ESCOLA DE GUERRA NAVAL

CC (AFN) Ozéias Braz de Mattos

O EMPREGO DAS CAPACIDADES RELACIONADAS À INFORMAÇÃO EM OPERAÇÕES CONTRA AMEAÇAS HÍBRIDAS

Rio de Janeiro

2022

CC (AFN) Ozéias Braz de Mattos

O EMPREGO DAS CAPACIDADES RELACIONADAS À INFORMAÇÃO EM OPERAÇÕES CONTRA AMEAÇAS HÍBRIDAS

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

Orientador: CMG(RM1-FN) Jorge Luís de Araujo Mello

Rio de Janeiro

Escola de Guerra Naval

2022

RESUMO

O emprego das ameaças híbridas está cada vez mais presente no cenário mundial. Embora esse *modus operandi* possa parecer novo, já é bastante antigo. Por certo, o espectro híbrido vem sendo utilizado pelos principais países, tanto antes da Segunda Guerra Mundial quanto após, nas condições de mundo bipolar. Sua aplicação se tornou muito mais atraente e devastadora devido à influência ao poder proporcionados pelas Operações de Informação. De fato as ameaças híbridas deram uma face mais obscuras às Operações de Informação. Portanto, as Operações de Informação são apropriadas tanto para a aplicação das ameaças híbridas quanto para combatê-las. Assim, O propósito da pesquisa é demonstrar as possibilidades das Capacidades Relacionadas à Informação para combater as ameaças híbridas. Para atingir o objetivo, foram realizadas análises de documentos normativos da MB e de outras Forças Armadas, bem como documentos e trabalhos da Escola Superior de Guerra e pesquisa bibliográfica, principalmente literatura estrangeira, já que é raro encontrar o assunto em português. O estudo selecionou e explicou exemplos de realização de Operações de Informação e de ameaças híbridas apontando seus consequentes resultados. A fim de otimizar o entendimento, foram utilizados os conceitos de Operações de Informação e guerra/ameaças híbridas. Ao final, concluiu-se que este trabalho alcançou seu intuito, por meio da apresentação de possibilidades de emprego das OpInfo frente as ameaças híbridas, bem como indicou a necessidade do estudo do assunto, acompanhado de propostas para tal.

Palavras chaves: Operações de Informação. Ameaças Híbridas. Guerra irregular. Propaganda. Comunicação Social. Operações Psicológicas. Zona Cinzenta. Estratégia e Defesa.

LISTA DE ABREVIATURAS E SIGLAS

ACISO - Ação Cívico Social

CIA - *Central Intelligence Agency*

ComSoc - Comunicação Social

CRI - Capacidades Relacionadas à Informação

DNC - *Democratic National Committee*

EB - Exército Brasileiro

EMA - Estado-Maior da Armada

EUA - Estados Unidos da América

FBI - *Federal Bureau of Investigation*

ICA - *Islamic Cyber Army*

ISIS - *Islamic State Hacking Division*

JCOIE - *Joint Concept for Operating in the Information Environment*

JD- *Joint Publication*

MB - Marinha do Brasil

MCDC - *Multinational Capability Development Campaign*

MD - Ministério da Defesa

MISO- *Military Information Support Operations*

ONU - Organização das Nações Unidas

OpInfo - Operações de Informação

OpPsc - Operações Psicológicas

OTAN - Organização do Tratado do Atlântico Norte

PEM - Plano Estratégico da Marinha

PND - Política Nacional de Defesa

PNM - Programa Nuclear da Marinha

SOAMAR - Sociedade Amigos da Marinha

SUMÁRIO

1 INTRODUÇÃO

A humanidade tem presenciado o valor e o poder da influência da informação. Não é mais segredo que em um confronto entre vontades, a habilidade de explorar o ambiente informacional provou ser mais eficaz do que a completa dominação pela força. Em consequência disso, o termo "Operações de Informação" (OpInfo), ganha notoriedade no cenário mundial, particularmente no meio militar, midiático, político e acadêmico.

Em relação à definição de OpInfo, antes de mais nada, é necessário ressaltar que quaisquer tipos de operações[1](BRASIL, 2015, p. 189), em princípio, fazem parte do contexto de uma guerra. As OpInfo, por sua vez, também são conduzidas em tempo de paz, embora dificilmente as potências militares assumam atuar nesse sentido (Pocheptsov, 2000).

De fato, as OpInfo tornaram-se um recurso estatal importante. Pocheptsov (2000) afirma que os círculos militares da Rússia, por exemplo, reconhecem o significativo impacto que as OpInfo causam em uma sociedade ou em um combate. Dessa forma, segundo o autor, os russos focaram alguns estudos sobre o conceito de "Guerra da informação[2]"(BRASIL, 2015), utilizado na doutrina americana.

Nessa perspectiva, Pocheptsov (2000) foi particularmente específico ao escrever que na tradução russa, o termo soa de forma mais completa, significando "Guerra Psicológica da Informação", uma vez que possuem a tarefa de influenciar o inimigo mesmo antes do início das hostilidades ativas, com o fim de garantir o controle do lado oposto e os processos de tomada de decisão.

Na Marinha do Brasil (MB), a definição de OpInfo está norteada pelo Manual de Doutrina de OpInfo – EMA-335 (BRASIL, 2018), o qual está alinhado com as principais definições apresentadas no mundo ocidental, como por exemplo, o manual do Estado-Maior Conjunto Americano (USD, JP3-13, 2014).

---

1 "Ação militar, para a execução de uma missão de natureza estratégica ou tática de combate ou logística, em adestramento ou instrução".

2 No Glossário das Forças Armadas do Brasil a Guerra é definida como um conflito com a violência em seu grau máximo, cuja condução implica a mobilização de todo o Poder Nacional. Assim, quando se usa expressão "Guerra de Informação" entende-se que se aplica enquanto Estados já estão em situação beligerante, ou seja, quando uma guerra está realmente acontecendo, enquanto as operações são aquelas que podem ser sempre implementadas.

Dessa forma, o EMA-335 (BRASIL, 2018) conclui que as OpInfo consistem em coordenar as Capacidades Relacionadas à Informação[3] (CRI), com a finalidade de informar e influenciar grupos-alvo e alcançar objetivos políticos e militares, bem como conduzir o processo decisório dos oponentes ou potenciais oponentes em benefício à Força, sem deixar de garantir a integridade do próprio processo (BRASIL, 2018, p. 2-6 e 2-7).

Nesse sentido, a doutrina americana assinala que as OpInfo visam usar a própria informação como arma, sendo os meios físicos apenas complementos, ou seja, se não precisar utilizá-los, melhor. A doutrina americana ainda possui definição, similar ao EMA-335 (2018):

> As operações de informação são o emprego das capacidades centrais de guerra eletrônica, operações de rede de computadores, operações psicológicas e segurança de operações, em conjunto com recursos específicos de suporte e relacionados, para afetar ou defender informações e sistemas de informação e influenciar a tomada de decisões (FM 3-13, 2003, p. 3, tradução nossa).

Ainda no que se refere a evolução das operações, outro termo frequentemente articulado, principalmente pela mídia, é a ameaça híbrida. Trata-se do mais recente dos desafios de defesa nas últimas três décadas (KEFELI; KOMLEVA, 2020). O General russo Gerasimov (2013) em seu artigo intitulado: "O valor da ciência na previsão", afirma que para se impor à superioridade do adversário, os oponentes desenvolveram meios alternativos para atingir seus objetivos, de modo que os oponentes híbridos constituem-se como combinações difíceis e muitas vezes poderosas em constante aprimoramento.

De forma geral, as ameaças híbridas se popularizaram em 2007, devido ao artigo de Hoffman (2007) intitulado: "Conflito no Século 21: A Ascensão das Guerras Híbridas". Segundo o autor, as ameaças híbridas empreendem a combinação dos modus operandi do conflito convencional com o fervor fanático das guerras irregulares, como o terrorismo, os movimentos de resistência, a guerrilha, a insurreição, entre outros. Nesse sentido, Murray e Mansoor (2020) complementam essa interpretação. Segundo os autores, as ameaças híbridas podem compreender atores estatais e não estatais, cujo objetivo é alcançar um propósito político comum.

---

3 "Aptidões requeridas para afetar a capacidade de oponentes ou potenciais adversários de orientar, obter, produzir e difundir informações, em qualquer uma das três perspectivas da dimensão informacional".

Diante dessas considerações, as ameaças híbridas podem ser interpretadas como um modelo de conflito que tenta esconder sua natureza militar. Assim, o meio utilizado para tal abrange o papel das Capacidades Relacionadas à Informação, as quais passaram a ter atuação relevante, pois são indispensáveis para que as ameaças híbridas tenham sucesso desde o início de sua aplicação, já que os contextos físicos são substituídos por contextos informacionais, ocultando e fechando o estado real das coisas com mais intensidade do que em uma guerra convencional. É exatamente neste ponto que esta pesquisa enveredará.

Nesse contexto, o objetivo deste trabalho reside em demonstrar como as Capacidades Relacionadas à Informação podem ser empregadas para combater as ameaças híbridas. Para isso, o seguinte questionamento passa a nortear esta pesquisa: Quais as possibilidades de emprego das Capacidades Relacionadas à Informação para combater as ameaças híbridas?

