ISSN: 2525-457X
ANÁLISE ESTRATÉGICA
VOL 20 (2) MAR/ MAIO 2021

GUERRA HÍBRIDA: ANEXAÇÃO DA CRIMEIA E CRISE DA UCRÂNIA SOB A PERSPECTIVA POLÍTICO-ESTRATÉGICA DA OTAN

HYBRID WAR: CRIMEA ANNEXATION AND UKRAINE CRISIS FROM NATO'S POLITICAL-STRATEGIC PERSPECTIVE

*Fernando da Silva Rodrigues

RESUMO

O objetivo do ensaio foi analisar a Anexação da Crimeia e a Crise da Ucrânia sob a perspectiva político-estratégica da Organização do Tratado Atlântico Norte (OTAN). As seções do ensaio foram desenvolvidas em quatro partes. A primeira fez a introdução ao estudo. A segunda envolveu a construção do conceito de Guerra Híbrida na perspectiva político-estratégica da OTAN, a partir do debate com a literatura ocidental e com os documentos produzidos pela Aliança. A terceira teve como proposta discutir a reorganização e a preparação da OTAN para enfrentar a "Guerra Híbrida" da Federação Russa. Por fim, foram apresentadas reflexões finais e implicações para o Exército Brasileiro.

PALAVRAS-CHAVE:

Guerra Híbrida. Crimeia. Política. OTAN. Ucrânia.

KEYWORDS:

Hybrid Warfare. Crimea. Policy. NATO. Ukraine

ABSTRACT

The purpose of the essay is to analyze the Crimean Annexation and the Ukraine Crisis from the political and strategic perspective of the North Atlantic Treaty Organization (NATO). The essay sections were developed in four parts. The first part refers to the introduction to the study. The second part involves the construction of the concept of hybrid war in the political-strategic perspective of NATO, based on the debate with Western literature and with documents produced by the Alliance. The third part proposed to discuss NATO's reorganization and preparation to face the Russian Federation's "Hybrid War". Finally, final reflections and implications for the Brazilian Army were presented.

*Doutor em História Política, professor do PPGH da Universidade Salgado de Oliveira, coordenador do Grupo de Pesquisa História Militar, Política e Fronteiras do CNPq, coordenador do GT de História Militar da ANPUH-RJ e da ANPUH-Nacional, pesquisador do Centro de Estudos Estratégicos do Exército, diretor da Rede Hermes - Pesquisadores Internacionais de Fronteiras, Integração e Conflitos, e Jovem Cientista do Nosso Estado da FAPERJ.

Sumário Executivo

Este ensaio teve por objetivo analisar a Anexação da Crimeia e a Crise da Ucrânia sob a perspectiva político-estratégica da Organização do Tratado Atlântico Norte (OTAN). O estudo faz parte de uma proposta mais ampla de pesquisa sobre conflitos armados e emprego militar, que integra a agenda de investigação do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército para o ano de 2020/2021, relacionada à análise da operacionalidade do conceito de guerra híbrida nos conflitos contemporâneos e seu suposto impacto para a segurança nacional.

Desde 2010, a OTAN utiliza o termo guerra híbrida para descrever ações adotadas por adversários com a capacidade de empregar, simultaneamente, meios convencionais e não convencionais de forma adaptativa na execução dos seus objetivos. O conceito de *Guerra Híbrida* utilizado até o momento foi produzido por militares e analistas ocidentais com o objetivo de compreender essa nova dinâmica de conflito que desafia o pensamento militar contemporâneo. Tem-se empregado a expressão, por exemplo, para descrever as ações do Hezbollah contra Israel em 2006; as ações do Estado Islâmico; e as operações militares russas na Ucrânia, que culminaram na anexação da Crimeia, em 2014.

A questão da "guerra híbrida russa" tornou-se tema central dos debates, após a guerra que levou à intervenção no Leste da Ucrânia e à anexação da Crimeia, em 2014. A tensão pode ser percebida, com bastante clareza, com os resultados da Cimeira de Gales, de 2014. Entre os resultados, destacamos o lançamento do Plano de Ação de Prontidão (*Readiness Action Plan*), impulsionador da transformação na estratégia de dissuasão e defesa da Aliança, que levou à criação de quatro batalhões multinacionais de "Presença Avançada" na Estônia, Letônia, Lituânia e Polônia, em 2016. A criação dos Centros de Excelência, da Divisão Conjunta de Inteligência e Segurança e das Equipes de Apoio Contra-Híbrido foram outras medidas importantes.

Sobre as implicações do tema para o Exército Brasileiro, deve-se ressaltar que a ascensão de um novo tipo de guerra representa um acréscimo nas dificuldades para o planejamento militar nas futuras operações. Assim, a Força Terrestre deveria ficar atenta à sua comunicação estratégica, à dimensão informacional e às atividades de interação do seu serviço de inteligência com o Sistema Brasileiro de Inteligência (SISBIN), com ênfase na cooperação e na integração dos esforços. É fundamental que o Exército antecipe os acontecimentos, de forma pró-ativa, dando ênfase aos estudos e à preparação a estas novas ameaças, em sinergia e em cooperação com outras organizações nacionais, com responsabilidade em segurança e defesa.

Apesar dos fenômenos que compõem a chamada *Guerra Híbrida* não serem novos [...] a ascensão desse novo tipo de guerra representaria um elemento importante para a segurança e a defesa dos países membros da OTAN e, mais concretamente, para o planejamento estratégico e para a resposta a ser dada no emprego contra ameaças futuras.

1. Introdução

Após a Guerra Fria, houve uma intensificação no debate relacionado às alterações no modelo de guerra contemporânea. Nesse sentido, o objetivo deste terceiro ensaio é investigar o conceito de *Guerra Híbrida* usado pelos analistas ocidentais, em uma perspectiva político-estratégica da Organização Tratado do Atlântico Norte (OTAN), tomando por base o caso da anexação da Crimeia, durante a guerra contra a Ucrânia, em 2014.

No entanto, antes mesmo de começar a desenvolver este estudo, precisamos deixar claro que o tema em si é muito complexo e, dificilmente, chegaremos a uma única conclusão sobre o fato abordado. Observando a biblioteca digital da OTAN (*NATO Multimeida Library)*[1] é possível encontrar mais de 400 publicações registradas (artigos científicos, artigos da Web e artigos em periódicos), além de 43 relatórios, 7 documentos oficiais e 10 outras fontes, quase todos com seus links, para serem baixados, lidos e analisados. A biblioteca possui, ainda, a indicação de cerca de 35 livros sobre o assunto.

