nossa capacidade de alertar e detectar oportunamente (SØRENSEN; NYEMANN, 2019).

Outro ponto que merece destaque refere-se ao fato de que as Ameaças Híbridas empregam o uso extensivo de proxies[11] em domínios onde a atribuição de responsabilidades pelas ações tomadas é muito demorado e bastante desafiador. Devido ao fato de as ações empregadas pelas Ameaças Híbridas, na maioria das vezes ficarem aquém de um ataque armado direto, elas desafiam a nossa capacidade de resposta, mesmo sabendo que as ações possam ser maliciosas. Outro aspecto refere-se ao fato de que é bastante complexo conseguir-se identificar, detectar e atribuir uma resposta rígida contra as Ameaças Híbridas, o que a torna uma ferramenta estratégica de baixo risco, baixo custo, mas com um elevado potencial de ganhos (SØRENSEN; NYEMANN, 2019).

Analisando diversas publicações da Marinha do Brasil (MB), do Exército Brasileiro (EB), da Força Aérea Brasileira (FAB) e do Ministério da Defesa (MD), observa-se que o assunto Guerra Híbrida e Ameaça Híbrida ainda é pouco explorado, carecendo, portanto, de estudos mais aprofundados. A MB possui na COMOPNAVINST Nº 30-01 uma definição bem abrangente de Ameaças Híbridas:

> 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.2).

Após as diversas conceituações abordadas, pode-se chegar à conclusão de que o emprego de determinados tipos de medidas híbridas ativas de um ator tendo como foco um

11 *Proxy* refere-se ao intermediário entre o servidor e o usuário. O servidor disponibiliza todos os dados que se deseja acessar na internet. Dessa forma os dados do usuário são repassados à frente pelo servidor *proxy*. O usuário solicita algum tipo de serviço conectando-se ao servidor *proxy* e esse tem a função de enviar a solicitação do endereço para o servidor. O proxy pode conectar o seu computador a internet, possibilitando que você navegue de forma anônima (OLIVEIRA, 2011).

outro ator é o que define a Guerra Híbrida. A Ameaça Híbrida pode fazer uso de medidas passivas, não necessitando, portanto, limitar-se a medidas ativas. A Ameaça Híbrida atua desde o momento de paz absoluta até a guerra (RODRIGUES, 2021; WEISSMANN *et al.*, 2021).

Observa-se que pelo que foi abordado, notamos que não há um consenso na definição de Guerra Híbrida, sendo a mesma um conceito. Dessa forma este trabalho irá abordar a definição de Guerra Híbrida formulada por Frank G. Hoffman e a definição de Ameaça Híbrida formulada pelo *Hybrid Coe.*

2.3 Definição de metas estratégicas para combater a Guerra Híbrida

Torna-se imprescindível elaborar uma resposta estratégica para a Guerra Híbrida devido ao seu potencial de gerar efeitos desestabilizadores no sistema internacional. A identificação da respectiva ameaça é o primeiro passo para combater a Guerra Híbrida (MONAGHAN; CULLEN; WEGGE, 2019).

No momento em que se identifica a ameaça da Guerra Híbrida, o passo seguinte diz respeito a se decidir o que fazer. Dependendo do tipo de ator envolvido, o nível de vontade de combater a Guerra Híbrida poderá variar. Isso dependerá da vontade política, capacidade de contra-ataque, intensidade da ameaça e do contexto. As disponibilidades de opções políticas podem variar entre adotar medidas mais retaliatórias ou assertivas de forma a prevenir ou interromper novos ataques, dissuadir agressões ou até mesmo absorver os ataques (MONAGHAN; CULLEN; WEGGE, 2019).

O estabelecimento de metas estratégicas torna-se o elemento de articulação das escolhas políticas. Essas metas devem ser continuamente revisadas e devem ser estabelecidas na fase inicial de uma campanha de guerra contra-híbrida[12], envolta em um ambiente estratégico dinâmico. Todas as ações e medidas implementadas para combater a

12 A expressão Guerra contra-híbrida, refere-se ao emprego pelo Estado de uma gama variada de ferramentas e estratégias que tem como objetivo detectar, deter e responder as Ameaças Híbridas ou a Guerra Híbrida perpetrada contra esse respectivo Estado, atuando dentro dos seus respectivos campos, que são Político, Militar, Econômico, Social, Informacional e de Infraestrutura (PMESII).

Guerra Híbrida devem cooperar para se alcançar uma ou mais metas. Qualquer ator que tenha como finalidade a projeção de uma estratégia para combater a Guerra Híbrida pode se amparar em 3 metas estratégicas genéricas conforme especificadas a seguir (MONAGHAN; CULLEN; WEGGE, 2019).

2.3.1 Meta Estratégica 1: manter a capacidade de atuação independente

Manter a capacidade de atuação e governamental independentes é encarado como o objetivo mais básico, sendo uma condição para quaisquer outros objetivos subsequentes, além de combater os efeitos da Guerra Híbrida no funcionamento da sociedade e do Governo. Por meio do emprego de uma grande quantidade de ferramentas a sociedade e o Governo devem construir resiliência contra Ameaças Híbridas, estabelecendo uma abordagem comum e coordenada para enfrentá-las, assim como avaliar as suas vulnerabilidades (MONAGHAN; CULLEN; WEGGE, 2019).

2.3.2 Meta Estratégica 2: dissuadir ou desencorajar um adversário de agressão híbrida

O ato de desencorajar ou dissuadir um oponente de conduzir uma Guerra Híbrida torna a segunda meta mais exigente do que a primeira. Com a finalidade de ameaçar ou impor custos (dissuasão por punição)[13], a dissuasão abrangente requer ir além da resiliência, enquanto as ações para manter a capacidade de ação independente podem ter efeito dissuasor (por meio da dissuasão por negação)[14]. A dissuasão híbrida deve levar em consideração a capacidade e a intenção do adversário e os interesses dos defensores,

---

13 Dissuasão por punição - tem como objetivo fazer com que o adversário entenda que a partir do momento em que ele adotar um comportamento indesejado, sofrerá um grande dano que lhe será imposto (NOLL; BOJANG; RIETJENS, 2020).

14 Dissuasão por negação – tem como objetivo fazer com que o adversário seja convencido de que é praticamente improvável que consiga a um custo razoável atingir seus objetivos (NOLL; BOJANG; RIETJENS, 2020).

devendo ser estabelecida desde o início e restabelecida se falhar, com limites estabelecidos (MONAGHAN; CULLEN; WEGGE, 2019).

2.3.3 Meta Estratégica 3: interromper ou impedir que um adversário prossiga com a agressão híbrida

Impedir que o oponente prossiga com a agressão híbrida torna-se a terceira meta e a mais exigente. Essa meta tem como finalidade a adoção de medidas que irão degradar ou interromper a capacidade de atuação de um oponente, indo dessa forma além da dissuasão, embora a adoção dessas medidas possua um respectivo valor de dissuasão intrínseco. A adoção dessa meta faz-se necessária porque é muito difícil que um agressor híbrido altere seu comportamento para degradar a sua vontade ou capacidade de realizar uma agressão híbrida sem que haja uma retaliação (MONAGHAN; CULLEN; WEGGE, 2019).

2.4 Elaboração de um modelo de *Framework* para combater a Guerra Híbrida

As formas e os meios necessários para alcançar as metas estratégicas que são consideradas os fins de uma estratégia geral para combater a Guerra Híbrida, estão representados pelos 3 componentes do *Framework* de combate à Guerra Híbrida que são detectar, deter e responder, especificados na Figura 1 (MONAGHAN; CULLEN; WEGGE, 2019).

FIGURA 1 - Visualizando a estrutura de combate à Guerra Híbrida
Fonte: MONAGHAN; CULLEN; WEGGE, 2019, p.22, tradução do autor.

2.4.1 Detectar os agressores híbridos

As ações a serem tomadas para combater a Guerra Híbrida são abordadas neste tópico. A análise tradicional de ameaça centrada no inimigo torna-se inadequada, devido ao fato de que as Ameaças Híbridas são difíceis de detectar (MONAGHAN; CULLEN; WEGGE, 2019).

A implementação de uma Inteligência de alerta nos fornece uma prevenção sobre intenções ou ações hostis por meio do emprego de atividades de inteligência. Ele se ampara em métodos alicerçados em indicadores, nos quais indicadores-chave são monitorados e identificados ao longo do tempo de forma a definir uma linha de base das operações normais e atividades de um oponente (MONAGHAN; CULLEN; WEGGE, 2019).

A detecção de relevantes mudanças no status operacional, as quais podem fornecer aos tomadores de decisão e aos analistas de inteligência um alerta de atividade indesejável, é o foco da inteligência de alerta baseada em indicadores. Apesar da importância dos indicadores tradicionais e militares, torna-se necessário ultrapassar essa abordagem unidimensional com a finalidade de detectar a Guerra Híbrida e alertar a inteligência para focar no que realmente é interessante observar (MONAGHAN; CULLEN; WEGGE, 2019).

Há necessidade da elaboração de processos de inteligência de alerta, objetivando a proteção de vulnerabilidades críticas em toda a sociedade contra possíveis ataques. O compartilhamento de informações de forma coordenada também torna-se muito importante para a detecção de ataques híbridos sincronizados e multivetoriais, os quais são projetados de forma intencional para permanecerem abaixo ou fora dos limites de detecção tradicionais (MONAGHAN; CULLEN; WEGGE, 2019).

2.4.2 Deter os agressores híbridos

Devido ao fato de poder impedir a ocorrência de ataques em primeiro lugar, a dissuasão talvez seja a ferramenta mais importante para combater a Guerra Híbrida, porém a dissuasão tradicional pode ter seu cálculo complicado pelas características intrínsecas da Guerra Híbrida (MONAGHAN; CULLEN; WEGGE, 2019).

Os “três C” da dissuasão eficaz fornecem a compreensão da mesma: a credibilidade é o desejo de empreender atos que instituam custos ao oponente; a capacitação é a aptidão ou capacitação técnica para empreender atos que instituam custos ao oponente e a comunicação é o entendimento e a percepção bidirecionais que comunica cálculos de custo-benefício para os dois lados (MONAGHAN; CULLEN; WEGGE, 2019).

A dissuasão por negação e dissuasão por punição são as duas grandes categorias atinentes as estratégias de dissuasão, sendo que a dissuasão por negação intenciona prejudicar a capacitação do oponente para alcançar sua meta em primeira instância e a dissuasão por punição intenciona persuadir o oponente de que os custos para alcançar sua meta serão impeditivos ao intimidar represália ao ato agressivo (MONAGHAN; CULLEN; WEGGE, 2019).

2.4.3 Responder os agressores híbridos

Conforme Monaghan, Cullen e Wegge (2019), segue a apresentação de instrumentos em conjunto para fornecer uma resposta às Ameaças Híbridas, usando as alavancas de potência Militar, Político, Econômico, Civil e Informação (MPECI):

– Militar: A maximização do potencial coercitivo do instrumento militar com o intuito de alvejar as vulnerabilidades dos agressores híbridos deve ser ajustada pela ação militar de forma a garantir a proporcionalidade. Dependendo dos objetivos estratégicos que se almeja alcançar, a resposta a ataques híbridos pode ser obtida empregando-se a grande quantidade de opções da força militar. O emprego da força militar pode contribuir para medidas de prevenção, dissuasão e resiliência;

– Político: As seguintes medidas direcionadas para o domínio político podem ser empregadas: retirada de direitos de voto de estados individuais em organizações internacionais, expulsão de diplomatas, suspensão de filiações, restrições de viagem para funcionários políticos ou para os próprios políticos;

– Econômico: Existem diversos exemplos de efeitos e influências de sansões bem empregadas de modo que não se pode subestimar a eficácia da adoção de medidas econômicas. A eficácia de determinados tipos de penalidades financeiras voltadas para indivíduos como o congelamento de ativos e sansões também podem ser visualizadas a curto prazo. A redução do comércio, causando um impacto maior na sociedade, pode ser adotada como uma segunda ordem de sansões, a fim de criar o efeito primário pretendido;

– Civil: Um dos pilares da democracia é, sem dúvida, o Estado democrático de direito. A nomeação pública de suspeitos nos envenenamentos de Skripal[15] e o processo público após as eleições presidenciais de 2017 nos EUA são exemplos notórios que podem comprovar a sua eficácia. O fortalecimento da confiança da sociedade nas instituições públicas pode ser obtido, por exemplo, por meio de nomeações públicas e pela transparência; e

15 Serguei Skripal era um ex-espião russo que foi envenenado na Inglaterra em março de 2018, juntamente com sua filha Yulia. O caso provocou uma grave crise diplomática envolvendo Moscou e Londres, que atingiu também outros países. O atentado foi perpetrado pelo serviço secreto russo, utilizando o agente nervoso Novichok (MANNTEUFEL, 2018).

– Informação: O aumento do acesso à informação e o aumento da confiança no seio da sociedade podem ser obtidos com a implementação de medidas para apoiar a transparência e abertura da mídia, por meio de regulamentação. A educação torna-se a principal ferramenta para combater a desinformação, sendo necessária também a exposição, por meio da transparência para a aplicação de penalidades por meio da adoção de ações legais. Atualmente pode-se observar uma grande sofisticação por parte do emprego de medidas cibernéticas ofensivas (MONAGHAN; CULLEN; WEGGE, 2019).

2.5 O emprego da comunicação estratégica contra as Ameaças Híbridas

Há necessidade de ser realizada uma ação coordenada em diferentes domínios[16] para se obter uma resposta eficaz contra as Ameaças Híbridas. Ela logrará êxito se não houver uma comunicação adequada para os públicos específicos, por meio dos canais e formatos adequados, em tempo hábil e com mensagens precisas. A comunicação estratégica é essencial para montar uma espécie de barreira, de forma a combater o vazamento de informações roubadas, ciberespionagem, manipulação, desinformação e demais formas de informação empregadas pelos autores que praticam essas ameaças, principalmente devido ao fato de estarmos envoltos em uma sociedade sobrecarregada de mensagens contraditórias e informações (GARCÍA *et al.*, 2021).

Com o objetivo de controlar a narrativa política, radicalizar os indivíduos e desestabilizar a sociedade, os perpetradores de Ameaças Híbridas podem realizar campanhas direcionadas nas redes sociais com o intuito de espalhar a desinformação. A adoção de um planejamento fundamentado de comunicação estratégica é primordial para responder a Ameaças Híbridas (COMISSÃO EUROPEIA, 2018).

A construção de uma resiliência social pode ser obtida com a elevação da conscientização pública sobre Ameaças Híbridas e o fornecimento de respostas rápidas. O emprego de uma comunicação estratégica eficaz deve utilizar ferramentas de áudio, da

16 Os domínios são os campos de um Estado, onde pode-se aplicar as combinações de ferramentas das Ameaças Híbridas, de forma a explorar as suas vulnerabilidades. Entre os diversos tipos de domínios pode-se citar: infraestruturas, cibernético, espaço, economia, militar, cultura, social, administração pública, jurídico, inteligência, diplomacia, política e informações. (GIANNOPOULOS; SMITH; THEOCHARIDOU, 2021).

internet, da mídia tradicional visual e de mídia social. A reação à desinformação deve ser obtida com o emprego de pessoas com larga experiência em redes sociais, de forma a controlar informações não pertencentes ao Estado, assim como, o emprego de linguistas fluentes em línguas não pertencentes ao país (COMISSÃO EUROPEIA, 2018).

As comunicações estratégicas objetivam uma grande diversidade de públicos e são planejadas com atividades contínuas para longos períodos de tempo. O objetivo principal é possibilitar a implementação de determinadas metas políticas que foram definidas e o grau de progresso do atingimento dessas metas pode ser o ponto de medição de sua eficácia (GARCÍA *et al.*, 2021).

A mensagem, o público-alvo, a avaliação de impacto, as formas de comunicar e o resultado pretendido constituem-se nos elementos fundamentais da comunicação estratégica (GARCÍA *et al.*, 2021).

O elemento que mais influencia a definição da comunicação estratégica é o público-alvo. Sua definição pode ser realizada em tipo de grupos (apoiadores de adversários, grupos insurgentes, toda a sociedade, grupos terroristas, Governos), tipo de relacionamento (adversários, aliados) e em termos de geografia (audiência doméstica ou estrangeira) (GARCÍA *et al.*, 2021).

2.6 O fenômeno da Desinformação na Guerra Híbrida

Segundo García *et al.* (2021), a desinformação constitui-se em um elemento essencial das Ameaças Híbridas.

A definição de desinformação pode ser explicada como informações confirmadas como enganosas ou falsas que são geradas, divulgadas e difundidas com a finalidade de ludibriar o público intencionalmente ou obter ganho econômico, podendo acarretar danos públicos. Esses danos públicos compreendem ameaças à segurança da União e dos cidadãos, à saúde, ao ambiente, aos bens públicos e aos processos democráticos (COMISSÃO EUROPEIA, 2018).

As campanhas de propaganda utilizam-se tanto de meios digitais (redes sociais) como de meios tradicionais (canais de rádio e televisão), ajustando as mensagens tanto ao público doméstico como ao estrangeiro. No momento em que determinados Estados começam a patrocinar os meios de comunicação, eles inclinam-se a disseminar informações sob o ponto de vista daquele respectivo Estado. Como forma de exemplificar, podemos citar os RT e o Sputinik, que são dois meios de comunicação russos, que possuem conteúdos em vários idiomas e delegações em vários países do ocidente, cuja finalidade é favorecer os interesses russos, comunicando ao público do ocidente sobre os acontecimentos atuais do ponto de vista do Kremlin (GARCÍA *et al.*, 2021).

A disseminação da desinformação avançou com o advento das mídias sociais. Ela está sendo cada vez mais disseminada pelos serviços de mensagens privadas. Entre as diversas técnicas utilizadas podemos citar: o emprego de softwares automatizados de internet (bots) para amplificar e disseminar debates nas redes sociais; roubo de informações; ataques de

troll[17] em perfis de mídia social; falsificação de documentos oficiais e manipulação de vídeo (*deep-fakes*) (COMISSÃO EUROPEIA, 2018).

Conforme García *et al*. (2021), a desinformação é capaz de: fazer com que os debates se tornem polêmicos; causar dano à democracia, ao impor obstáculos à capacidade dos cidadãos de tomar decisões; intensificar as tensões na sociedade; desacreditar os sistemas eleitorais; colocar em risco a proteção do meio ambiente, da segurança e da saúde dos cidadãos; minar a credibilidade nas mídias digitais e nas instituições; colocar em perigo os processos de formulação de políticas e os processos democráticos políticos.

Segundo García *et al.* (2021), a fabricação ou manipulação de conteúdo, a atribuição de identidades falsas, os argumentos falsos, o impacto na mídia e a tecnologia atuando como facilitadora, são os 5 componentes primordiais da desinformação que representam seu maior perigo, quando devidamente combinados pelo invasor.

17 *Troll* significa uma pessoa que tem como objetivo realizar a provocação de forma emocional de determinados membros de uma comunidade por meio da disseminação de mensagens irrelevantes ou controversas, com o intuito de provocar conflitos entre os participantes ou cessar uma discussão sadia, tirando de foco o objetivo principal do assunto que estava sendo debatido (PEREIRA, 2009).

A geração de um conteúdo manipulado, abordando sob uma perspectiva distorcida um fato real, constitui-se na primeira fase de uma campanha de desinformação. A partir do momento em que o conteúdo falso é gerado, busca-se atribuir o mesmo a fontes fidedignas. Essa ação tem 2 finalidades: desacreditar a reputação da fonte a partir do momento em que a desinformação é revelada e elevar a confiabilidade da informação falsa para amplificar sua repercussão. Os argumentos falsos apoiam e complementam o conteúdo falso, dependendo, portanto, de plataformas digitais e meios de comunicação para atingir públicos amplos e seus objetivos que são: enfraquecer as instituições democráticas e ludibriar a opinião pública para comprometer a coesão política e social (GARCÍA *et al.*, 2021).