O estudo teórico é de natureza exploratória e qualitativa (LAKATOS; MARCONI, 2003). O trabalho buscará respostas para o problema da pesquisa por meio de estudos bibliográficos que abordem o assunto “Operações de Informação relacionadas com as ameaças híbridas”, por meio de análise de literatura concernente ao assunto abordado, tais como documentos normativos da MB e de outras Forças Armadas, assim como documentos e trabalhos da Escola Superior de Guerra.

Em relação ao método da pesquisa, este foi balizado no método dedutivo para buscar expor e correlacionar os conceitos e definições de OpInfo e Ameaças Híbridas, apontando a importância para a Defesa Nacional.

Assim, no capítulo que se segue foi realizada uma abordagem sobre a OpInfo, suas características, conceitos e finalidades. A partir dessa conceituação, são citados exemplos de acontecimentos em que a realização de OpInfo teve grande relevância no cenário mundial.

No terceiro capítulo foram apresentadas as definições e características das ameaças híbridas e, paralelamente, como as Organizações Internacionais e as grandes potências estão lidando com essa hostilidade.

Findando o terceiro capítulo, e com o propósito de respondermos a questão colocada na pesquisa, é posta em discussão como as Capacidades Relacionadas à Informação (CRI) compõe e representam as condições básicas para emprego das ameaças híbridas e as

possibilidades de emprego das Capacidades Relacionadas à Informação para combater as ameaças híbridas. Ainda, enfatizamos o desenvolvimento de uma abordagem de prevenção e proatividade, com objetivo de vencer as investidas hostis.

Finalmente, ainda no terceiro capítulo, com o propósito de consubstanciar as contribuições geradas ao longo dos capítulos, descrevemos brevemente o que foi estudado e expomos o grau de importância das CRI no combate às ameaças híbridas. Também, de forma resumida, explanamos as bases de conhecimento utilizadas como sugestões às futuras pesquisas, com a finalidade de colaborar no aprimoramento da detecção, controle e redução do risco de um adversário explorar as vulnerabilidades a ponto de consolidar a aplicação de ameaças híbridas, que, por fim, responde à problemática escopo deste trabalho.

2 A APLICAÇÃO DO PODER DAS OPERAÇÕES DE INFORMAÇÃO

No presente capítulo, será realizada uma abordagem sobre o poder proporcionado pelo emprego integrado das Capacidades Relacionadas à Informação (CRI) coordenado pelas Operações de Informação (OpInfo). Ademais, para que o propósito deste capítulo seja atendido em sua plenitude, primeiramente será demonstrado o entendimento sobre a OpInfo, bem como as suas definições e o poder de influência que ela exerce sobre todas as ações militares.

2.1 As Operações de Informação

A epígrafe **"**O poder da informação" trata sobre o assunto e aparece constantemente em diversos trabalhos, manuais e artigos sobre Operações de Informação (OpInfo). De forma geral, o controle da informação propicia o poder para persuadir, influenciar ou para conduzir a decisão de agentes decisores e, consequentemente, estabelecer as condições necessárias para impor os interesses dos envolvidos.

Nesse sentido, no século atual, as atenções se voltam intensamente à Dimensão Informacional, no qual se pode angariar significativas vantagens sem o uso da força por meio de Operações de Informação. Embora a aplicação das OpInfo não seja compreendida como uma hostilidade física, pela capacidade delas de, na maioria das vezes, serem imperceptíveis e estarem abaixo do nível de uma agressão violenta, seus efeitos são igualmente

devastadores, com o agravante de ocorrem principalmente em tempos de paz e com ausência de qualquer declaração de guerra.

No ocidente, a maioria das Doutrinas sobre OpInfo encontram-se em fontes abertas, e há um consenso sobre a sua definição. Assim, a publicação EMA-335 (2018) é a Doutrina direcionada ao tema na Marinha do Brasil (MB). Suas instruções e características são similares, por exemplo, à Publicação Conjunta 3-13 de Operações de Informação (2016), do Departamento de Defesa dos Estados Unidos da América (EUA). Além disso, ela está balizada com o Manual de Campanha de Operações de Informação (2019) do Exército Brasileiro (EB) (BRASIL, 2019a).

De forma geral, pode-se constatar que as doutrinas lecionam as OpInfo como parte de um plano de operação[4], e não como uma entidade única, como o termo implica (BRASIL, 2006, p. 1-3). Salienta-se ainda que, segundo o EMA-335 (2018), as OpInfo são responsáveis por integrar com as diversas capacidades que atuam na Dimensão Informacional, seja na perspectiva cognitiva ou nas perspectivas humana, lógica e física.

Para entender melhor o escopo deste trabalho é necessário expor as perspectivas da Dimensão Informacional, às quais o EMA-335 (2018) se refere. Assim, segundo a doutrina, a perspectiva física é a infraestrutura facilitadora da transmissão, do armazenamento e da recepção de informações, como jornais e computadores, por exemplo. Já a perspectiva lógica inclui as redes que permitem que o conteúdo e o fluxo de dados sejam coletados, processados, armazenados e disseminados, ou seja, é a ligação com a perspectiva física.

Por último, mas não menos importante, a perspectiva cognitiva abrange as mentes individuais e coletivas, suas crenças, vulnerabilidades, emoções, experiências, saúde mental e ideologias, ou seja, todos que agem e são afetados pelos fluxos de informação.

Com relação à Dimensão Informacional, o EMA-335 (2018), a explica de forma resumida. Entretanto, uma definição mais completa e atualizada é encontrada na publicação Conjunta para Operação no Ambiente de Informação (USA, 2018) qual seja:

> Ambiente Informacional compreende e agrega inúmeros atributos sociais, culturais, cognitivos, técnicos e físicos que atuam e afetam o conhecimento, a compreensão, as crenças, as visões de mundo e, em última análise, as ações de um indivíduo, grupo, sistema, comunidade ou organização. O ambiente informacional também

4 "É a Diretiva relativa a operações a serem realizadas em futuro não imediato, envolvendo tempo e espaço consideráveis. É expedida por um Comandante de Força para transmitir orientações aos Comandantes subordinados para o preparo de seus Planos ou Ordens dela decorrentes".

> inclui sistemas técnicos e seu uso de dados. O ambiente informacional afeta diretamente e transcende todos os ambientes operacionais (USA, 2018, p. 42, tradução nossa).

Como se pode notar, as OpInfo são abrangentes. Desse modo, para afetar qualquer uma das perspectivas da Dimensão Informacional, as OpInfo empregam a chamada Capacidade Relacionada à Informação (CRI)[5], que, como já mencionado, possuem definições similares nas doutrinas ocidentais. Portanto, para este trabalho utilizaremos a definição do EMA-335 (BRASIL, 2018, p. 2-6).

Outras doutrinas apresentam diversas CRI, mas a Doutrina da Marinha e o Manual de Campanha de OpInfo do EB (2019) destacam somente sete. Dentre elas, se notabilizam: as Operações Psicológicas (OpPsc), as atividades de Comunicação Social (ComSoc) e as ações cibernéticas. O objetivo comum dessas três CRI está no nível psicológico do público-alvo, ou seja, visa conquistar seus corações e mentes, como será demonstrado na próxima seção.

2.1.1 As Ações Cibernéticas integradas às Operações Psicológicas (OpPsc)

Parece conveniente dizer que com a potencialização das tecnologias digitais, das mídias sociais e da velocidade de propagação de ideias, principalmente pela internet, nossa percepção de mundo pode ser manipulada com mais facilidade. Dessa forma, o emprego das OpPsc na Dimensão Informacional tornou-se um multiplicador de forças para influenciar e impor a vontade adversa. No Manual de Comando e Controle de Fuzileiros Navais consta o ensinamento de que as OpPsc estão voltadas a influenciar as emoções, as motivações, as razões e o comportamento de um público-alvo, que pode ser a população em geral ou tropas, organizações, associações e indivíduos. O seu propósito principal é conquistar corações e mentes (BRASIL, 2020a, p. 7-3).

Já na doutrina americana, há uma atualização do termo OpPsc. Segundo Cowan e Cook (2018), devido à conotação negativa do termo, a política do Exército americano resolveu alterar para *Military Information Support Operations* (MISO). Todavia, no Comando de Operações Especiais dos EUA, ainda há resistência quanto tal alteração, pois afinal, sua função e significado permanecem inalterados.

5 Dentre as CRI, destacam-se: Operações Psicológicas, Ações de Guerra Eletrônica, de Despistamento e de ações cibernéticas, Segurança da Informação, Destruição Física e atividades de Comunicação Social, as quais serão discutidas com mais detalhes no capítulo seguinte.

Nesse sentido, as OpPsc são ferramentas capazes de influir em convicções mais profundas, tal como a decisão do inimigo de abandonar a luta e render-se (BRASIL, 1999). É por meio dela que as verdades são selecionadas e manipuladas com o objetivo de moldar a formação de certas ideias, visões, crenças ideológicas ou políticas, e ao mesmo tempo, causar emoções, sentimentos positivos ou negativos e até reações violentas em massa.

Atualmente as OpPsc são largamente empregadas com o auxílio de ações cibernéticas pelo mundo todo. Em resumo, segundo o EMA-335, as ações cibernéticas consiste na aplicação de ferramentas específicas, disponíveis na área de tecnologia da informação e comunicação (TIC), com a finalidade de desestabilizar ativos de informação hostis e permitir a proteção de recursos de TIC de interesse (BRASIL, 2018, p. 3-12).