Apesar dos fenômenos que compõem a chamada *Guerra Híbrida* não serem novos para alguns autores, como apresentamos no primeiro ensaio, a ascensão desse novo tipo de guerra representaria um elemento importante para a segurança e a defesa dos países membros da OTAN e, mais concretamente, para o planejamento estratégico e para a resposta a ser dada no emprego contra ameaças futuras.

Nesse contexto, no início do século XXI, o conceito de *Guerra Híbrida* começou a ser formulado, quando as forças armadas ocidentais se viram no meio de operações militares complexas, tais como a guerra no Afeganistão, em 2001, e os conflitos no Iraque, em 2003.

Para prosseguir na abordagem do tema, cabe ressaltar a diferença entre

[1] Disponível em: https://natolibguides.info/hybridwarfare/articles/archives. Acesso em 31 dez. 2020.

ameaças híbridas e o próprio conceito de *Guerra Híbrida.* As *ameaças híbridas* são tipos de atores, a *guerra híbrida* é um modelo de conflito, caracterizado pela ação. A expressão *ameaça híbrida* é utilizada de forma muito próxima à de *Guerra Híbrida*, devido à complementaridade dos atores envolvidos, como forças regulares e irregulares, grupos criminosos e grupos terroristas, que empregam meios convencionais e não convencionais de forma simultânea ou não. Além disso, estão conectados pela natureza das tensões, como conflitos religiosos, étnicos, ou terrorismo, entre outros possíveis.

O conceito de *ameaça híbrida* tem sido debatido desde que foi inserido no Glossário da Defesa da OTAN. Os autores contrários ao conceito argumentam que é simplesmente o termo mais recente para métodos irregulares ou assimétricos usados para combater um inimigo convencionalmente superior (PUYVELDE, 2015). Os críticos afirmam, ainda, que a expressão *ameaça híbrida* é muito abstrata e corre o risco de se tornar uma "expressão de efeito" para todas as ações de ameaça não lineares (JASPER, e MORELAND, 2014).

Para muitos analistas ocidentais, ações como a campanha do Hezbollah, no Líbano, em 2006, e a atuação do Estado Islâmico, nos últimos anos, constituiriam exemplos clássicos de ameaças híbridas. A definição mais clara é a de que as *ameaças híbridas,* simultaneamente e adaptativamente, empregam uma mistura combinada de armas convencionais, táticas irregulares, armas de destruição em massa, terrorismo, ataques cibernéticos e comportamento criminoso, apoiados por uma campanha de informações maliciosas. As principais características são: táticas misturadas, estrutura flexível e adaptável, terrorismo, propaganda e guerra de informações, atividade criminosa e desrespeito ao direito internacional (JASPER, MORELAND, 2014).

A OTAN descreve o conceito de *ameaça híbrida* como o tipo de ameaça que é imposta por um adversário real ou potencial, inclusive, atores (estatais, não estatais e terroristas) com capacidade real ou provável, para, ao mesmo tempo, empregar meios convencionais e não convencionais de forma combinada na busca de seus objetivos (NATO, 2010, p. 02).

Nesse panorama, a ascensão do conceito da *Guerra Híbrida* não representa o fim da guerra tradicional regular e das ameaças representadas por Estados Nacionais. No entanto, esse novo tipo de guerra representa dificuldades para o processo de tomada de decisão e para a coordenação de respostas às novas ameaças, que transcendem, na atualidade, o campo exclusivamente militar em termos de competências e de atribuições.

2. O Conceito de *Guerra Híbrida* na perspectiva político-estratégica da OTAN

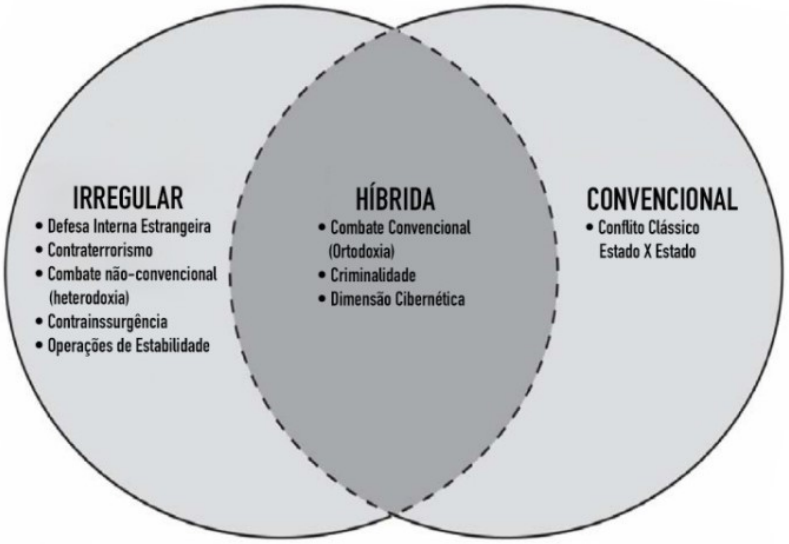
A OTAN (2010) utiliza a expressão *Guerra Híbrida* para descrever ações adotadas por adversários com a capacidade de empregar, simultaneamente, meios convencionais e não convencionais de forma adaptativa na execução dos seus objetivos (JASPER, e MORELAND, 2014).

O conceito que tem sido utilizado até o presente momento foi produzido por militares e analistas ocidentais (europeus e estadunidenses) com o objetivo de compreender essa nova dinâmica de conflito. O ataque terrorista aos EUA, em 11 de setembro de 2001, e a guerra entre Israel e o Líbano, em 2006, contribuíram, exponencialmente, para o desenvolvimento dos estudos sobre o tema, enfatizando a dimensão assimétrica do modelo. Fica claro que a maior parte das definições sobre a *Guerra Híbrida* foram construídas sob esse olhar ocidental.

A partir desse momento, os analistas tentaram entender o que seria esse novo e complexo tipo de guerra que estava sendo utilizado. No entanto, o tema ganhou grande projeção nos debates envolvendo a Guerra Russo-Ucraniana com a anexação da Crimeia e a intervenção russa em Donbass, no leste da Ucrânia, levando a OTAN a enfatizar os estudos e planejamentos com relação ao emprego da guerra híbrida. A guerra russa ganhou tanta importância que passou a ser o principal tema na preparação operacional dos aliancistas.