A tentativa de deslegitimização do setor jornalístico, um dos atores fundamentais nas democracias é um dos objetivos das campanhas de desinformação. Com a finalidade de elevar a credibilidade da informação falsa é realizado um esforço para tentar minar a crença dos cidadãos em determinados jornalistas, empresas e nos veículos de comunicação, pois se não há confiabilidade em nenhum jornalista ou veículo de comunicação, a informação classificada como falsa torna-se tão aceitável como qualquer outro tipo de informação, elevando assim o seu resultado (GARCÍA *et al.*, 2021).

A responsabilidade das plataformas de mídia social, atinente à veracidade do conteúdo nela exposto, torna-se uma questão sensível e extremamente importante ao lidar com a desinformação disseminada por meios digitais. Pode-se observar que o combate à desinformação é uma tarefa árdua e extremamente difícil, principalmente para as democracias liberais, pois o direito à liberdade de informação e à liberdade de expressão devem ser respeitados (GARCÍA *et al.*, 2021).

O Plano de Ação contra a Desinformação da Comissão Europeia destaca 4 pilares para a adoção de uma resposta coordenada no combate à desinformação: estimular a participação do setor privado no combate à desinformação; aperfeiçoar a resiliência social e elevar a conscientização; consolidar respostas conjuntas e coordenadas no combate à desinformação; aperfeiçoar as capacitações das instituições para analisar, detectar e expor a desinformação (COMISSÃO EUROPEIA, 2018).

O combate à desinformação exige uma mobilização de todas as partes do Governo (comunicação estratégica, cibersegurança, proteção de dados, eleitorais, inteligência, autoridades de mídia, contra-híbridas e policiais), além de necessitar de uma ação unificada e determinação política. Exige ainda uma estreita cooperação entre a sociedade civil, o setor privado, as plataformas digitais, as instituições e os Estados-Membros (COMISSÃO EUROPEIA, 2018).

2.7 Conclusões parciais.

É notório que o advento da internet e das mídias sociais, associado à velocidade de disseminação das informações e aos diversos dispositivos (tablets, smartphones e notebooks) que permitem nos comunicarmos em qualquer parte do planeta, além da facilidade de podermos enviar fotos, áudios, documentos e vídeos de forma instantânea, causaram uma verdadeira revolução tecnológica nesse século.

Essas inovações tecnológicas, apesar de trazerem diversas facilidades, também mostraram algumas vulnerabilidades. Dessa forma, determinados tipos de atores utilizam esses mecanismos como armas, com o intuito de desestabilizar Estados, enfraquecer democracias consolidadas, espalhar a desinformação, minar as instituições sérias, atacar vulnerabilidades críticas, sem a necessidade de empregar a força cinética e letal, utilizando-se apenas de meios não convencionais.

Pode-se notar que diversos países e organismos importantes, tais como UE, OTAN e a Federação da Rússia, estão estudando de forma profunda esses novos fenômenos conhecidos como Guerra Híbrida e Ameaças Híbridas, com o objetivo de traçar metas estratégicas para se contraporem a essa nova ameaça.

A criação pela OTAN de Equipes contra-híbridas e da DCIS visa atuar de forma estratégica com enfoque na preparação, dissuasão e defesa contra Ameaças Híbridas, além de atuar também em OpInfo e propaganda enganosa que são os principais focos da Guerra Híbrida. O mapeamento eficaz de todas as infraestruturas críticas de um Estado, torna-se essencial para mitigar os efeitos dessa nova ameaça.

A definição de metas estratégicas genéricas para combater a Guerra Híbrida facilitou para que países como o Brasil, que ainda não possuem tais medidas implementadas, amparem-se nessas metas para consolidarem as suas respostas estratégicas.

A comunicação estratégica possui uma alta relevância no combate às Ameaças Híbridas, principalmente no que se refere à desinformação. Dessa forma, o combate à desinformação tornou-se uma tarefa árdua, pois ele exige que diversas partes do Estado atuem em conjunto, de forma unificada e com uma forte determinação política, sendo essencial uma cooperação ampla entre a sociedade civil, o setor privado, as plataformas digitais e as diversas instituições.

Dessa forma, o mais importante nesse contexto é compreender o tipo de fenômeno que se está enfrentando, conhecer as suas fragilidades, fortalecer-se contra as suas ações e ter a plena consciência de que sozinho não há como se contrapor a essa ameaça, sendo a união de esforços um fator preponderante para se contrapor a essa nova modalidade de conflito.

Segundo Jonsson (2021), o local mais importante para a Guerra Híbrida está concentrado no domínio da informação. Atualmente a legitimidade, o poder e a forma como entendemos o mundo estão regularizados pelas mídias sociais. Dessa forma, no capítulo seguinte, serão abordadas as OpInfo para entendimento de sua dinâmica no contexto da Guerra Híbrida.

3 AS OPERAÇÕES DE INFORMAÇÃO (OpInfo) NO CONTEXTO DA GUERRA HÍBRIDA

O presente capítulo tem como objetivo analisar como ocorre a atuação das OpInfo no contexto da Guerra Híbrida; diferenciar as OpInfo da Guerra de informação; analisar a vantagem da aplicação do ciclo OODA no processo de tomada de decisão; analisar o Ambinete Operacional e a Dimensão Informacional; analisar as Capacidades Relacionadas à Informação (CRI) com enfoque para as Operações Psicológicas (OpPsc), Guerra Eletrônica (GE), Comunicação Social (ComSoc), Ações Cibernéticas e Operação Civil-Militar; observar as OpInfo à luz do Direito Internacional e como a Federação da Rússia faz uso dessa ferramenta nas suas operações militares, com enfoque para a anexação da Crimeia, ocorrida em 2014.

3.1 As OpInfo, a Guerra de Informação e o ciclo OODA

Com o intuito de entender o que são as OpInfo e a Guerra de Informação, seguem abaixo as definições extraídas da Doutrina de OpInfo (EMA-335) e do Glossário das FA do Ministério da Defesa, respectivamente:

> Consistem na coordenação do emprego integrado das Capacidades Relacionadas à Informação, em contribuição a outras operações ou mesmo compondo o esforço principal, para informar e influenciar pessoas ou grupos hostis, neutros ou favoráveis, capazes de impactar positivamente ou negativamente o alcance dos objetivos políticos e militares, bem como para comprometer o processo decisório dos oponentes ou potenciais oponentes, enquanto garantindo a integridade do nosso processo (BRASIL, 2018, p. 2-6, 2-7).

> Guerra de Informação - Conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos (BRASIL, 2015, p. 135).

A Guerra de Informação tem atuação nas expressões Política, Econômica, Militar, Psiccossocial e Científico-Tecnológica, ou seja age em todas as expressões do Poder Nacional, sendo assim muito mais abrangente do que as OpInfo, as quais agem somente na Expressão do Poder Militar. Dessa forma, a Guerra de Informação obtém a superioridade após a fase

inicial do conflito, pois possui quantidades mais elevadas de capacidades em comparação às OpInfo, com o intuito de serem empregadas para afetarem o processo decisório do adversário[18] (MELLO, 2023).

Segundo Corrêa (2012), as OpInfo devem buscar atingir 3 funções na sua totalidade e em um curto intervalo de tempo, devido ao fato de que as OpInfo têm o seu início na época de paz, expandindo-se durante todo o período de crise propriamente dita, findando somente depois de a paz ser alcançada novamente e, logo em seguida, vigorar a situação de equilíbrio. Essas 3 funções são:

– Confundir os planos do oponente e salvaguardar os seus, possibilitando, assim, potencializar o resultado de suas forças, conseguindo vantagem excessiva, enquanto o adversário emprega seus meios para conseguir efeitos limitados ou exíguos;

– Preservar as suas próprias redes e suas comunicações e obter o controle das do oponente, impossibilitando, assim, a capacidade do oponente de se defender e de se organizar, enquanto defende o efetivo Comando e Controle de suas forças; e

– dissuadir, impedir, desestimular e orientar um oponente por meio da fragmentação da sua unidade de comando e pretensão de engajar no efetivo combate, ao mesmo tempo em que resguarda a sua unidade pessoal.

Para entender a real importância das OpInfo, deve-se ter a perfeita noção de que a informação é o elemento essencial para a concepção da decisão. A teoria elaborada por John Richard Boyd, descreve que para triunfar sobre o oponente será necessário intervir no seu ciclo OODA que corresponde a "observação – orientação – decisão – ação", de forma a efetuar o ciclo completo com uma velocidade maior do que a do adversário (BOYD, 1986 *apud* BARBOZA; TEIXEIRA, 2020).

A intenção adotada por Boyd, que foi um piloto estadunidense de aviões de caça, tendo atuado na Guerra da Coreia, consistia em utilizar manobras inesperadas, súbitas e rápidas com o intuito de fazer com que o oponente sempre estivesse buscando prever seus

18 Informações inseridas nos slides 47 e 48 constantes da apresentacao realizada no dia 08 de maio de 2023, na Escola de Guerra Naval (EGN) pelo CMG (RM1-FN) Jorge Luís de Araujo Mello (Instrutor de Op Psico e Op Info - AE-III da EGN) (MELLO, 2023).

objetivos e para desorientá-lo, retardando, assim, seu processo decisório, de forma a pressupor a localização exata da sua aeronave (BOYD, 1986 *apud* BARBOZA; TEIXEIRA, 2020).

Observa-se que a atual "era do conhecimento" possibilitou a implementação de diversos tipos de mecanismos para que se consiga influenciar, manipular ou interromper o processo decisório não somente do adversário, mas de todo tipo de ator que tenha a sua relevância ou de determinado tipo de público-alvo com alguma forma de interesse na consequência de um conflito específico (BARBOZA; TEIXEIRA, 2020).

A partir do momento em que as OpInfo inviabilizam o processo decisório do oponente, ao mesmo tempo em que protegem os nossos próprios, elas encontram-se colaborando para a iniciativa das ações, pois fazem com que o inimigo tenha que estar sempre em uma posição de reação frente às nossas Forças (BARBOZA; TEIXEIRA, 2020).

Dessa forma, para que haja sucesso no emprego da OpInfo, elas devem ser priorizadas conforme a necessidade, repleta de recursos, sincronizadas com a manobra, bem assimiladas e integradas (BARBOZA; TEIXEIRA, 2020).

Podem-se observar as diferenças existentes entre as OpInfo e a Guerra de Informação extraídas de publicações doutrinárias da MB e do MD, ressaltando-se as atuações de cada uma nas expressões do Poder Nacional. Em relação à importância do ciclo OODA nas OpInfo e à forma como a informação influencia no processo decisório, conforme observado no capítulo 2, nota-se que a Guerra Híbrida visa atingir o processo de tomada de decisão do oponente e o ciclo OODA ressalta justamente essa ação. Dessa forma, pode-se observar que as OpInfo têm uma grande relevância no contexto da Guerra Híbrida.

3.2 O Ambiente Operacional

A comunicação global foi muito facilitada no mundo atual devido ao incremento das redes de informação e comunicação, fato esse que reduziu o isolamento populacional mundial e fortaleceu um número significativo de grupos armados. Esse acontecimento possibilitou o avanço de alguns grupos radicais específicos pelo mundo, dando aos mesmos uma maior influência nas suas respectivas áreas de atuação (BRASIL, 2018).

Nesse contexto, a opinião pública, tanto internacional como nacional, aparece como um componente de elevada expressão, pois a mesma está menos inclinada a admitir a aplicação da força na solução de determinados tipos de conflitos e na administração de certos tipos de crise, o que impacta de forma direta as ações de caráter militar, pois as mesmas devem ser reguladas na legitimidade da causa (BRASIL, 2018).

A performance dos equipamentos militares atualmente possui uma grande dependência da TI. Dessa forma, um ataque ou um simples defeito nesses equipamentos pode neutralizar uma parcela da Força Militar, o que demonstra assim o seu elevado grau de vulnerabilidade (BRASIL, 2018).

O ambiente operacional caracteriza-se pela interação de diversos tipos de fatores, em cada situação e de forma específica, levando-se em consideração três dimensões: a humana, a informacional e a física (BRASIL, 2018; BRASIL, 2019).

A dimensão informacional possui uma grande importância, pois os avanços na área de TIC, afetam diretamente os aspectos referentes às mudanças sociais contemporâneas, sendo que esses avanços possibilitam uma grande capacidade de acesso, o compartilhamento da informação e a sua transmissão (BRASIL, 2019).

Devido à globalização, ao enlace de dados e redes de comunicação e ao avanço da tecnologia, determinados tipos de grupos hostis foram se adaptando a essas inovações, fortalecendo-se e conseguindo angariar simpatizantes ao redor do mundo. Como exemplo pode-se citar o grupo terrorista denominado Estado Islâmico (EI).

A opinião pública atualmente é bastante sensível a questões envolvendo conflitos armados e especial atenção deve ser dispendida nesse assunto, de forma a se conseguir obter a legitimidade para uma eventual necessidade do emprego da força.

Os equipamentos militares são muito dependentes da tecnologia, fazendo com que a força tenha a sua vulnerabilidade exposta. No passado a dimensão física era o ponto mais importante do ambiente operacional, porém, com o avanço da tecnologia esse status passou a pertencer à dimensão informacional.

3.3 As Capacidades Relacionadas à Informação (CRI)

Existem diversas definições no mundo para as CRI, porém elas basicamente se restringem ao conceito de que são habilidades intrínsecas que têm como objetivo influenciar a capacidade dos adversários ou potenciais oponentes de difundir, produzir, obter e orientar informações, em quaisquer espectros das perspectivas da dimensão informacional, sejam elas a lógica, a cognitiva ou a física, podendo, para atingir tal objetivo, incluir ações não cinéticas, ações cinéticas e ataques físicos (BRASIL, 2018; BRASIL, 2019).

As CRI na MB englobam as seguintes Capacidades: Operações Psicológicas (OpPsc); Guerra Eletrônica (GE); Comunicação Social (ComSoc), que se divide em Relações Públicas (RP) e Publicidade; Ações Cibernéticas; Operação Civil-Militar. Ela pode englobar ainda outras Capacidades, tais como: Ações de Despistamento; Ações de Superfície; Ações de Guerra Acústica; Operação de Ataque; Ações Cívico-Sociais (ACISO); Combate Câmera; e Operações Especiais (OpEsp) (BRASIL, 2018).

Observa-se que na MB a Inteligência não aparece como uma CRI, sendo a sua função apenas apoiar as OpInfo. A argumentação reside no fato de que a inteligência na MB serve de base para uma série de outras atividades concebidas na esfera de uma Operação Militar e ela não tem a capacidade de causar impacto na dimensão informacional. Nota-se, porém que o EMA-335 ressalta a sua importância dentro das OpInfo, devido ao fato de que a Inteligência possui a capacidade de produzir diversos dados que são essenciais para o planejamento e o sucesso da operação (BRASIL, 2018).

Em virtude de existir uma grande quantidade de CRI, este trabalho terá como ênfase as Operações Psicológicas (OpPsc); Guerra Eletrônica (GE); Comunicação Social (ComSoc); Ações Cibernéticas e Operação Civil-Militar (BRASIL, 2018).

3.3.1 Operações Psicológicas (OpPsc)

No contexto das Operações Navais, observa-se que as OpPsc estão diretamente interligadas com as OpInfo, sendo portanto motivo de preocupação e de atenção de todos os Comandos Subordinados e não apenas do Comando da Força Naval (BRASIL, 2018).

As OpPsc visam obter a rendição do inimigo, tentando levá-lo a uma situação de descrença, impotência, insegurança, por meio da tentativa de influenciar a sua vontade para que o inimigo não consiga obter o êxito, comprometendo assim a liderança do mesmo (BRASIL, 2018).

O outro objetivo das OpPsc é persuadir o oponente a uma incorreta percepção da consciência situacional predominante. Nessa situação torna-se imprescindível uma coordenação minuciosa das demais CRI da força com as OpPsc, levando-se em consideração tanto as não cinéticas quanto as cinéticas (BRASIL, 2018).

As OpPsc também trabalham para que se consiga obter a colaboração e o auxílio do Público-Alvo (Pub A) indeciso e neutro, além de fortalecer e encorajar a devoção dos Pub A admiradores e amigos em favor da nossa causa (BRASIL, 2018).

Observa-se que as OpPsc têm uma atuação direta nas atitudes, no raciocínio, nas motivações, na percepção, no comportamento e nas emoções dos respectivos Pub A de interesse, agindo de forma enfática na perspectiva cognitiva da dimensão informacional (BRASIL, 2018).

Como forma de exemplificar a importância das OpPsc no contexto das OpInfo, pode-se citar que durante a Operação Tempestade no Deserto (1990-1991), as Operações Psicológicas estadunidenses empregaram diversos tipos de transmissões de rádio, panfletos e mensagens de alto-falantes contra algumas unidades iraquianas conseguindo assim o pleno êxito, com a rendição de cerca de 87 mil combatentes iraquianos. Levando-se em consideração a deserção e a rendição dos soldados iraquianos, tais fatores contribuíram para o baixo moral da tropa, para a redução da capacidade de resposta e para a incapacitação do comando e controle iraquiano (BARBOZA; TEIXEIRA, 2020).

3.3.2 Guerra Eletrônica (GE)

A GE corresponde ao conglomerado de ações que tem como objetivo específico atuar na faixa de todo o espectro eletromagnético, de forma a conseguir explorar as emissões do adversário, com o intuito de descobrir quais são as suas capacitações, ideias e a sua ordem de batalha eletrônica, além de adotar providências apropriadas para impedir a utilização do seus sistemas, ao mesmo tempo em que se resguarda e emprega, com êxito, os seus próprios sistemas (BRASIL, 2018).

A GE poderá em um futuro próximo ser utilizada contra adversários não estatais ou estatais, ou ainda contra determinados tipos de sistemas de interesse, em razão do emprego cada vez maior das FA em diversas áreas de atuação, sempre se respeitando o preconizado na legislação vigente (BRASIL, 2018).

A GE na MB ampara-se na sua Capacidade de Guerra Eletrônica (CGE), que se distingue entre o Aprestamento Eletrônico (APEL), que é responsável pelas atividades de apoio e o Reconhecimento Eletrônico (RETRON), que é responsável pela parte das atividades afetas à inteligência. As ações conhecidas como Medidas de Proteção Eletrônica (MPE), Medidas de Ataque Eletrônico (MAE) e Medidas de Apoio a Guerra Eletrônica (MAGE), abrangem um conglomerado de medidas operativas que descrevem o emprego eficiente dos meios em determinados tipos de ações militares (BRASIL, 2018).

A proteção de assuntos afetos ao nosso interesse e a degradação do processo decisório do adversário demonstram a estreita ligação existente entre a GE e as OpInfo. Os impactos das ações oponentes na dimensão informacional, podem ser neutralizados, impedidos ou até mesmo evitados, a partir do momento em que haja uma integração da GE com as outras CRI (BRASIL, 2018).

Como forma de exemplificar a importância da GE no âmbito das OpInfo, pode-se vislumbrar o seu emprego contra uma rede de comando e controle de radares inimigos ou de determinados tipos de mísseis balísticos, com o objetivo de mitigar a sua capacidade de lançamento. Existe ainda a possibilidade de ser empregado com o intuito de isolar uma determinada parcela da população de determinados tipos de propagandas estatais, atuando

de forma direta com o objetivo de causar interferências nas estações de TV e rádios estatais (CLARK, 2010).

3.3.3 Comunicação Social (ComSoc)

Tem como objetivo persuadir a opinião pública, por meio de um amplo espectro de atividades, com a finalidade de se certificar da sua aquiescência pela sociedade e a clara compreensão da instituição. Na ComSoc estão inseridas as atividades de Publicidade, Relações Públicas e Assessoria de Imprensa (BRASIL, 2018).

A ComSoc tem como objetivo estabelecer com a sua audiência um relacionamento de estrita confiança. Dessa forma, ela deverá sempre informar a sua audiência e nunca influenciar a mesma, sob o riso de perder a sua credibilidade perante o público (BRASIL, 2018).

No contexto das operações, a célere disseminação de informações exatas, para públicos internacionais e nacionais, auxilia a atingir os objetivos operacionais, estratégicos e nacionais; corrói a propaganda do adversário e proporciona percepções (BRASIL, 2018).