Nesse ponto de vista não é de se estranhar que a conexão das ações cibernéticas com o terrorismo está cada vez mais intensa, bem como seu emprego tem alcançado com sucesso o efeito desejado, cujo objetivo principal é impor as orientações ideológicas e religiosas desses grupos por meio do medo (WOOD, 2015).

Por exemplo, o *Islamic State Hacking Division* (*ISIS*), que é a fusão de vários grupos de hackers, os quais se identificam como o exército digital do Estado Islâmico, difundiu no ano de 2015 em seu *Twitter* um vídeo brutal e impactante. O vídeo, com duração de vinte e dois minutos, expõe a morte do Tenente Moaz al-Ka sasbeh, piloto da Força Aérea Real da Jordânia, que foi capturado perto da cidade de Raqqa, na Síria. O piloto morreu em chamas, trancado em uma gaiola. As imagens foram impactantes como pode ser observada na FIG. 1.

As fortes imagens foram utilizadas como propaganda do medo, com o objetivo de enviar a mensagem de morte brutal, com a ausência de piedade ou remorso, contra aqueles que lutassem em desfavor do *ISIS*. O vídeo foi filmado profissionalmente, complementado por técnicas e efeitos sonoros destinados a gerar medo.

FIGURA 1 – Imagens da morte do Tenente Moaz al-Ka sasbeh.
Fonte: GAYLE, 2015.

Theohary (2018) afirma que o *ISIS* é também conhecido por "*Cyber Caliphate*" ou "*Islamic Cyber Army*" (*ICA*), e possui recorrente histórico de conduzir uma variedade de operações na Dimensão Informacional.

De forma similar, o modus operandi de OpPsc em paralelo com Ações Cibernéticas é comumente empregado por algumas Organizações e Estados. Há fortes indícios que agentes apoiados pela Rússia, por exemplo, utilizaram as mídias sociais e a Dimensão Informacional para influenciar os rumos das eleições nos EUA em 2016. Segundo o relatório da *Central Intelligence Agency* (CIA) de 2017 (USA, 2017) intitulado: "Background to *Assessing Russian Activities and Intentions in Recent US Elections: The Analytic Process and Cyber Incident Attribution"*, o presidente russo Vladimir Putin ordenou a realização de OpInfo com o emprego, em particular, de OpPsc e Ações Cibernéticas.

Os objetivos da Rússia eram minar a fé pública no processo democrático dos EUA, denegrir a candidata Hillary Clinton, prejudicar sua elegibilidade a presidência, e fazer a eleição pender em favor de seu adversário, Donald Trump.

Ainda de acordo com o referido relatório da CIA (USA, 2017), em 2015, o *Federal Bureau of Investigation* (FBI) já havia alertado que um sistema de computadores pertencentes ao Comitê Nacional Democrata (DNC) dos EUA tinha sido comprometido por hackers, conhecidos como "*The Dukes*", uma equipe ligada ao governo Russo. O DNC não levou a sério o alerta, pois achava que se tratava de um trote. Entretanto, já era o primeiro sinal de uma campanha de OpInfo arquitetada para interferir na eleição presidencial de 2016.

Dessa forma, algo que começou como uma operação para coletar informações, transformou-se em vazamentos de informações planejadas dia após dia. Documentos com grau de sigilo e diversos e-mails privados foram postados no *WikiLeaks* e em outros sites e, além disso, noticiados pela mídia americana.

Vale acrescentar ainda que muitas notícias falsas foram difundidas, assim como ataques propagandistas planejados foram conduzidos. Os impactos foram devastadores em desfavor de Hillary Clinton (ICA, 2017).

Em continuação, segundo a CIA, o Kremlin inseriu recursos significativos para expandir o alcance de suas operações, financiou canal de TV e empresas de análises, como a *Cambridge Analytica*, bem como recrutou e terceirizou hackers, manipulando os apoiadores e assessores. Com isso, conseguiu desestimular o apoio a Hillary Clinton, que era o objetivo principal.

A partir desses exemplos, vale acrescentar que, embora as OpPsc tenham recebido inúmeros nomes durante a história, tais como Guerra Política, Propaganda, Guerra Psicológica, Guerra de Nervos, Guerra Diplomática, Guerra Fria e Desinformação (BRASIL, 1999, p. 1-4), seu emprego já era uma tradição consagrada desde o mundo antigo. Na Alemanha Nazista, por exemplo, Adolf Hitler, percebia claramente o poder influenciador proporcionado pelas OpPsc, a ponto de dedicar dois capítulos inteiros sobre propaganda em seu livro *Mein Kampf*[6]. Da mesma forma era comum o líder nazista abordar o assunto em seus fervorosos discursos (BARTLETT, 2001 *apud* MATTOS, 2016, p. 20).

Assim, sob a coordenação das OpInfo, as OpPsc, integradas às Ações Cibernéticas, foram levadas a um novo patamar. Em um mundo globalizado e conectado, a utilização dessas operações possibilitou modificar opiniões, processos democráticos, culturas e até destruir qualquer Instituição ou Estado com mais velocidade e eficácia. Em outras palavras, as OpInfo possibilitaram coordenar um inquestionável poder que impulsiona um comportamento desejado e o curso dos eventos.

2.1.2 A Comunicação Social como Capacidade Relacionada à Informação (CRI)

6 É o título do livro de dois volumes de autoria de Adolf Hitler, no qual ele expressou suas ideias antissemitas, racialistas e nacional-socialistas então adotadas pelo partido nazista. O primeiro volume foi escrito na prisão e editado em 1925, e o segundo foi escrito por Hitler fora da prisão e editado em 1926.

No final de janeiro de 1968, ocorreu a maior Ofensiva coordenada da Guerra do Vietnã. Combatentes da Frente Nacional para a Libertação do Vietnã e guerrilheiros sul vietnamitas atacaram, de forma violenta, diversos alvos das tropas dos EUA e do Governo do Vietnã do Sul.

A data escolhida coincidia intencionalmente com as comemorações do Ano Novo Lunar, conhecido como Tet, conforme a cultura local. Desse modo, além dos danos em 36 capitais provinciais, na localidade de Da Nang, onde estava instalada a maior base aérea dos EUA, 30 aeronaves foram destruídas (PENELAS, 2015).

Em uma desesperada resposta, os americanos intensificaram os bombardeios e massacres indiscriminados contra povoados e cidades. Assim, embora os americanos deixassem claro a superioridade de armas, a ação os levou à derrota em relação ao assentimento da opinião pública[7](BRASIL, 2017, p. 62). A mídia atacou impiedosamente as decisões tomadas em relação ao conflito. Ficou claro ao público americano que uma vitória geral no Vietnã não era iminente, e tampouco era desejável a sua continuação (MURRAY; MANSOOR, 2020, p. 21-22).

Conforme ilustra esse exemplo, não basta alcançar a vitória somente em relação ao inimigo, o sucesso militar deve gerar um resultado proporcional junto à opinião pública, principalmente no momento em que os recentes e sofisticados sistemas de comunicação, como a Internet, os aparelhos celulares, a televisão e o rádio via satélite, expandiram radicalmente o nível de transmissão de informações públicas, como assinala Murray e Mansoor (2020). Para tanto, a Comunicação Social (ComSoc) desempenha um papel indispensável nos processos de tomada de decisão.

Essa concepção nos reverte aos ensinamentos contidos no Manual de Comunicação Social da Marinha, o EMA-860 (BRASIL, 2021), que normatiza as atividades de ComSoc na MB. O referido Manual deixa claro que a ComSoc é responsável em gerenciar as informações nas operações militares, e à luz da verdade, é a ferramenta proativa contra as investidas informacionais hostis (BRASIL, 2021, p. 14-3).

Vale ressaltar que pelo fato da ComSoc ser considerada uma CRI das OpInfo, pode ser confundida com as OpPsc, pois seus *modus operandi* possui sutis diferenças. Em

7 Opinião Pública – Pode ser entendida como a manifestação do público. Há uma equivalência entre reação pública e opinião pública, entendendo-se então a opinião pública como a manifestação da vontade coletiva acerca de um determinado tema.

resumo, enquanto a ComSoc é destinada a influenciar e divulgar informações precisas e verdadeiras, bem como se relacionar com o cidadão, as OpPsc são destinadas a potencializar as atividades militares, causar impactos psicológico no público-alvo ou induzir o adversário a uma falsa compreensão da consciência situacional.

Entretanto, há de se considerar que a ComSoc, inserida nas OpInfo, pode ultrapassar o propósito de somente divulgar informações ou esclarecimentos precisos. Ela é imprescindível nas Operações Militares, uma vez que possui a capacidade de ser empregada para manipular os meios comunicacionais, além de ser uma ferramenta de defesa importante contra a desinformação inimiga, que o glossário das Forças Armadas (2015) define como a técnica especializada que manipula de forma planejada as informações com o objetivo de induzir um agente decisor ao erro de avaliação.

Não é de se estranhar que no passado a MB já teve que empregar a ComSoc nesse sentido, embora naquele tempo ainda não se fizesse menção a OpInfo, tampouco a CRI. A instalação do Centro Experimental ARAMAR localizado em Iperó, Distrito de Sorocaba, São Paulo, foi um fato que não pode fugir à atenção. A instalação daquele Centro ocorreu entre os anos de 1979 e 1985, e passou a ser responsável pelo desenvolvimento de pesquisas, trabalhos de domínio da tecnologia nuclear, bem como a construção do submarino com propulsão nuclear.