Em uma perspectiva mais generalista, nos estudos da teoria da guerra, o conceito de *Guerra Híbrida* pode ser definido como a combinação no emprego de meios convencionais e não convencionais (ou irregulares), ou a combinação de métodos convencionais e não convencionais, com o uso do componente regular e irregular, conforme o diagrama a seguir.

Figura 1: Conceito de guerra híbrida



Fonte: FERNANDES, 2016, p. 21.

Para o analista estadunidense Frank Hoffmman (2007, p. 14), a Guerra Híbrida incorpora diferentes modelos de guerra, incluindo capacidades convencionais, táticas e formações irregulares, desordem criminal, atividades terroristas com violência e coerção indiscriminada. Se antes o emprego de meios regulares e irregulares ocorria em diferentes espaços de batalha,

nas ações de Guerra Híbrida, esses meios são empregados de forma combinada na mesma força e no mesmo campo de conflito, com a atividade irregular, muitas vezes, tornando-se a ação decisiva, pois, nesse novo modelo de guerra, o principal objetivo é desestabilizar o governo inimigo e as suas instituições, estabelecendo o caos e o vazio de poder.

Outra importante definição de *Guerra Híbrida* pode ser observada no documento da *European External Action Service* (*Food-for-though paper - Countering hybrid threats*), de maio de 2015, quando a União Europeia caracterizou o conflito como uso, centralmente concebido e controlado, de várias táticas encobertas e abertas, utilizadas por meios militares e não militares, que vão desde operações de informações e cibernéticas, a partir de pressão econômica até o uso de forças convencionais (EUROPEAN EXTERNAL ACTION SERVICE, 2015, p. 2).

Uma maior preocupação com a anexação da Crimeia pode ser observada na Proposta de Resolução do Parlamento Europeu sobre a situação na Ucrânia[2] (2014/2841 (RSP)) e na Declaração Final da Cimeira de Gales[3], em 2014, feita pelos líderes políticos dos 28 Estados membros, os quais reafirmaram a necessidade da OTAN estar efetivamente preparada para fazer frente às ameaças da Guerra Híbrida, que se utiliza de meios militares cobertos e encobertos, paramilitares e civis, empregados numa elevada integração (NATO; 2014). Uma das principais decisões foi o aumento das despesas militares para o gasto do valor mínimo de 2% do Produto Interno Bruto de cada país[4], em um prazo de 10 anos, em uma reunião que deveria discutir a saída das forças atlânticas do Afeganistão.

A Cimeira de Gales alterou a postura estratégica da OTAN, dando prioridade às ameaças no Leste do continente e reforçou o paradigma da defesa coletiva, por meio da instrumentalização intencional das identidades estratégicas da Europa Meridional, na construção de uma nova cultura geopolítica da organização. Na estratégia de Gales, além de unir a Europa contra o inimigo tipificado como híbrido, os países da Europa Meridional serviram como meio para reafirmar o papel da OTAN na segurança internacional, por meio de: projeção de forças para o Leste Europeu; reconfiguração da tropa de prontidão; e demonstração de força dissuasória a partir dos exercícios realizados. (MARQUES, 2017, p. 69-73).

Entre a imensa quantidade de estudos produzidos para combater ameaças híbridas, Hoffmman (2007) ainda é considerado um dos principais proponentes do desenvolvimento do conceito. Esse autor

[2]Disponível em: https://www.europarl.europa.eu/doceo/document/B-8-2014-0122_PT.html. Acesso em: 23 dez. 2020.
[3]Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm. Acesso em: 23 dez. 2020.

[4]O valor estipulado é de 2% para cada país membro, entretanto, nenhum país atingiu esse valor de investimento em Defesa.

foi um dos primeiros a propor características claras de ameaças híbridas, contribuindo para a formulação, o embasamento e a defesa de um conceito complexo e bastante divergente, que oferece significativas contribuições para o planejamento militar.

Grande parte dos autores ocidentais define o conceito de *Guerra Híbrida* a partir da atuação militar russa no seu entorno estratégico. Para esses autores, o caráter cultural do pensamento militar russo tem sido ignorado. No entanto, analistas já identificaram que acadêmicos e militares russos não reconhecem o conceito de *Guerra Híbrida*, tampouco sinalizam que usam tais modelos. Essa questão se torna problemática a partir do momento em que pensadores ocidentais criam um modelo de guerra, baseado na atuação russa, que não é reconhecido pelos próprios russos.

3. Reorganização e preparação da OTAN para enfrentar a guerra híbrida da Federação Russa

A questão da Guerra Híbrida russa tornou-se tema central dos debates sobre segurança da OTAN. Essa ênfase pôde ser percebida com bastante clareza com os resultados da Cimeira de Gales, realizada no mesmo ano, quando os líderes políticos da Aliança condenaram a intervenção russa na região, classificando-a como violação das leis internacionais e como um desafio à segurança do Atlântico Norte europeu (FERNANDES, 2016, p. 26).

Em 08 de agosto de 2019, a OTAN publicou, em sua página na Internet, a informação de que métodos híbridos de guerra, tais como propaganda, engano e sabotagem, entre outras táticas não militares, vinham sendo utilizados como ferramentas de desestabilização do inimigo (NATO, 2019a). Os novos tempos propiciaram um conjunto de características contemporâneas: a velocidade, a escala e a intensidade do conflito, ações facilitadas pelas rápidas mudanças tecnológicas e interconectividade global. Nesse novo cenário, a Aliança sugere uma estratégia própria, com a definição do seu papel no combate à guerra híbrida e se considera pronta para defender os Estados Aliados contra qualquer ameaça convencional ou híbrida.

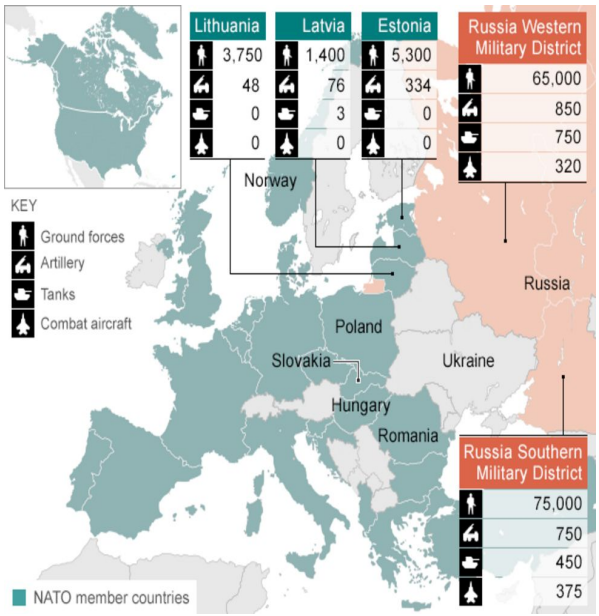
Fruto da Cimeira de Gales de 2014, a OTAN lançou o Plano de Ação de Prontidão (*Readiness Action Plan*), um dos principais impulsionadores da transformação na estratégia de dissuasão e defesa da Aliança. O Plano foi criado para garantir a prontidão da organização em resposta rápida e firme a novos desafios de segurança, a partir do Leste e do Sul. Por meio do Plano, os chefes de Estado e de Governo da OTAN aprovaram uma postura de dissuasão e de defesa, reforçada na Cúpula de Varsóvia, em julho de 2016. O Plano fornece à Aliança uma extensa gama