3.3.4 Ações Cibernéticas

As ações cibernéticas fazem uso de mecanismos que encontram-se disponibilizados nos domínios da TIC, com o intuito de permitir o resguardo de determinados tipos de ativos de TIC de importância e para desestruturar os ativos de informação do adversário. Essas respectivas ações são desencadeadas em um dos domínios operacionais denominado de espaço cibernético, que além de permear os outros domínios, interpõe-se entre o aeroespacial, o marítimo e o terrestre, todos interdependentes entre si. O espaço virtual constituído por ativos de informação interligados ou não em redes, por meio do qual as informações digitais são arquivadas, processadas e por onde elas deslocam-se é conhecido como espaço cibernético (BRASIL, 2018).

O enquadramento das ações cibernéticas ocorre da seguinte forma: o nível de emprego pode ser tático, operacional ou estratégico; o tipo pode ser de exploração cibernética, de proteção cibernética ou de ataque cibernético; o efeito desejado pode ser de caráter defensivo ou ofensivo (BRASIL, 2018).

Exemplificando o descrito, por ocasião da anexação da Crimeia em 2014, pode-se destacar, como exemplo, a grande quantidade de ações cibernéticas desencadeadas naquele país, utilizando-se para tal de diversos equipamentos militares, além de armas com elevado grau de tecnologia e sofisticação, dentre as quais pode-se destacar: software inovador; sistemas inovadores de controle de armas; sistemas espacias e de controle ambiental; sistemas robóticos (em particular, complexos de veículos aéreos não tripulados) e contramedidas; complexos integrados de ataque e reconhecimento; complexos para a realização de operações e ações informacionais-psicológicas no ciberespaço; modernos sistemas de comunicação e informação; sistemas e complexos militares eletrônicos e outros tipos de contramedidas eletrônicas (DANIK; MALYARCHUK; BRIGGS, 2019).

3.3.5 Operação Civil-Militar

A operação civil-militar caracteriza-se pelo conglomerado de tarefas que procura instituir, preservar preponderância ou explorar as relações de coordenação e cooperação entre as autoridades e organizações não governamentais ou governamentais, a população civil e as FA, com a finalidade de colaborar para o gerenciamento de demais ações e operações, assim como o êxito com relação a deteminados objetivos militares (BRASIL, 2018).

Esse tipo de operação difere das Ações Cívico-Sociais (ACISO), pois ela não é somente assistencialista e tem sempre um propósito militar, podendo ser conduzida em ambiente permissivo, incerto e hostil (BRASIL, 2018).

A operação civil-militar colabora para garantir a confiabilidade da nossa Força, a lisura das ações e a legalidade das operações, tendo como foco as instituições locais e a população da respectiva área de operações, com o intuito de gerar um ambiente propício às

operações militares. Elas agem no sentido de contribuir para que as OpPsc e a ComSoc sejam integradas de forma a apoiar o atingimento de determinado objetivo. Dessa forma, verifica-se que é essencial o total apoio às OpInfo, por meio da efetiva integração das demais CRI com a Operação Civil-Militar BRASIL, 2018).

Após um estudo preliminar das principais CRI, pode-se observar que a Guerra da Ucrânia, ocorrida em 2014, pode ser analisada como um exemplo do emprego sincronizado e integrado das CRI na OpInfo. A desinformação foi empregada em sua plenitude pela Federação da Rússia de forma que a comunidade internacional fosse induzida a desconfiar das informações que estava recebendo. Nesse ínterim, a Ucrânia não conseguia responder de forma eficaz porque era atacada de forma impiedosa, por meio de OpPsc, GE e operações no espaço cibernético (BARBOZA; TEIXEIRA, 2020).

Os tomadores de decisão do Ocidente ficaram confusos e paralisados frente ao poderio e a eficácia da Guerra de Informação da Federação da Rússia, fazendo com que a mesma obtivesse a sua supremacia e conseguisse alcançar seus objetivos políticos e estratégicos, antes mesmo que as lideranças do Ocidente conseguissem responder tais atos (BARBOZA; TEIXEIRA, 2020).

As OpInfo fazem com que o Comandante tenha opções dissuasórias que são flexíveis e não possuem grau de letalidade. Dessa forma, o emprego das OpInfo torna-se viável tanto em relação a oponentes não estatais, quanto em relação a oponentes estatais. A especificidade da capacidade que o oponente possuir é o que determinará o grau de impacto. O objetivo estratégico principal das OpInfo é impedir as ameaças de potenciais oponentes (CLARK, 2010).

Pressionar um determinado grupo de líderes ou um líder central a adotar uma postura coadunável com os nossos interesses ou a abdicar de um determinado tipo de ação específica é a principal meta da OpInfo no nível estratégico (CLARK, 2010).

A simples aplicação individual de qualquer uma das CRI não caracteriza as OpInfo, mas sim a integração coordenada e sincronizada das combinações dessas capacidades, podendo evitar que o conflito armado ocorra, pois, nesse caso, pode-se produzir o componente ofensivo “não cinético” da força (CLARK, 2010).

Observa-se que o Direito Internacional é o que rege o conflito armado entre Estados. As OpInfo não obedecem ao preconizado nesse arcabouço jurídico. O Direito Internacional não faz menção ao emprego das OpInfo como um componente do conflito armado, sendo assim, o emprego das OpInfo como um elemento de dissuasão da guerra não pode ser encarado como um ato de guerra (CLARK, 2010).

A não classificação das OpInfo como um ato de guerra pode ser visualizada no artigo 41 da Carta da ONU, o qual é um exemplo da legislação vigente sobre o assunto em lide. O artigo enfatiza que ações com o objetivo de cessar as comunicações de um oponente poderão ser adotadas, sem que envolvam o uso de FA, após a aquiescência do Conselho de Segurança. Sendo assim, o emprego das OpInfo em operações de dissuasão, como o ataque a redes de computadores e a guerra eletrônica, não são considerados atos de guerra (CLARK, 2010).

Dessa forma, pode-se verificar que é muito mais exequível custear e divulgar a desinformação em associação com determinados tipos de atores não estatais do que dispersar carros de combate no terreno de outros Estados ou empregar a aviação de caça no espaço aéreo de outrem (WIELAND, 2022).

3.4 O emprego das OpInfo na anexação da Crimeia pela Federação da Rússia

As campanhas de informação têm como objetivo principal minar a confiança das pessoas nos procedimentos e nas estruturas do Estado, nas sociedades e nas instituições, gerando confusão, criando notícias falsas, veiculando as próprias narrativas do Estado agressor, prejudicando a reputação do sistema oponente, manipulando a opinião pública de forma agressiva (GAREIS, 2017). Observa-se que foram justamente essas ações que a Federação da Rússia implementou contra a Ucrânia em 2014.

A revolução Maidan, que estava em andamento na Ucrânia desde 2013, foi o estopim para que fosse iniciada a anexação da Crimeia em 2014, obrigando o então presidente do país, na época Viktor Yanukovych, a deixar o país em fevereiro de 2014, devido a uma série

de confrontos agressivos entre autoridades policiais e diversos manifestantes (WEISSMANN *et al.*, 2021).

O fato de existir na época um ambiente operacional totalmente propício para a Federação da Rússia na Península da Crimeia fez com que a operação de anexação transcorresse de forma eficaz e célere, em virtude de a Rússia possuir condições favoráveis no local. Destacam-se a existência de uma grande população de língua pró-russa e russa na península, a existência de uma brigada de infantaria naval, uma presença militar forte e um sistema de inteligência eficaz, em virtude da localização da sua frota do Mar Negro estar sediada em Sevastopol, além de possuírem o elemento surpresa a seu favor (WEISSMANN *et al.*, 2021).

A Federação da Rússia conseguiu atrair a população da Crimeia de língua russa a seu favor, assim como empregou as OpInfo em sua plenitude para disseminar que o novo governo da Ucrânia seria dominado por fascistas e o mesmo representava uma total ameaça para o povo russo e para os que falassem a língua russa, disseminando dessa forma um forte temor na população (WEISSMANN *et al.*, 2021).

A Rússia então elaborou uma nova fase de sua operação, transferindo os elementos de forças especiais conhecidos como Spetnaz para a Crimeia em 22 de fevereiro, sendo que esses militares não possuíam nenhum tipo de identificação e ficaram conhecidos como os “homenzinhos verdes”. Esses militares das forças especiais russas assumiram o controle de diversos locais importantes da península da Crimeia, entre eles o aeroporto de Simferopol, determinados prédios importantes do governo local e o controle do Parlamento da Crimeia (WEISSMANN *et al.*, 2021).

As forças militares ucranianas não conseguiram responder de forma eficaz, pois tiveram as suas bases militares sitiadas pelas unidades de infantaria de fuzileiros navais russos. Os tomadores de decisão ucranianos não conseguiram elaborar respostas eficientes devido à obscuridade do desenrolar das ações no campo de batalha. Dessa forma, as tropas russas assumiram o controle da Crimeia e foi instalado um novo governo pró-Rússia (WEISSMANN *et al.*, 2021).

Observa-se que o surgimento da internet e das mídias sociais alavancaram as OpInfo no contexto das operações militares. A Federação da Rússia desponta como um dos principais países detentores do conhecimento intrínseco nesse tipo de operação. Antes de ter a necessidade de empregar as operações cinéticas, a Federação da Rússia emprega as OpInfo que são menos onerosas e, dessa forma, o país explora as mesmas contra os seus adversários, conseguindo assim aperfeiçoá-las cada vez mais. A Federação da Rússia está diretamente envolvida nessas operações em diversos locais do mundo, contra diversos tipos de atores.

3.5 Conclusões Parciais

Pode-se observar que as OpInfo atualmente desempenham um papel essencial na evolução da Guerra Híbrida. Nota-se que sem o advento da evolução tecnológica, tal como a internet, as mídias sociais e os diversos dispositivos dotados de um alto grau de avanço tecnológico, assim como a velocidade e a facilidade com que as informações são disseminadas, dificilmente as OpInfo alcançariam o protagonismo observado atualmente.

Observa-se que o ciclo OODA possui uma relevância significativa no contexto das OpInfo, pois ele sempre procura afetar o processo de tomada de decisão do oponente, o que é uma das características intrínsecas da Guerra Híbrida.

Nota-se a necessidade das OpInfo serem mais bem estudadas pela MB e empregadas com maior intensidade nas diversas operações em que a mesma participa, de forma a obter-se maior conhecimento com relação a esse tipo de operação, uma vez que são menos onerosas e existe a possibilidade de se conseguir aperfeiçoá-las cada vez mais.

As CRI possuem um alto grau de relevância no contexto das OpInfo, porém elas nunca devem ser empregadas sozinhas sob o risco de perderem a sua eficácia. Pode-se observar ainda que as OpInfo possuem uma interconexão grande com as OpPsc. Elas devem ser sempre empregadas de forma sincronizada, pois o seu emprego de forma correta evita que haja a necessidade de ser usada a força.

A Federação da Rússia pode ser citada como um Estado que emprega as OpInfo com primazia contra seus adversários e segue aperfeiçoando cada vez mais esse tipo de operação com os conhecimentos obtidos por meio de suas ações no campo inimigo. O que a Federação da Rússia fez com a Ucrânia em 2014 e continua fazendo nos dias atuais, empregando de forma acentuada as OpPsc, a GE, a ComSoc, as ações cibernéticas, as operações civil-militares e a Desinformação, ressalta cada vez mais a real importância do papel das OpInfo na evolução da Guerra Híbrida.

O capítulo seguinte tem como propósito realizar uma abordagem de como a OTAN está se preparando, dentro da sua concepção estratégica, de forma a se contrapor às Ameaças Híbridas; como é realizado o seu combate à propaganda e à desinformação; verificar o seu Plano de Ação de Prontidão (PAP), a sua Força de Resposta (FR), a sua Força-Tarefa Conjunta de Alta Prontidão (FTCAP) e as suas Unidades de Integração de Forças (UIF).

4 A ESTRATÉGIA DA OTAN PARA SE PREPARAR, DISSUADIR E SE DEFENDER CONTRA AMEAÇAS HÍBRIDAS, A ELABORAÇÃO DO SEU PLANO DE AÇÃO DE PRONTIDÃO (PAP) E DA SUA FORÇA DE RESPOSTA (FR)

Este capítulo tem como objetivo analisar como a OTAN vem se preparando estrategicamente para se contrapor às Ameaças Híbridas, por meio da análise de como ela efetua sua preparação, dissuasão e defesa contra essas novas ameaças. Serão observadas as questões atinentes ao fortalecimento de sua resiliência nacional, o emprego de suas "Equipes contra-híbridas", o aperfeiçoamento de sua consciência situacional por meio da criação da Divisão Conjunta de Inteligência e Segurança (DCIS), que possui um ramo específico voltado para a análise híbrida e o seu quadro de Ameaças Híbridas.

Será realizada uma análise de seu combate à propaganda enganosa e à desinformação; como ocorre a sua avaliação, compartilhamento e coleta de informações com a finalidade de detectar e atribuir qualquer tipo de atividade híbrida que esteja sendo desenvolvida.

Será verificada a elaboração de seu Plano de Ação de Prontidão (PAP), da sua Força de Resposta (FR), da sua Força-Tarefa Conjunta de Alta Prontidão (FTCAP) e das suas Unidades de Integração de Forças (UIF).

A organização escolhida para servir de parâmetro para o estudo foi a OTAN, pois conforme se observa no capítulo 2, ela juntamente com a UE são as duas organizações que mais possuem estruturas e condições de se contraporem às Ameaças Híbridas.

4.1 A atual estratégia empregada pela OTAN para se preparar, dissuadir e se defender contra Ameaças Híbridas

Os países membros da OTAN enfrentam diversos desafios e ameaças de atores não estatais e estatais que empregam uma ampla gama de atividades híbridas para minar a segurança dos seus cidadãos, influenciar a opinião pública e afetar determinadas instituições políticas. Os métodos híbridos empregados para desestabilizar os oponentes incluem dentre

outros, a sabotagem, a propaganda, os ataques cibernéticos e o emprego de diversas outras táticas não militares, conforme foram observadas no capítulo 2 (NATO, 2023).

A intensidade, a escala e a velocidade que são facilitadas pela interconectividade global e pela rápida mudança tecnológica são a novidade com relação aos ataques perpetrados no decorrer dos últimos anos, mas precisamente após a anexação da Crimeia em 2014 (NATO, 2016; 2022; 2023).

Em face do exposto, a OTAN elaborou uma estratégia com relação ao seu papel não apenas no combate às Ameaças Híbridas como também na preparação para o combate a uma possível Guerra Híbrida, possuindo, portanto, plenas condições de prontificação para defender não somente a organização, mas também todos os países membros contra qualquer tipo de ameaça, seja ela híbrida ou até mesmo convencional (NATO, 2023).

Os países membros da OTAN conseguiram melhorar as suas capacidades de compreender, em toda a organização, o quadro de Ameaças Híbridas, e também conseguiram fortalecer a sua resiliência nacional, sendo o país-alvo responsável por responder a ataques ou Ameaças Híbridas de forma primária (NATO, 2023).

A OTAN elaborou diversas diretrizes visando o fortalecimento da resiliência de seus países-membros de forma a traçar uma referência para autoavaliações nacionais em áreas específicas, tais como comunicações e energia. Com o advento da constante evolução tecnológica, tal como a tecnologia de comunicação 5G, observa-se a necessidade de atualização regular desses requisitos (RÜHLE, 2021a).

As ações híbridas perpetradas contra a OTAN ou um de seus países-membros pode levar à evocação do Artigo 5°[19] da OTAN, sendo tal decisão declarada publicamente pela organização desde 2016 (NATO, 2023).

Analisando-se os parágrafos acima, pode-se observar portanto que essa evolução das Ameaças Híbridas somente se tornou possível graças ao advento das inovações tecnológicas, uma vez que as mídias sociais e as diversas facilidades no campo da internet facilitaram a proliferação dessas respectivas ameaças.

19 O artigo 5° da OTAN estabelece que qualquer ataque contra um ou demais aliados da OTAN na América do Norte ou na Europa será considerado um ataque contra todos os seus membros (MATTHYS, 2022).

A OTAN começou a abordar o assunto com um enfoque estratégico, por meio de sua dissuasão e defesa, fortalecendo assim a sua resiliência nacional e elevando a sua consciência situacional. A união dos seus países membros possibilitou o seu fortalecimento e a sua compreensão com relação à interpretação do seu quadro de Ameaças Híbridas.

A sua postura firme com relação à evocação do Artigo 5°, caso ocorra uma falha na sua dissuasão, mesmo que para isso seja necessário o emprego da força, faz com que ela seja respeitada em todo o mundo.

A criação de “Equipes contra híbridas” mostra o seu elevado grau de profissionalismo, comprometimento e a sua seriedade com relação ao assunto afeto às Ameaças Híbridas.

A organização combate de forma ativa e intensa a propaganda enganosa e a desinformação, com a apresentação de fatos tanto na mídia impressa quanto nas mídias sociais, ao invés de utilizar apenas o emprego de mais propaganda como mecanismo de autodefesa (NATO, 2023).

Observa-se ainda que a OTAN prioriza o emprego da comunicação estratégica, principalmente no que diz respeito ao combate de propaganda enganosa e desinformação.

A área afeta à inteligência constitui-se como essencial para o combate às Ameaças Híbridas e pode-se observar que a OTAN encontra-se em um nível bastante elevado com relação à questão atinente ao compartilhamento de informações.

Outro quesito que se pode observar no que diz respeito à preocupação da OTAN, refere-se ao mapeamento das infraestruturas críticas, a identificação das vulnerabilidades críticas e o fortalecimento da resiliência, que são essenciais para o combate às Ameaças Híbridas.

Para se contrapor às Ameaças Híbridas, a OTAN está determinada a agir imediatamente, quando e onde for necessário. Ela continua a elevar a preparação e a prontidão de suas forças e tem reforçado a sua estrutura de comando e o seu processo de decisão como parte da adoção de uma postura de defesa e dissuasão. Esse ato pode ser entendido como um sinal de que a OTAN está aperfeiçoando a sua capacidade de envio de forças específicas para o local certo no momento adequado e a sua capacidade de resposta militar e política (NATO, 2023).

Os países-membros da organização conseguiram desenvolver opções de resposta e de prevenção abrangentes, possibilitando que a organização aumente a sua caixa de ferramentas para combater Ameaças Híbridas. Essas opções desenvolvidas possibilitam combinar ferramentas militares e civis, que podem sofrer adaptações com o objetivo de responderem a determinados tipos de situações específicas (NATO, 2023).

Caso ocorra uma falha no processo de dissuasão, a OTAN encontra-se pronta para defender quaisquer de seus países-membros contra qualquer tipo de ameaça. Dessa forma, as forças da OTAN devem ser capazes de reagir de maneira ágil e rápida, onde e quando for necessário (NATO, 2023).

A cooperação da OTAN com parceiros, como os países da UE, com o objetivo de aumentar a resiliência e combater Ameaças Híbridas, torna-se essencial, pois é extremamente difícil combater essas ameaças de forma isolada. Visando o combate a ataques cibernéticos, a UE e a OTAN têm intensificado essa cooperação (NATO, 2023).

Além disso, visando o combate à desinformação, a OTAN também está trocando experiências com países parceiros na região do Indo-Pacífico, tais como: Coreia do Sul, Austrália, Nova Zelândia e Japão, com a finalidade de combater as questões afetas à segurança na Península Coreana, o elevado crescimento e a ambição estratégica da República Popular da China (NATO, 2023; 2023a).

A OTAN ampliou a sua capacidade de envio de forças específicas para auxiliar seus países-membros em diversos locais do mundo, aumentando assim a sua mobilidade, flexibilidade e rápida resposta. Além disso, ela ampliou a sua caixa de ferramentas para combater Ameaças Híbridas, elevando assim a sua quantidade de recursos disponíveis para resposta.

A gama de ferramentas empregadas pelas Ameaças Híbridas é extremamente complexa e extensa, fazendo com que seja necessário recorrer ao apoio de demais parceiros para se contrapor a essas ameaças, pois sozinho torna-se bastante difícil efetuar um combate de forma eficaz.

A criação de Centros de Excelência para combater Ameaças Híbridas foi uma forma encontrada para contribuir com experiência e conhecimento para a OTAN. Eles são centros

de pesquisa internacionais com financiamento e equipe multinacional ou nacional (NATO, 2023).

