ISSN: 2525-457X
ANÁLISE ESTRATÉGICA
VOL 21 (3) JUN/AGOSTO 2021

AVALIAÇÃO DAS IMPLICAÇÕES DO CONCEITO DE GUERRA HÍBRIDA PARA A SEGURANÇA NACIONAL

EVALUATION OF THE IMPLICATIONS OF THE CONCEPT OF HYBRID WAR FOR NATIONAL SECURITY

Fernando da Silva Rodrigues

RESUMO

Este artigo investigou as implicações do conceito de Guerra Híbrida, a partir da evolução das formas de fazer a guerra na atualidade. As seções foram desenvolvidas em quatro partes. Na primeira, foi feita a introdução ao estudo, na qual desenvolvemos o conceito de *Segurança Nacional* ao longo da história do Estado Moderno, com a assinatura do Tratado de Westfália, em 1648, articulado à definição do conceito de *Guerra Híbrida*. Na segunda, abordamos o conceito de *Guerra da Informação* como dimensão do espaço da batalha ao longo do século XXI, assim como seu impacto na formação de novos conceitos. Na terceira parte, discutimos as novas ameaças do século XXI, entendidas como ameaças híbridas no contexto da segurança contra a guerra cibernética. Por fim, foram apresentadas reflexões finais e implicações para o Exército Brasileiro.

ABSTRACT

The objective of the investigation is to evaluate the implications of the concept of hybrid war, based on the evolution of the ways of making war theoretically recognized today, for National Security in Brazil. The article sections were developed in four parts. The first refers to the introduction to the study, where we developed the concept of national security throughout the history of the Modern State, with the signing of the Treaty of Westphalia, in 1648, articulating the definition of the concept of Hybrid War. The second part involves the construction of the concept of information warfare as a battle space dimension throughout the 21st century, and how it impacted the formation of new concepts. The third part proposed to discuss the new threats of the 21st century, understood as hybrid threats in the context of security against cyber warfare. Finally, final reflections and implications for the Brazilian Army were presented.

PALAVRAS-CHAVE:
Segurança Nacional. Guerra Híbrida. Guerra da Informação. Guerra Cibernética.

KEYWORDS:
National security. Hybrid War. Information War. Cyber War.

*Doutor em História Política, professor titular 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

Este artigo tem por objetivo avaliar as implicações do conceito de guerra híbrida, desenvolvido ao longo de três ensaios (RODRIGUES, 2020, 2021a, 2021b), 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, relacionada à análise da operacionalidade do conceito de Guerra Híbrida nos conflitos contemporâneos e seu suposto impacto para a Segurança Nacional.

Desde a assinatura do Tratado de Westfália, a Segurança Nacional é uma prerrogativa do Estado moderno. O objetivo é assegurar, em todos os lugares, a todo o momento, e em todas as circunstâncias, a integridade do território, a proteção da população e a soberania contra todo tipo de ameaça e agressão externa ou interna. Com o novo cenário após a Guerra Fria e o avanço da dimensão tecno-informacional no campo de batalha, a preocupação com as ameaças híbridas passou a ser considerada como parte importante na política de segurança dos Estados, balizada pelo caso da anexação da Crimeia em 2014, quando foram empregados ataques contra as infraestruturas críticas, as conexões de internet e os meios de comunicação local.

Como parte da evolução dos conflitos, nos anos 1990, ocorreram intensos debates sobre as operações de informações e a guerra de informações, que consolidaram essa forma de fazer a guerra. O termo guerra de informação passou a ser utilizado para tipificar novos modos de combate em que a destruição física não ocupava mais o lugar principal da tática operacional. As operações de informação podem ser utilizadas para modificar o ambiente operacional, por meio de um conjunto de atividades, predominantemente não militares, que são orientadas para a identificação de potenciais riscos e de fontes perenes de instabilidade, além da redução de antagonismos e erradicação de ameaças em sua origem. A sua principal característica é a prioridade para as dimensões informacional e humana do ambiente operacional. No século XI, as operações de informação visam moldar a percepção do inimigo sobre as suas intenções e chances de vitória. É a ideia de que a cognição, o aparato mental do adversário, como por exemplo a opinião pública, é um centro de gravidade a ser atingido mediante operações de informação.

Nesse sentido, a complexidade do ambiente de operações no século XXI sugere a evolução no pensamento militar doutrinário em relação às novas formas de guerrear. Assim sendo, com a atualização da Estratégia Nacional de Defesa (END), observa-se que o investimento na Defesa passou a se desenvolver baseado na capacidade de monitorar/controlar o território nacional e o seu entorno estratégico, com intensificação do importante papel destinado às capacidades de informação em setores estratégicos, como o cibernético. Com a END 2020, adota-se um conceito de segurança ampliado, que passa a abranger os campos políticos, militar, econômico, psicossocial, científico-tecnológico e ambiental.