de opções para poder responder a quaisquer ameaças de onde quer que surjam, com o objetivo de proteger o território dos Aliados, a população, o espaço aéreo e as linhas de comunicação marítimas. Nesse cenário, em 2016, quatro batalhões multinacionais de Presença Avançada foram implantados na Estônia, Letônia, Lituânia e Polônia.

Figura 2:
Implementação do plano de ação de prontidão da OTAN

Fonte: https://twitter.com/usnato/status/742728044788494336

Figura 3:
Força de Ação Rápida da OTAN Forma Ideal e Capacidades



Fonte: https://www.bbc.com/news/world-europe-29087105

Uma importante reorganização ocorreu em 2017, quando a OTAN criou a Divisão Conjunta de Inteligência e Segurança, um ramo de análise híbrida, com o objetivo de ajudar a melhorar a qualidade e a utilidade da inteligência fornecida, aumentando com isso a consciência situacional. Para estar preparada, a Aliança coleta, continuamente, compartilha e avalia as informações com o objetivo de detectar e definir uma possível ameaça híbrida em andamento. A Divisão Conjunta de Inteligência e Segurança tem a função de: realizar a análise dessas informações sobre as ameaças contra os aliancistas e fornecê-las aos tomadores de decisão para fundamentar suas decisões políticas. A OTAN apoia o trabalho dos Estados aliados na identificação de vulnerabilidades nacionais e no fortalecimento de sua própria conduta contra a ameaça, quando solicitada. A remodelação inclui o trabalho em estreita colaboração com outras lideranças da inteligência da OTAN, principalmente, com a Direção de Inteligência do Quartel-General Supremo das Potências Aliadas na Europa ou Operações do Comando Aliado (NATO, 2019b).

O estabelecimento da Divisão Conjunta de Inteligência e Segurança também marcou a criação da primeira unidade civil e militar conjunta da OTAN. Reunir as equipes de inteligência civil e militar, anteriormente separadas, não foi uma tarefa fácil. Na época, algumas pessoas

temiam que as culturas profissionais e as abordagens da inteligência entrassem em conflito. A fusão das unidades de inteligência permitiu fornecer análises e avaliações coerentes, aumentar a eficiência, evitar a duplicação de esforços e aproveitar os pontos fortes que as organizações civis e militares trouxeram para o processo decisório, ao mesmo tempo em que se fomentava uma nova cultura de cooperação na Área de Inteligência. Mais importante ainda, posicionou a Divisão para enfrentar, eficazmente, as ameaças híbridas, cibernéticas e terroristas que cada vez mais confrontam os países-membros da OTAN (NATO, 2019b).

Em 2018, entre as principais ações identificadas na Cimeira da NATO, em Bruxelas, os líderes da Aliança concordaram com a criação de Equipes de Apoio Contra-Híbrido para o fornecimento de assistência direcionada e personalizada aos seus aliados, como forma de preparação e de resposta ao novo tipo de guerra. A unidade tem a função de combater campanhas híbridas hostis que possam ameaçar: a coesão da Aliança; infraestruturas críticas; estabilidade do governo; processos de tomada de decisão e serviços essenciais. A OTAN implantou sua primeira Equipe de Apoio Contra-Híbrido no final de 2019, nas eleições parlamentares de Montenegro, a pedido do governo. A organização fortaleceu sua coordenação com outros parceiros, incluindo a União Europeia, no esforço de combater as ameaças híbridas (NATO, 2019a).

A OTAN tem atuado também como centro de especialização, fornecendo apoio aos aliados na preparação civil e na resposta a incidentes químicos, biológicos, radiológicos e nucleares (DQBRN), proteção de infraestrutura crítica, comunicações estratégicas, proteção de civis, defesa cibernética, segurança energética e contra terrorismo. A OTAN coordena treinamento, exercícios e cursos para a preparação no enfrentamento contra as ameaças híbridas, incluindo o exercício de processos de tomada de decisão e resposta militares e não militares conjuntas em cooperação com outros atores (NATO; 2019a).

Nesse novo ambiente do século XXI, a OTAN tem uma posição bem definida, de agir prontamente, quando for necessário. Com isso, a organização tem aumentado o nível de prontidão e a preparação de suas forças. Também tem fortalecido seu processo de tomada de decisão e sua estrutura de comando como parte de sua estratégia dissuasória e de defesa do Atlântico Norte. Nesse contexto, a Aliança tem melhorado sua capacidade de resposta política e militar, com destaque para a rápida capacidade de desdobramento de forças no terreno.

Quando observamos a parte que destaca a cooperação e a coordenação da OTAN no tratamento de ameaças híbridas,

bem como a escolha de seus parceiros, é possível identificar que o principal objetivo da organização está direcionado contra a Rússia.

A cooperação foi intensificada com a União Europeia, com enfoque contra os ataques cibernéticos. Para tanto, foram criados os Centros de Excelência (CoE), que são organizações militares internacionais com a finalidade de dar treinamento e capacitar líderes e especialistas dos países membros e parceiros da OTAN. Para isso, auxiliam no desenvolvimento da doutrina; identificam lições aprendidas; melhoram a interoperabilidade e as capacidades; e testam e validam conceitos por meio de experimentação. Os CoE contribuem com conhecimento e experiência, oferecendo expertise reconhecida e apoiando a transformação da OTAN, evitando duplicidade de ativos, recursos e capacidades já existentes na Aliança (NATO, 2019a).

Os Centros de Excelência atuam em uma variedade de áreas, como cooperação civil-militar, defesa cibernética, descarte de artilharia explosiva, engenharia militar, medicina militar, segurança energética, defesa contra terrorismo, contrainteligência, operações climáticas, guerra de Montanha, polícia militar, policiamento de estabilidade, assistência às Forças de Segurança e dispositivos explosivos contraimprovisados (*Counter-Improvised Explosive Device Integration*). Esses centros são espaços de pesquisa internacionais, financiados por entidades nacionais e multinacionais. Portanto, a OTAN não financia diretamente os CoE e esses Centros não fazem parte da estrutura de comando da organização.