Podemos citar os seguintes Centros de Excelência que contribuem com a OTAN para combater as Ameaças Híbridas: o Centro de Excelência em Segurança Energética em Vilnius, Lituânia; o Centro Cooperativo de Excelência em Defesa Cibernética em Tallinn, Estônia; o Centro de Excelência em Comunicações Estratégicas em Riga, Letônia e o Centro Europeu de Excelência para Combater Ameaças Híbridas localizado em Helsinque, Finlândia, o qual funciona como um centro de especialização, apoiando os países membros a elevar a sua resiliência, a sua preparação para combater Ameaças Híbridas e as suas capacidades civis-militares (NATO, 2023).

O Centro Europeu de Excelência para Combater Ameaças Híbridas é apoiado pela UE, OTAN e por mais 30 países, tendo sido criado em outubro de 2017 por uma iniciativa do Governo da Finlândia (NATO, 2023).

Fortalecer, construir e reconstruir a confiança continua sendo essencial para gerar uma resiliência consistente perante as Ameaças Híbridas, que colocam em risco a segurança nos níveis social e estatal. Para que qualquer resposta estratégica ou política se concretize, a confiança continua sendo condição essencial para que se consiga atingir tal objetivo (BILAL, 2021).

O combate às Ameaças Híbridas constitui-se em um desafio de longo prazo para a OTAN e seus aliados, além de ser estratégico. Dessa forma, dentre os diversos mecanismos elaborados pela OTAN em sua caixa de ferramentas para combater Ameaças Híbridas, podem-se destacar os seguintes: aperfeiçoamento de sua consciência situacional por meio de sua DCIS; adaptação de seus exercícios com a inserção de elementos híbridos; garantia da resiliência das infraestruturas civis nacionais aliadas; aperfeiçoamento da sua defesa cibernética; implantação de “Equipes contra-híbridas”; deter Ameaças Híbridas por meio de dissuasão, seja ela por negação ou por punição; aproximar elementos civis e militares por meio da criação de pacotes de medidas que deverão permitir respostas mais personalizadas e uma tomada de decisão mais rápida; analisar a viabilidade de emprego de tecnologias disruptivas emergentes, como a inteligência artificial; detecção e resposta à desinformação;

analisar novas formas de envolver todo o Governo no combate às Ameaças Híbridas; aprofundar as relações OTAN-UE e ampliar a cooperação com parceiros (RÜHLE, 2021).

Observa-se que uma excelente iniciativa da OTAN foi a criação dos Centros de Excelência para combater Ameaças Híbridas, possibilitando que pessoas com diversas expertises possam compartilhar seus conhecimentos para elaborarem mecanismos para se contraporem às Ameaças Híbridas.

A elaboração de diversos mecanismos em sua caixa de ferramentas para combater Ameaças Híbridas, visando um enfoque estratégico e a longo prazo, credenciam a OTAN como uma das organizações que se encontra bastante avançadas nos assuntos atinentes às Ameaças Híbridas e à Guerra Híbrida.

4.2 Plano de Ação de Prontidão (PAP) da OTAN

O PAP da OTAN constitui-se na adoção de um pacote com a implementação de diversas medidas denominadas de “medidas de adaptação” e “medidas de garantia”, adotadas pela organização e consideradas essenciais estrategicamente para a implementação de sua defesa e dissuasão. Ele foi concebido em setembro de 2014 e tem como objetivo garantir que a OTAN esteja sempre pronta para responder aos novos desafios de segurança com celeridade e solidez (NATO, 2022).

Com relação às medidas de garantia, pode-se enfatizar que a área Euro-Atlântica tem sofrido desde 2014 mudanças no seu ambiente de segurança. Dessa forma, o PAP tem como finalidade prover medidas de garantia para os países membros da OTAN na Europa Oriental e Central com o intuito de reforçar a sua defesa, impedir possíveis agressões e tranquilizar suas populações (NATO, 2022);

As medidas de garantia, dependendo da situação de segurança, podem ser intensificadas ou reduzidas. Elas foram implementadas como uma resposta às ações agressivas da Rússia contra a Ucrânia que resultou na anexação da Crimeia em 2014 (NATO, 2016; 2022). A Rússia alcançou seus objetivos por meio do emprego de desinformação, exploração da polarização sociopolítica na Ucrânia, emprego de atores armados locais,

influência econômica e negação do emprego de forças especiais (os chamados "homenzinhos verdes") (BILAL, 2021).

As Medidas de Garantia adotadas pela OTAN incluem:

– Aumento do número de aviões de caça empregados em patrulhas de policiamento aéreo sobre os Estados Bálticos; envio de aviões de caça para a Polônia, Romênia e Bulgária, sendo tais ações implementadas desde maio de 2014 (NATO, 2016; 2022);

– Adoção de um pacote de medidas de garantia para a Turquia, desde dezembro de 2015, com o objetivo de implementar a adoção de respostas para os crescentes desafios de segurança provenientes do sul (NATO, 2022);

– Realização pela OTAN, ao longo das fronteiras orientais do território aliado, de voos de aeronaves de patrulha marítima e voos regulares de vigilância AWACS[20] (NATO, 2022);

– Destaque pela OTAN de diversas Forças Marítimas Multinacionais (FMM) para realizarem Patrulhas Marítimas (PM) no Mar Mediterrâneo, Mar Negro e Mar Báltico, com a finalidade de fornecer segurança marítima. Entre seus componentes podemos destacar 1 Grupo Marítimo Permanente (GMP), que realiza patrulhas antiterroristas e conduz medidas de segurança marítima, e 2 Grupos Permanentes de Contramedidas de Minas (GPCM), que patrulham o Mediterrâneo Oriental e o Mar Báltico (NATO, 2016; 2022);

– Elevação pela OTAN, de forma significativa, da realização dos seus exercícios militares, pois eles representam uma importante demonstração do grau de prontidão da organização para responder a potenciais Ameaças Híbridas e proporcionam importantes oportunidades para aperfeiçoar a capacidade para que os parceiros e países-membros trabalhem em conjunto. Esses exercícios são realizados no ciberespaço, no ar, no mar e em terra com cenários focados na gestão de crises e na defesa coletiva (NATO, 2022); e

– As medidas de garantia são mantidas sob revisão anual pelo Conselho do Atlântico Norte (CAN), além de serem escaláveis e flexíveis em resposta à evolução da situação de segurança (NATO, 2022).

20 O AWACS constitui-se de um centro móvel de longo alcance para defesa aérea com a finalidade de realizar o controle e a vigilância por meio de radar. A sua sigla significa Airborne Warning And Control System (Sistema de Alerta e Controle Aerotransportado). Ele é montado em uma aeronave Boeing 707 modificada para esse tipo de emprego. O sistema de radar consegue identificar, rastrear e detectar aeronaves voando baixo a cerca de 200MN, além de conseguir operar em qualque terreno e clima e rastrear o tráfego marítimo (BRITANNICA, 2023).

Observa-se que a implementação do PAP foi uma forma encontrada para efetuar uma resposta rápida contra possíveis Ameaças Híbridas desencadeadas contra a OTAN ou um de seus países-membros. As medidas de garantia e as medidas de adaptação têm um enfoque estratégico visando a implementação de sua defesa e dissuasão.

A adoção pela OTAN das medidas de garantia visam reforçar a sua defesa, impedir possíveis agressões e tranquilizar suas populações, principalmente levando-se em consideração os acontecimentos ocorridos na Ucrânia que resultaram na anexação da Crimeia em 2014.

O emprego de aviões de caça para patrulha e alarme aéreo antecipado, o emprego de navios para realizarem PM com ênfase em ações antiterroristas, a realização de caça de minas, o aumento dos exercícios militares, a realização de exercícios no ciberespaço, no ar, no mar e em terra com cenários focados na gestão de crises e na defesa coletiva são algumas das medidas de garantia adotadas pela OTAN.

As medidas de adaptação abordam diversas mudanças de longo prazo na estrutura de comando e nas forças da OTAN, de forma que ela tenha capacidade de empreender uma reação ágil e decisiva a possíveis crises repentinas que venham a surgir (NATO, 2016; 2022).

As medidas de adaptação estabeleceram Forças Navais Permanentes (FNP) aprimoradas, uma Força-Tarefa Conjunta de Alta Prontidão (FTCAP) com a capacidade de ser destacada em um curto espaço de tempo e triplicaram o tamanho da sua Força de Resposta (FR) (NATO, 2022).

As Medidas de Adaptação adotadas pela OTAN incluem:

– Uma FR com composição multinacional, tecnologicamente avançada e altamente preparada, composta por elementos das Forças de Operações Especiais (FOpEsp), aéreos, marítimos e terrestres, os quais a OTAN pode destacar rapidamente para pronto emprego (NATO, 2022);

– A FTCAP fica localizada dentro da FR da OTAN, sendo seu elemento terrestre suportado por uma brigada terrestre multinacional com elementos das FOpEsp, marítimos e aéreo. Essa Força possui em torno de 20.000 soldados, dos quais cerca de 5.000 integram as forças terrestres estando no momento operacional e os seus componentes conseguem

realizar o seu deslocamento para a cena de ação em um curto espaço de tempo, normalmente entre 2 e 3 dias. Os componentes da FTCAP e da FR da OTAN podem ser desdobrados de seus países de origem para onde for necessário responder a crises, participar de exercícios ou realizar defesa coletiva, sendo a liderança da FTCAP exercida por seus países membros de forma rotativa (NATO, 2016; 2022; 2022a); e

– As Unidades de Integração de Forças (UIF) da OTAN correspondem a pequenos quartéis-generais com composições multinacionais que possibilitam o célere destacamento das Forças de Acompanhamento Aliadas (FAA) e da FTCAP. Atualmente existem 8 UIF localizadas na Europa Oriental e Central. A sua tarefa é aperfeiçoar a coordenação e cooperação entre as Forças Nacionais e a OTAN, assim como apoiar e preparar destacamentos e exercícios necessários (NATO, 2016; 2022).

Dentro da Estrutura de Comando da OTAN, foi estabelecido um quartel-general permanente do Grupo de Apoio Logístico Conjunto (GALC) para possibilitar ao PAP implementar uma série de melhorias logísticas, incluindo o pré-posicionamento de suprimentos e equipamentos, com o objetivo de elevar o grau de prontidão da OTAN para responder a qualquer desafio que afete a segurança dos países membros (NATO, 2022).

Observa-se que a adoção pela OTAN das medidas de adaptação visam a abordagem de diversas mudanças de longo prazo na estrutura de comando e nas forças da OTAN. A implementação de 1 FR com FopEsp; meios aéreos, marítimos e terrestres; 1 FTCAP; 8 UIF; 1 GALC, mostram o quão avançada está essa organização para se contrapor a Ameaças Híbridas e até mesmo a uma Guerra Híbrida.

4.3 A Força de Resposta (FR) da OTAN

Apesar de ter sido citada no item 4.2, é oportuno um aprofundamento a cerca dos detalhes envolvendo a FR da OTAN.

A FR pode ser empregada para se obter maior cooperação em treinamento e educação, melhor emprego da tecnologia, suporte para socorro em desastres e aumento de exercícios, além do cumprimento de seu papel operacional, possuindo como principal

objetivo o de ter a capacitação de possibilitar uma resposta militar célere a uma possível crise procedente, seja para diversas outras operações de resposta a determinadas crises ou para fins de defesa coletiva (NATO, 2022a).

Os países-membros da OTAN fornecem unidades de FOpEsp, marítimas, aéreas e terrestres para a composição da FR por um período de 12 meses e dentro de um sistema de rotatividade. Não são somente os países-membros da OTAN que podem compor a FR, mas também alguns países parceiros, desde que sejam aprovados pelo CAN (NATO, 2022a).

A criação da FTCAP, denominada como uma espécie de “Força de Ponta de Lança”, foi uma forma encontrada pelos países-membros da OTAN para aprimorar a FR, sendo que esse aprimoramento tem como objetivo responder às mudanças no ambiente de segurança, o que é uma das medidas do PAP (NATO, 2022a).

Segundo a NATO (2022a), a FR da OTAN é composta pelos seguintes elementos:

– Comando e Controle: O Comando Operacional da FR tem sua alternância delimitada entre os Comandos das Forças Conjuntas Aliadas (CFCA) em Nápoles, na Itália, e Brunssum, nos Países Baixos. O Comando-Geral da FR pertence ao Comandante Supremo Aliado da Europa;

– O Grupo Inicial de Forças de Acompanhamento (GIFA): é formado por 2 brigadas multinacionais, que podem ser desdobradas de forma rápida logo após a FTCAP, com a finalidade de responder a uma crise, sendo assim classificadas como Forças de Alta Prontidão (FAP);

– Componente marítimo: Composto por Grupos Permanentes de Contramedidas de Minas (GPCM) e Grupo Marítimo Permanente (GMP); e

– A FTCAP; uma Força-Tarefa Nuclear, Biológica, Química e Radiológica (NBQR); elementos das FopEsp; um componente de combate aéreo e de apoio aéreo.

A FR possui cerca de 40.000 soldados e a sua liderança é escalada anualmente de forma rotativa, com um país-membro classificado como o país líder e os outros países-membros participantes. As FR podem ser implantadas onde forem necessárias para defesa coletiva, resposta a crises ou para realização de exercícios, apesar de estarem baseadas em seus países de origem (NATO, 2022a).

A FR é testada regularmente por ocasião da realização dos diversos exercícios dos quais participa de forma, a aprimorar a sua capacitação de implantar e responder a qualquer crise que apareça. O seu primeiro exercício de implantação ocorreu em junho de 2015, na Polônia (NATO, 2022a).

Pode-se destacar que os componentes da FR foram empregados em setembro de 2004 para apoiar as eleições presidenciais afegãs e também em apoio aos Jogos Olímpicos de verão de 2004 em Atenas, na Grécia (NATO, 2022a).

A criação do Plano de Resposta Graduada (PRG) foi uma ferramenta de planejamento avançado elaborada pela OTAN e aprovada pelos seus países-membros, a qual possibilita que os Planos de Operações, executáveis conforme os requisitos de prontidão das forças, sejam gerados com excepcional rapidez (NATO, 2022a).

A Capacidade Operacional Inicial (COI) da OTAN, visando a iniciativa Conjunta de Inteligência, Vigilância e Reconhecimento, tem como objetivo aperfeiçoar a consciência situacional da FR, por meio de maior capacidade no processamento, troca e coleta de informações (NATO, 2022a).

O exercício Cold Response 2022, realizado na Noruega entre março e abril de 2022, com a participação de 27 países, reunindo mais de 30.000 militares, teve como finalidade testar a capacidade da FR de prover a integração das FA dos países-membros e demais parceiros com o objetivo de defender o território da OTAN e de fortalecer a Noruega (NATO, 2022a).

Pode-se observar que o principal objetivo para a criação da FR foi o de fornecer uma resposta militar célere a uma possível crise procedente. A sua composição contempla unidades de FOpEsp, marítimas, aéreas e terrestres. Ela foi aprimorada com a implementação da FTCAP em seu contexto. A composição da FR com Comando e Controle, GIFA, componente marítimo, Força-Tarefa NBQR, FopEsp, um grande número de militares componentes, a sua participação em diversos exercícios e a capacidade de ser empregada em diversas áreas de atuação, ressaltam a sua importância para a OTAN e seus países-membros como elementos de dissuasão contra Ameaças Híbridas.

4.4 Conclusões Parciais

Ao final deste capítulo, pode-se observar que a OTAN tem avançado de forma significativa na sua preparação para se contrapor às Ameaças Híbridas, mesmo com o advento das inovações tecnológicas. A organização começou a abordar o assunto com um enfoque estratégico, por meio de sua dissuasão e defesa, fortalecendo assim a sua resiliência nacional e elevando a sua consciência situacional.

A OTAN conseguiu compreender como funciona o quadro de Ameaças Híbridas, elaborou diversas diretrizes, criou "Equipes contra-híbridas" e uniu-se com a UE para ampliar a sua gama de ferramentas. Criou o DCIS para melhorar a consciência situacional e priorizou um ramo específico voltado especificamente para a análise híbrida, mostrando assim o seu elevado grau de profissionalismo, comprometimento e a sua seriedade com relação ao assunto afeto às Ameaças Híbridas.

A organização priorizou a identificação de suas vulnerabilidades críticas nacionais e forneceu apoio aos países-membros em diversas áreas, tais como: proteção de infraestrutura crítica; segurança energética; contraterrorismo; comunicações estratégicas; defesa cibernética; proteção de civis e resposta a incidentes NBQR.

A implementação do PAP, FR, FTCAP e UIF, foi uma forma encontrada para efetuar uma resposta rápida contra possíveis Ameaças Híbridas desencadeadas contra a OTAN ou um de seus países-membros, mostrando o quão avançada está essa organização para se contrapor a Ameaças Híbridas e até mesmo a uma Guerra Híbrida.. As medidas de garantia e as medidas de adaptação têm um enfoque estratégico visando a implementação de sua defesa e dissuasão.

Assim, torna-se essencial se estudar essas organizações para se obter conhecimento com as mesmas sobre o assunto em lide, uma vez que no Brasil existem raríssimas obras e artigos afetos a Ameaças Híbridas e Guerra Híbrida.

No capítulo seguinte, será realizada uma abordagem com relação aos possíveis cenários para Ameaças Híbridas Marítimas segundo o Hybrid CoE, com o objetivo de se angariarem subsídios para a formulação de medidas que possam ser implementadas na MB.

5 A GUERRA HÍBRIDA MARÍTIMA E AS AMEAÇAS HÍBRIDAS MARÍTIMAS.

Este capítulo tem como objetivo analisar aspectos intrínsecos à Guerra Híbrida Marítima (GHM) e às Ameaças Híbridas Marítimas (AHM). Será estudada a questão atinente as "Milícias Marítimas Chinesas" (MMC), também intituladas como "Forças Navais Civis Híbridas" (FNCH).

Serão analisados os possíveis cenários para as AHM, por meio de estudos realizados pelo Centro Europeu de Excelência para Combater Ameaças Híbridas (*Hybrid CoE*), sendo dado enfoque para análise de um cenário visando a proteção de um gasoduto submarino. Será analisada, como um exemplo específico, a explosão dos gasodutos entre a Rússia e a Europa, Nord Stream 1 e 2, de forma a serem obtidos ensinamentos para subsidiar o estudo para adoção de ações específicas para a MB no que tange à prevenção contra possíveis acontecimentos em Águas Jurisdicionais Brasileiras (AJB).

Observa-se que atualmente o extremismo transnacional[21], a proliferação da tecnologia avançada e a globalização corroboram para que as Marinhas operem em uma época de elevada complexidade, ocasionada pelo agravamento de um ambiente de completa incerteza, acentuando o desafio para a compreensão de qual o ambiente operacional atual de atuação das FA (WIELAND, 2022).

Conforme Kremidas-Courtney (2018), há uma grande vulnerabilidade no domínio marítimo com relação ao advento das AHM, pois como observado no Mar da China Meridional e na Crimeia, o emprego de atores híbridos faz com que seja menos onerosa uma anexação territorial ou uma alteração de regime, reduzindo assim o custo político da respectiva agressão.