Segundo Cezar (2009), a MB tentava convencer que o Programa Nuclear da Marinha (PNM) era pacífico, mas os argumentos não sensibilizaram a opinião pública, pois alguns personagens utilizaram os meios de comunicação de Sorocaba para desmentir, divulgar informações desencontradas e estabelecer polêmicas em torno do PNM. A população sorocabana ficou totalmente propensa às ações propagandistas dos desinformantes[8], uma vez que a propaganda era direcionada a despertar o medo pelas atrocidades “produzidas pelas explosões nucleares de Hiroshima e Nagasaki, e os acidentes de Chernobyl e de Goiânia” (CEZAR, 2009, p. 48-49).

Mesmo com o fato de terem ocorrido tentativas de convencimento de que o Programa Nuclear da Marinha era totalmente seguro e que não havia riscos, a falta de coordenação na divulgação e as deficientes argumentações das autoridades navais só

8 Gabriel Bittencourt: estudante da Faculdade de Filosofia, Ciências e Letras de Sorocaba, o Vereador Osvaldo Noce e mais algumas pessoas.

aumentaram o descompasso com a sociedade e municiaram ainda mais os argumentos dos agentes adversos (CEZAR, 2009, p. 48-49).

Sendo assim, a desinformação causou medo e estimulou a propagação de diversos protestos contra o ARAMAR por toda a região de Sorocaba. Nos protestos era comum visualizar faixas e cartazes incitando a população para parar e pensar se realmente valia a pena o Programa, conforme se pode observar na FIG. 2. A desinformação conduzida, induziu, inclusive, protestos de jejum e silêncio, os quais foram comparados ao processo da demonstração de Ghandi. A imprensa divulgou: “O silêncio protesta contra ARAMAR” (CEZAR, 2009, p. 49).

FIGURA 2 – Manifestações contra ARAMAR.
Fonte: EQUIPE ONLINE, Jornal Cruzeiro, 2015.

O slogan: “ARAMAR não vale a pena” também foi largamente empregado, sob a coordenação do jornal Cruzeiro do Sul, um dos maiores jornais do interior de São Paulo naquele período. A situação ficava cada vez mais complexa, a ponto de o problema atingir as famílias dos empregados de ARAMAR, as quais recebiam ameaças de toda ordem (CEZAR, 2009, p. 50). A opinião pública e a agitação popular alcançaram índices de rejeição pela MB nunca vistos na região.

Nesse contexto, a MB procurou retomar o controle das informações. Ela empregou as atividades englobadas pela ComSoc, e aos poucos a população sorocabana se acostumou com a presença da MB naquela região (CEZAR, 2009). Dentre essas atividades,

destacam-se as operações de Ação Cívico Social (ACISO), que possibilitaram visitas a escolas, asfaltamentos etc. A atuação ainda é contínua. A criação, em 1997, da Sociedade Amigos da Marinha (SOAMAR) mantém a influência naval no local.

Com esses exemplos, pode-se inferir que o emprego das OpInfo melhorou significativamente a atuação da ComSoc, integrando às outras CRI, e possibilitou meios prontamente disponíveis para discernir a verdade.

Desse modo, fica evidente que falar em OpInfo na Dimensão Informacional, particularmente nos dias atuais, sem associar à ComSoc torna-se uma prática não recomendada, pois a primeira viabiliza as ações da segunda, e confirma-se como ferramenta imprescindível contra as investidas mal-intencionadas. Assim, as OpInfo dispõem de CRI que, quando empregadas com coordenação e sintonia, tornam-se ferramentas poderosas em qualquer operação militar em tempos de paz ou de conflitos.

3 AS AMEAÇAS HÍBRIDAS

As ameaças híbridas representam a nova face do confronto entre vontades, pois permite que os variados atores se envolvam em conflitos sem ter que recorrer a combates diretos ou declarações de guerra abertas. Nos dias atuais, as armas de destruição em massa e a superioridade multipolar de algumas potências impõem limites ao confronto direto, retornando a estratégias obscuras e métodos já considerados primitivos, como guerras de guerrilha, crime organizado e terrorismo junto à abordagens convencionais (KORYBKO, 2018).

Sendo assim, neste capítulo serão abordadas as ameaças híbridas e os contextos teóricos que sustentam esse novo termo. A seguir, será apresentado como as Capacidades Relacionadas à Informação se enquadram nesse paradigma.

3.1 As Ameaças híbridas e sua aplicação

No Mar da China Meridional, que faz parte do Oceano Pacífico, situado ao sul da China, entre o Vietnã, a Malásia e as Filipinas, há uma disputa por águas e arquipélagos que já se arrasta por algum tempo. Segundo o Almirante Stavridis (2016), da Marinha dos EUA, não são raros navios chineses assediarem navios de pesca vietnamitas e filipinos.

Nesse contexto, Stavridis (2016) narra que, em certa noite, um navio cargueiro de 2.000 toneladas se aproximou de uma frota pesqueira vietnamita na área econômica exclusiva do Vietnã, permanecendo na área por uma ou duas horas. De forma repentina, foram lançadas ao lado do navio, três lanchas rápidas armadas com armamentos de calibre 50 e lançadores de foguetes portáteis.

Essas lanchas atacaram dezenas de embarcações de pesca e atiraram nos sobreviventes na água. Os remanescentes que sobreviveram nos barcos de pesca enquanto fogem em direção à costa, transmitem freneticamente pedidos de socorro por rádio, que são bloqueados por pequenos drones em operação. Na manhã seguinte, a Guarda Costeira vietnamita chega ao local e encontra apenas sangue na água, misturado com óleo e gasolina, e vários cascos fumegantes, bem como minas prontas para afundar embarcações desavisadas.

Sucessivamente, as redes sociais vietnamitas começam a divulgar aos pescadores de que suas águas estão cheias de terroristas. Ataques cibernéticos paralisam o sistema de vigilância por radar *offshore* vietnamita. A China, por sua vez, diz que suas forças armadas não estavam envolvidas, bem como alega suspeitar de piratas ou terroristas vietnamitas. Além disso, de forma imediata, a China usou suas redes sociais e canais oficiais para oferecer proteção contra novos ataques. Aproveita ainda a oportunidade, para divulgar que o Vietnã é incapaz de controlar suas águas e reafirma as suas reivindicações de soberania sobre todo o Mar do Sul da China. Com isso, uma sensação de caos e instabilidade se desenvolve nos canais de navegação mais congestionadas do mundo (STAVRIDIS, 2016, p. 30-31).

Como sugere o exemplo, a sincronicidade dos métodos empregados constituem em combinações complexas que, apesar de não haver nada de glamoroso, representa os passos para analisar as ameaças híbridas, cuja presença no cenário mundial ganha impulso. Em que pese o termo ameaça híbrida ser relativamente novo, pode-se afirmar que as técnicas já foram, e estão sendo constantemente empregadas.

Vale acrescentar que as ameaças híbridas ganharam reconhecimento, pela primeira vez, quando o Hezbollah teve algum sucesso militar tangível contra as Forças de Defesa de Israel no Líbano em 2006, durante a Segunda Guerra do Líbano (FARQUHAR, 2009 p. 5).

De acordo com Fernandes (2016), embora equipado com armas típicas das forças armadas convencionais, o Hezbollah operava de forma descentralizada, empregando uma combinação de capacidades convencionais e táticas de guerrilha, guerra psicológica, terrorismo e atividade criminosa. Para amenizar a superioridade israelense, o Hezbollah alterou a natureza do conflito, negando a capacidade de Israel de tirar proveito de suas vantagens tecnológicas (FERNANDES, 2016 *apud* SANTOS, 2017, p. 22).

Sendo assim, Hoffman (2007), pesquisador do Centro de Ameaças e Oportunidades Emergentes do Congresso Americano, popularizou o termo "ameaças híbridas" com a publicação de seu estudo intitulado como "*Conflict in the 21st Century: The Rise of Hybrid Wars",* no qual a definição original apresentada para o espectro híbrido versa sobre fatores físicos, como sistemas de armas que estavam nas mãos de atores não estatais.

Não obstante, na MB ainda não há manuais tratando do assunto. Todavia, já é possível observar que a Força Naval está preocupada, como se pode notar na publicação do Comando de Operações Navais divulgada em 2020, em cujo documento consta uma contextualização e a definição de ameaça híbrida para a MB, a qual será adotada para fins desse estudo:

> 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, 2020b, p. 2).

De qualquer forma, o conceito para ameaça híbrida é complexo e os doutrinadores atribuem significados diferentes ao termo (MURRAY; MANSOOR, 2020). Entretanto, a definição da MB está alinhada com a maioria das definições internacionais, entre elas a adotada pelo *Hybrid COE*[9] o qual afirma que "ameaça híbrida" se refere à ação conduzida por atores estatais ou não estatais, cujo objetivo é estabelecido para alcançar um

9 Centro de Excelência que desenvolve estudos e capacidades para seus 31 Estados participantes, com o fim de combater ameaças híbridas e cooperar estreitamente com a UE e a OTAN.

propósito político comum, minar ou prejudicar um alvo, combinando meios militares e não militares abertos e encobertos.

Com o intuito de complementar a definição, Coning (2021) apresenta um dos modelos conceituais desenvolvido pelo *Hybrid COE.* Segundo o autor, o modelo do *Hybrid COE* expõe que para as ameaças híbridas serem caracterizadas devem existir pelo menos quatro pilares principais: os atores (e seus objetivos estratégicos), as vulnerabilidades críticas, as ferramentas e as fases.