Um dos principais Centros Europeus de Excelência para o Combate a Ameaças Híbridas está localizado em Helsinque, na Finlândia. Ele funciona como um centro de especialização, auxiliando os Estados aliados a melhorarem suas capacidades de cooperação civil-militar nas mudanças de cenários e na preparação para enfrentar ameaças híbridas. O Centro foi inaugurado em outubro de 2017, pelo Secretário-Geral da OTAN, Jens Stoltenberg, juntamente com a Alta Representante da União Europeia para os Negócios Estrangeiros e a Política de Segurança, materializando a iniciativa do Governo da Finlândia, apoiado por outras 14 nações, além da NATO e da UE.

Além dessa unidade, outros Centros de Excelência contribuem para as atividades da OTAN no combate às ameaças híbridas: o Centro de Cooperação Civil-Militar em Haia, nos Países Baixos; o de Comando e Controle em Utrecht, na Holanda; o contra Dispositivos Explosivos Improvisados em Madri, na Espanha; o de Descarte de Explosivo de Artilharia em Trencí, na Eslováquia; o de Defesa Química, Biológica, Radiológica e Nuclear em Fetos, na República Tcheca; o de Engenharia Militar em Ingolstadt, na

Alemanha; o de Guerra na Montanha em Poljce, na Eslovênia; o de Medicina Militar em Budapeste, na Hungria; e o de Defesa Contra o Terrorismo em Ancara, na Turquia.

No entanto, para direcionar nossa indagação inicial sobre cooperação, destacamos o Centro de Excelência de Defesa Cibernética Cooperativa em Tallinn, Estônia, criado um ano após o ataque massivo de 2007, que interrompeu a infraestrutura digital do parlamento

Figura 4: Centros de Excelência da OTAN

Name	Location	Accreditation
Joint Air Power Competence Centre	Kalkar, Germany	2005
Centre of Excellence Defence Against Terrorism (COE-DAT)	Anakra, Turkey	2006
Naval Mine Warfare Centre of Excellence (NMW COE)	Ostend, Belgium	2006
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)	Norfolk, United States	2007
Civil-Military Cooperation Centre of Excellence (CIMIC COE)	Hague, Netherlands	2007
Joint Chemical, Biological, Radiological and Nuclear Defence Centre of Excellence (JCBRN COE)	Vyškov, Czech Republic	2007
Command and Control Centre of Excellence (C2 COE)	Utrecht, Netherlands	2008
Centre for Analysis and Simulation of Air Operations (CASPOA)	Lyon, France	2008
Cooperative Cyber Defence Centre of Excellence (CCD COE)	Tallinn, Estonia	2008
Counter-Improvised Explosive Devices Centre of Excellence (C-IED COE)	Madrid, Spain	2010
Operations in Confined and Shallow Waters Centre of Excellence (CSW COE)	Kiel, Germany	2008
Human Intelligence Centre of Excellence (HUMINT COE)	Oradea, Romania	2010
Modelling and Simulation Centre of Excellence (M&S COE)	Rome, Italy	2012
Military Engineering Centre of Excellence (MILENG COE)	Ingolstadt, Germany	2010
Cold Weather Operations Centre of Excellence (CWO COE)	Bodø, Norway	2007
Explosive Ordnance Disposal Centre of Excellence (EOD COE)	Trenčín, Slovakia	2001
Energy Security Centre of Excellence (ENSEC COE)	Vilnius, Lithuania	2012
Military Medicine Centre of Excellence (MILMED COE)	Budapest, Hungary	2009
Strategic Communications Centre of Excellence (StratCom COE)	Riga, Latvia	2014
Crisis Management and Disaster Response Centre of Excellence (CMDR COE)	Sofia, Bulgaria	2015
Military Police Centre of Excellenc (MP COE)	Bydgoszcz, Poland	2014
Stability Policing Centre of Excellence (SP COE)	Vicenza, Italy	2015
Mountain Warfare Centre of Excellence (MW COE)	Poljče, Slovenia	2015
Counter Intelligence Centre of Excellence (CI COE)	Kraków, Poland	2015
Security Force Assistance Centre of Excellence (SFA COE)	Rome, Italy,	2018

Fonte: https://southfront.org/nato-cooperative-cyber-defense-center-of-excellence-in-estonia/

estoniano, servidores e caixas de correios ministeriais, sistemas bancários, bem como jornais eletrônicos e serviços de emissoras. Esse ataque mostrou como ações combinadas podem enfraquecer os estados e servir como base para uma operação híbrida mais ampla. Além deste, destacam-se também: o Centro de Excelência de Comunicações Estratégicas em Riga, Letônia; o CoE de Contrainteligência na Cracóvia, Polônia; o CoE de Segurança Energética em Vilnius, Lituânia; e o CoE da Finlândia, todos localizados nas fronteiras com a Rússia (NATO; 2019a).

No total, 25 Centros de Excelência contribuem com a OTAN, conforme se pode observar na figura 4.

4. Reflexões finais e Implicações para o Exército

A partir da análise de autores europeus ocidentais sobre o modelo de guerra empregado pela Rússia contra a Ucrânia, em 2014, conclui-se que a ameaça híbrida russa se traduz numa mistura de diversas capacidades, em vários níveis: tático, operacional e estratégico (FERNANDES; 2016, p. 29).

No nível tático, os russos empregaram forças regulares, irregulares, operações de forças especiais e táticas com armamento convencional moderno, apoiando de forma dissimulada grupos paramilitares pró-Rússia, levando-os a executar operações de guerrilha em uma campanha não convencional. Nessa campanha, foi feito o uso de meios cibernéticos, para desestabilizar o poder político ucraniano, criando o caos e aproveitando a ausência de comando e controle.

No nível operacional, a Rússia conseguiu coordenar ações efetivas de guerra de informação e guerra psicológica, ao mesmo tempo em que mobilizava e deslocava tropas regulares em demonstração de força. Por outro lado, de forma encoberta, fez a infiltração de meios e de homens que apoiaram a causa rebelde na Ucrânia, conduzindo o desenvolvimento do conflito.

No nível estratégico, os russos empregaram, de forma coordenada e sincronizada, os campos do poder militar, diplomático, econômico e informacional, de maneira a atingir seus objetivos contra o inimigo.