Ainda segundo Kremidas-Courtney (2018), foram identificadas 7 vulnerabilidades às AHM:

– **Comércio marítimo**: a não autorização para acesso a algumas instalações portuárias críticas, as interferências em determinados sistemas de navegação, os danos ambientais, a

21 O extremismo transnacional desenvolveu-se com a advento das mídias sociais e da internet, pois tais mecanismos possibilitaram que extremistas, que utilizam um alto grau de violência, desenvolvessem por meio de publicações online; vídeos; plataformas de imagens e mensagens a sua forte presença na internet. Determinados tipos de indivíduos que são simpatizantes a mensagens extremistas são facilmente recrutados e radicalizados por esses grupos (FBI, 2023).

sabotagem, os ataques cibernéticos perpetrados contra sistemas de informações da cadeia de suprimentos, ocasionando a interrupção ou perdimento da carga, são alguns exemplos de vulnerabilidades às Ameaças Híbridas que os portos comerciais e as embarcações estão sujeitos a enfrentarem;

– **Cibernética**: os sistemas de informação portuária e os sistemas de navegação são alguns dos recursos de habilitação cibernética aos quais as atividades militares e marítimas comerciais possuem dependência, sendo que os mesmos possuem grande vulnerabilidade a ataques cibernéticos, que podem ser perpetrados por organizações criminosas ou por atores híbridos;

– **Energia**: a variação das distribuições de energia ocasionou uma elevação da relevância do Gás Natural Liquefeito (GNL), englobando as instalações de descarga em terra e os navios de transporte. O transbordo de GNL e petróleo no mar, assim como a exploração de petróleo e gás, fazem com que a cadeia de abastecimento de energia tenha sua vulnerabilidade elevada com relação às Ameaças Híbridas, principalmente contra entidades comerciais que transportam, extraem e exploram essas *commodities*;

– **Comunicações**: os cabos submarinos atualmente concentram cerca de 97%[22] das comunicações intercontinentais, sendo que os mesmos apresentam grandes vulnerabilidades e, somando-se a isso, observa-se que as economias nessa era da globalização são extremamente dependentes da infraestrutura global de Tecnologia da Informação (TI). O montante de recursos em transações financeiras que é transportado diariamente pelos cabos submarinos equivale a cerca de 10 trilhões de dólares estadunidenses[23], o que demonstra a elevada dependência que a economia global possui com relação a esses cabos. Segundo Wieland (2022), esses cabos são de propriedade de entidades privadas, sendo que os Estados possuem certa dependência estratégica com relação à sua operacionalidade e à sua integridade;

– **Vulnerabilidades Territoriais:** os atores híbridos podem contestar e até interromper as Zonas Econômicas Exclusivas (ZEE) e as fronteiras de nações costeiras, sob o argumento de

22 Informação disponível em: <https://maritime--executive-com.translate.goog/editorials/countering-hybrid-threats-in-the-maritime-environment?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em: 02 jun. 2023.

23 Informação disponível em: <https://maritime--executive-com.translate.goog/editorials/countering-hybrid-threats-in-the-maritime-environment?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em: 02 jun. 2023.

estarem atuando para contestar a governança de seu território soberano em nome de um Estado. Sendo um aspecto fundamental da governança a capacidade de proteger, manter e controlar o território soberano, essas estão entre as tarefas centrais das Forças Navais (FN) e da Guarda Costeira (GC). A GC possui Regras de Engajamento (RE) pré-estabelecidas, com o objetivo de respaldar-se para, caso seja necessário, utilizar a força letal;

– **Ameaças às Forças de Segurança Marítima**: objetivando surpreender determinadas embarcações militares, com o intuito de impedir que as mesmas tenham capacidade de responder a outros elementos de um ataque híbrido, são empregadas embarcações não identificadas disfarçadas de embarcações pesqueiras ou comerciais, além de mergulhadores armados pelos atores híbridos clandestinos. As Forças de Segurança Marítima (FSM) possuem como grande desafio a capacidade de responder, atribuir e detectar essas ameaças. Além disso, os atores híbridos atualmente podem ter acesso à sofisticada tecnologia comercial pronta para uso, de forma que a mesma seja empregada para obterem sucesso em suas missões, obrigando então que as FSM se adaptem de forma constante para mitigar esses riscos; e

– **Desinformação**: com a finalidade de se criar uma falsa narrativa, a fim de minar a confiança regional e interna, são realizadas as campanhas de desinformação pelos atores híbridos adversários. As atividades e intenções das FSM amigas, bem como seus respectivos Governos, podem ter as suas legitimidades questionadas por meio de campanhas de desinformação em toda a mídia, tanto interiormente entre seu próprio povo como em outros países.

Kremidas-Courtney (2018) relaciona alguns requisitos emergentes para combater AHM, tais como: a capacidade de recuperar e operar o controle do ciberespaço contestado; a capacidade de atribuir e detectar Ameaças Híbridas no mar e em terra; a capacidade de operar de forma decisiva e rápida em um ambiente de contestada informação pública; a capacidade de recuperar e operar o controle de espaços comerciais contestados; a capacidade de diferenciar embarcações privadas e comerciais de embarcações de Ameaças Híbridas clandestinas; a realização de um processo de triagem com relação ao investimento estrangeiro nacional, assim como em toda a UE para tecnologias sensíveis e infraestrutura

crítica; a elaboração de uma revisão das RE das FSM e dos Quadros Jurídicos Nacionais (QJN), de forma a garantir que sejam apropriadas e suficientes para a tarefa de combater e dissuadir as AHM; realização de discussões baseadas na prospecção de cenários e na elaboração de exercícios abrangentes, com o intuito de desenvolver o compartilhamento de informações entre entidades privadas e públicas, assim como uma cooperação mais profunda.

Observa-se que, com o advento do avanço tecnológico, as Ameaças Híbridas não se restringem somente ao ambiente terrestre e já estão operando no ambiente marítimo. As vulnerabilidades observadas no ambiente marítimo são enormes, pois a grande maioria do comércio mundial ocorre pelo modal marítimo. O comércio marítimo, as instalações portuárias, os navios de guerra e os navios mercantes, os gasodutos, as plataformas petrolíferas e os cabos submarinos são algumas das vulnerabilidades observadas e que podem ser utilizadas como porta de acesso para as AHM. Dessa forma, mapear essas vulnerabilidades torna-se essencial para se contrapor às mesmas, assim como a elaboração de RE perfeitamente bem definidas.

Segundo Stavridis (2016), as águas costeiras dos litorais serão o palco para a condução da GHM. O emprego de meios, tais como: pequenas embarcações rápidas com grande manobrabilidade, grandes embarcações empregadas na pesca, navios petroleiros costeiros leves e até embarcações pequenas com motores de popa, serão os mecanismos adotados para a GHM, ao invés do uso da força de forma direta, por meio dos navios de guerra.

Ela também será conduzida e possivelmente controlada e comandada a partir das GC de algumas nações, que são conhecidos como os “cascos brancos”. Observa-se que a República Islâmica do Irã está empregando a sua Guarda Revolucionária no Golfo Pérsico e a República Popular da China está empregando a sua GC no Mar da China Meridional (STAVRIDIS, 2016).

Devido à ousadia, à evolução e ao ineditismo da República Popular da China no que diz respeito à GHM, a questão atinente ao emprego da GC no Mar da China Meridional será objeto de estudo no item 5.1 deste capítulo, porém será realizada abaixo uma rápida abordagem sobre o assunto em lide, de forma a se compreender esse complexo contexto.

Elementos que não são exatamente funcionários uniformizados, conhecidos como “pequenos marinheiros azuis”, serão os condutores das embarcações empregadas para a GHM.

Eles podem ser classificados como terroristas, atores desonestos, nacionalistas ou até mesmo como marinheiros de férias e agindo por sua livre e espontânea vontade, tudo isso para dar a aparência de uma ação desencadeada por um ator não estatal (STAVRIDIS, 2016).

Esses “pequenos marinheiros azuis”, como são chamados, se forem capturados serão orientados a negarem que façam parte de qualquer tipo de Força Armada organizada, não portarão passaportes e não possuirão nenhum tipo de identificação em suas roupas. Dentro dos meios empregados para a GHM, haverá uma grande variedade de armas, desde metralhadoras de grosso calibre até armas leves, além de mísseis superfície-ar leves e mísseis superfície-superfície portáteis. Eles deverão ter acesso a canhões de água, outros tipos de armas não letais, emissores de som, bombas de gás lacrimogêneo e ofuscadores de laser de alta intensidade (STAVRIDIS, 2016).

Analisando-se a elevação do nível de sofisticação da GHM com o decorrer dos anos, pode-se inferir que há possibilidade de que algumas nações construam uma pequena força de determinados tipos de navios, especialmente projetados para se assemelharem com embarcações comerciais de médio e pequeno porte ou navios costeiros, além de possuírem estrutura portuária para facilitar a sua logística na ocultação de armamentos, possibilidade de lançamento de lanchas do interior de suas respectivas baías e a capacidade de operarem navios-mãe para apoiar embarcações menores e com grau de sofisticação menos elevado para a condução da GHM (STAVRIDIS, 2016).

Segundo Stavridis (2016), existem 4 vantagens com relação à GHM:

– Possibilita que um determinado país consiga conduzir operações específicas e direcionadas para destruir, degradar e intimidar as capacidades de um adversário sem que lhe seja atribuída qualquer culpa, permitindo que não lhe sejam imputadas sanções e determinados tipos de críticas por meio da comunidade internacional;

– O fator surpresa é uma vantagem intrínseca à GHM, pois o oponente pode não ter a menor noção das consequências que lhe serão imputadas por meio de uma ação;

– A sua ambiguidade possibilita ao usuário ter um controle positivo da linha do tempo e do andamento dos eventos por meio do emprego de suas técnicas; e

– O baixo custo em comparação com os elevados gastos afetos à Guerra Costeira Convencional.

Observa-se uma grande necessidade para que os Estados desenvolvam mecanismos para se defenderem, dissuadirem e se prepararem contra AHM, uma vez que cerca de 90%[24] do transporte mundial é realizado pelo modal marítimo (KOTMAN, 2021).

Nota-se que é vislumbrado o emprego de diferentes tipos de meios para a condução de uma GHM, sendo que algumas ações já se encontram sendo realizadas pela República Popular da China, República Islâmica do Irã e até mesmo pela Federação da Rússia na questão atinente à Guerra da Ucrânia (2022 – presente). O emprego dos "pequenos marinheiros azuis" pela República Popular da China é uma evolução das ações utilizadas pela Federação da Rússia durante a anexação da Crimeia em 2014, quando foram empregados os "pequenos homenzinhos verdes". A adoção de uma GHM possui algumas vantagens, pois opera na chamada zona cinzenta, utiliza-se do fator surpresa, possui características ambíguas e possui um baixo custo. O emprego de recursos de inteligência modernos e eficazes, o compartilhamento de informações e o emprego de recursos tecnológicos modernos são essenciais para se contrapor a esse novo tipo de ameaça.

5.1 As Milícias Marítimas Chinesas (MMC)

Conforme contextualizado acima e devido aos constantes acontecimentos relacionados ao Mar do Sul da China, os chineses desenvolveram uma espécie de "Milícia Marítima" (MM), onde pode ser percebida uma certa confusão entre a linha tênue que separa as Forças Navais dos barcos de pesca sendo para esse caso específico, essencial a interpretação do Direito Marítimo Internacional (DMI) (KORKMAZ, 2020).

Esses barcos de pesca funcionam como componentes militares e atuam juntamente com a Guarda Costeira Chinesa (GCC) e as Forças Navais Chinesas (FNC) (KORKMAZ, 2020).

Os elementos que conduzem essas embarcações, apesar de se vestirem com trajes civis, são na realidade reservistas navais com treinamento específico para operações navais.

---

24 Informação disponível em: <https://www.marseccoe.org/wp-content/uploads/2021/08/Maritime-Hybrid-Threat.pdf>. Acesso em 02 jun. 2023.

Eles possuem equipamentos específicos para poderem se comunicar com a GCC e as FNC (MORRIS *et al.*, 2019).

No ano de 2019, o exército da República das Filipinas detectou na área de Sandy Cay, perto da ilha de Thitu, cerca de 275 navios. A República Popular da China alega que as embarcações não possuíam nenhum tipo de armamento, sendo somente barcos de pesca, porém alguns especialistas sobre o assunto abordam o complexo tema como uma guerra de guerrilha no mar (KORKMAZ, 2020).

Essas MM dificultam o acesso às áreas em disputa e realizam atividades de reconhecimento ou, reivindicações regionais, com a finalidade de alcançar seus objetivos estratégicos (KORKMAZ, 2020).

Esses barcos conseguem coletar informações no mar e disseminá-las para suas cadeias de comando, além de rastrear a localização de contatos de interesse, devido aos seus avançados equipamentos de navegação por satélite (KORKMAZ, 2020).

Amparando-se em leis que regulam que os barcos de pesca a menos que estejam envolvidos em um ato de guerra devem ser protegidos, a República Popular da China amplia a sua frota de barcos pesqueiros com o intuito de obter apoio no que tange às suas reivindicações geopolíticas no Mar da China Meridional (KORKMAZ, 2020).

Estima-se que existam cerca de 23.000 barcos de pesca atuando como MM chinesas. O setor de pesca chinês emprega cerca de 14 milhões de pessoas e possui cerca de 200.000 barcos. Essas MM são denominadas também como “Forças Navais Civis Híbridas”, e desenvolvem um papel preponderante contra o Vietnã e o Japão no que tange à promoção da diplomacia marítima coercitiva (KORKMAZ, 2020).

Os navios de guerra chineses também recebem apoio logístico das MM, sendo observado que a construção de ilhas artificiais no Mar da China Meridional tem recebido o apoio dessas embarcações de pesca, por meio da transferência de materiais de construção (KORKMAZ, 2020).

O emprego de MM pela República Popular da China, sem que haja a real necessidade de ocorrer um conflito armado, possibilita o fortalecimento de uma abordagem hegemônica à medida que as tensões com a República da Indonésia, a República das Filipinas e a

República Socialista do Vietnã aumentam, não se esquecendo da disputa com o Estado do Japão pelas Ilhas Senkaku (KORKMAZ, 2020).

A estratégia chinesa de obter apoio para consolidar a sua hegemonia regional é vislumbrada por meio do emprego de MM de barcos pesqueiros, pois é uma ferramenta menos provocativa e um importante instrumento para manter os interesses regionais e para evitar sanções internacionais (KORKMAZ, 2020).

Realizando-se uma análise estratégica do Brasil, observa-se que na extensão que compreende 8.500 km de faixa litorânea, são produzidos 90% do produto interno bruto (PIB) do País, localizam-se os principais destinos turísticos nacionais e há uma concentração de 80% da população brasileira (CCSM, 2023).

Ressalta-se ainda, que pelo mar, o Brasil consegue escoar mais de 95% do seu comércio exterior, além de retirar 45% do seu pescado, 80% do seu gás natural e cerca de 95% do seu petróleo. Dessa forma é essencial que a MB consiga garantir a sua preservação e a sua proteção, pois existem inúmeras riquezas contidas no mar e esse ambiente marítimo possui uma elevada importância estratégica para o País (CCSM, 2023).

Além disso, devido ao fato de a maior parte da produção de petróleo do País ser realizada por meio das plataformas, elas são consideradas, de acordo com a Estratégia Nacional de Defesa (END), um dos 4 objetivos estratégicos permanentes sob a responsabilidade da MB (BRASIL, 2012).

Em face do exposto, torna-se extremamente imperiosa a real necessidade de se possuir plenas condições de elaboração de medidas para contraposição às Ameaças Híbridas.

5.2 Possíveis cenários para as Ameaças Híbridas Marítimas

O Centro Europeu de Excelência para Combater Ameaças Híbridas (*Hybrid CoE*) vem realizando, desde março de 2018, uma série de reuniões, seminários, *workshops*, simpósios, conferências, exercícios e análise de eventos, visando detalhar as questões afetas às AHM, tendo elaborado diversos cenários para aprofundar seus estudos (GIANNOULIS, 2023).

A análise desses cenários permitiu que o Hybrid CoE conseguisse chegar à conclusão de que determinadas atividades marítimas maliciosas e as interrupções no transporte marítimo podem ocasionar sérios danos políticos e econômicos, além de terem efeitos imediatos e/ou de longo prazo (GIANNOULIS, 2023).

Segundo Giannoulis (2023), a análise de cada cenário ampara-se em um estudo com enfoque também jurídico, permitindo que seja observado o preconizado no Direito Internacional Humanitário (DIH) e no Direito do Mar (DM).

Os cenários analisados pelo Hybrid CoE para as AHM atualmente são: Bloqueio de estreitos; Declaração de uma zona de controle ao redor de uma ilha; Pesca em águas distantes; Zona de inspeção de navios em frente aos países Alfa e Beta; Exploração de uma plataforma continental contestada/ZEE; Ataque por meio de barco inflável de casco rígido; Ampla área de proteção de força; Ataques cibernéticos contra a frota; Uso clandestino de armas subaquáticas; Defesa de área marítima restrita; Declarar uma área de tiro e exercício e bloquear linhas marítimas de comunicação; Zona de inspeção de navios em frente aos países Alfa e Beta/Escalada; Operações de liberdade de navegação; Embarcações de pesca como atores não estatais; Cortes de cabos submarinos; Proteção de um gasoduto submarino; Exploração de recursos marinhos em ZEE contestada; Detenção de uma embarcação por um Estado terceiro com base em um suposto ataque terrorista; Detenção de uma embarcação por um Estado costeiro com base em um suposto ataque terrorista (GIANNOULIS, 2023).

Devido à grande quantidade de cenários elaborados, este trabalho irá delimitar o seu objeto de estudo com enfoque para a proteção de um gasoduto submarino (GIANNOULIS, 2023).

5.2.1 Análise de um cenário visando a proteção de um gasoduto submarino

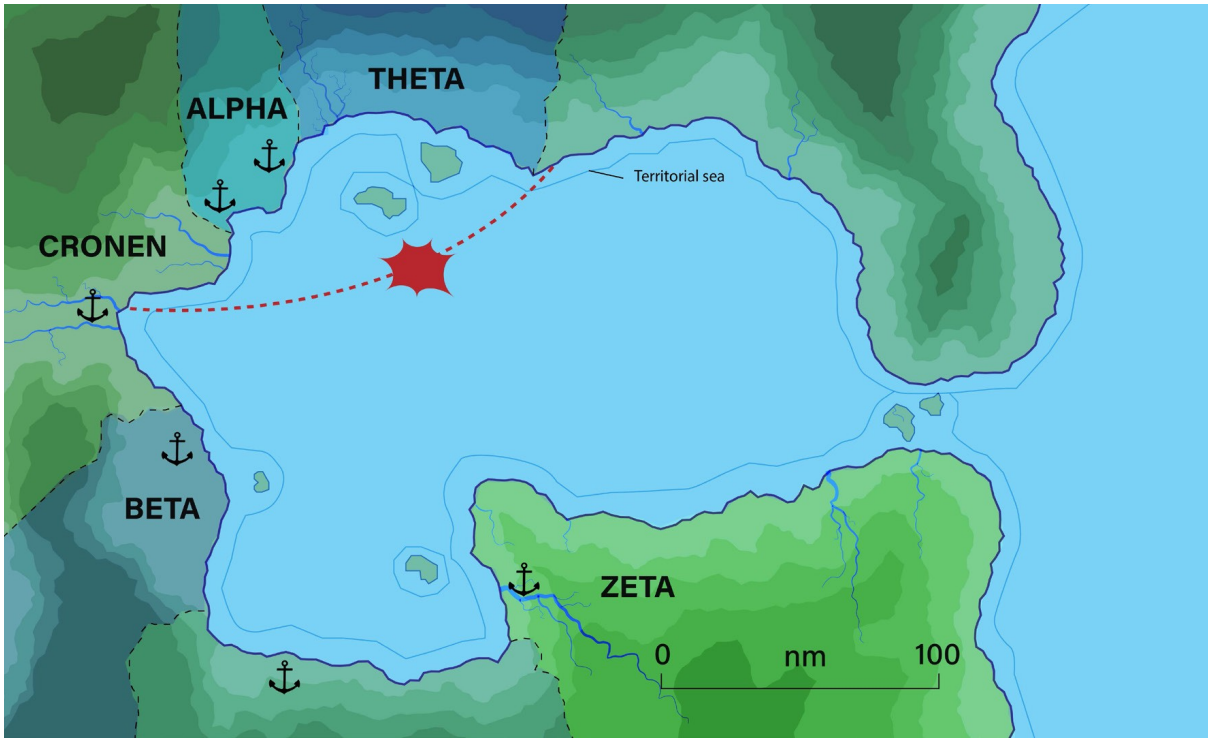

FIGURA 1 – Modelo elaborado para exemplificar um cenário de proteção de um gasoduto submarino.

Fonte: GIANNOULIS, 2023, p. 12.

