ISSN: 2525-457X
Análise Estratégica
Vol 22 (4) Set/ Nov 2021

Análise da operacionalidade do conceito de guerra híbrida nos conflitos contemporâneos e seu suposto impacto para a segurança nacional no Brasil

Analysis of the operationality of the concept of hybrid war in contemporary conflicts and its supposed impact on national security in Brazil

Fernando da Silva Rodrigues*

RESUMO

O objetivo da investigação do ciclo 2020-2021 foi avaliar as implicações do conceito de guerra híbrida para a Segurança Nacional no Brasil. A partir dessa proposta inicial, a pesquisa foi sendo desenvolvida, tomando como base o debate sobre a definição do conceito de guerra híbrida, sua relação com os conflitos contemporâneos e seus reflexos no Planejamento Estratégico do Exército. A partir da definição de guerra híbrida, adotamos um estudo de caso e analisamos a anexação da Crimeia e a crise da Ucrânia, sob a perspectiva político-estratégica da Rússia e da OTAN, enfatizando a renovação da doutrina militar russa com o emprego de um novo tipo de guerra, a reorganização e a preparação da OTAN para enfrentar a guerra híbrida da Federação Russa, até chegar à discussão sobre as novas ameaças do século XXI para o Brasil, no contexto da segurança contra a Guerra Cibernética. Por fim, foram apresentadas reflexões e implicações para o Exército Brasileiro.

Palavras-chave: Guerra híbrida, Rússia, Segurança Nacional, OTAN.

ABSTRACT

The objective of the investigation was to evaluate the implications of the hybrid war concept for National Security in Brazil. From this initial proposal, the research was developed based on the debate on the definition of the concept of Hybrid War, its relationship with contemporary conflicts and its effects on the Army's Strategic Planning. From the definition of hybrid war, we adopted a case study and analyzed the annexation of Crimea and the crisis in Ukraine under the political-strategic perspective of Russia and NATO, emphasizing the renewal of Russian military doctrine with the use of a new type of war, reorganization and preparation of NATO to face the “hybrid war” of the Russian Federation, until reaching the discussion on the new threats of the 21st century for Brazil, in the context of security against cyber war. In this context, reflections and implications for the Brazilian Army were presented.

Keywords: Hybrid Warfare, Russia, National Security.

*Doutor em História Política, professor e coordenador 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 (2017-2021).

SUMÁRIO EXECUTIVO

O presente texto aborda as implicações do conceito de guerra híbrida para a Segurança Nacional no Brasil. O estudo faz parte de uma proposta mais ampla de pesquisa sobre conflitos armados e emprego militar, que integrou a agenda de investigação do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército para o ano de 2020/2021.

Inicialmente, discutimos a definição do conceito de guerra híbrida, sua relação com os conflitos contemporâneos e seus reflexos no Planejamento Estratégico do Exército. O trabalho foi desenvolvido a partir do debate sobre os conflitos vistos pela História e pela Teoria da Guerra. Posteriormente, desenvolvemos o conceito sobre guerra híbrida, a partir da identificação de estudos sobre as principais guerras e conflitos globais e sua relação com as mudanças nas condições políticas, socioeconômicas e tecnológicas ocorridas desde o fim da Guerra Fria.

A partir da definição conceitual, analisamos a anexação da Crimeia e a Crise da Ucrânia sob a perspectiva político-estratégico da Rússia. A pesquisa foi desenvolvida a partir do debate sobre os estudos da crise na região, demonstrando que nenhum país está imune às ameaças e às tensões surgidas no mundo contemporâneo, pós-Guerra Fria, principalmente, quando pensamos na manutenção da soberania, na preservação da democracia e na integridade do território.

A investigação demonstrou um aspecto importante da guerra russa na Ucrânia, em 2014: o aproveitamento do estado de convulsão social existente, favorecido pelo ambiente político com grandes índices de corrupção, para criar diferentes interpretações dos acontecimentos, tanto da população local afetada pelos ataques, como da comunidade internacional. Essa condição, estabelecida na primeira fase operacional da guerra russa, permitiu a construção de uma narrativa dominante como "verdadeira" sobre o que estava acontecendo, dificultando o seu entendimento e moldando a opinião pública. De fato, o estudo mostrou as ferramentas utilizadas pela Rússia, que criou uma forma bastante eficaz de lutar em um ambiente de amplo espectro. Ao utilizar uma variada forma de estratégias contra seus inimigos, a Rússia soube potencializar todas as facilidades desse ambiente, operando com atores estatais e não estatais, com grupos criminosos, com forças de operações especiais e com a diplomacia, para alavancar a convulsão social e a instabilidade do inimigo, dificultando sua tomada de decisão. Fica claro que esse novo tipo de guerra, empregado na Ucrânia, contém elementos que podem ser melhor estudados pela Força Terrestre brasileira.