Por fim, ao longo do estudo, ficou claro, que a Guerra Híbrida é caracterizada pela intensificação do uso de meios irregulares no nível político-estratégico, por ser um tipo de guerra com modelagem militar estatal e tropa privada usada em atividades clandestinas. Nesse contexto, 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 a solução dos problemas militares contemporâneos, como o uso combinado do emprego de forças especiais com guerra cibernética, ou operações de informações e operações de dissimulação.

1. Introdução

A Segurança Nacional é considerada historicamente, como uma atribuição fundamental do Estado moderno, desde a assinatura do Tratado de Westfália em 1648. O objetivo é assegurar, em todos os lugares, a todo o momento e em todas as circunstâncias, a integridade do território, a proteção da população e a soberania contra todo tipo de ameaça e agressão externa ou interna. Com esse paradigma, a origem de qualquer Estado pressupõe a criação e delimitação de suas fronteiras, sendo elas necessárias para assegurar a soberania e a defesa do país. Na atualidade, a Segurança Nacional continua com a ideia original de que o Estado está no centro do debate, com a capacidade militar estatal como fiadora desse modelo (HERZ, 2010). Essa ideia remete ao Estado *hobbesiano* cuja noção de fronteira serve legitimamente como parte da proteção do território. Para o autor do *Leviatã*, esse Estado deveria ser forte, com a capacidade de superar o terror que caracteriza o estado por natureza, com os indivíduos movidos pelos sentidos e pelas paixões, inerentes à essência do homem natural. A **figura 1** sintetiza a visão de Hobbes a respeito da função do Estado e do seu soberano como promotor da segurança e da defesa tanto de problemas internos, quanto de ameaças externas.

> E dado que a condição do homem [...] é uma condição de guerra de todos contra todos, sendo, neste caso, cada um governado por sua própria razão [...], segue-se daqui que numa tal condição todo homem tem direito a todas as coisas [...]" (HOBBES, 1979, p. 78).

Figura 1: Leviatã

Fonte: https://pt.wikipedia.org/wiki/Leviatã_(livro)

Nesse sentido, a fronteira foi utilizada, frequentemente, como elemento de proteção. Assim, desde os primeiros delineamentos, a linha de fronteira caracterizou-se como um elemento de vulnerabilidade natural, apesar do significado inicial de demarcação geográfica como fruto da preocupação política em isolar as populações em seus respectivos territórios.

Na atualidade, corroborando com a definição histórica de *Segurança Nacional*, o manual sobre Fundamentos do Poder Nacional, da Escola Superior de Guerra (2019, p. 153), define basicamente o conceito como: "Segurança Nacional é a condição que permite a preservação da soberania e da integridade territorial, a realização dos interesses nacionais, livre de pressões e ameaças de qualquer natureza, e a garantia aos cidadãos do exercício dos direitos e deveres constitucionais". Nesse processo em andamento, mais do que uma simples continuidade de atribuição, o conceito de segurança nacional foi sendo alterado, ao longo de mais de trezentos anos, no contexto da evolução histórica das civilizações mundiais e na evolução do debate sobre o conceito de fronteiras.

O debate em torno do conceito de *fronteira* envolve uma discussão entre distintas áreas do conhecimento. A Geografia, por exemplo, destaca-se por ser a área que mais tem se dedicado a essa investigação, especialmente no campo da Geopolítica. Foucher (1986) afirma que as fronteiras se inserem na formação territorial do Estado moderno e que seu surgimento se deu a partir de estruturas espaciais, de modo linear, sendo constituídas de duas partes, uma interna e outra externa, que visam a manter a soberania nacional.

Do ponto de vista do Realismo nas Relações Internacionais, as fronteiras são imaginadas a partir da perspectiva *estadocêntrica*, ou seja, somente seriam relevantes porque representam uma região delicada para o Estado, reduzindo-se a questões de defesa e soberania. Quando analisamos a teoria do Liberalismo, entretanto, a definição de fronteira se torna mais flexível, mesmo que a noção de região de fronteira seja igualmente considerada secundária. Sob tal perspectiva, a globalização cria redes que não respeitariam as fronteiras nacionais delimitadas. Essas redes são tanto de atividades lícitas (comércio, finanças), quanto ilícitas (tráfico de drogas, armas, pessoas, imigração ilegal), sendo que as últimas comprometem a Segurança do Estado, podendo criar fissuras na sociedade. Nesse caso, caberia aos Estados intervir nas fronteiras de modo a controlar os fluxos, facilitando a entrada dos fluxos de interesse e restringindo as redes de ilícitos (SHERMA, 2012, p. 11-12).