Com a chegada de uma tempestade oriunda de Sudeste, foram observadas degradações meteorológicas no mar. O país THETA é um Estado costeiro da UE e observou-se que um navio graneleiro de grandes dimensões estava adentrando a sua ZEE, devido a um apagão que o mesmo havia sofrido. O navio padecendo o risco de perder a sua carga, em virtude de estar sendo pressionado pela ventania por seu barlavento, necessitou realizar um fundeio de emergência (GIANNOULIS, 2023).

O ferro do navio não unhou conforme o previsto e o navio começou a ser levemente arrastado pela corrente. Quando cessa o segmento do navio, observa-se que ele se encontra provavelmente em cima de um gasoduto subaquático (GIANNOULIS, 2023).

O respectivo gasoduto subaquático é de responsabilidade da corporação ETA, cujo acionista majoritário encontra-se no país CRONEN. Após o intervalo de algumas horas, a

situação é normalizada e o navio iça o ferro, suspendendo para prosseguir viagem, de forma a cumprir a sua derrota em direção ao seu porto de destino (GIANNOULIS, 2023).

Passados dois dias do ocorrido, o acionista majoritário do gasoduto subaquático da corporação ETA, que se encontra no país CRONEN, juntamente com o apoio do Ministério das Relações Exteriores do país CRONEN, interpelam o governo do país THETA (GIANNOULIS, 2023).

Eles reivindicam para que o país THETA arque com todas as despesas necessárias para que sejam realizadas inspeções técnicas e, caso necessário, eventuais reparos no gasoduto subaquático. Eles alegam ainda que o país THETA deveria ter tido uma precaução, de forma a proteger o gasoduto, não realizando fundeio próximo do mesmo, além de ter a preocupação de providenciar rebocadores para auxiliar o navio durante as manobras de fundear e suspender, evitando o arrastamento do ferro (GIANNOULIS, 2023).

A elaboração desse cenário questiona se, devido ao fato de o navio Graneleiro estar em uma situação de iminente perigo, a corporação ETA pode atribuir responsabilidades ao país THETA, por eventuais destruições causadas pelo navio dentro da ZEE/na plataforma continental do país THETA? (GIANNOULIS, 2023).

O Governo do país CRONEN em total apoio à corporação ETA, a qual é a acionista majoritária do gasoduto subaquático, está envidando esforços, de forma a atribuir responsabilidades ao Governo do país THETA por possíveis prejuízos causados pelo navio graneleiro que se encontrava em perigo iminente, dentro da ZEE/na plataforma continental do País THETA (GIANNOULIS, 2023).

Baseando-se em uma possível obrigação que o Estado costeiro deveria ter para prover a segurança do gasoduto subaquático, o país CRONEN e a corporação ETA reivindicam a ocorrência de uma suposta violação consumada pelo país THETA. Deveria haver respaldo perante o Direito Internacional Público (DIP) para que tal reivindicação pudesse lograr êxito (GIANNOULIS, 2023).

Observa-se, no entanto, que tal obrigação por parte do país THETA não existe, pois o que o país CRONEN e a corporação ETA argumentam é que essa obrigação deveria ser uma

prevenção total contra possíveis danificações no gasoduto e não um certo cuidado por parte do país THETA na adoção de medidas para mitigar o problema (GIANNOULIS, 2023).

O artigo 79, item (2) da Convenção das Nações Unidas sobre o Direito do Mar (CNUDM), especifica que o Estado costeiro não tem o direito de obstruir a instalação de dutos ou cabos submarinos. E o artigo 56, item (2), ressalta que os Estados costeiros têm a obrigação de respeitar o direito de outros respectivos Estados de instalarem dutos ou cabos submarinos (GIANNOULIS, 2023).

A cautela com relação a determinados tipos de condutas fora da jurisdição do Estado costeiro não está inserida nas obrigações acima especificadas, o que não contempla atividades alusivas ao exercício da liberdade de navegação de embarcações estrangeiras e aos dutos submarinos, conforme o artigo 58, item (1) da CNUDM (GIANNOULIS, 2023).

A responsabilidade pela proteção de gasodutos subaquáticos estrangeiros na sua respectiva ZEE não é responsabilidade do Estado costeiro, tendo o mesmo somente o direito de adotar medidas para o controle, a redução e a prevenção com relação a possíveis poluições oriundas dos gasodutos e não uma obrigação para realizar a garantia da segurança do gasoduto de transporte internacional marítimo (GIANNOULIS, 2023).

Por outro lado, os Estados de nacionalidade das pessoas envolvidas e os Estados de bandeira, de acordo com os artigos 58 (item – 2) e 113 da CNUDM, são os responsáveis pela adoção de medidas para realizarem a proteção dos cabos submarinos na ZEE contra avarias acarretadas pela navegação internacional (GIANNOULIS, 2023).

O país THETA não pode assumir nenhuma responsabilidade internacional e tampouco violou nenhuma obrigação internacional, pois não há nenhum argumento que ampare o fato de que o país THETA pudesse evitar o incidente em questão, mesmo que se suponha a existência de uma responsabilidade para que os Estados costeiros tivessem a obrigação de realizar a proteção dos gasodutos subaquáticos estrangeiros nas suas ZEE (GIANNOULIS, 2023).

Dessa forma, o país THETA não pode de forma alguma ser responsabilizado pelo país CRONEN e nem pela corporação ETA, em razão dos danos causados devido ao fundeio do navio graneleiro de bandeira da UE (GIANNOULIS, 2023).

Realizando-se uma análise estratégica do Brasil, observa-se que o projeto do gasoduto submarino brasileiro denominado de Rota 3, que tem como objetivo conectar o Polo Pré-Sal situado na Bacia de Santos-SP até o Complexo Petroquímico do Estado do Rio de Janeiro (COMPERJ), localizado no município de Itaboraí, possui cerca de 48 km de trecho terrestre e 307 km de trecho marítimo, somando portanto um total 355 km de extensão, e foi projetado para realizar o escoamento de gás natural com uma vazão em torno de 18 milhões de m³ de gás diários (PETROBRAS, 2022).

A operação do gasoduto submarino brasileiro começou a ser realizada de forma parcial no mês de junho de 2022 (PETROBRAS, 2022a).

5.2.2 As explosões dos gasodutos Nord Stream 1 e 2.

Dessa forma, com o intuito de exemplificar o cenário acima abordado, analisa-se o caso de repercussão mundial que ocorreu em 26 de setembro de 2022, com as explosões dos gasodutos Nord Stream 1 e 2.

A estatal russa de energia Gazprom detém as ações majoritárias dos gasodutos Nord Stream 1 e 2, sendo os mesmos utilizados para transportar o gás russo até os terminais da Alemanha e para todo o restante da Europa respectivamente, atravessando o Mar Báltico (LEE, 2023).

Após a invasão da Ucrânia pela Federação da Rússia, ocorrida no dia 24 de fevereiro de 2022, o Nord Stream 2, apesar de concluído, não teve a sua operacionalização efetivada, devido a não concessão de permissão por parte do Governo alemão. O Nord Stream 1 foi concluído e teve a sua operacionalização efetivada em 2011 (LEE, 2023).

Apesar dos gasodutos passarem pela Ucrânia, o país não pode usufruir do gás que transporta e nem aufere receitas com taxas de trânsito. Esses gasodutos possibilitam a Federação da Rússia um controle total sobre o abastecimento de energia da Europa, tornando-se uma constante preocupação para o Ocidente. A Federação da Rússia pode perfeitamente utilizar esses gasodutos como arma política contra seus adversários (LEE, 2023).

Devido às severas restrições impostas pelo Ocidente contra a Federação da Rússia, em virtude da Guerra da Ucrânia, a Gazprom interrompeu o fluxo de gás por meio do gasoduto em setembro de 2022. Foram verificadas explosões nos dois gasodutos 3 semanas depois, fazendo com que os mesmos ficassem inoperantes e ocasionando vazamentos de gás nos dutos (LEE, 2023).

Devido à complexidade do emprego de explosivos submarinos e à grande profundidade dos gasodutos, tais ações levam a crer que somente um ator estatal poderia realizar tal ato, porém nenhum Estado reivindicou a autoria do ataque. Houve diversas acusações entre a Federação da Rússia, os EUA e a Grã-Bretanha, porém até o momento nenhum tipo de investigação produziu um relatório conclusivo de quem foi o verdadeiro responsável pela explosão (LEE, 2023).

Observa-se no exemplo acima que a explosão do gasoduto submarino obrigou a adoção de medidas para que navios não adentrassem uma determinada área específica, restringindo assim a navegação marítima no local. O emprego de possíveis armas subaquáticas para a realização da explosão, a desinformação gerada para causar confusão sobre o real autor, a poluição ambiental causada pelo vazamento, a pressão econômica ocasionada com o desabastecimento, e a pressão política gerada, são todos componentes de uma Guerra Híbrida.

Ressalta-se ainda que, no contexto acima, podem ser identificados vários assuntos que estão diretamente especificados no Plano Estratégico da Marinha (PEM – 2040), tais como: a perfeita compreensão do Ambiente Operacional marítimo e fluvial com o objetivo de analisar a existência de possíveis Ameaças Híbridas (BRASIL, 2020).

5.3 Conclusões Parciais

Nota-se que nos dias atuais a tecnologia torna-se uma via de mão dupla, pois da mesma forma que facilita diversas ações em nossas vidas também serve como ponto de vulnerabilidade para diversos tipos de novas Ameaças Híbridas.

O ambiente marítimo tornou-se um palco para determinados tipos de atores híbridos, devido à sua elevada importância no contexto globalizado e devido ao fato da grande maioria do comércio mundial ser escoado pelo modal marítimo.

A identificação de 7 vulnerabilidades no domínio marítimo permite traçar diversos tipos de cenários com o objetivo de se angariarem conhecimentos e técnicas para contraposição a essas novas ameaças.

O emprego de recursos de inteligência modernos e eficazes, o compartilhamento de informações e o uso de recursos tecnológicos modernos são essenciais para se contrapor às AHM.

A adoção de RE bem elaboradas e definidas e o completo conhecimento do arcabouço jurídico atinente ao complexo assunto, são essenciais para um sólido embasamento. Os estudos de casos dos eventos envolvendo AHM que ocorrem ao redor do mundo e a análise das ações adotadas pelas respectivas Marinhas envolvidas nos eventos, fornecem um ensinamento para possibilidade de adoção de ações específicas para a MB no que tange à prevenção contra possíveis acontecimentos em AJB.

O Brasil é extremamente dependente do mar, pois, como foi observado, ele tem participação direta no seu PIB, nos destinos turísticos nacionais, na concentração da sua população, na produção de petróleo por meio das plataformas petrolíferas, nos seus cabos submarinos utilizados para a transmissão de dados, nos seus gasodutos para o transporte de combustíveis e na sua pesca.

O perfeito conhecimento e a disseminação do PEM (2040) para toda a sociedade brasileira é essencial para que se consiga incutir na mesma a real importância que o mar possui para o seu povo, de forma a elevar a mentalidade marítima dos seus habitantes.

O capítulo seguinte tem como objetivo realizar uma análise do DOPEMAI, constante no Guia de Planejamento Baseado em Capacidades (PBC), com o intuito de verificar qual o nível de preparo que a MB possui atualmente para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida ofensiva perpetrada por um ator estatal ou não estatal externo. Serão ainda contempladas algumas ações para elevar a capacidade de resposta da MB para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida de forma a reduzir a sua vulnerabilidade no tocante a essas novas ameaças.

6 A APLICAÇÃO DO DOPEMAI NA GUERRA HÍBRIDA

Com o objetivo de responder qual o nível de preparo que a MB possui atualmente para se contrapor a uma Ameaça Híbrida ou Guerra Híbrida ofensiva, perpetrada por um ator estatal ou não estatal externo, será realizada uma análise do DOPEMAI, constante no Guia de Planejamento Baseado em Capacidades (PBC) com enfoque na Guerra Híbrida e nas Ameaças Híbridas.

O DOPEMAI tem sua fundamentação pautada nos aspectos Doutrina, Organização, Pessoal, Ensino, Material, Adestramento e Infraestrutura, os quais agrupados compõem um determinado tipo de capacidade (BRASIL, 2022). Analisando-se o DOPEMAI para a Guerra Híbrida segundo o referido guia (BRASIL, 2022), observa-se:

– **Doutrina:** Não existe no âmbito nacional uma doutrina para a Guerra Híbrida e nem sequer uma definição de Guerra Híbrida nos manuais e publicações vigentes[25]. Observa-se ainda uma escassez de obras, artigos acadêmicos e documentos nacionais afetos ao tema (LEAL, 2016);

– **Organização:** O Comando Naval de Operações Especiais (CoNavOpEsp) teve a iniciativa de inserir na sua estrutura organizacional uma Assessoria de Ameaças Híbridas, com o objetivo de tratar de assuntos afetos a essas novas ameaças (DIAS, 2022);

– **Pessoal:** Não há na grande maioria das Organizações Militares pessoal com capacitação e qualificação para lidar com as atividades intrínsecas à Guerra Híbrida e às Ameaças Híbridas. O nível de conscientização do pessoal sobre a real importância do tema ainda é baixo. Existe um mapeamento elaborado pelo Centro de Desenvolvimento Doutrinário de Guerra Naval (CDDGN) de militares da MB que produziram artigos, ensaios, TCC, dissertações e teses sobre o tema Guerra Híbrida ou Ameaças Híbridas[26];

– **Ensino:** A ESG, a EGN e a ECEME abordam as novas ameaças nos seus currículos escolares, porém há necessidade do assunto ser expandido para as demais escolas;

---

25 Informação verbal obtida com o Capitão de Fragata Rodrigo Bouças, que atualmente exerce a função de Encarregado da Divisão de Coleta e Difusão do CDDGN.

26 Ibidem.

– **Material:** Conforme divulgado pela CNN (2023), que devido à redução de recursos a modernização das FA sofreria impactos, nota-se que podem haver problemas para a aquisição de equipamentos, meios e sistemas adequados em quantidades suficientes para atuar de forma eficaz contra a Guerra Híbrida e as Ameaças Híbridas, principalmente no que diz respeito aos avanços tecnológicos de emprego militar;

– **Adestramento:** No período de 28 de setembro a 9 de outubro de 2020, a MB, o EB e a FAB, participaram da Operação Poseidon que foi coordenada pelo Comando da 2ª Divisão da Esquadra (ComDiv-2) e pelo CoNavOpEsp, sendo que um dos exercícios tinha como objetivo elevar as capacidades de contraposição às Ameaças Híbridas (WILTGEN; PADILHA, 2020). A EGN promoveu em 03 de junho de 2022 um seminário sobre Guerra Híbrida e Defesa NBQR, abordando o tema (BARROS, 2022). Houve a iniciativa da EGN em conduzir esse ano, o 1° jogo híbrido no Centro de Jogos (BARROS, 2023). No dia 18 de julho do corrente ano, o Comando do 3° Distrito Naval (COM3°DN) realizou o 1° exercício teórico de segurança da informação e cibernética visando no escopo da guerra cibernética, aprofundar os conhecimentos sobre as novas ameaças (BARROS, 2023a). Observa-se que há uma iniciativa na realização de adestramentos frente a novas ameaças, porém eles devem ser intensificados; e

– **Infraestrutura:** As infraestruturas das FA possuem algumas vulnerabilidades que podem ser exploradas por atores híbridos, havendo portanto a necessidade de ser realizado um mapeamento eficaz de todas elas.

6.1 Sugestões a serem implementadas

Após a análise dos capítulos anteriores, atinentes a esse complexo fenômeno intitulado como Guerra Híbrida e Ameaças Híbridas, e após a análise do DOPEMAI, foram elaboradas algumas sugestões a serem implementadas não apenas na MB, mas também no âmbito do MD, EB e FAB, com o intuito de se poder efetuar contraposição a essa nova ameaça, pois adotando-se as sugestões propostas, a MB terá grandes possibilidades de

definir as ações que deverão ser implementadas para elevar a sua capacidade de resposta. Entre as diversas sugestões, podem-se destacar:

– Fomentar o interesse pelo assunto em lide, com o objetivo de: estimular os alunos do Curso de Estado-Maior para Oficiais Intermediários (CEMOI), Curso de Estado-Maior para Oficiais Superiores (CEMOS) e Curso de Política e Estratégia Marítimas (C-PEM) para elaborarem trabalhos de conclusão de curso (TCC), dissertações e teses sobre o tema Guerra Híbrida e Ameaças Híbridas; estimular a realização de Ensaios pelos futuros alunos do CEMOS e C-PEM sobre o assunto Guerra Híbrida e Ameaças Híbridas; propor para o Almirantado que nos próximos Processos de Tomada de Decisão (PTD) seja incluído o tema Guerra Híbrida e Ameaças Híbridas;

– Devido à grande complexidade, ao ineditismo, à quantidade de informações levantadas e à elevada importância para a MB, sugere-se que seja aprofundado o tema GHM e AHM na elaboração de teses futuras da EGN;

– Verificar a necessidade de composição de um Grupo de Trabalho (GT) sob a coordenação do MD, com a participação de representantes das 3 Forças, com a finalidade de elaborar uma definição de Guerra Híbrida e Ameaça Híbrida, de forma que possa ser inserida na Estratégia Nacional de Defesa (END), Política Nacional de Defesa (PND) e Livro Branco de Defesa Nacional (LBDN);

– Realizar seminários, *workshops*, simpósios sobre o tema Guerra Híbrida e Ameaças Híbridas;

– Efetuar gestões objetivando enviar militares para as diversas reuniões e congressos que são realizados pela OTAN e UE sobre Guerra Híbrida e Ameaças Híbridas;

– Verificar a viabilidade de serem criadas equipes de apoio para combater Ameaças Híbridas - “Equipes contra-híbridas”, semelhantes às que a OTAN criou em 2018;

– Mapear as infraestruturas críticas na MB ou em AJB, quanto às suas vulnerabilidades para o caso de serem alvos de uma Guerra Híbrida ou Ameaças Híbridas, tais como: o Projeto do Submarino de Propulsão Nuclear; o Sistema de Gerenciamento da Amazônia Azul (SisGAAz); os portos; as plataformas petrolíferas; os cabos submarinos; os gasodutos submarinos, os terminais de contêineres, os principais estaleiros, as Bases

Navais, o sistema de saúde (Hospitais Navais); a Estação Antártica Comandante Ferraz e o Sistema Naval de Comando e Controle (SISNC2). Especial atenção deve ser dada ao mapeamento dos riscos quanto: ao emprego de ataques cibernéticos contra a nossa Força; ao uso de armamento NBQR contra a nossa Força; e aos efeitos de poluição hídrica, sobre os quais, como exemplo pode-se citar o caso das manchas de óleo que surgiram na costa do litoral brasileiro em agosto de 2019;

– De forma análoga ao item anterior, alertar as Forças coirmãs para que efetuem o mapeamento de suas infraestruturas críticas, destacando como exemplos: o Sistema Integrado de Monitoramento de Fronteiras (SISFRON), o Sistema de Vigilância da Amazônia (SIVAM) e o Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo (CINDACTA);

– Definir RE para ações no nível híbrido e analisar a necessidade de ser elaborado um Manual para combater Ameaças Híbridas, visando monitorar também as nossas vulnerabilidades;

– Sugerir que o Centro de Comunicação Social da Marinha (CCSM) inclua no EMA-860 (Manual de Comunicação Social da Marinha) um tema abordando “O emprego da comunicação estratégica na Guerra Híbrida”;

– Sugerir que o MD, em contatos horizontais com os demais Ministérios, elabore um Plano de Ação contra a Desinformação, semelhante ao que foi elaborado pela Comissão Europeia em dezembro de 2018;

– Analisar a necessidade de serem elaborados pelo Centro de Inteligência da Marinha (CIM), os processos de inteligência de alerta, objetivando a proteção de nossas vulnerabilidades críticas em toda a sociedade contra possíveis ataques. O compartilhamento de informações de forma coordenada também torna-se essencial para a detecção de ataques híbridos;

– Sugerir análise, por parte do MD, sobre a viabilidade da elaboração de um quadro de ameaças híbridas com o intuito de fortalecer a sua resiliência nacional e elevar a sua consciência situacional;

– Intensificar, por parte da MB, no que diz respeito à realização de exercícios, treinamentos e melhorias na educação de forma a se preparar para combater as Ameaças Híbridas;

– Implementar noções de Guerra Híbrida inicialmente nas seguintes instituições de ensino: Colégio Naval (CN), Escola Naval (EN), Centro de Instrução Almirante Wandenkolk (CIAW), Centro de Instrução Almirante Graça Aranha (CIAGA), Centro de Instrução Almirante Braz de Aguiar (CIABA). Após uma análise da verificação da evolução dos ensinamentos obtidos, pode-se pensar em implementar essas noções de Guerra Híbrida nas Escolas de Aprendizes de Marinheiros e no Centro de Instrução Almirante Alexandrino (CIAA);

– Sugerir que o MD analise a viabilidade da implementação de Centros de Excelência para combater ameaças híbridas inicialmente com foco na defesa cibernética, comunicações estratégicas, desinformação, segurança energética, resposta a incidentes NBQR e AHM, expandindo para demais áreas posteriormente;

– Sugerir que o Brasil capitaneie a reativação do Conselho de Defesa Sul-Americano (CDS)[27], com a finalidade de desenvolver a integração no campo da Segurança e da Defesa entre os países-membros da América do Sul, para que se consigam elaborar estratégias conjuntas para contraposição a Ameaças Híbridas, além de incentivar o aumento do fluxo de informações entre os diversos órgãos de inteligência do continente, o que possibilitaria elaborar Planos e ações integradas com relação a essas ameaças, além de ter a capacidade de detectar e atribuir qualquer tipo de atividade híbrida que esteja sendo desenvolvida, pois observa-se que combater Ameaças Híbridas de forma isolada é extremamente complexo até mesmo para organizações como a OTAN e a UE;

– Sugerir que o MD analise a viabilidade da adoção de um PAP que aborde no seu escopo as medidas de garantia e medidas de adaptação, a criação de uma FR, uma FTCAP, uma UIF e um GALC;

---

27 O Conselho de Defesa Sul-Americano (CDS) é uma ferramenta que visa promover o intercâmbio na área de segurança entre os Estados participantes da União de Nações Sul-Americanas (UNASUR), dentre os quais podemos citar a permuta de diversos tipos de análises com relação aos cenários globais na área de defesa; execução da interoperabilidade no que tange aos exercícios militares; atuação em operações de manutenção de paz da ONU; o intercâmbio de militares entre as FA de diversos Estados; formulação de políticas comuns na área de defesa; incorporação de bases industriais de equipamentos militares; providências para promover a reciprocidade com relação a confiança; assistência coordenada em áreas afetadas por desastres provocados pela natureza. (SGB,2023).