Como podemos perceber, as ameaças atuais passaram a ser de várias ordens, em múltiplos conflitos sobrepostos. As novas guerras têm capacidade para se desenvolver em diversos ambientes operacionais, com ênfase no uso da subversão. Essas guerras se adaptam a cada caso, apresentam novos atores e evoluem de uma forma muito rápida. Dessa forma, o papel principal deixa de ser exclusividade dos atores estatais, em um ambiente onde atores não estatais mostram-se dispostos a empregar todos os meios à sua disposição para atingir os seus objetivos.

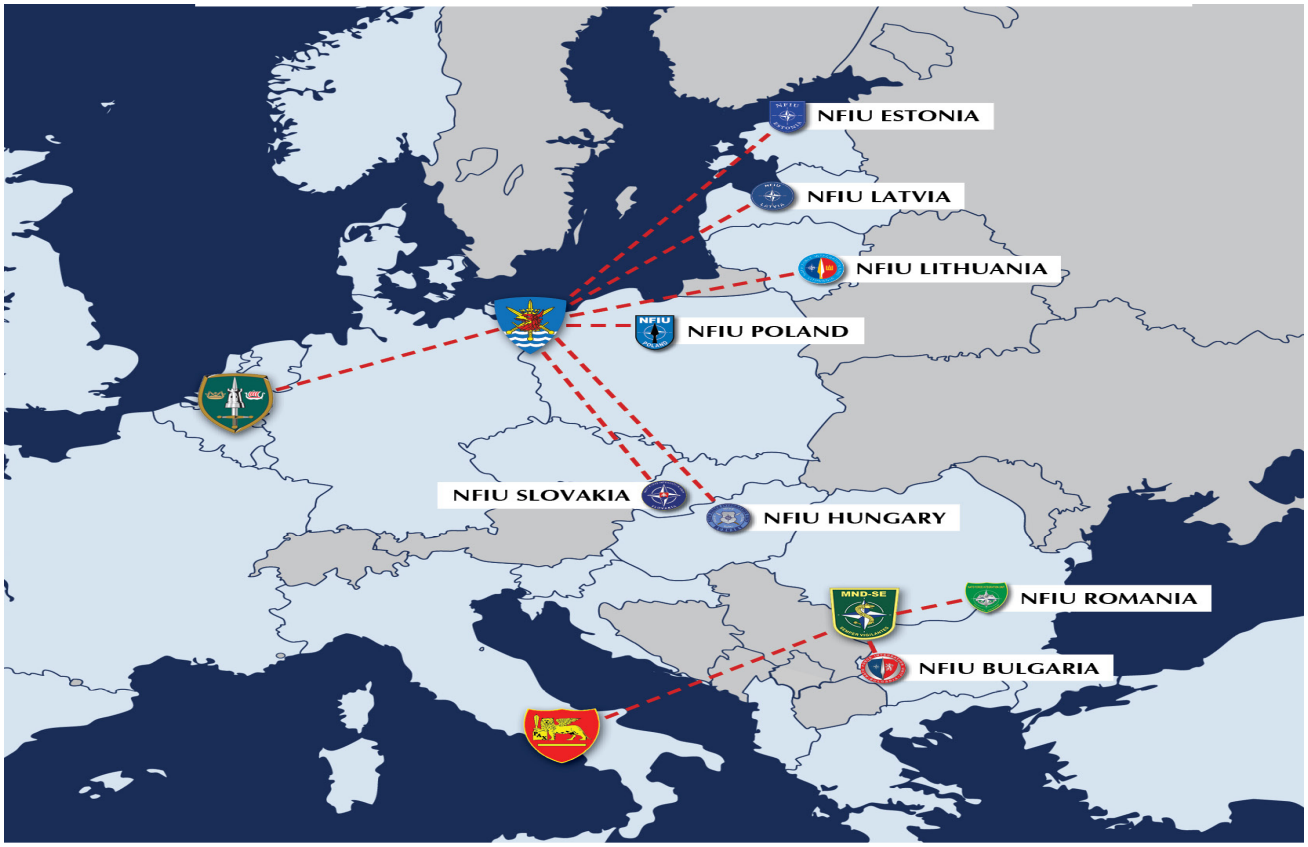
Os desafios estratégicos dispostos pelas ações da Federação Russa na Ucrânia, com a utilização de novos modelos de guerra, evidenciaram, para a OTAN, a sua vulnerabilidade e a necessidade de mudanças estratégicas que considerem os desafios de novas ameaças, identificadas pelos aliancistas como guerra híbrida. Nesse novo cenário, uma das principais medidas tomadas foi a adoção do Plano de Ação de Prontidão (*Readiness Action Plan*), iniciada na Cimeira do País de Gales, em 2014, e implantada em 2016, que visa a responder de forma rápida e firme os novos

desafios da segurança, com a implementação de medidas de garantia e adaptação (NATO; 2016).

As medidas de garantia foram focadas na defesa coletiva e na gestão de crises dos países membros da Aliança, principalmente, naqueles localizados na Europa Central e Oriental. Essas medidas incluem atividades de terra, mar e ar, contra possíveis agressões.

As medidas de adaptação são mudanças de longo prazo na estrutura de comando das forças, com o objetivo de tornar a OTAN melhor capacitada para reação rápida e decisiva diante de novas crises. As medidas de adaptação incluíram triplicar o tamanho da Força de Resposta da OTAN (*NATO Response Force*) e o estabelecimento de uma Força-Tarefa Conjunta de Alta Prontidão (*High Readiness Joint Task Force*), capaz de atuar em um tempo bastante curto. Para facilitar a prontidão e a rápida implantação de forças, a OTAN estabeleceu oito Unidades de Integração (*NATO Force Integration Units*)[5], na Europa Central e Oriental, para melhorar a cooperação e a coordenação com as forças locais no preparo e no apoio em eventuais projeções de força na região, conforme **figura 5**. Também foram montadas sedes do Corpo Multinacional Nordeste em Szczecin, na Polônia, e da

Figura 5: Unidades de Integração de Forças da OTAN



Fonte: https://jfcbs.nato.int/page5725819/nato-force-integration-units/nato-force-integration-units-fact-sheet

[5]Essas unidades no formato de pequenas sedes estão localizadas na Bulgária, Estônia, Letônia, Lituânia, Polônia, Romênia, Hungria e Eslováquia.

Divisão Multinacional Sudeste em Bucareste, na Romênia. Além disso, foi criada uma sede do grupo de apoio logístico conjunto (NATO; 2016).