Em um terceiro momento, analisamos a Anexação da Crimeia e a Crise da Ucrânia sob a perspectiva político-estratégica da Organização do Tratado Atlântico Norte (OTAN). A "guerra híbrida russa" tornou-se tema central dos debates, após a intervenção no Leste da Ucrânia e a anexação da Crimeia, em 2014. Percebeu-se essa tensão de forma clara 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, levando à criação, em 2016, de quatro batalhões multinacionais de "Presença Avançada", na Estônia, Letônia, Lituânia e Polônia. Outras medidas importantes foram a criação dos Centros de Excelência, da Divisão Conjunta de Inteligência e Segurança e das Equipes de Apoio Contra-Híbrido.

Por fim, avaliamos as implicações do conceito de guerra híbrida para a Segurança Nacional, a partir da discussão sobre as novas ameaças do século XXI, no contexto da segurança contra a Guerra Cibernética.

ISSN: 2525-457X
Análise Estratégica
Vol 22 (4) Set/ Nov 2021

1. Guerra Híbrida nos Conflitos Armados Contemporâneos: principais aspectos revelados para o Emprego Militar

a. Formas de Guerra do mundo contemporâneo

Para uma melhor compreensão da guerra híbrida, é necessário definir as principais formas de guerra reconhecidas teoricamente na atualidade. Nesse sentido, escolhemos trabalhar com as definições das seguintes formas de guerras:

Quarta Geração - surgiu após a Segunda Guerra Mundial (2ª GM), quando atores estatais e não estatais passaram a usar outros tipos de táticas, para compensar os diferentes níveis de capacidades tecnológicas. Pode ser observada no desenvolvimento dos conceitos da guerra de guerrilha, de insurgência e da guerra popular, por descrever um tipo de conflito cuja força, com capacidades militares convencionais inferiores, emprega meios de combate não convencionais ou irregulares como forma de compensar as forças assimétricas no conflito. Nesse novo modelo de guerra, a população do inimigo e a sua cultura tornam-se alvos do ataque adversário.
Guerras Compostas - uso simultâneo de operações regulares e irregulares sob uma coordenação estratégica, atuando de forma separada. Esse tipo de guerra se aplica quando um Estado mais fraco tem seu território ocupado por outro de poder superior. Na medida em que as tropas inimigas avançam suas posições no território ocupado, o país invadido pode iniciar uma guerra composta. A atuação das forças regulares e forças irregulares dos *Vietcongs*, na Guerra do Vietnã, exemplifica essa modalidade.

Guerra Irrestrita - em virtude da superioridade bélica de um dos países em conflito nas operações regulares, devido ao emprego de um grande número de capacidades, articuladas à alta tecnologia, o outro país deve buscar uma forma de combate em que atores estatais e não estatais possam ser empregados de maneira combinada com meios políticos, econômicos, culturais, diplomáticos, étnicos e religiosos, como esforço principal, complementado por recursos militares limitados. Nesse caso, os ataques terroristas, financeiros e cibernéticos podem causar danos tão profundos quanto os ataques militares convencionais.

Guerra Assimétrica - enfrentamento entre dois ou mais adversários com capacidades bélicas diferentes, com a superioridade clara de um dos oponentes, levando a parte mais fraca a tentar definir a natureza do confronto de maneira a minimizar o poder tecnológico da potência envolvida.

Guerra Irregular - nessa forma de guerra, a mobilização das massas é um ponto estratégico, assim como o controle do terreno. Parte-se do princípio de que não existem regras na condução do conflito e baseia-se no uso de pequenos escalões operacionais. A guerra irregular é todo o conflito conduzido por uma força que não dispõe de organização militar formal e, sobretudo, de legitimidade jurídica institucional. É a guerra travada por uma força não regular.

b. Ameaça Híbrida

A definição do conceito de ameaça híbrida envolve o tipo de atores, contrapondo-se ao conceito de guerra híbrida, que é um modelo de guerra. As ameaças híbridas (sujeitos) incorporam diferentes modos de guerra, incluindo capacidades convencionais, táticas e formações irregulares, atos terroristas, com uso de violência e coerção indiscriminada e desordem criminal, que podem ser empregados por Estados Nacionais ou por atores não estatais.

O conceito de ameaça híbrida tem sido debatido desde que passou a fazer parte do Glossário da defesa da OTAN. A definição mais clara é 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.

A OTAN descreve o conceito de ameaça híbrida como o tipo de ameaça que é imposta por um adversário real ou potencial, o que inclui Estados, não Estados e terroristas, que tenham capacidade real ou provável, para, ao mesmo tempo, empregar meios convencionais e não convencionais de forma combinada na busca de seus objetivos.

> “Aqueles atores que recorrem à guerra híbrida têm como objetivo dominar o controle operacional sem restrições, podendo ultrapassar as fronteiras, as leis impostas e as leis morais da guerra.”

c. Guerra Híbrida

A ideia de guerra híbrida apareceu no início do século XXI, quando as forças armadas ocidentais se viram no meio de operações militares complexas, como a guerra no Afeganistão, em 2001, e no Iraque, em 2003. A partir daquele 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 à Organização do Tratado do Atlântico Norte (OTAN) a enfatizar os estudos e planejamentos com relação ao emprego da guerra híbrida como parte da doutrina militar russa.