– Intensificar as Patrulhas Marítimas em áreas que possuem infraestruturas críticas e possam ser alvo de Ameaças Híbridas, tais como as plataformas petrolíferas, de forma a fornecer segurança marítima, com enfoque na realização de patrulhas antiterroristas;

– Intensificar a realização de exercícios marítimos militares com outras Marinhas, de forma a aperfeiçoar a consciência situacional, através de maior capacidade no processamento, troca e coleta de informações;

– Fortalecer a resiliência nacional, elevando-se a consciência situacional, assim como a coesão interna;

– Enfatizar os estudos sobre as questões afetas ao DMI com ênfase na GHM e AHM;

– Elaborar, de forma inicial pela EGN, a análise dos seguintes cenários focados nas AHM: Exploração de uma plataforma continental contestada/ZEE; Ataque por meio de Barco inflável de casco rígido; Ataques cibernéticos contra a frota; Uso clandestino de armas subaquáticas; Embarcações de pesca como atores não estatais; Cortes de cabos submarinos; Proteção de um gasoduto submarino e Detenção de uma embarcação com base em um suposto ataque terrorista;

– Realizar estudos de casos atinentes aos eventos envolvendo AHM que ocorrem ao redor do mundo e realizar a análise das ações adotadas pelas respectivas Marinhas envolvidas nos eventos, com o objetivo de obter ensinamentos para adoção de ações específicas para a MB no que tange à prevenção contra possíveis acontecimentos em AJB;

– Fomentar a alocação de mais recursos para serem empregados em Inteligência e na aquisição de equipamentos de vigilância (drones), para a coleta de informações;

– Verificar a viabilidade de serem criados think tanks[28] dentro de uma estrutura organizacional que contemple os níveis estratégico e operacional, com a finalidade de se estudar o tema;

---

28 Think tank são determinados tipos de instituições que têm como objetivo a produção de conhecimentos sobre temas científicos, econômicos e políticos. A sua principal meta é exercer influência no processo de tomada de decisão das esferas privada e pública. Através da participação de seus componentes na mídia, além da publicação de estudos e artigos, os debates sociais são pautados por essas instituições. Os think tank também idealizam efeitos de prováveis impasses da sociedade, assim como, alternativas para os mesmos. Disponível em: <https://mmurad.com.br/blog/o-que-e-um-think-tank/#>. Acesso em: 01 maio 2023.

– Verificar a necessidade de ser efetuada uma reestruturação do Grupamento de Mergulhadores de Combate com ênfase para ações contra AHM; e

– Promover uma disseminação do PEM (2040) para toda a sociedade brasileira, de forma que se consiga incutir na mesma a real importância que o mar possui para o seu povo, de forma a elevar a mentalidade marítima dos seus habitantes.

7 CONCLUSÃO

Pode-se observar ao final deste trabalho que o uso, a correlação e a análise de uma enorme e complexa gama de informações ganhou um elevado grau de protagonismo e definitivamente alterou o curso das guerras. O surgimento de diversas inovações tecnológicas, tais como a internet e as mídias sociais, além de dispositivos modernos (como smartphones, tablets e notebooks), tornou possível a comunicação de forma célere, a partir de qualquer lugar no mundo, além de permitir a obtenção de fotos, vídeos, áudios, documentos e outras informações de interesse. Em tal contexto, o ponto relacionado à alta velocidade com que a informação é propagada nos dias atuais merece especial destaque, sendo crucial para ações de ataque, defesa e monitoração no esforço de guerra, muitas vezes explorando vulnerabilidades, fazendo com que ele seja o cerne da Guerra Híbrida.

Nota-se que esses dispositivos em mãos erradas podem se transformar em armas que atuam de forma não cinética, sem a real necessidade de ter que se empregar a força. Determinados tipos de atores podem fazer uso da informação para minar as instituições que gozam de credibilidade, atacar vulnerabilidades críticas de um Estado, enfraquecer democracias consolidadas e disseminar a desinformação. Esse é novo modelo de guerra moderna, denominado de Guerra Híbrida.

Apesar do ineditismo do termo Guerra Híbrida, assim como da confusão que costuma permear as diversas acepções que lhes são destinadas, como foi mostrado, pode-se recorrer à teoria do general prussiano Carl Von Clausewitz que, mesmo sem ter usado o termo discorreu sobre a dinâmica complexa e flexível da guerra. Observa-se, portanto, que apesar do surgimento de diversas inovações tecnológicas, a guerra não perdeu a sua essência e suas características intrínsecas constantes na sua trindade, sendo comparada a um camaleão, conseguindo assim adaptar-se de acordo com a sua evolução. A Guerra Híbrida se configura, pois, como um desdobramento do próprio conceito de guerra clausewitziano aplicado aos dias atuais.

Diversos países e organismos respeitados no mundo compreenderam a real importância da Guerra Híbrida e das Ameaças Híbridas na atualidade e os severos danos que

elas podem causar a um Estado. Dessa forma, eles se debruçaram para estudar essa nova realidade e então traçar metas estratégicas para se contraporem à ameaça, visando fortalecer a resiliência nacional, elevar a consciência situacional e a coesão interna. Observa-se ainda que a dissuasão, seja ela por negação ou por punição, constitui-se em um mecanismo muito importante no combate à Guerra Híbrida.

A elaboração de um modelo genérico de *Framework* para combater a Guerra Híbrida baseado em detectar, deter e responder os agressores híbridos, serve de parâmetro para que países como o Brasil, que ainda não têm o seu modelo definido, amparem-se no modelo criado para então elaborar o seu próprio.

Observa-se que a comunicação estratégica deve ser empregada na sua plenitude, de forma a combater a desinformação e a propaganda enganosa que são os focos da Guerra Híbrida. Outras ferramentas muito importantes são a Inteligência e o compartilhamento de informações, que visam a prevenção diante de ações que possam ser perpetradas contra o Estado.

A união de todos os setores em um Estado é essencial para o combate à Guerra Híbrida e às Ameaças Híbridas, pois sozinho torna-se muito difícil enfrentar essa nova ameaça, sendo necessário compreender o tipo de fenômeno que se está enfrentando, fortalecendo-se contra as suas ações e conhecendo as suas fragilidades.

O processo de tomada de decisão e as vulnerabilidades do Estado são o ponto crucial da Guerra Híbrida. Dessa forma, é essencial que se tenha o mapeamento de todas as infraestruturas críticas, com o intuito de mitigar possíveis ações. O ciclo OODA tem elevada importância nesse contexto.

Observa-se a necessidade de que a MB dispenda uma atenção maior às OpInfo, havendo a demanda de serem empregadas com maior intensidade nas diversas operações em que a Força participa.

Nota-se que as CRI possuem um alto grau de relevância no contexto das OpInfo, porém elas nunca devem ser empregadas sozinhas, sob o risco de perderem a sua eficácia. Elas devem ser sempre empregadas de forma sincronizada, pois o seu emprego de forma correta pode minimizar a necessidade de ser usada a força. Apesar de ser citada a

importância que a Inteligência possui no contexto da Guerra Híbrida, por questões doutrinárias ela não é considerada uma CRI, porém observa-se que ela é extremamente importante no contexto do apoio às OpInfo.

O emprego de OpPsc, GE, ComSoc, ações cibernéticas, operações civil-militares e a Desinformação, tal como implementado pela Federação da Rússia contra a Ucrânia em 2014, exemplifica e ressalta a real importância do papel das OpInfo na evolução da Guerra Híbrida.

Observa-se que a OTAN, em relação a assuntos afetos a Guerra Híbrida, serve de modelo, pois é uma das poucas organizações no mundo que compreende a real importância da Guerra Híbrida no atual contexto e encontra-se trabalhando de forma ativa para se contrapor a essa nova ameaça. A OTAN emprega mecanismos como dissuasão e defesa para fortalecer sua resiliência nacional e aumentar a sua consciência situacional, abordando o tema de maneira estratégica.

A OTAN atualmente encontra-se adotando uma abordagem altamente estruturada e abrangente para lidar com a Guerra Híbrida e com as Ameaças Híbridas. Com o intuito de conseguir alcançar esse objetivo a organização criou equipes especializadas, conhecidas como "Equipes contra-híbridas", compostas por especialistas de diversos campos e com diversas expertises. Além disso, a OTAN desenvolveu diretrizes específicas para lidar com esse complexo assunto, demonstrando, assim, um alto grau de comprometimento e profissionalismo.

A OTAN vem se esforçando para entender o funcionamento do quadro de Ameaças Híbridas e tem buscado parceria com a UE, com o objetivo de ampliar suas capacidades e ferramentas. A criação do DICS destaca o foco da OTAN em melhorar a sua consciência situacional. A priorização de um ramo voltado especificamente para a análise híbrida ressalta a importância de analisar e compreender as nuances da Guerra Híbrida e das Ameaças Híbridas de maneira detalhada.

Nota-se a seriedade com que a OTAN aborda o tema estudado, a partir do momento em que ela envida esforços para identificar, priorizar e mapear todas as suas vulnerabilidades

críticas nacionais, fornecer apoio abrangente aos seus países-membros e lidar com uma ampla gama de desafios para garantir a estabilidade e a segurança da organização.

O treinamento intenso, o aumento da sua coesão interna, a realização de diversos tipos de exercícios e a evolução da educação são as metas estabelecidas pela OTAN para se fortalecer contra as Ameaças Híbridas e a Guerra Híbrida.

A criação dos Centros de Excelência para combater Ameaças Híbridas é considerado um marco importante no combate a essas novas ameaças. Esses centros foram estabelecidos para tratar de assuntos intrínsecos à Guerra Híbrida e às Ameaças Híbridas, possuindo, como propósito, melhorar a capacidade de resposta e a resiliência, fomentando a colaboração e o intercâmbio de conhecimentos entre diversos tipos de especialistas.

Observa-se que a OTAN, visando efetuar uma resposta de forma rápida contra uma Guerra Híbrida ou possíveis Ameaças Híbridas desencadeadas contra a organização ou um de seus países-membros, implementou o PAP, as medidas de garantia, as medidas de adaptação e criou a FR.

É essencial que sejam estudados não apenas os países-membros da OTAN, mas também os diversos países e organizações que encontram-se adiantados em relação ao combate às Ameaças Híbridas e à Guerra Híbrida, com o intuito de obter-se conhecimento com os mesmos sobre o assunto em lide, uma vez que no Brasil existem raríssimas obras e artigos afetos ao tema. Observa-se ainda que, com base nos estudos realizados no decorrer desta tese, a OTAN encontra-se em um nível bastante elevado com relação à sua estratégia para se preparar, dissuadir e se defender contra Ameaças Híbridas e até mesmo contra uma Guerra Híbrida.

Em termos de ambientes, verifica-se que a Guerra Híbrida e as Ameaças Híbridas ultrapassaram os limites terrestres e estão atuando também no ambiente marítimo, principalmente devido à sua elevada importância no contexto globalizado e devido ao fato de a grande maioria do comércio mundial ser escoado pelo modal marítimo.

Os estudos atinentes à identificação de 7 vulnerabilidades no domínio marítimo, realizados por Kremidas-Courtney no ano de 2018 e que foram abordados neste trabalho, permitem projetar diversos tipos de cenários com a finalidade de que seja efetuada contraposição às novas ameaças.

Nota-se que a República Popular da China aparece como um ator importante com relação à GHM e às AHM, possuindo as suas MMC, também intituladas como FNCH, e empregando com ineditismo os seus "pequenos marinheiros azuis", servindo assim de modelo para estudo sobre esse assunto.

Entende-se que é primordial o conhecimento do arcabouço jurídico que envolve esse assunto tão complexo, assim como a necessidade da formulação de RE bem definidas. Os estudos de casos dos eventos envolvendo AHM que ocorrem ao redor do mundo, assim como a análise das ações adotadas pelas respectivas Marinhas envolvidas nos eventos, fornecem um ensinamento para possibilidade de adoção de ações específicas para a MB no que tange à prevenção contra possíveis acontecimentos em AJB.

O Brasil pode se tornar alvo de uma AHM ou GHM, principalmente devido ao fato do País possuir uma grande dependência do mar, pois, como foi observado, ele tem participação direta no seu PIB, nos seus cabos submarinos utilizados para a transmissão de dados, na produção de petróleo por meio das plataformas, nos seus gasodutos para o transporte de combustíveis, na concentração da sua população, na sua pesca e nos destinos turísticos nacionais.

Visando-se elevar a mentalidade marítima da sociedade brasileira, objetivando ressaltar para a mesma a real importância que o mar possui para a sua população, observa-se a necessidade de uma ampla divulgação do PEM (2040).

Ao final da elaboração desta tese, pode-se constatar a importância do papel das OpInfo na evolução da Guerra Híbrida. A aplicação do DOPEMAI serviu como parâmetro para nos mostrar que apesar dos esforços envidados não somente pela MB, mas pelas FA, para entender as nuances e a complexidade características dessas novas ameaças, visando se preparar contra as mesmas, observa-se que atualmente o nível de preparo para se contrapor a uma Guerra Híbrida ou a uma Ameaça Híbrida ofensiva, perpetrada por um ator estatal ou não estatal externo, precisa ser aprimorado. Estabelecendo-se o presente estudo como uma base metodológica de consulta, as sugestões elaboradas têm como objetivo fornecer subsídios para que se consiga efetuar uma contraposição a essas novas ameaças, elevando assim a capacidade de resposta.

REFERÊNCIAS

ARON, Raymond. **Pensar a Guerra, Clausewitz**. Tradução Elisabeth Maria Speller Trajano. Brasília: Ed. Universidade de Brasília, 1986 *apud* MARENUCCI, Roberto. **A TEORIA DA TRINDADE DE CLAUSEWITZ E SUA APLICABILIDADE AO ESTUDO DO TERRORISMO DO SÉCULO XXI.** 2021. 31 f. Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior. Escola de Guerra Naval, 2021.

BARBOZA, Carlos Eduardo de Matos; TEIXEIRA, Luís Henrique Vighi. **Resgatando a Essência das Operações de Informação na Guerra Convencional**. Army University Press, 2020. Disponível em: <https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Quarto-Trimestre-2020/Resgatando-a-Essencia-das-Operacoes-de-Informacao-na-Guerra-Convencional/>. Acesso em: 03 jul. 2023.

BARROS, Marcelo. **Escola de Guerra Naval promoveu o seminário: A Guerra Híbrida e a Defesa Nuclear, Biológica, Química e Radiológica (NBQR)** – um desafio para o futuro do Brasil e para o Ensino Militar. Defesa em Foco, 2022. Disponível em: <https://www.defesaemfoco.com.br/escola-de-guerra-naval-promoveu-o-seminario-a-guerra-hibrida-e-a-defesa-nuclear-biologica-quimica-e-radiologica-nbqr/>. Acesso em: 17 ago. 2023.

BARROS, Marcelo. **Centro de Jogos de Guerra conduz Primeiro Jogo Híbrido para Elaboração da Estratégia de Defesa Marítima**. Defesa em Foco, 2023. Disponível em: <https://www.defesaemfoco.com.br/centro-de-jogos-de-guerra-conduz-primeiro-jogo-hibrido-para-elaboracao-da-estrategia-de-defesa-maritima/>. Acesso em: 17 ago. 2023.

BARROS, Marcelo. **Comando do 3º Distrito Naval realiza "1º Exercício Teórico de Segurança da Informação e Cibernética"**. Defesa em Foco, 2023a. Disponível em: <https://www.defesaemfoco.com.br/comando-do-3o-distrito-naval-realiza-1o-exercicio-teorico-de-seguranca-da-informacao-e-cibernetica/>. Acesso em: 17 ago. 2023.

BASSFORD, Christopher. The Primacy of Policy and the "Trinity" in Clausewitz's Mature Thought. In: STRACHAN, H.; HERBERG-ROTHE, A. (Eds.). **Clausewitz in the Twenty-first Century**. New York: Oxford University Press, 2007 *apud* MARENUCCI, Roberto. **A TEORIA DA TRINDADE DE CLAUSEWITZ E SUA APLICABILIDADE AO ESTUDO DO TERRORISMO DO SÉCULO XXI**. 2021. 31 f. Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior. Escola de Guerra Naval, 2021.

BILAL, Arsalan. **Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote**. NATO REVIEW. 30 nov. 2021. Disponível em:<https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>. Acesso em 25 mar. 2023.

BOYD, John Richard. **PATTERNS OF CONFLICT.** 1986. Disponível em: < https://www.ausairpower.net/JRB/poc.pdf>. Acesso em: 03 jul. 2023 *apud* BARBOZA, Carlos Eduardo de Matos; TEIXEIRA, Luís Henrique Vighi. **Resgatando a Essência das Operações de Informação na Guerra Convencional**. Army University Press, 2020. Disponível em: <https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Arquivos/Quarto-Trimestre-2020/Resgatando-a-Essencia-das-Operacoes-de-Informacao-na-Guerra-Convencional/>. Acesso em: 03 jul. 2023.

BRASIL. Estado-Maior do Exército. **EB70-MC-10.213: Manual de Campanha de operações de Informação do Exército Brasileiro**. 2. ed Brasília, DF, 2019.

BRASIL. Ministério da Defesa. **MD-35 - Glossário das Forças Armadas**. 5. ed. Brasília, DF, 2015.

BRASIL. Marinha do Brasil. Comando de Operações Navais. **COMOPNAVISNT Nº 30-01**. Rio de Janeiro, 2020.

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

BRASIL. Ministério da Defesa - Estado-Maior Conjunto das Forcas Armadas. **GUIA DO PLANEJAMENTO BASEADO EM CAPACIDADES (PBC)**. 1ª edição. Brasília, DF, 2022.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Brasil, 2012. Disponível em: <https://www.gov.br/defesa/pt-br/arquivos/estado_e_defesa/END-PNDa_Optimized.pdf>. Acesso em: 10 jun. 2023.