Outras medidas importantes foram a criação dos Centros de Excelência, a criação da Divisão Conjunta de Inteligência e Segurança e a criação das Equipes de Apoio Contra-Híbrido.

A criação dos Centros de Excelências (CoE), organizações militares internacionais, teve como finalidade treinar e capacitar líderes e especialistas dos países membros e parceiros da OTAN. Os CoE auxiliam no desenvolvimento de doutrinas, aperfeiçoam a interoperabilidade e as capacidades, mas, principalmente, testam e validam novos meios e TTP. A Divisão Conjunta de Inteligência e Segurança teve como objetivo aprimorar o ramo de análise híbrida para ajudar a melhorar a qualidade e a utilidade da inteligência fornecida, aumentando com isso a consciência situacional. Por fim, as Equipes de Apoio Contra-Híbrido trabalham no fornecimento de assistência direcionada e personalizada aos seus aliados, na preparação e na resposta às novas formas de fazer a guerra, o que pode ser identificado como *warfare*.

Com base no exposto, buscando identificar as implicações estratégicas extraídas do tema para o planejamento militar no Brasil, é importante ressaltar que as ameaças tipificadas como híbridas vão requerer, por parte das forças armadas brasileiras, estratégias diferentes da pensada para a guerra regular e, no mínimo, uma definição mais consistente do que o modelo de guerra empregado pela Rússia na Ucrânia, em 2014, visto que são atores estratégicos diferentes. Nesse sentido, haverá necessidade de uma mentalidade estratégica de cooperação entre as forças, com o objetivo de um maior comprometimento e vontade política para enfrentar novas ameaças.

O Exército Brasileiro deve, não só estar capacitado para projetar força em diversos ambientes operacionais, como também estar apto para identificar e acompanhar a evolução de novas ameaças, para ter tempo e capacidade de rápida resposta a crises, em complexos e instáveis ambientes, que possam atingir as fronteiras e transbordar para o interior do país.

A ascensão de uma forma diferente de fazer a guerra não representa o fim dos conflitos convencionais, mas sim um acréscimo nas dificuldades para o planejamento da Força nas operações futuras contra novas ameaças.

Cada vez mais o Exército deve dar importância às operações de informação, incentivando a consolidação de uma cultura militar integradora, no nível tático das capacidades explicitadas no Manual de Operações de Informação: inteligência, Guerra Eletrônica, operações psicológicas, operações de forças especiais, comunicação social e guerra cibernética. Essas

capacidades devem ser cada vez mais aprimoradas, em um contexto mais amplo, de maneira que haja o desenvolvimento eficaz das operações de informação, no nível operacional.

É importante enfatizar que um ataque cibernético pode limitar uma ação inimiga, incapacitando o agressor de coordenar o funcionamento de diversos órgãos civis e militares, em função da dificuldade de comunicação ampla do governo com a comunidade local, com setores governamentais e entre os setores de defesa, internamente. Ademais, esse tipo de investida tem causado grande impacto psicológico sobre a população local, ao gerar pânico e angústia diante da incapacidade de resposta do Estado, como foi o ataque *hackers* à Estônia em 2007.

Nesse contexto de intensas mudanças no ambiente operacional, a possibilidade da utilização de diversos tipos de operações de informações não pode ser negada. É possível perceber que as operações de informação no Exército Brasileiro estão em desenvolvimento, mas esbarram em problemas internos -de uso sinérgico das capacidades relacionadas à informação- e externos, de adequação do seu planejamento estratégico com os interesses de outras forças na realização de operações conjuntas. Isso dificulta a integração e a sincronização das capacidades relacionadas à informação e dos recursos atinentes às operações de informação.

Assim sendo, o Exército Brasileiro deve dar atenção especial: à comunicação estratégica, comunicação social tradicional e mídias digitais com intenção de conquistar objetivos institucionais; à dimensão informacional; e às atividades de interação do seu serviço de inteligência com o Sistema Brasileiro de Inteligência (SISBIN), com ênfase na cooperação e na integração dos esforços e nos trabalhos em rede. É fundamental que o Exército antecipe os acontecimentos, adotando uma postura pró-ativa, dando ênfase aos estudos e à preparação contra novas ameaças, em sinergia e em cooperação com outras organizações nacionais, como universidades, que tenham responsabilidade em segurança e defesa. A Força Terrestre deve, cada vez mais, preocupar-se com o desenvolvimento de dispositivos de proteção adequados para os seus sistemas de informação, os quais devem incluir defesa cibernética, medidas contra guerra eletrônica, operações contra forças irregulares, uso de guerra por procuração, operações contra terrorismo e uso de operações psicológicas.

É importante a adoção de mecanismos de defesa capazes de reduzir os riscos contra os nossos sistemas de informação e contra a infraestrutura crítica, tornando-os menos vulneráveis contra ameaças híbridas.

Cada vez mais, o Brasil deve traçar estratégias de fortalecimento da inteligência de estado e incentivar o trabalho integrado

na área, unindo informações de Segurança Pública e de Defesa, ampliando os bancos de dados das Secretarias Estaduais de Segurança Pública, incrementando investimentos em tecnologia e capacitação de novos profissionais, além de melhorar a articulação desses setores estaduais com as atividades do Ministério da Justiça e Segurança Pública, da ABIN e dos setores de inteligência militares. Em países mais desenvolvidos, a atividade de inteligência é utilizada para obter informações para que o Estado reduza o risco e a incerteza de sua atuação, agindo de maneira mais racional e eficiente. Assim, o principal objetivo da inteligência é melhorar a qualidade do planejamento estatal e melhorar a qualidade do gasto público, permitindo uma melhor alocação de recursos. Nesse sentido, a inteligência estatal deve: prevenir ações terroristas; antecipar informações estratégicas sobre conjuntura e estabilidade política, aspectos econômicos e sociais de outros países que possam criar instabilidade; proteger informações estratégicas com a contrainteligência; e proteger e analisar o risco das infraestruturas.

Apesar da negação da existência do terrorismo no Brasil (GONZALES, 2019, p. 2), algo tratado como muito distante, o contraterrorismo talvez seja uma opção operacional, a partir do controle de uma autoridade nacional, legitimado pela ação estatal de um Sistema Nacional Contraterrorista, responsável por coordenar as atividades de preparo e emprego de forças militares, policiais e de inteligência. No Brasil, estudos recentes de pesquisadores demonstram como a operação "*hashtag*"[6] confirmou a presença de grupos radicais, fato comprovado pelo estreitamento das fronteiras realizadas por meio de comunicações (SAINT PIERRE, 2015).