Nesse sentido, o conceito de guerra híbrida expande as possibilidades de atuação dos atores estatais e não estatais, sendo que ambos podem usar organização, técnicas, táticas e procedimentos tanto da guerra regular, quanto da guerra irregular. Aqueles atores que recorrem à guerra híbrida têm como objetivo dominar o controle operacional sem restrições, podendo ultrapassar as fronteiras, as leis impostas e as leis morais da guerra. A guerra híbrida é, nesse caso, a combinação dos múltiplos meios da guerra convencional e não convencional, que podem usar forças militares regulares, forças irregulares, forças especiais, guerra econômica, ataque cibernético, diplomacia, propaganda com guerra de informação e apoio à manifestação local, conforme a figura 1.

FIGURA 1
Diversidade de meios da Guerra Híbrida

Fonte: o autor.

Como foi observado, a guerra híbrida é um tipo de conflito que articula uma grande diversidade de meios militares ou não militares com o objetivo de atingir as vulnerabilidades de um Estado fragilizado. O ataque normalmente começa pelo incentivo a uma agitação social interna (às vezes, conhecidas como Revoluções Coloridas), ou disputas territoriais, que são apoiadas por uma intensa campanha de informação, construída com base em uma narrativa eficaz, atuando no limite da legalidade e da legitimidade, sem recorrer aos meios militares nesse momento.

Desde 2010, a OTAN utiliza o termo guerra híbrida para descrever situações em que os adversários contam 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 presente momento foi produzido por militares e analistas ocidentais (europeus e estadunidenses) com o objetivo de compreender essa nova dinâmica de conflito que desafia o pensamento militar ocidental.

O analista militar Frank Hoffmman, Tenente-coronel do Corpo de Fuzileiros Navais dos EUA, afirma que a guerra híbrida incorpora diferentes modelos de guerra, incluindo: capacidades convencionais; táticas e formações irregulares; atividade terrorista com violência e coerção indiscriminada; e desordem criminal. Se, antes, o emprego de meios regulares e irregulares ocorria em diferentes espaços de batalha, na guerra híbrida, esses meios são empregados de forma combinada na mesma força e no mesmo campo de conflito, com a atividade irregular tornando-se, muitas vezes, a ação decisiva. Essa modalidade de guerra tem como principal objetivo desestabilizar o governo inimigo e suas instituições, estabelecendo o caos e o vazio de poder.

Com base em grande parte dos autores ocidentais, fica evidente a definição do conceito de guerra híbrida, com enfoque na relação e atuação militar russa no seu entorno estratégico. Para esses autores, o caráter cultural do pensamento militar russo tem sido ignorado. No entanto, muitos analistas já identificaram que acadêmicos e militares russos não reconhecem o conceito de guerra híbrida, muito menos sinalizam que usam tais modelos.

No nosso entendimento, está claro que a grande variedade de tipos de conflitos atuais, somada à nova forma de fazer a guerra, tem uma relação direta tanto com os novos e avançados meios tecnológicos, quanto com as novas estratégias e ações militares remodeladas ao longo do tempo. A guerra híbrida busca destruir ou limitar as ações do inimigo com ações de combate e meios não letais, cujo objetivo é controlar a população local na área das operações, obter seu apoio e buscar a adesão da opinião pública e da comunidade internacional. Dessa forma, para conseguir alcançar os objetivos estratégicos, é necessário ter sucesso nos campos de batalha convencional e assimétrico. Por isso, o planejamento das atividades operacionais e estratégicas não pode ser realizado como se houvesse duas guerras separadas, uma no campo de batalha convencional e outra com relação à segurança e à estabilização da população.

Também ficou evidente que, no emprego de guerra híbrida, existe a necessidade de potencializar meios irregulares no nível político estratégico, por ser um tipo de guerra com modelagem militar estatal e tropa privada, usada em atividades clandestinas. Nesse sentido, as implicações operacionais podem ser significativas e terão que ser cuidadosamente pensadas, pois o planejamento militar deverá buscar abordagens novas e criativas, com base no pensamento inovador para solução dos problemas militares contemporâneos, como o emprego combinado de forças especiais com Guerra Cibernética, ou Operações de informações e Operações de dissimulação. No entanto, a utilização das forças especiais, dentro do contexto híbrido, vai além do uso tradicional e tem alcance político. Atingir objetivos em cenários sem combates é um exemplo de emprego desse tipo de tropa em um ambiente híbrido. Foi nesse tipo de missão que as forças especiais russas se converteram na principal ferramenta da guerra híbrida, articulada ao uso da Guerra Cibernética.