BRASIL. **Plano Estratégico da Marinha (PEM 2040)**. Estado-Maior da Armada, Brasília-DF: 2020. Disponível em: <https://www.marinha.mil.br/sites/all/modules/pub_pem_2040/book.html>. Acesso em: 17 jun. 2023.

BRITANNICA. **AWACS**: aircraft and military technology. Encyclopedia Britannica, 2023. <Disponível em:<https://www.nato.int/cps/en/natohq/topics_49755.htm?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 07 mai. 2023.>. Acesso em 06 maio 2023.

ČAJIĆ, Jasmin. **The Relevance of Clausewitz's Theory of War to Contemporary Conflict Resolution**. Connections: The Quarterly Journal. 15(1), 72-78, 2016. Disponível em:<http://connections-qj.org/article/relevance-clausewitzs-theory-war-contemporary-conflict-resolution>. Acesso em 25 mar. 2023.

CCSM. **Economia Azul**. Centro de Comunicação Social da Marinha, 2023. Disponível em: <https://www.marinha.mil.br/economia-azul/sobre>. Acesso em: 10 jun. 2023.

CLARK, Blane R. **As Operações de Informações como um Elemento Dissuasório do Conflito Armado.** Army University Press, 2010. Disponível em: <https://www.armyupress.army.mil/Journals/Edicao-Brasileira/artigos-em-destaque/2018/as-operacoes-de-informacoes-como-um-elemento-dissuasorio-do-conflito-armado/>. Acesso em: 02 jul. 2023.

CLAUSEWITZ, Carl von. **Da Guerra**. Tradução Maria Teresa Ramos. 3. ed. São Paulo: WMF Martins Fontes Ed., 2010.

CNN. **Redução de recursos atrasa modernização das Forças Armadas**. CNN BRASIL, 2023. Disponível em: <https://www.cnnbrasil.com.br/politica/reducao-de-recursos-atrasa-modernizacao-das-forcas-armadas/>. Acesso em: 17 ago. 2023.

COMISSÃO EUROPEIA. **Action Plan against Disinformation**. Bruxelas, 2018. Disponível em: < https://commission.europa.eu/system/files/2018-12/eu-communication-disinformation-euco-05122018_en.pdf>. Acesso em: 14 abr. 2023.

COMISSÃO EUROPEIA. **Joint Framework on countering hybrid threats.** Bruxelas, 2016. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250>. Acesso em: 10 nov. 2023.

CORRÊA, Alessandro José. **Operações de informações**: um antigo conceito com um novo paradigma. Coleção Meira Mattos, revista das ciências militares, n° 27, 3° quadrimestre 2012. Rio de Janeiro: ECEME, 2012. 27f. Disponível em: <http://www.ebrevistas.eb.mil.br/RMM/article/view/123/211>. Acesso em: 02 jul. 2023.

DANIK, Yuri; MALYARCHUK, Tamara; BRIGGS, Chad. **Guerra Híbrida: Hi-Tech, Informação e Conflitos Cibernéticos**. Conexões: The Quarterly Journal 18, n° 1 (2019): 110-129. Disponível em:<https://connections-qj.org/ru/article/gibridnaya-voyna-hay-tek-informacionnye-i-kiber-konflikty?_x_tr_sch=http+HYPERLINK>. Acesso em: 01 jul. 2023.

DIAS, Claudio Eduardo Silva. **O COMANDO NAVAL DE OPERAÇÕES ESPECIAIS**. Revista do Clube Naval, v.4 n. 404 (2022). Disponível em: <https://portaldeperiodicos.marinha.mil.br/index.php/clubenaval/article/view/3706/3696>. Acesso em: 17 ago. 2023.

DUMLUPINAR, Nihat; EROL, Mehmet Seyfettin**. THE FINAL STATE OF WAR: HYBRID WAR.** Journal: **Uluslararası Kriz ve Siyaset Araş**tırmaları Dergisi, n. 2, 156-186, 2020. Disponível em: <https://dergipark.org.tr/en/download/article-file/1480694>. Acesso em: 13 abr. 2023.

FBI. **WHAT WE INVESTIGATE**. FEDERAL BUREAU OF INVESTIGATION, 2023. Disponível em: <https://www.fbi.gov/investigate/terrorism>. Acesso em: 29 jul. 2023.

GARCÍA, Juan Pablo Villar; QUIRÓS, Carlota Tarín; SORIA, Julio Blázquez; PASCUAL, Carlos Galán; CORDERO,Carlos Galán. **Strategic communications as a key factor in countering hybrid threats.** European Parliamentary Research Service. Brussels, European Union, 2021. ISBN: 978-92-846-7812-9. Disponível em: <https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2021)656323>. Acesso em: 11 abr. 2023.

GAREIS, Sven Bernhard. **Hybrid War and Hybrid Threats**. Journal of European Security and Defense Issues (Per Concordiam), 2017. Disponível em: <https://perconcordiam.com/hybrid-war-and-hybrid-threats/>. Acesso em 01 jul. 2023.

GIANNOPOULOS, Georgios; SMITH, Hanna; THEOCHARIDOU, M. **The Landscape of Hybrid Threats: A conceptual model**. EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305. Disponível em: <https://www.hybridcoe.fi/wp-content/uploads/2021/02/conceptual_framework-reference-version-shortened-good_cover_-_publication_office.pdf>. Acesso em 06 abr. 2023.

GIANNOULIS, Georgios. **Handbook on maritime hybrid threats: 15 scenarios and legal scans**. The European Centre of Excellence for Countering Hybrid Threats. Hybrid CoE, 2023. Disponível em: <https://www.hybridcoe.fi/wp-content/uploads/2023/03/NEW_web_Hybrid_CoE_Paper-16_rgb.pdf>. Acesso em 02 jun. 2023.

GIL, Javier Miguel. **El tratamiento informativo de la guerra híbrida de Rusia**. Revista Latinoamericana de Estudios de Seguridad, URVIO n. 25 Quito jul./dez. 2019. Versão online ISSN 1390-4299. Madrid, España, . Disponível em:<http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S1390-42992019000200108>. Acesso em 01 abr. 2023.

HOFFMAN, Frank G. **Conflict in the 21st Century: The Rise of Hybrid Wars.** Potomac Institute for Policy Studies, Arlington, Virginia, 2007. Disponível em: <https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf >. Acesso em 24 jun. 2023.

HOFFMAN, Frank G. **Hybrid vs. Compound War. The Janus choice: Defining today's multifaceted conflict.** Armed Forces Journal, Oct. 2009. Disponível em: <https://www.semanticscholar.org/paper/Hybrid-vs-.-compound-war-The-Janus-choice-%3A-today-%E2%80%99-Hoffman/1dd5a837b35bf511d787d40c998646790da07a2d>. Acesso em: 02 abr. 2023.

HYBRID COE. **Hybrid threats as a concept**. The European Centre of Excellence for Countering Hybrid Threats, 2023. Disponível em: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>. Acesso em: 02 abr. 2023.

JONSSON, Oscar. **The Evolution of Russian Hybrid Warfare: EU/NATO**. Center for European Policy Analysis (CEPA), 2021. Disponível em:<https://cepa-org.translate.goog/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-eu-nato/?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 24 jun. 2023.

KORKMAZ, Huseyin. **ANALYSIS: Hybrid warfare and maritime militia in China**. Anadolu Ajansı, 2020. Disponível em: <https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259#>. Acesso em: 07 jun. 2023.

KOTMAN, Türkay. **Maritime Hybrid Threat.** MARSEC COE, 2021. Disponível em: <https://www.marseccoe.org/wp-content/uploads/2021/08/Maritime-Hybrid-Threat.pdf>. Acesso em 02 jun. 2023.

KREMIDAS-COURTNEY, Chris. **Countering Hybrid Threats in the Maritime Environment**. The Maritime Executive, 2018. Disponível em: <https://maritime--executive-com.translate.goog/editorials/countering-hybrid-threats-in-the-maritime-environment?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 02 jun. 2023.

LEAL, Paulo Cesar. **A Guerra Híbrida**: Reflexos para o Sistema de Defesa no Brasil. In: Doutrina Militar Terrestre em Revista, vol.4, n.9, pp. 6-17, 04 jan. 2016. Brasília – DF: EME. Disponível em: <http://www.ebrevistas.eb.mil.br/DMT/article/view/722>. Acesso em 24 jun. 2023.

LEE, Mattew. **A global mystery: What's known about Nord Stream explosions**. The Associated Press, 2023. Disponível em: <https://apnews.com/article/us-germany-russia-denmark-ukraine-gas-pipeline-attack-nord-stream-2561f98ba6462db700f7609352a28c24>. Acesso em: 08 jun. 2023.

MAHNKEN, Thomas G. Strategic Theory. In: BAYLIS, John; WIRTZ, James J.; GRAY, Colin S. **Strategy in the contemporary world**. 3. ed. New York: Oxford University Press, 2010 *apud* MARENUCCI, Roberto. **A TEORIA DA TRINDADE DE CLAUSEWITZ E SUA APLICABILIDADE AO ESTUDO DO TERRORISMO DO SÉCULO XXI.** 2021. 31 f. Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior. Escola de Guerra Naval, 2021.

MANNTEUFEL, Ingo. **A prova conclusiva no caso Skripal**. DW made for minds, 2018. Disponível em: <https://www.dw.com/pt-br/opini%C3%A3o-a-prova-conclusiva-no-caso-skripal/a-45660453>. Acesso em: 29. abr. 2023.

MARENUCCI, Roberto. **A TEORIA DA TRINDADE DE CLAUSEWITZ E SUA APLICABILIDADE AO ESTUDO DO TERRORISMO DO SÉCULO XXI.** 2021. 31 f. Monografia apresentada à Escola de Guerra Naval, como requisito parcial para a conclusão do Curso Superior. Escola de Guerra Naval, 2021.

MATTHYS, Olivier. **O que dizem o Artigo 4º e 5º da NATO?**. EURONEWS, 2022. Disponível em: <https://pt.euronews.com/2022/11/16/o-que-dizem-o-artigo-4-e-5-da-nato>. Acesso em: 07 maio 2023.

MCCULLOH, Timothy; JOHNSON, Richard. **Hybrid Warfare**. Joint Special Operations University (JSOU) Report 13-4. The JSOU Press MacDill Air Force Base, Florida 2013. ISBN: 978-1-933749-77-8

MELLO, Jorge Luís de Araújo. **OPERAÇÕES DE INFORMAÇÃO (OpInfo) APLICADOS AO NÍVEL ESTRATÉGICO**. Escola de Guerra Naval (EGN), 2023.

MONAGHAN, Sean; CULLEN, Patrick; WEGGE, Njord. MCDC, Multinational Capability Development Campaign. **Countering Hybrid Warfare (CHW) Project**. Oslo: Norwegian Institute of lntemational Affairs, 2019. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/784299/concepts_mcdc_countering_hybrid_warfare.pdf>. Acesso em: 07 abr. 2023.

MORRIS, Lyle J.; MAZARR, Michael J. ; HORNUNG, Jeffrey W. ; PEZARD, Stephanie; BINNENDIJK, Anika; KEPE, Marta. **Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War**. Santa Monica, CA: RAND Corporation, 2019. Disponível em: <https://www.rand.org/pubs/research_reports/RR2942.html#download>. Acesso em: 02 jun. 2023.

NATO. **NATO's Readiness Action Plan**. NORTH ATLANTIC TREATY ORGANIZATION, 2016. Disponível em:<https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf>. Acesso em 06 maio 2023.

NATO. **NATO Response Force**. NORTH ATLANTIC TREATY ORGANIZATION, 2022a. Disponível em:<https://www.nato.int/cps/en/natohq/topics_49755.htm?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 07 maio 2023.

NATO. **NATO's response to hybrid threats**. NORTH ATLANTIC TREATY ORGANIZATION, 2023. Disponível em:<https://www.nato.int/cps/en/natohq/topics_156338.htm?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 24 jun. 2023.

NATO. **Readiness Action Plan (RAP)**. NORTH ATLANTIC TREATY ORGANIZATION, 2022. Disponível em:<https://www.nato.int/cps/en/natohq/topics_119353.htm?_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 06 maio 2023.

NATO. **Relations with partners in the Indo-Pacific region.** NORTH ATLANTIC TREATY ORGANIZATION, 2023a. Disponível em:<https://www.nato.int/cps/en/natohq/topics_183254.htm>. Acesso em 26 jul. 2023.

NOLL, Jörg; BOJANG, Osman; RIETJENS, Sebastian. **Deterrence by Punishment or Denial? The eFP Case.** In: Osinga, F., Sweijs, T. (eds) NL ARMS Netherlands Annual Review of Military Studies, 2020. NL ARMS. T.M.C. Disponível em: < https://link.springer.com/chapter/10.1007/978-94-6265-419-8_7>. Acesso em: 29 abr. 2023.

OLIVEIRA, Arize. **O que é proxy? Descubra o significado desse termo.** TechTudo, 2011 . Disponível em: <https://www.techtudo.com.br/noticias/2011/05/o-que-e-proxy-descubra-o-significado-desse-termo.ghtml>. Acesso em: 19 abr. 2023.

PEREIRA, Douglas Leandro. **O que é Troll?**. Tecmundo, 2009. Disponível em: < https://www.tecmundo.com.br/msn-messenger/1730-o-que-e-troll-.htm>. Acesso em: 29 abr. 2023.

PETROBRAS. **BACIA DE SANTOS – ROTA 3**. COMUNICAÇÃO BACIA DE SANTOS, 2022. Disponível em: < https://comunicabaciadesantos.petrobras.com.br/web/comunica-bacia-de-santos/rota-3>. Acesso em: 15 jun. 2023.

PETROBRAS. **GASODUTO ROTA 3 INICIA OPERAÇÃO PARCIAL DE ESCOAMENTO DE GÁS NATURAL**. COMUNICAÇÃO BACIA DE SANTOS, 2022a. Disponível em: < https://comunicabaciadesantos.petrobras.com.br/w/gasoduto-rota-3-inicia-operacao-parcial-de-escoamento-de-gas-natural>. Acesso em: 15 jun. 2023.

POLYAKOVA, Alina; BOULÈGUE, Mathieu; ZAREMBO, Kateryna; SOLODKYY, Sergiy; STOICESCU, Kalev; CHATTERJE-DOODY, Precious N; JONSSON, Oscar. **THE EVOLUTION OF RUSSIAN HYBRID WARFARE**. Center for European Policy Analysis (CEPA), 2020. Disponível em:<https://cepa.org/wp-content/uploads/2021/01/CEPA-Hybrid-Warfare-1.28.21.pdf>. Acesso em 07 jul. 2023.

POMERLEAU, Mark. **How Army leaders envision non-kinetic capabilities enabling traditional forces**. DEFENSESCOOP, 2023. Disponível em: <https://defensescoop.com/2023/09/19/how-army-leaders-envision-non-kinetic-capabilities-enabling-traditional-forces/#:~:text=In%20U.S.%20military%20parlance%2C%20the,and%20other%20means%20of%20attack.>. Acesso em: 10 nov. 2023.

PRATT, Mary K. **ICT (information and communications technology, or technologies)**. Tech Target, 2019. Disponível em: <https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies>. Acesso em: 19 abr. 2023.

REICHBORN-KJENNERUD, Erik; CULLEN, Patrick. MCDC, Multinational Capability Development Campaign. Countering Hybrid Warfare (CHW) Project. **Understanding Hybrid Warfare.** Information note. Oslo: Norwegian Institute of lntemational Affairs, 2017. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/717539/MCDC_CHW_Information_Note-Understanding_Hybrid_Warfare-Jan_2018.pdf>. Acesso em: 07 abr. 2023.

ROCKCONTENT. **Entenda o que é a Era da Informação e quais os seus impactos no marketing.** Redator Rock Content, 2019. Disponível em: <https://rockcontent.com/br/blog/era-da-informacao/>. Acesso em: 19 jun. 2023.

RODRIGUES, Fernando da Silva. **Guerra Híbrida**: por uma discussão conceitual. Centro de Estudos Estratégicos do Exército (CEEEx), vol. 18, n. 4, pp. 23-36, 12 mar. 2021. Brasília – DF. Disponível em: < http://www.ebrevistas.eb.mil.br/CEEExAE/article/view/7012> Acesso em: 02 mar. 2023.

RÜHLE, Michael; ROBERTS, Clare. **Enlarging NATO's toolbox to counter hybrid threats**. NATO, 2021. Disponível em:< https://www.nato.int/docu/review/articles/2021/03/19/enlarging-natos-toolbox-to-counter-hybrid-threats/index.html?utm_medium=email&utm_campaign=NATO+Review+NATOs+response+to+hybrid+threats&utm_content=NATO+Review+NATOs+response+to+hybrid+threats+CID_1b42125209149d6086a0df00e726dec5&utm_source=Email+marketing+software&utm_term=READ+MORE&_x_tr_sl=en&_x_tr_tl=pt&_x_tr_hl=pt-BR&_x_tr_pto=sc>. Acesso em 08 maio 2023.

RÜHLE, Michael. **NATO's Unified Response to Hybrid Threats.** CEPA, 2021a. Disponível em:<https://cepa.org/article/natos-unified-response-to-hybrid-threats/>. Acesso em 27 maio 2023.

SGB. **Conselho de Defesa Sul-Americano – CDS**. Serviço Geológico do Brasil - CPRM, 2023. Disponível em:< http://www.sgb.gov.br/publique/Sobre/Assuntos-Internacionais/Conselho-de-Defesa-Sul-Americano---CDS-3937.html>. Acesso em 07 maio 2023.

SØRENSEN, Heine; NYEMANN, Dorthe Bach.. MCDC, Multinational Capability Development Campaign. Countering Hybrid Warfare (CHW) Project. **Deterrence by Punishment as a way of Countering Hybrid Threats – Why we need to go 'beyond resilience' in the gray zone**. Information note. Oslo: Norwegian Institute of lntemational Affairs, 2019. Disponível em: <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/783151/20190304-MCDC_CHW_Information_note_-_Deterrence_by_Punishment.pdf>. Acesso em: 06 abr. 2023.

STARLING, Clementine G.; LYER, Arun; GIESLER, Robert J. **Today's wars are fought in the 'gray zone.' Here's everything you need to know about It.** Hybrid Conflict Project. Atlantic Council.February 23, 2022.

STAVRIDIS, James. **Maritime Hybrid Warfare Is Coming**. U.S. Naval Institute, 2016. Proceedings, vol. 142/12/1,366. Disponível em: <https://www.usni.org/magazines/proceedings/2016/december/maritime-hybrid-warfare-coming>. Acesso em: 03 jun. 2023.

WEISSMANN, Mikael; NILSSON,Niklas; PALMERTZ, Björn; THUNHOLM, Per. **Hybrid Warfare: Security and Asymmetric Conflict in International Relations.** London: I.B. Tauris, 2021. Bloomsbury Collections. Disponivel em: <https://www.bloomsburycollections.com/book/hybrid-warfare-security-and-asymmetric-conflict-in-international-relations/>. Acesso em 01 abr. 2023.

WIELAND, Eduardo Augusto. **GUERRA HÍBRIDA NO AMBIENTE MARÍTIMO:** Uma compreensão inicial. In: Revista do Centro de Estudos Estratégicos e Planejamento Espacial Marinho, vol.2, n.1, pp. 34-41, jan. a mar. 2022. ISSN: 2763-8111. Pelotas - RS. Disponível em: <https://wp.ufpel.edu.br/cedepem/files/2022/11/Volume-2-Numero-1-1.pdf#page=34>. Acesso em 24 jun. 2023.

WILTGEN, Guilherme; PADILHA, Luiz. **Operação Poseidon: Exército, Marinha e Aeronáutica operam juntos pela primeira vez a partir do PHM 'Atlântico'.** Defesa Aérea & Naval, 2020. Disponível em: <https://www.defesaaereanaval.com.br/artigos/operacao-poseidon-exercito-marinha-e-aeronautica-operam-juntos-pela-primeira-vez-a-partir-do-phm-atlantico>. Acesso em: 17 ago. 2023.