Cabe ainda ressaltar que é comumente fácil confundir as definições de "Guerra[10] Híbrida" com "Ameaças Híbridas"(BRASIL, 2015, p. 133). Rodrigues (2020) esclarece que os termos possuem formas muito semelhantes, por conta da complementaridade dos atores envolvidos, como forças regulares, irregulares e grupos criminosos ou terroristas que empregam, simultaneamente ou não, meios convencionais e não convencionais. Todavia, as ameaças híbridas referem-se ao tipo de atores, que é diferente do conceito de Guerra Híbrida, a qual é o modelo de conflito, ou seja, os atores podem empregar recursos de Guerra Híbrida contra oponentes que podem ser tecnologicamente superiores (MINNITI, 2018).

A história tem muito a dizer sobre a natureza das ameaças híbridas, pois foram largamente aplicadas pelos Estados conflituosos. Durante a Segunda Guerra Mundial, por exemplo, o Exército Alemão sofreu inúmeras interrupções em suas linhas de comunicação em consequência das atividades de milhares de *partisans* (FIG. 3) e forças irregulares soviéticas, de forma que acarretou prejuízos significativos aos alemães. Nem mesmo as unidades policiais da SS alemã, as *Einsatzgruppen*, bem como as forças de segurança conseguiram extinguir os guerrilheiros (MURRAY; MANSOOR, 2020, p. 16).

Ainda hoje forças *partisans* são empregadas. A título de exemplo, em entrevista, Pinto Silva (2022) afirma que a Rússia emprega *partisans* em ações secretas na tentativa de alcançar seus objetivos políticos. Quando esse modus operandi são ineficientes ou insuficientes, a Rússia, normalmente, empregará tropas convencionais com o fim de manter o "status quo".

---

10 Conflito no seu grau máximo de violência. Em função da magnitude do conflito, pode implicar a mobilização de todo o Poder Nacional, com predominância da expressão militar, para impor a vontade de um ator ao outro.

FIGURA 3 – Partisans.
Fonte: PARTISANS, 2022.

Há de considerar ainda que na Segunda Guerra, o primeiro-ministro Winston Churchill também tinha ciência do poder que poderia obter com o emprego do espectro híbrido. Após julho de 1940, agentes britânicos auxiliaram e fizeram parte dos movimentos de resistência locais em toda a Europa Ocidental e nos Bálcãs. Armas e munições foram entregues à população e às forças irregulares que realizavam operações de sabotagens nas instalações nazistas em toda a Europa Ocidental e nos Bálcãs (MURRAY; MANSOOR, 2020, p. 16).

Aplicações similares são possíveis de serem observadas nos conflitos mais atuais. Um dos fatos que se destaca é o que ocorreu durante a anexação da Crimeia pela Rússia em 2014. Segundo Caliskan (2018), os estudiosos geralmente mencionam esse conflito como um exemplo principal para modelar o conceito de ameaça híbrida.

Em suma, esse exemplo típico de ameaças híbridas russas foi a ação dos “homenzinhos verdes”, como eram chamados pelos civis e a mídia. Apesar daqueles homens esconderem os rostos sob máscaras e não usar insígnias em seus uniformes camuflados, era de conhecimento geral que se tratavam de militares das forças regulares russas, fato que o presidente russo Vladimir Putin admitiu mais tarde, alegando que era uma força de proteção aos civis ucranianos (DELAHUNTY, 2014).

A Rússia não poupa esforços para empregar as ameaças híbridas. Esse fato reflete os ensinamentos do General Gerasimov, então Chefe do Estado-Maior Geral das Forças Armadas da Federação Russa. Neville (2015) afirma que o discurso do General russo ficou

conhecido como a “Doutrina Gerasimov” e é vista por muitos acadêmicos e militares ocidentais como um novo rumo das políticas militares russas.

Assim, Gerasimov (2013) expõe que as regras da guerra mudaram de tal forma que houve o aumento de métodos não militares na busca de objetivos políticos e estratégicos. Dessa forma, do ponto de vista do autor, há maior ênfase no implemento de métodos com a finalidade de influenciar as medidas políticas, econômicas e informativas dos adversários e, principalmente, um forte implemento para levar populações-alvo a protestos.

Diante dessa realidade, Caliskan (2018) corrobora ao afirmar que a Rússia continuará a usar táticas híbridas para proteger sua esfera de influência. Isso faz crer que enquanto os países ocidentais, encabeçados pelos EUA, estão estudando e desenvolvendo doutrinas, alguns países do oriente, direcionados pela Rússia, estão as colocando em prática.

Nesse contexto, quando se fala em guerras híbridas, a Rússia está sempre em pauta. Entretanto, nos dias de hoje, até mesmo potências menores empregam os métodos híbridos. Bristol (2021) narra como exemplo, as operações do Marrocos no Saara Ocidental. Segundo o autor, depois de cessar fogo com a frente POLISÁRIO em 1991, o rei marroquino elaborou uma política de incentivo à imigração marroquina para os territórios, com o fim de diluir a população nativa, inviabilizando um referendo de independência organizado pela ONU.

Devido ao sucesso do plano, o referendo foi adiado indefinidamente. Enquanto isso, Marrocos governava o território sob ocupação militar. Trinta anos depois, as atividades híbridas marroquinas parecem ter tido sucesso com o reconhecimento americano da anexação (BRISTOL, 2021).

Com o intuito de buscar o entendimento da complexidade que gira em torno da abrangência e das limitações que constituem as ameaças híbridas é lícito trazer mais alguns complementos conceituais. Desse modo, Pozubenkov (2016) explica que o espectro híbrido se estende a várias esferas da vida pública: política, econômica, social e cultural. Ele possui como característica essencial, o desrespeito a todas as normas de moralidade e utiliza as mais sujas tecnologias sociais, de modo a atrair a população para o antagonismo.

Com efeito, Hoffman (2014) em seu artigo intitulado “*On Not-So-New Warfare: Political Warfare vs. Hybrid Threats”,* corrobora com a tentativa de consolidação conceitual de ameaça híbrida. Sendo assim, o autor afirma que as ameaças híbridas se concentram em

combinações de táticas associadas à violência e à guerra sendo insipiente em incluir outras ações não violentas. Dessa forma, ele se refere pouco às ferramentas como atos econômicos e financeiros, como atos políticos subversivos, como o estabelecimento ou atividades de sindicatos e organizações não governamentais como uma fachada, ou como atividades de informação usando sites e artigos falsos. Portanto, do ponto de vista do autor esse fato é uma das limitações da definição de ameaças híbridas (HOFFMAN, 2014).

Entretanto, no contexto atual já existe uma atualização em relação a esse ponto de vista. Desse modo, em última análise, apesar dos termos Guerra/Ameaças Híbridas obscurecerem mais do que explicarem a ausência de conceitos consolidados, não evita sua aplicação, particularmente nos momentos atuais.

Por conseguinte, para contrapor ao ponto de vista de Hoffman (2014) quanto às limitações da definição de ameaças híbridas, é relevante notar o estudo de caso da aplicação do espectro híbrido apresentado por Javier Jordan na *Multinational Capability Development Campaign* (MCDC) em 2019.

Em síntese, Jordan (2019) narra que em 11 de julho de 2002, em uma pequena ilha de soberania disputada entre o Marrocos e a Espanha, militares dos Marrocos desembarcaram e fixaram duas bandeiras na pequena ilha, conhecida na Espanha como Perejil e em Marrocos como Leila e Tura. A ilha se localiza mais próxima de Marrocos do que da Espanha, no Estreito de Gibraltar. Consequentemente, poucas horas depois do desembarque Marroquino, a Espanha exigiu a retirada dos invasores. Todavia, os militares marroquinos se recusaram.

A importância física e estratégica da ilha é insignificante, pois apesar de não haver soberania definida, houve um acordo para mantê-la desabitada. Desse modo, a relevância nesse caso é o fato consumado do lado marroquino, que só cessou após a ação de militares espanhóis. Atualmente a ilha se mantém desocupada.

Como se pode notar, o ataque se concentrou no *status quo* da delimitação e legitimidade das fronteiras territoriais no norte da África, entre Espanha e Marrocos, particularmente no Estreito de Gibraltar, o que se constitui a principal vulnerabilidade crítica entre os dois Estados (JORDAN, 2019).

De forma geral, os instrumentos de poder[11] do espectro híbrido foram aplicados conforme modelo de Escalação Híbrida desenvolvida pelo *The Multinational Copability Development Campaign (MCDC)*, que pode ser observado na FIG. 4:

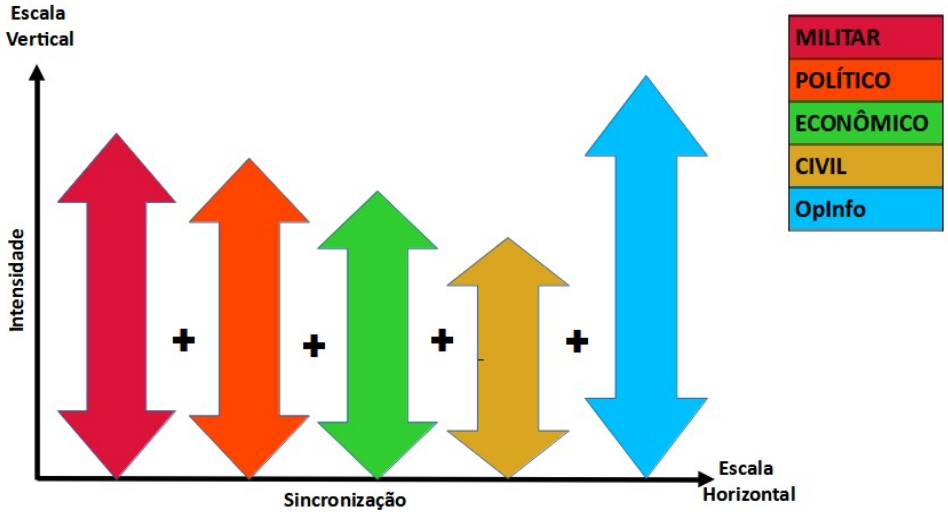

FIGURA 4 – Escalação Híbrida
Fonte: CULLEN e REICHBORN-KJENNERUD, 2017, p. 9.