Contudo, é importante esclarecer que guerra híbrida não pode ser considerada apenas uma resposta assimétrica, empregada por um poder militar mais fraco, estatal ou não estatal. O novo tipo de guerra aparece nos conflitos atuais, com a capacidade de engajar de modo efetivo as diversas formas de fazer a guerra simultaneamente. Seguindo uma proposta com melhor definição, esse tipo de guerra envolve o emprego de armas convencionais avançadas, táticas irregulares, tecnologias agressivas, terrorismo e criminalidade, com o objetivo de desestabilizar a ordem política estabelecida, ou seja, a guerra híbrida foi planejada para corroer o poder estatal do inimigo por dentro.

d. Teoria de Guerra Russa

A evolução do modelo de guerra russa tem ocorrido com bastante intensidade desde o final dos anos 1970. Um importante modelo foi a Teoria das Operações Profundas, desenvolvida pelo Marechal Marshal Mikhail Tukachevsky, nos anos 1980, baseada no emprego combinado de

armas e de carros de combate, em operações cujo objetivo era destruir a logística e a retaguarda inimiga e cortar as comunicações, por meio de grande poder de fogo. Também cabe relembrar a Teoria do Controle Reflexivo, referente aos métodos sistemáticos que moldaram as percepções do inimigo, de forma que suas decisões se tornassem voluntárias e favoráveis aos interesses estratégicos da Rússia.

A partir desses modelos, a Rússia desenvolveu, nas operações contra a Geórgia (2008), uma Nova Teoria das Operações Profundas, com uma diferente modelagem, utilizando o emprego de forças de operações especiais, guerra de informações, operações de inteligência e ataques cibernéticos contra o setor político, econômico e a opinião pública, de modo a enfraquecer o governo local e permitir a operação das fases seguintes da guerra, como a invasão de tropas regulares estatais. Na Ucrânia, em 2014, a Rússia utilizou Guerra Não Linear, reflexo de um novo ou renovado pensamento militar, amparada em dois aspectos teóricos combinados que ajudaram na formação do modelo: a Teoria da Operação Profunda e a Teoria do Controle Reflexivo. O conceito de guerra não linear deve ser observado com o uso articulado de: forças militares; operações de informações; campo político; e, organizações não militares (nesse caso, forças de operações especiais, forças irregulares e tropa de mercenários, como foi usado na anexação da Crimeia).

Esse novo modelo de guerra está presente na Doutrina Militar Russa, aprovada pelo governo Putin em 25 de dezembro de 2014, que identifica a permanência dos conflitos regionais, inclusive nas regiões fronteiriças com a Federação Russa. Para tanto, dentre as características dos conflitos atuais, a doutrina identifica, como primeiro item, o emprego integrado de força militar com medidas políticas, econômicas, operações de informações e emprego de medidas não militares implantadas com amplo uso de protesto popular e forças de operações especiais.

No **nível tático**, os russos empregaram, na Ucrânia (2014), 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**, os russos conseguiram coordenar ações efetivas de guerra de informação e guerra psicológica, ao mesmo tempo que mobilizavam e deslocavam tropas regulares em demonstração de força. Por outro lado, de forma encoberta, fizeram a infiltração de meios e homens na Ucrânia, que apoiando a causa rebelde e conduzindo o desenvolvimento do conflito. No **nível estratégico**, os russos empregaram de forma coordenada e sincronizada os seus campos do poder militar, diplomático, econômico e informacional, de maneira a atingir seus objetivos contra o inimigo.

e. Pensamento militar de Gerasimov

Em artigo sobre o Pensamento Militar Russo, publicado em 2013, o general Valery Gerasimov, chefe do Estado-Maior Geral da Federação Russa, discutiu sobre os novos métodos de enfrentamento nos conflitos armados. Gerasimov identificou o uso dissolvido e não aberto da força, com a utilização de unidades insurgentes paramilitares e civis. Também enfatizou a necessidade de confiar nos métodos assimétricos e indiretos. Além da realidade física do combate, o general afirmou que a guerra deve incluir o espaço informacional, em apoio a ações cinéticas, com a coordenação em tempo real dos meios e ferramentas utilizadas. Ele enfatizou que os ataques direcionados e bem conduzidos atrás das linhas inimigas devem ter como objetivo a destruição da infraestrutura crítica, tanto as relacionadas aos seus elementos militares como civis, de preferência em um curto período temporal. Defendeu também o uso

intenso de forças de operações especiais e de armas automatizadas, como os drones. Por fim, Gerasimov definiu que as forças regulares devem ser usadas apenas no final das fases operacionais do conflito, muitas vezes, sob o disfarce de Forças de Manutenção de Paz ou forças de gestão de crises.

Nesse contexto, o general Gerasimov revelou o modelo russo sobre as novas estratégias dos conflitos modernos, identificado como Guerra Não Linear, destacando que, de acordo com as mudanças ocorridas na forma de conduzir a guerra, esses novos modelos empregados requerem o uso de diferentes instrumentos de poder (militares ou não militares) à disposição de um Estado para que ele alcance os seus objetivos desejados.

As ideias-chave do pensamento militar de Gerasimov estão sintetizadas na figura 2.

FIGURA 2
Pensamento militar de Gerasimov

Fonte: o autor.

f. Reorganização Militar da OTAN

Com o fim 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. 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.

Como resultado desse momento, foram criados novos tipos de unidades militares na OTAN. Em 2016, Batalhões multinacionais de Presença Avançada foram implantados na Estônia, Letônia, Lituânia e Polônia, como medidas tomadas para reforçar a segurança na região sudeste da Aliança, frente às tensões com a Rússia.