Como analisa o Coronel Visacro, frente a essas mudanças de realidade no combate, a forma tradicional de pensar e de planejar a guerra tornou-se obsoleta. Com os novos ambientes incertos e ambíguos, que caracterizam a guerra do século XXI, não há mais condições de simples abordagens. Atualmente, muitos fatores não militares têm interferido e, até mesmo, limitado o processo decisório, calculado no estudo do terreno, do inimigo e das condições meteorológicas. Nesse momento, cada vez mais ferramentas complexas devem ser incorporadas à metodologia de planejamento tático, operacional e

[6]De acordo com as ações penais nº 5026758-35.2017.4.04.7000 e 5001839-45.2018.4.04.7000, as condutas apuradas, praticadas pelos investigados, eram identificadas, não obstante ambas estivessem voltadas à investigação de atos de promoção do Estado Islâmico e de possível execução de atos preparatórios para a realização de atentados terroristas e outras ações criminosas na denominada "Operação *Hashtag*". Embora as condutas tenham sido praticadas em ambiente virtual, algumas vezes comum, os elementos a serem demonstrados em cada uma das ações penais para busca da verdade real foram bastante diversos, notadamente em razão da finalidade aparente de cada agente com a prática de publicações voltadas à promoção de grupos terroristas.

estratégico, para proporcionar coerência sistemática ao uso do instrumento militar (2018, p. 120-121).

Por fim, com relação às novas capacidades necessárias às forças armadas para atuarem nos conflitos do século XXI, as organizações militares necessitam estar aptas a:

- formular estratégicas que contemplem igualmente o uso de meios não militares;
- desenvolver ações integradas e sinérgicas nas dimensões física, humana, e informacional;
- combinar o emprego de meios letais e não letais para alcançar o objetivo desejado;
- dar respostas ágeis e flexíveis em ambientes em constante mudança;
- agregar valor psicológico às ações de combate;
- fazer uso de profissionais das ciências humanas com capacidade analítica etnográfica, para atuar em ambientes multiculturais, como antropólogos, por exemplo;
- interagir com a mídia; e
- fazer uso habilidoso dos instrumentos jurídicos que lhe estão disponíveis, para assegurar a legitimidade do uso da força (VISACRO; 2018, p. 159).

Referências

EUROPEAN EXTERNAL ACTION SERVICE. Food-for-though paper – "Countering hybrid threats". Council of the European Union. Brussels, 13 may 2015. Disponível em: https://www.statewatch.org/media/documents/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf. Acesso em 23 dez. 2020.

FERNANDES, Hugo Miguel Moutinho. As novas guerras: o desafio da guerra híbrida. *Revista de Ciências Militares*. Lisboa, Vol. IV, n. 2, novembro 2016.

GONZALES, Neryse Pires Nery do Prado. O terrorismo e o contraterrorismo no Brasil: a resposta da legislação. Dissertação de Mestrado. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna, 2019. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/33129/1/Disserta%C3%A7%C3%A3o%20de%20Mestrado%20-%20Neryse%20Pires%20Nery%20do%20Prado%20Gonzales_Atualizada.pdf. Acesso em: 18 mar. 2021.

HOFFMMAN, Frank G. Future Warfare: The Rise of Hybride Wars. *Proceedings Magazine*. United State Naval Institute, 2005, vol. 132/111, 233. Disponível em: http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf Acesso em: 18 mar. 2021.

___. *Conflict in the 21ST century*: the rise of hybrid wars. Virgínia: Potomac Institute for Policy Studies, 2007. Disponível em: https://potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf Acesso em: 18 mar. 2021.

JASPER, Scott; MORELAND, Scott. The Islamic State is a Hybrid Threat: Why Does That Matter? Small Wars Journal, 12/02/2014. Disponível em: https://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter. Acesso em 23 dez. 2020.

MARQUES, Pedro Gonçalves. A geopolítica da NATO e a estratégia de Gales: o recurso à Europa do Sul. Dissertação de Mestrado em Relações Internacionais. Coimbra: Universidade de Coimbra, 2017. Disponível em: https://eg.uc.pt/bitstream/10316/82330/1/A%20Geopol%C3%ADtica%20da%20NATO%20e%20a%20estrat%C3%A9gia%20de%20Gales%20-%20o%20recurso%20%C3%A0%20Europa%20do%20Sul%20_%20Pedro%20Marques.pdf. Acesso em 23 dez. 2020.

MURRAY, Williamson e MANSOOR, Peter R (Eds.). *Hybrid Warfare*: fighting complex opponents from the Ancient World to the Present Hardcover. Cambridge: Cambridge University Press, 2012.

NEMETH, William J. *Future War na Chechnya*: a case for hybrtid warfare. Thesis. California: Naval Postgraduate School, 2002.

NATO. North Atlantic Treaty Organization. *NATO Multimedia Library*. Disponível em: https://natolibguides.info/hybridwarfare/articles/archives. Acesso em 31 dez. 2020.

NATO. North Atlantic Treaty Organization. *Bi-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats*. Supreme Allied Commander (Europe / United States of America), 25 August 2010. Disponível em: https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf. Acesso em: 28 dez. 2020.

NATO. North Atlantic Treaty Organization. Wales Summit Declaration. By the Heads of State and Government participating in the North Atlantic Council meeting in Wales, 05 september 2014. Disponível em: https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en. Acesso em 29 dez. 2020.

NATO. North Atlantic Treaty Organization. NATO's Readiness Action Plan 2016. Disponível em: https://www.nato.int/cps/en/natohq/topics_119353.htm. Acesso em: 29 dez. 2020

NATO. North Atlantic Treaty Organization. NATO's response to hybrid threats. 08 Agust 2019a. Disponível em: https://www.nato.int/cps/en/natohq/topics_156338.htm. Acesso em: 28 dez. 2020.

NATO. North Atlantic Treaty Organization. A New Era for NATO Intelligence. 29 October 2019b. Disponível em: https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html. Acesso em: 31 dez. 2020.

PUYVELDE, Damien Van. Hybrid War – does it even exist? *Nato Review*. NATO, 7 may 2015. Disponível em: https://www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html. Acesso em 13 dez. 2020.

SAINT-PIERRE, Héctor L.11 de Setembro: do terror à injustificada arbitrariedade e o terrorismo de Estado. Revista de Sociologia e Política, 23(53), pp. 9-26, 2015.

VISACRO, A. *A Guerra na Era da Informação*. São Paulo: Contexto, 2018.