Conforme afirma Jordan (2019), a escalada ocorreu principalmente no eixo horizontal com a sincronização dos instrumentos de poder. Já no eixo vertical, o que se destaca é o fato consumado por meio da realização das ações de OpInfo. Portanto, observa-se que as ameaças híbridas deixaram de dar ênfase nas combinações de táticas associadas à violência e à guerra e passaram a investir fortemente nas CRI das OpInfo.

Diante dessas considerações, há de se convir que o alvo das ameaças híbridas, primeiramente, é influenciar e ganhar os "corações e mentes" das populações, tanto para reforçar o compromisso do público amigo, quanto para destruir o moral dos adversários. Nesse contexto, entendê-la seria uma maneira apropriada para começar.

Por fim, as ameaças híbridas requerem muito o emprego das CRI por algumas razões. Em primeiro lugar, a realização de OpInfo ocorrem antes, durante e depois da introdução de forças armadas em conflitos. Em segundo lugar, há a necessidade de constantes interpretações e reinterpretações de informações, já que a propaganda e a desinformação tem presença acentuada. Em terceiro, as direções de desenvolvimento das

11 A MCDC define Instrumentos de poder como elementos do ambiente do poder militar, político, econômico, civil e OpInfo.

ameaças híbridas envolvem muitas questões, entre as quais pode-se destacar: inteligência, OpPsc, ComSoc, ações cibernéticas (BARTOSH, 2022).

3.2 Aplicação das CRI Como Instrumentos de poder das Ameaças Híbridas

As CRI das OpInfo e as ameaças híbridas estão intimamente ligadas. Em resumo, ambas se concentram, seja em ação inicial ou total, em influenciar opiniões, emoções e motivos de um público-alvo. Entretanto, embora esses termos possam parecer serem empregados de forma intercambiável, é um equívoco esse entendimento, pois as ameaças híbridas, como já demonstrado, têm um significado muito mais amplo, uma vez que são projetadas para explorar vulnerabilidades nacionais no campo político, militar, econômico, social, informacional e de infraestruturas, diferente das OpInfo que se concentram somente na Dimensão Informacional.

Partindo dessa concepção, em um mundo altamente interconectado, significa que os potenciais pontos de partida para emprego das ameaças híbridas estão inseridos nas capacidades relacionadas à informação. Citam-se os casos clássicos de revoluções coloridas, por exemplo, nas quais, por meio de coordenação e emprego das CRI, é facilitada uma ampliação das divisões políticas ou outras já presentes nas sociedades visadas (WEISSMANN *et al*., 2021).

Korybko (2018) postula que o início da revolução colorida é a disseminação de informações manipuladas entre a população estabelecida como alvo. Essas informações atingem segmentos específicos da população ou da sociedade como um todo. Assim, os protestos se iniciam com a intenção de minar a estrutura do Estado e tomar o poder. A população manipulada passa a ser usada como arma. Weissmann *et al.* (2021) exemplifica:

> A questão catalã ilustra como as vulnerabilidades existentes na coesão social podem ser exploradas através de atividades de informação/desinformação; constitui uma questão política interna que pode ser utilizada por atores híbridos para diferentes objetivos. Esses tipos de questões políticas, altamente polarizadas e que dividem as sociedades, podem ser exploradas por atores externos em campanhas de influência da informação, direcionadas ao público estrangeiro ou doméstico. Essas questões podem ser utilizadas para legitimar decisões e ações políticas na arena doméstica, ou por transmitir representações distorcidas de sistemas e sociedades políticas estrangeiras por diferentes razões, incluindo o enfraquecimento da coesão interna dessas sociedades visadas ou redes políticas transnacionais (WEISSMANN *et al*., 2021, p. 240, tradução nossa).

É interessante ter presente a questão catalã apontada por Weissmann *et al.* (2021). A Espanha é um dos principais locais do mundo a possuir movimentos separatistas. É um território multinacional, ou seja, formada por diversos grupos étnicos regionais com identidade nacional própria que buscam independência. Esse é o caso dos catalães (FIG. 5), que possuem até idioma específico, bem como um parlamento próprio.

Em resumo, no ano de 2017, nas semanas que antecederam um referendo sobre a independência da Catalunha, ocorreram tensões naquela região, uma vez que tal referendo foi considerado ilegal pelo governo da Espanha. Dessa forma, houve forte repressão da polícia espanhola, que fechou locais de votação e agrediu os eleitores catalães. Como era de se esperar, vídeos foram demasiadamente publicados na internet com as agressões e excessos, fato que atiçou ainda mais a população. Apesar do "sim" vencer nas urnas, o governo Espanhol não reconheceu o referendo e pediu a prisão de vários líderes separatistas (CAETANO, 2017).

FIGURA 5 - Manifestação pela independência da Catalunha, em Barcelona.
Fonte: CAETANO, 2017.

Como se pode ver, a aplicação das CRI como instrumentos de poder das ameaças híbridas é especialmente importante, uma vez que propicia velocidade, amplitude, profundidade e precisão para atingir o objetivo antes mesmo que a vítima perceba que está sob ataque híbrido. Assim, contribui para com que as ameaças híbridas permaneçam com

sua abordagem silenciosa, indireta e ambígua de modo a dificultar a responsabilização e identificação dos atores.

3.3 As ameaças híbridas hoje

Embora as ameaças híbridas possam aparentar ser uma novidade, são tão antigas quanto a própria guerra convencional[12]. Desse modo, o que está em constante mudança é o nível de esforço colocado por grandes e pequenas nações, bem como a tendência de aplicação visando as vantagens táticas e estratégicas conferidas por este método, pois são de baixo risco e custo, e oferece a oportunidade de lançar suspeitas, obscurecendo a responsabilidade daquele que as empregam.

Com efeito, o Secretário-Geral da Organização do Tratado do Atlântico Norte (OTAN), Stoltenberg (2015), não nega que os Estados-membros da OTAN empregam o espectro híbrido para, segundo ele, estabilizar países. Tal fala pode lançar luz a progressão lógica em que as ameaças híbridas são implantadas.

Dessa forma, como já demonstrado, geralmente o emprego integrado das Capacidades Relacionadas à Informação (CRI) oferecem um vasto potencial para ser aplicado como instrumento de poder para a realização de ações do espectro híbrido, tanto de forma ofensiva quanto defensiva, particularmente em tempos de paz.

As ameaças híbridas desafiam as interfaces entre guerra/paz e amigo/inimigo, e essa tendência, de acordo com Murray e Mansoor (2020), exige que os Estados-alvo possuam a capacidade de impedir que seus possíveis adversários controlem suas vulnerabilidades e principalmente sua população. Stavridis (2016) reforça que a ideia fundamental da guerra híbrida é encontrar o espaço aquém da ação militar, com ênfase no campo de batalha das ideias e ideologias e a luta pelos “corações e mentes” das pessoas.

Ainda de acordo com Stavridis (2016), as guerras/ameaças híbridas possuem princípios amplamente aceitos, tais como: o elevado uso das CRI, particularmente OpPsc com a disseminação de rumores falsos e inflamatórios para desestabilizar uma região, fortes atividades nas redes sociais para gerar propaganda, desinformação e emprego de técnicas

---

12 “Conflito armado realizado dentro dos padrões clássicos e com o emprego de armas convencionais, podendo ser total ou limitada, quer seja pela extensão da área conflagrada, quer seja pela amplitude dos efeitos a obter. É o principal propósito da preparação e do adestramento das Forças Armadas da maioria dos países” (BRASIL, 2015, p. 134).

insurgentes, incluindo carros-bomba, tortura e sequestro, com o fim de assustar a população.

Sob tal ótica, hoje as ameaças híbridas são fortalecidas pela globalização e a interconectividade internacional. Por essa razão, por mais positivas e desejáveis que possam ser, têm o potencial de abrir pontos de partida para exploração das vulnerabilidades do Estado-alvo, principalmente com a aplicação das CRI. Portanto, é oportuno apontar que no mundo contemporâneo, as sociedades democráticas, nas quais a passividade da população é uma questão existente, são particularmente vulneráveis a esse tipo de atividade, principalmente aquelas que carecem de vigilância estratégica.

Em última análise, tratando-se do espectro híbrido, a tarefa de identificar os ataques antes que eles ocorram é um fator complicador, pois há uma diversidade significativa de instrumentos de poder não militar que precisam ser compreendidos e monitorados diuturnamente para fornecer alerta adequado (CULLEN, 2018). Os indícios de atividades que podem se transformar em ameaças híbridas vão além do domínio tradicional militar, e se estende a muitos domínios diferentes, sendo que o agregamento: da informação com mais o comportamento, no campo de batalha das mentes, são exemplos óbvios.