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.

Em 2018, 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, na preparação e 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 e processos de tomada de decisão e serviços essenciais.

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 ensinar líderes e especialistas dos países membros e parceiros da OTAN. Auxiliam no desenvolvimento da doutrina, identificam lições aprendidas, melhoram a interoperabilidade e as capacidades, testam e validam conceitos por meio da experimentação. Eles oferecem conhecimento e expertise reconhecida que são importantes para a organização e apoiam a sua transformação, evitando duplicidade de ativos, recursos e capacidades já existentes na Aliança. 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).

Na reestruturação para enfrentar as novas ameaças, o Exército do Reino Unido organizou a 6ª Divisão (HQ 6 UK Div) com capacidade de ponta na preparação e geração de forças de manobras de informação e guerra não convencional. De sua sede em Wiltshire, a Divisão reúne uma série de especialistas com habilidades necessárias para ajudar no preparo e na realização de operações internas e externas. A unidade fornece a capacidade assimétrica ao Exército britânico, além de coordenar o campo da inteligência, contrainteligência, ciberespaço, guerra eletrônica, operações de informação e guerra não convencional. A Divisão está estruturada em quatro brigadas especializadas com recursos exclusivos.

g. Segurança Cibernética Social

A segurança cibernética social é identificada como uma área científica emergente, que emprega a ciência para caracterizar, entender e prever transformações causadas pelas ações cibernéticas no comportamento humano, assim como seus resultados sociais, culturais e políticos. Ela também é destinada à construção da infraestrutura cibernética para a segurança da sociedade no ambiente informacional, constantemente sob ameaças cibernéticas sociais reais ou iminentes. Ademais, a tecnologia capacita atores estatais e não estatais a manipularem o mundo de crenças e ideias à velocidade de algoritmos.

A segurança cibernética social é diferente da segurança cibernética tradicional, pois essa última está associada às pessoas que usam a tecnologia para hackear tecnologia, cujos alvos são os sistemas de informações. Já a segurança cibernética social envolve seres humanos que empregam a tecnologia para hackear outros seres humanos, ou seja, os alvos dos ataques são as pessoas e a sociedade. Como parte de uma guerra de informação, esse tipo de ataque usa: o meio cibernético para difusão em massa de suas ideias; as operações psicológicas de persuasão; a fragilidade da sociedade por causa de intensa corrupção nos meios políticos caracterizados pelas relações criminosas entre instituições privadas e agentes do Estado; as ciências sociais no emprego de operações de informação coordenadas com o objetivo de conseguir efeitos estratégicos.

O domínio sociocibernético oferece diferentes formas de manobra da Segurança Cibernética Social. No domínio, o adversário tem capacidade de manipular a informação das redes de conhecimento, assim como manipular as redes que podem ser redes sociais (Facebook e Instagram), redes de conversa (WhatsApp), ou redes informacionais (#COVID19), a fim de aumentar a agitação e reduzir a confiança interna, independente da narrativa, e criar fissuras na sociedade atacada.

h. *"Blitzkrieg Informacional"*

A tecnologia permite que atores estatais e não estatais ampliem exacerbadamente seu poder no domínio informacional. Se não houver uma maior atenção para o fato, ocorrerá uma "blitzkrieg informacional", com os mesmos efeitos estratégicos do emprego da blitzkrieg alemã na 2ª GM.

Essa ideia foi construída com base nas análises sobre a máquina de propaganda persuasiva russa que, durante muito tempo, foi empregada contra seu público interno nas cidades satélites da antiga URSS, mudando para atacar alvos no exterior, cuja missão seria a disseminação de narrativas distorcidas, a fim de promover agitação e discordância entre os povos. Pôde ser legitimada, com a fala do general Valery Gerasimov, no artigo O Valor da Ciência Está na Previsão [The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", Voyenno-Promyshlennyy Kurier online, 26 February 2013], que definiu a guerra de informação como um instrumento importante da estratégia russa a partir daquele momento, pois a guerra de informação abria enormes possibilidades assimétricas de diminuir o potencial de combate do oponente.

A sua função seria abrir caminho entre todas as possíveis fissuras existentes em um Estado, fraturando a nação ou a coalizão, incluindo medidas de exploração de dissidências entre partidos políticos, religiões, sociedades, forças armadas e alianças internacionais, para enfraquecer suas defesas contra um ataque externo.

2. Implicações para o Exército Brasileiro

A definição do conceito de guerra híbrida, do ponto de vista teórico, assume uma grande importância estratégica para o Planejamento do EB com relação ao emprego militar, no contexto de mudanças paradigmáticas nos conflitos contemporâneos.

A tendência de operações de combate com pouca definição no tempo e no espaço, disputado em diferentes níveis, por forças estatais e não estatais, indica que, no futuro, provavelmente, a guerra ficará cada vez mais incerta, com dificuldade de identificação do inimigo dominante e de definição de categorias operativas.

O futuro aponta para a ampliação da ocorrência de conflitos de menor intensidade, conduzidos por grupos guerrilheiros, milícias urbanas, facções criminosas, grupos terroristas, organizações político-partidárias extremistas e crime organizado.

As principais tendências e incertezas de possíveis ameaças híbridas para o Brasil e de interesse direto ao Exército serão os ataques cibernéticos; as tensões na região Amazônica, causadas pela variedade de riquezas naturais e seu papel relevante na agenda climática mundial; a emergência climática e os seus possíveis impactos na geopolítica mundial; a militarização do Atlântico Sul; a instabilidade política no entorno estratégico; e as consequências advindas da chamada "Nova Guerra Fria" entre a China e os EUA.

Diante dessas novas ameaças, é imprescindível adotar uma mentalidade crescente no Exército Brasileiro sobre a importância da guerra de informação, bem como sobre o surgimento de redes de comunicações globais em comando e controle e a potencialidade de emprego de capacidades combinadas de ataques. Importante, também, considerar, na Força Terrestre do Brasil, uma maior integração das capacidades relacionadas à guerra de informação, composta por: inteligência, guerra eletrônica, guerra cibernética, uso de forças de operações especiais, operações psicológicas e comunicação social.

Nesse novo cenário global em construção no século XXI, com as chamadas ameaças híbridas, os elementos de forças de operações especiais devem ganhar protagonismo no campo de batalha assimétrico, deixando para trás a condição de coadjuvantes das operações militares convencionais.

Assim, cada vez mais o Exército Brasileiro 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, comunicação social, e guerra cibernética. Essas capacidades devem ser amplamente desenvolvidas, de maneira que haja mais eficácia das operações de informação, no nível operacional. No 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 estão em intenso desenvolvimento, mas esbarram em problemas internos - uso combinado das capacidades relacionadas à informação - e externo - adequação do seu planejamento estratégico com os interesses de outras forças na realização de operações conjuntas - o que dificulta a necessidade real de integração e sincronização das capacidades relacionadas à informação e recursos relacionados às operações de informação. A Força Terrestre possui uma estrutura isolada dentro do próprio Exército, com sistemas fechados e com atividades bem específicas.

O ano de 2020, marcado pela Pandemia do COVID-19, serviu para realizar avaliações das condições de trabalho em home Office e da segurança cibernética, pois nesse momento a guerra cibernética e os crimes digitais tornaram-se as principais ameaças. A pandemia obrigou vários setores do governo brasileiro, incluindo a defesa, a trabalhar em casa. Nesse sentido, as análises de risco têm mostrado que o elo mais fraco da segurança cibernética é o homem. Assim sendo, as defesas cibernéticas deverão ficar atentas aos possíveis ataques por parte de

Estados oponentes ou de criminosos virtuais cada vez mais.

Com isso, efetivamente, ocorre um real crescimento dimensional do espaço cibernético. Além disso, percebe-se que o mundo está se tornando cada vez mais refém da tecnologia, pois o espaço cibernético tem atingido todas as áreas do nosso cotidiano, impactando na segurança das informações digitais, comunicações, sistemas de dados táticos e sistemas de armas. Nesse complexo ambiente informacional, é urgente fortalecer o setor de informacional, é urgente fortalecer o setor de defesa cibernética do Brasil. Em relação a esse ambiente cibernético, parece que estamos bastante defasados em relação ao resto do mundo, onde estão sendo criadas equipes táticas de guerra cibernética para operar junto às unidades operacionais. Além disso, seria fundamental, nesse novo ambiente de conflito, possuirmos tecnologias nacionais, a fim de suavizar as vulnerabilidades que poderão ser exploradas por um potencial oponente.

3. Recomendações

Estudos e debates conceituais sobre *guerra híbrida*

Aprofundar o estudo do conceito de Guerra híbrida a partir de discussões mais intensas, envolvendo especialistas militares e civis, a partir do Centro de Estudos Estratégicos do Exército. A partir desse debate conceitual, promover atualizações da Doutrina militar da Força Terrestre, considerando a complexidade do ambiente operacional atual, no qual as forças são levadas a atuar.

Diversificação dos conteúdos nos currículos das escolas militares

Incorporar ou diversificar conteúdos relacionados à geopolítica e à guerra híbrida nos currículos das escolas militares, de maneira que os quadros profissionais entendam as novas formas de fazer a guerra, em um ambiente de tensões geopolíticas da atualidade.

Incentivo à pesquisa científica sobre guerra híbrida

Incentivar a pesquisa científica sobre o uso da guerra híbrida nos conflitos da atualidade, articulada ao estudo da geopolítica, em todas as escolas militares, despertando o interesse e a manifestação de ideias que possam ajudar na construção de um pensamento militar moderno, a ser usado na transformação doutrinária.

Inclusão de elementos de *guerra híbrida* em exercícios

Incluir elementos da Guerra Híbrida no preparo e emprego das Forças, inclusive nos exercícios conjuntos.