Por fim, sustenta-se que a agressão por meio do emprego das CRI pode ser essencial a atores hostis, para cumprir a finalidade de lançamento de ataques híbridos, já que o lado atacante não anuncia sua participação. Embora isso possa levar a campanhas militares, a realização de OpInfo representa as condições para a conquista de grupos-alvo, oferecendo a oportunidade única de possuir as mentes de uma população desatenta.

3.4 As possibilidades de emprego das OpInfo frente as ameaças híbridas

As ameaças híbridas não se tratam de algo passageiro. Na verdade, representa um conjunto diversificado de desafios que se estende muito além do domínio militar e, como já mencionado, por meio da exploração das vulnerabilidades do alvo, cria ambiguidade capaz de paralisar o processo de tomada de decisão do oponente e ao mesmo tempo limitar suas opções de resposta. Concentra-se, preferencialmente, na desestabilização de um alvo ou nação, aprofundando sua narrativa por meio da realização de OpInfo (KORYBKO, 2018).

Sob essas circunstâncias, um esforço abrangente de OpInfo também pode, significantemente, reconduzir ou neutralizar o *modus operandi* híbrido de forças hostis. O

emprego das CRI possibilita as condições necessárias para motivar o oponente a desistir de seu intento e ao mesmo tempo pode evitar o convencimento da opinião pública vitimada. Um exemplo dessa relação pode ser tipificado na experiência imposta à MB no ocorrido em Aramar. O problema da oposição e revolta da população contra o Programa Nuclear da Marinha (PNM) foi superado por meio da aplicação de ComSoc (CEZAR, 2009).

Cada vez mais, o combate militar guiado por princípios tradicionais de guerra, ficará para um segundo plano (BURBRIDGE, 2013), pois as ações hostis serão mais vagas, interdisciplinares, cujo o objetivo principal é causar impactos cognitivos a um conflito, o que, segundo Mazarr (2007), tem mais a ver com psicologia e identidade do que com forças militares. Portanto, o combate às ameaças híbridas requer o emprego coordenado das CRI (HOFFMAN, 2007, p. 55).

Levando-se em conta o emprego das CRI dos EUA contra ameaças híbridas, a afirmação de Burbridge (2013) corrobora essa ideia. Segundo o autor, no cenário de hoje "a missão é a mensagem", pois da mesma forma que as CRI são essenciais para a aplicação das ameaças híbridas, servem também para combatê-las, bem como para controlar e isolar o adversário diplomaticamente e manter o apoio internacional a uma campanha militar. O autor ainda aponta que as CRI podem ser aplicadas contra as ameaças híbridas como esforço principal[13] (BRASIL, 2015, p. 104) ou como apoio[14] (BRASIL, 2015, p. 28).

Segundo ainda Burbridge (2013), como esforço principal, as OpPsc e a ComSoc podem atuar como instrumento de poder para neutralizar a narrativa de uma ameaça híbrida que tenta influenciar as emoções, raciocínio ou o comportamento de governos, grupos, instituições ou indivíduos. Além disso, como apoio, podem ser aplicados outros instrumentos de poder, como as Ações Cibernéticas para desestabilizar os ativos de informação do ator híbrido.

É importante ter em mente também que, nos dias atuais, um dos principais impulsionadores das ameaças híbridas, como já mencionado neste trabalho, são as facilidades proporcionadas pela comunicação global. Assim, as CRI devem ser planejadas e

13 Esta ação é caracterizada pelo ataque principal e os ataques secundários mais importantes, realizada na frente de ataque selecionado.

14 É a relação que o comando estabelece, entre subordinados. Nessa relação cabe ao comandado incumbir os elementos subordinados a serem os responsáveis por apoiar, proteger, reabastecer ou dar apoio logístico à outra força.

executadas sob coordenação das OpInfo para garantir que, na medida do possível, seja minimizado o fratricídio de informação. Nesse sentido, Burbridge (2013) enfatiza:

> É necessário empregar todas as formas concebíveis de comunicação para atingir o público na área de conflito e permear o ambiente de informação. Isso inclui rádio, televisão, mídia impressa, outdoors, internet (páginas da web, blogs e e-mails), mensagens telefônicas (chamada de robô usando equipamento idêntico ao usado em campanhas políticas nos EUA e no exterior), bem como formatos de DVD e CD, e onde possível, a comunicação face a face com membros influentes da população local. O desenvolvimento desses condutores requer uma extensa preparação OpInfo para determinar quais são mais eficazes para vários públicos. Essa preparação deve incluir o estabelecimento dos contratos comerciais para obter os talentos necessários para o desenvolvimento e divulgação do produto (BURBRIDGE, 2013, p.27).

Conforme se pode constatar, a aplicação das CRI oferece uma abordagem proativa e preventiva para combater as ameaças híbridas. A Doutrina americana *Joint Publication for Information Operations* acrescenta também a *Operations Security*[15] (U.S. NAVY & U.S. MARINE CORPS, 2017), como uma capacidade adequada para complementar tal abordagem.

De qualquer modo, já está previsto na Política Nacional de Defesa (BRASIL, 2020c), bem como na Política Naval (BRASIL, 2019b), a necessidade de assegurar, além dos interesses nacionais, a integridade psicológica dos brasileiros e inibir ameaças por eventuais instabilidades políticas e sociais, em tempos de paz ou de crise. Assim, é importante ressaltar que a MB explora satisfatoriamente as possibilidades na realização de OpInfo, bem como trata de forma positiva os estudos sobre ameaças híbridas, apesar de, até o momento, esse conhecimento ser restrito e possuir lacunas de entendimento por parte de seu efetivo.

4 CONCLUSÃO

As oportunidades de realização de OpInfo aumentaram na condução dos conflitos contemporâneos e são especialmente atraentes para potencializar a aplicação das

15 "OPSEC é uma capacidade que identifica e controla informações críticas e indicadores de ações de forças amigas em operações militares e incorpora contramedidas para reduzir o risco de um adversário explorar vulnerabilidades. Quando efetivamente empregado, nega ou mitiga a capacidade do adversário de comprometer ou interromper uma missão, operação ou atividade. Sem um esforço coordenado para manter o sigilo essencial de planos e operações, nossos inimigos podem prever, frustrar ou derrotar grandes operações militares. OPSEC bem executado ajuda a cegar nossos inimigos, forçando-os a tomar decisões com informações insuficientes" (U.S. NAVY & U.S. MARINE CORPS, 2017, p. 2-1, tradução nossa).

ameaças híbridas. Conforme se pode constatar no decorrer deste estudo, a OTAN já prospera com seu sistema de estudo, com o fim de garantir que seus Estados-membros tenham os recursos cognitivos para compreender e desenvolver capacidades de reconhecer, deter e responder a ameaças híbridas.

De maneira similar, os Fuzileiros Navais americanos já adotam algumas medidas para acompanhar as abordagens criativas inseridas nos conflitos, de tal forma que asseguram ao seu efetivo a possibilidade de desenvolver as capacidades cognitivas necessárias para enfrentar o espectro híbrido, independente se as táticas utilizadas nesses conflitos são novidades ou não (HOFFMAN, 2007, p. 57)

Compreender a natureza das ameaças Híbridas e considerar o poder de defesa proporcionado pelas Capacidades Relacionadas à Informação pode ser a maneira mais apropriada para o desenvolvimento de uma abordagem importante para prevenção e proatividade, com objetivo de vencer as investidas mal-intencionadas que podem estar ocorrendo sem alardes.

De fato, é de vital importância que o tema faça parte da grade curricular de todas as Escolas de Formação da MB e a exemplo da *Hybrid CoE,* sugere-se o desenvolvimento de estudos e ferramentas necessárias para reconhecer, deter e responder tais ameaças. Além disso, esse processo pode ser facilitado com a criação de uma Divisão de Segurança da Informação, baseado na contrainteligência, no Comando Naval de Operações Especiais.

Finalmente, este trabalho pretende ser um ponto de partida para que sejam vislumbradas as possibilidades de emprego das OpInfo frente as ameaças híbridas, pois o tema é complexo, amplo e além de estar em constante mudança, afeta profundamente toda a sociedade. Assim, aplicar o OpInfo é um desafio que deve estar sempre presente na agenda da MB, uma vez que a dissuasão sozinha não pode impedir a atividade inimiga na forma de ameaças híbridas.

REFERÊNCIAS

BARTOSH, A. A. **Questões da Teoria da Guerra Híbrida**, Moscou: Hot Line-Telecom, 2022.

BRASIL. Ministério da Defesa. **MD35-G-01**: Glossário das Forças Armadas. 5. ed. Brasília, DF, 2015.

BRASIL, Exército Brasileiro. **Manual de Campanha EB70-MC-10.213**: Operações de Informação, Brasília, DF, 2019a.

BRASIL, Marinha do Brasil. **Política Naval de Defesa**, Brasília, BR, 2019b.

BRASIL. Marinha do Brasil. Corpo de Fuzileiros Navais. Comando-Geral. **CGCFN-60**: Manual De Comando e Controle de Fuzileiros Navais, Rio de Janeiro, RJ, 2020a.