Fernando da Silva Rodrigues

Atualização do pensamento militar

Atualizar o pensamento militar, pois com o domínio das informações, a Força Terrestre deve estar apta a: formular estratégias que contemplem o uso de meios não militares; desenvolver ações integradas e sinérgicas nos ambientes físicos, humano e informacional; combinar o uso de meios letais e não letais para se alcançar o objetivo final de um combate; usar de forma precisa e eficaz o poder de combate, com maior controle de danos e redução dos efeitos colaterais; oferecer respostas ágeis e flexíveis em ambientes em constante mudança; agregar valor psicológico às ações de combate; interagir com a mídia, órgãos de defesa dos direitos humanos, organizações não governamentais e outras agências estatais ou não estatais que possam estar presentes na área de operações; e, utilizar com habilidade os instrumentos jurídicos disponíveis, a fim de assegurar a legitimidade do uso da força.

Atualização do Manual de Campanha EB20–MC–10.213 Operações de Informação, incluindo formas de atuação de combate e de emprego da *guerra híbrida*

Atualizar a doutrina militar da Força Terrestre, considerando a complexidade do ambiente operacional atual, a partir do aprofundamento do estudo do conceito de guerra híbrida, promovido por discussões mais intensas com especialistas militares e civis, a partir do Centro de Estudos Estratégicos do Exército.

Aprofundamento de meios operacionais em operações assimétricas

Atentar para o uso de Novas Tecnologias da Informação, pois elas permitiram que muitas mudanças, ocorridas nas regras da guerra, tenham aberto as portas para o amplo uso de operações assimétricas no combate ao inimigo, principalmente por meio de Operações Psicológicas, Operações de Contra Inteligência, Operações de Contrapropaganda e Operações de Assuntos Civis. A Força Terrestre brasileira deve ficar atenta e aprofundar cada vez mais esses meios operacionais na guerra de informação.

Mentalidade estratégica de cooperação

Melhorar a mentalidade estratégica de cooperação, pois 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 modelo de guerra empregada pela Rússia na Ucrânia, em 2014, visto que se trata de 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.

Atenção às mudanças de realidade do combate

Atentar para as mudanças de realidade do combate, pois a forma tradicional de pensar e planejar a guerra tornou-se antiquada. Com os novos ambientes voláteis, incertos e ambíguos, que caracterizam a guerra na Era da Informação do século XXI, não há mais condições de abordagens simplistas. Na atualidade, um grande número de fatores não militares tem interferido, e, até mesmo, inviabilizado o processo tradicional de decisão, calculado no estudo do terreno, do inimigo e das condições meteorológicas. Nesse sentido, cada vez mais ferramentas de pensamento complexo devem ser incorporadas à metodologia de planejamento tático, operacional e estratégico, para proporcionar coerência sistemática ao uso do instrumento militar.

Capacidades contra Forças Irregulares

Enfatizar o preparo e desenvolvimento de capacidades da Força Terrestre contra forças irregulares.

Priorização do emprego de tropas especializadas de combate

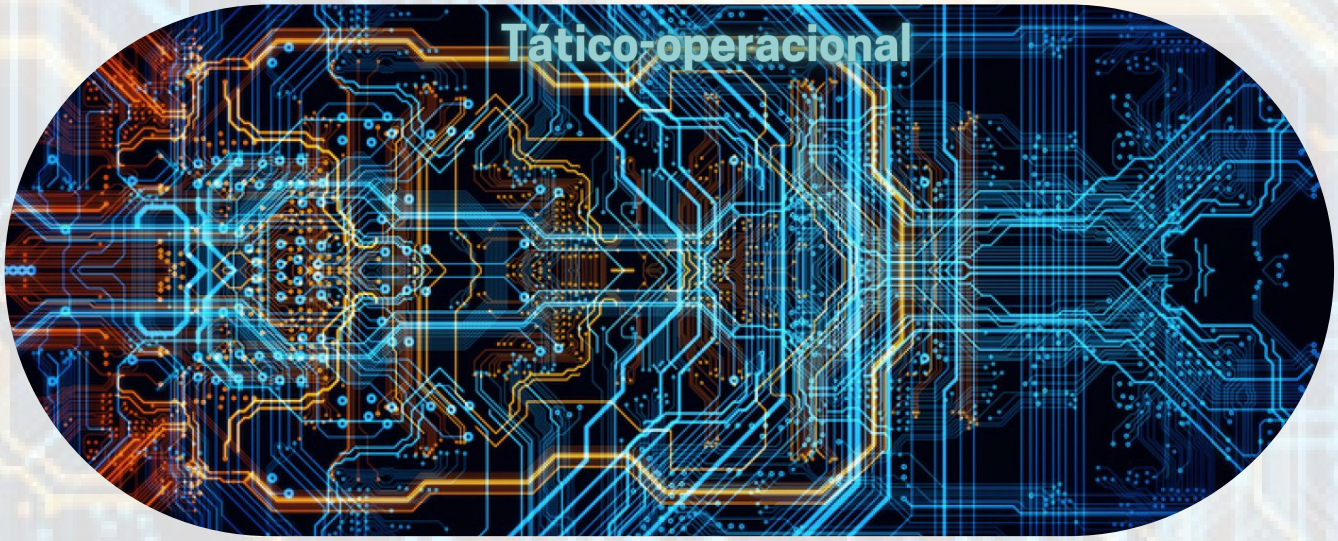
Atentar para um processo controlado de diminuição do efetivo das tropas regulares, usadas para a manutenção da Estratégia da Presença e para ações subsidiárias, priorizando, ainda mais, o emprego das tropas especializadas de combate, tornando o Exército mais leve e ágil, amparado no uso de novas tecnologias e sistemas de armas. Talvez, seja o caso modificar algumas unidades convencionais para emprego contra forças irregulares.

Atenção aos novos meios operacionais da guerra de informação

Atentar para o uso de Novas Tecnologias da Informação, pois elas permitiram que muitas mudanças, ocorridas nas regras da guerra, tenham aberto as portas para o amplo uso de operações assimétricas no combate ao inimigo, principalmente por meio de Operações Psicológicas, Operações de Contra Inteligência, Operações de Contrapropaganda e Operações de Assuntos Civis. A Força Terrestre brasileira deve ficar atenta e aprofundar cada vez mais esses meios operacionais na guerra de informação.

Mentalidade estratégica de cooperação

Melhorar a mentalidade estratégica de cooperação, pois 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 modelo de guerra empregada pela Rússia na Ucrânia, em 2014, visto que se trata de 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.



Desenvolvimento de dispositivos de proteção adequados aos SI

Atentar, cada vez mais, para o desenvolvimento de dispositivos de proteção adequados aos seus sistemas de informação. 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 ataques cibernéticos.

Atenção aos novos meios operacionais da guerra de informação

Atentar para o uso de Novas Tecnologias da Informação, pois elas permitiram que muitas mudanças, ocorridas nas regras da guerra, tenham aberto as portas para o amplo uso de operações assimétricas no combate ao inimigo, principalmente por meio de Operações Psicológicas, Operações de Contra Inteligência, Operações de Contrapropaganda e Operações de Assuntos Civis. A Força Terrestre brasileira deve ficar atenta e aprofundar cada vez mais esses meios operacionais na guerra de informação.

Ênfase na Defesa Cibernética

Aumentar a preocupação com a defesa cibernética brasileira e com a segurança nacional, contra potenciais ataques cibernéticos aos setores estratégicos e às infraestruturas críticas do país. O ataque hacker ao sistema de tecnologia da informação da EMBRAER e a tentativa de ataque ao sistema do Tribunal Superior Eleitoral, em 2020, exemplificam essa relevância. O Brasil ainda possui muitas fragilidades e vulnerabilidades na internet, somadas a poucos recursos orçamentários para o setor e pouca disponibilidade de mão de obra de qualidade para ser empregada na área de defesa cibernética.

Unidades de combate especializadas

Dotar a Força Terrestre com unidades militares de combate (batalhão) que integrem variadas capacidades como: guerra eletrônica, defesa antiaérea e apoio de fogos de longo alcance. Nesse sentido, é importante citar a concepção da Força Terrestre Componente (FTC) no contexto de um comando de operações conjuntas. A FTC constitui o elemento responsável por conectar os meios da Força Terrestre no esforço conjunto, contribuindo para o sucesso das operações, visando à eficácia das operações terrestres sem, entretanto, negligenciar a doutrina e as especificidades do EB.

Treinamento e Capacitação de pessoal

Intensificar o treinamento e a capacitação de pessoal das Forças de Operações Especiais, Operações de Informação e de Inteligência.

Preparo da tropa regular, por meio do apoio dos FE

Intensificar o uso de elementos das Forças de Operações Especiais, na preparação da tropa regular, por meio de disseminação de táticas, técnicas e procedimentos até então restritos às Forças de Operações Especiais e à expansão dos núcleos profissionais de operações especiais. Além disso, é necessário enfatizar o melhoramento na qualificação dos recursos humanos das forças convencionais, preparadas pelas forças de operações especiais, e a adoção de estruturas organizacionais mais leves e ágeis, para execução de determinadas tarefas, o que facilitaria a preservação física e mental com a subutilização das forças especiais.

Comunicação estratégica em sinergia com outras organizações nacionais responsáveis pela defesa

Atentar para a comunicação estratégica (comunicação social tradicional e mídias digitais com objetivo de conquista de objetivos institucionais), a dimensão informacional e as atividades de interação do 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 e se torne mais pró-ativo ao invés de reativo, dando ênfase aos estudos e à preparação às novas ameaças, em sinergia e cooperação com outras organizações nacionais responsáveis pela segurança e pela defesa.

Atenção aos sistemas com capacidade de proteção e vigilância

Atentar ao funcionamento dos modernos sistemas com capacidade de proteção e vigilância do território nacional, dando continuidade e intensificando projetos como o Sistema Integrado de Monitoramento de Fronteiras (SISFRON), que, além de monitorar as áreas de fronteiras, deve assegurar o fluxo contínuo e seguro de dados entre diversos escalões da Força Terrestre.