BRASIL. Marinha do Brasil. **Manual de Ações de Guerra Eletrônica (ComOpNavInst-220)**. Comando de Operações Naval. Rio de Janeiro, RJ, 2020b.

BRASIL. Presidência da República Federativa do Brasil. **Política Nacional de Defesa**. Brasília, 2020c.

BRASIL. Marinha. Estado-Maior da Armada. **EMA-860:** Manual de Comunicação Social da Marinha. Brasília, 2021.

BRISTOL, J. Hybrid War and What to Do About It. **The Strategy Bridge**, 21 abr. 2021. Disponível em: https://thestrategybridge.org/the-bridge/2021/4/21/hybrid-war-and-what-to-do-about-it. Acesso em: 06 jul. 2022.

BURBRIDGE, D. A. United States Army. **Employing U.S. Information Operations Against Hybrid Warfare Threats**. Philadelphia: U.S. Army War College, 2013. Disponível em: https://apps.dtic.mil/sti/pdfs/ADA589058.pdf. Acesso em: 20.jun. 2022.

CAETANO, G. O que está em jogo no referendo sobre a independência da Catalunha: Espanha pode perder região em que estão 20% de seu PIB e 16% da população. **Revista Época**, Rio de Janeiro, 02 out. 2017. Disponível em: https://epoca.oglobo.globo.com/mundo/noticia/2017/09/o-que-esta-em-jogo-no-referendo-sobre-independencia-da-catalunha.html Acesso em: 15 jun. 2022.

CEZAR, A. **O Programa Nuclear Brasileiro:** um Caminho com muitas saídas. São Paulo: Ottoni Editora, 2009.

CONING, C. Hybrid CoE Working Paper 9: Strengthening the resilience and adaptive capacity of societies at risk from hybrid threats. **Hybrid CoE**, 09 jun. 2021. Disponível em: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-9-strengthening-the-resilience-and-adaptive-capacity-of-societies-at-risk-from-hybrid-threats/. Acesso em: 05 jun. 2022.

COWAN, D.; COOK, C. Psychological Operations versus Military Information Support Operations and an Analysis of Organizational Change. **Army University Press**, 06 mar. 2018. Disponível em: https://www.armyupress.army.mil/Journals/Military-Review/Online-Exclusive/2018-OLE/Mar/PSYOP/#:~:text=During%20the%20Vietnam%20War%2C%20PSYOP,function%20previously%20known%20as%20PSYOP. Acesso em: 02 jul. 2022.

CULLEN, P. Hybrid threats as a new 'wicked problem' for early warning. **Hybrid CoE,** 4 jun. 2018.

CULLEN, P. J.; REICHBORN-KJENNERUD, E. MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare. Reino Unido, p. 9: **Multinational Capability Development Campaign – MCDC,** jan. 2017. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/647776/dar_mcdc_hybrid_warfare.pdf. Acesso em: 22 jun. 2022.

DELAHUNTY, R. J. The Crimean Crisis. **University of St. Thomas School of Law & PUB. POL'Y 125**, v, 9, n. 1, p. 125-187, 2014. Disponível em: https://ir.stthomas.edu/ustjlpp/vol9/iss1/5. Acesso em: 01 ago. 2022.

EQUIPE ONLINE. Protesto contra Aramar reuniu 10 mil pessoas em Sorocaba. **Jornal Cruzeiro do Sul**, 01 nov. 2015. Disponível em: https://www2.jornalcruzeiro.com.br/materia/651724/protesto-contra-aramar-reuniu-10-mil-pessoas-em-sorocaba. Acesso em: 22 jun. 2022.

FARQUHAR, S. C. **Back to Basics**: A study of the second Lebanon war and Operation CAST LEAD. Kansas, Estados Unidos da América: Combat Studies Institute Press - US Army Combined Arms Center, 2009.

FERNANDES, H. As Novas Guerras: O Desafio da Guerra Híbrida. **Revista de Ciências Militares**, v, 4, n. 2, p. 13-40, 2016.

GAYLE, D. Jordanian pilot who was burned to death in sickening ISIS video 'was so heavily sedated he had no idea what was about to happen to him'. **MailOnline**, Reino Unido, 10 fev. 2015. Disponível em: https://www.dailymail.co.uk/news/article-2946587/Jordanian-pilot-burned-death-sickening-ISIS-video-heavily-sedated-unaware-happen-him.html. Acesso em: 25 mai. 2022.

GERASIMOV, V. O valor da ciência na previsão: Novos desafios exigem repensar as formas e métodos de guerra. **VPK**, Rússia, 26 fev. 2013. Disponível em: https://vpk-news.ru/articles/14632. Acesso em: 22 jul. 2022.

HOFFMAN, F. G. Conflict in the 21st Century: The Rise of Hybrid Wars. **Potomac Institute for Policy Studies**, Arlington, Virginia, dez. 2007. Disponível em: http://https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf. Acesso em: 22 jun. 2022.

HOFFMAN, F. On Not-So-New Warfare: Political Warfare vs. Hybrid Threats. **War On The Rocks**, 28 jul. 2014. Disponível em: https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/. Acesso em: 23 jun. 2022.

KEFELI, I. F.; KOMLEVA N. A. Sobre o papel da segurança da informação e da segurança ideológica na guerra híbrida de contra estratégia na Eurásia. **Centro de Perícia Geopolítica do North-West Institute of Management da RANEPA,** São Petersburgo, Federação Russa, 2020.

KORYBKO, A. **Guerras híbridas**: das revoluções coloridas aos golpes. 1. ed. São Paulo: Expressão Popular, 2018.

KRYSKO, V. G. **Segredos da Guerra Psicológica (metas, objetivos, métodos, formas, experiência)**. Moscou: Minsk, 1999.

LAKATOS, E. M.; MARCONI, M. A. **Fundamentos de Metodologia Científica**. 5. ed. São Paulo: Atlas, 2003.

MINNITI, F. Hybrid Warfare and Hybrid Threats. **European eye on radilization**, 16 abr. 2018. Dsiponível em: https://eeradicalization.com/hybrid-warfare-and-hybrid-threats/. Acesso em: 01 abr. 2022.

MURRAY, W.; MANSOOR, P. R. **Guerra Híbrida**: a verdadeira face do combate no século XXI. Rio de Janeiro: BIBLIEx, 2020.

PARTISANS / Guerrilheiros Judeus. **Enciclopédia do Holocausto**, 2022. Disponível em: https://encyclopedia.ushmm.org/content/pt-br/article/jewish-partisans#:~:text=Partisans%20%2F%20Guerrilheiros%20Judeus%20Alguns%20judeus,se%20em%20%C3%A1reas%20densamente%20florestadas. Acesso em: 22 jun. 2022.

PINTO SILVA, C. A. A Guerra Híbrida e a Crise na Ucrânia. **Defesanet**, Brasília, DF, 02 fev. 2022. Disponível em: https://www.defesanet.com.br/us_ru_otan/noticia/43497/Gen-Ex-Pinto-Silva---A-Guerra-Hibrida-e-a-Crise-na-Ucrania/. Acesso em: 07 set. 2022.

POCHEPTSOV, Georgy. **Guerra de informação – psicológica**. Sinteg, 2000.

POZUBENKOV, P. S. Guerras híbridas no espaço moderno da informação. **Revista eletrônica científica e metodológica "Conceito",** 2016. Disponível em: http://e-koncept.ru/2016/86243.htm. Acesso em: 24 jul. 2022.

SANTOS, J. P. D. **O Emprego da Artilharia em Operações contra Ameaças Híbridas.** 2017. Relatório Científico Final (Trabalho de Investigação Aplicada) – Lisboa, Academia Militar, 2017.

STAVRIDIS, J. Maritime hybrid warfare is coming. **Proceedings,** United States Naval Institute, v, 142, n. 12, p. 30-33, 2016.

THEOHARY, C. A. Information Warfare: Issues for Congress. **Congressional Research Service**, Washington, DC, 2018. Disponível em: https://sgp.fas.org/crs/natsec/R45142.pdf. Acesso em: 23 jun. 2022.

U.S. NAVY; U.S. MARINE CORPS. Operations Security (OPSEC). **USA Department Of The Navy. Office Of The Chief Of Naval Operations. Headquarters, U.S. Marine Corps**, set. 2017. Tradução Ozéias Braz de Mattos. Disponível em:

https://media.defense.gov/2020/Oct/28/2002524943/-1/-1/0/NTTP-3-13.3M-MCTP-3-32B-OPSEC-2017.PDF. Acesso em: 23 jun. 2022.

USA. Central Intelligence Agency (CIA). **Background to "Assessing Russian Activities and Intentions in Recent US Elections":** The Analytic Process and Cyber Incident Attribution, jan. 2017. Disponível em: https://www.dni.gov/files/documents/ICA_2017_01.pdf. Acesso em: 02 abr. 2022.

USA. Department of Defense. **Joint Concept for Operating in the Information Environment (JCOIE)**, Tradução Ozéias Braz de Mattos. Washington, DC, 2018.

WEISSMANN, M.; NIKLAS N.; BJÖRN P.; PER T. **Hybrid Warfare:** Security and Asymmetric Conflict in International Relations, Tradução Ozéias Braz de Mattos. Massachusetts, Estados Unidos da América: Bloomsbury Publishing, 2021.

WOOD, G. What ISIS Really Wants. **The Atlantic,** mar. 2015. Disponível em: https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/. Acesso em: 02 abr. 2022.