No contexto dessas evoluções, a *Segurança Nacional* pode ser entendida, com ênfase em três dimensões: a política, a

jurídica e a militar. A dimensão política é a principal delas e articula os interesses do Estado com todas as forças existentes e seus agentes estatais. A dimensão jurídica é a que proporciona a legalidade do ambiente. A dimensão militar dá corpo e garante a aplicação às dimensões política e jurídica (COSTA; 2018, p. 125). Para fins de uma definição mais atual, segurança nacional não deve ser confundida com segurança pública, nem com a "Doutrina de Segurança Nacional[1]".

Como observamos no início do nosso estudo, desde o século XVII, o Estado possui atribuições exclusivas como o monopólio do uso da força e o estabelecimento e manutenção da ordem e paz social. Para o desenvolvimento dessas ações, o Estado pode usar o poder militar, político, econômico ou diplomático, sendo o último empregado para estabelecer alianças, tratados e acordos internacionais. Um dos meios utilizados para garantir a segurança nacional no mundo contemporâneo tem sido o uso, com mais intensidade, de atividades de Inteligência, de Contrainteligência, Guerra Eletrônica, uso de Forças Especiais e de Segurança Cibernética, na prevenção à espionagem, atentados terroristas ou contra-ataques cibernéticos.

O conceito de *Guerra Híbrida* apareceu no início do século XXI, quando as forças armadas ocidentais se viram no meio de operações militares complexas, como foi a guerra no Afeganistão, em 2001, e no Iraque, em 2003. A partir desse momento, os analistas tentaram entender o que seria esse novo e complexo tipo de guerra que estava sendo realizado. No entanto, o tema ganhou grande projeção nos debates envolvendo a Guerra Russo-Ucraniana em 2014, 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 seus estudos e planejamentos com relação ao emprego da guerra híbrida, entendida como parte integral da doutrina militar russa.

O conceito de *Guerra Híbrida*, nesse estudo, foi elaborado ao longo de intensas investigações (RODRIGUES, 2020, 2021a, 2021b), evidenciando que a sua definição não é tão recente assim e não surgiu com a interpretação do conflito da Rússia com a Ucrânia em 2014, tendo sua origem na evolução complexa das teorias da guerra de quarta geração (LIND, 2004), guerras compostas (HUBER, 2002), guerras irrestritas (LIANG e XIANGSUI, 1999) e guerras irregulares (HEYDTE, 1990). Nesse caso, a guerra híbrida é entendida, como forma de operacionalizar a guerra, quando falamos de

[1] Como parte dos desdobramentos da Guerra Fria e do processo de descolonização da África e da Ásia, os EUA elaboraram essa doutrina militar baseada no conceito de segurança e desenvolvimento, que tinha como um dos seus objetivos combater a guerra não convencional ou revolucionária, considerada a principal ameaça estratégica vinda do comunismo internacional e que visava conquistar os países do chamado "Terceiro Mundo" (COMBLIM, 1978, P. 44).

uma atividade em si, em referência aos tipos de armas, métodos, teorias, natureza da guerra, dentre outros detalhes associados ao combate.

Sobre a terminologia, a tradução de *War*[2] (guerra, fenômeno) é mais abrangente, mais totalizante, pois representa a luta entre dois ou mais Estados, ou seja, o conflito entre grandes potências, no contexto pela disputa geopolítica e pela definição de uma ordem internacional (TEIXEIRA JÚNIOR, 2019, p. 18). Já o termo *warfare*[3] representa a manifestação do fenômeno em formas de lutar (ofensiva, defensiva, guerra irregular), sendo usado para analisar subsistemas e subdivisões de um todo que é a guerra. Nesse sentido, acreditamos que a definição do conceito de *Guerra Híbrida*, do ponto de vista teórico, assume uma grande importância estratégica para o emprego militar do Exército Brasileiro, no contexto de mudanças paradigmáticas dos conflitos contemporâneos, como foi o caráter híbrido da conduta da guerra russa na Ucrânia, em 2014.

Nesse sentido, a possibilidade de conflito com operações de combate com pouca definição no tempo e no espaço, disputado em diferentes níveis, por forças estatais e não estatais, indica que, provavelmente, a guerra no futuro tende a ser cada vez mais incerta, com dificuldades para identificação do inimigo dominante e para definição de suas categorias operativas. No entanto, fica claro, que "a atuação do instrumento militar tenderá a se dar cada vez mais nas Operações Militares em Ambiente Urbano (MOUT)", em detrimento de espaços como selva, deserto, montanha, etc (com baixa densidade populacional) (TEIXEIRA JÚNIOR, 2019, p. 21).

O conceito de *Guerra Híbrida* expande as possibilidades de atuação dos atores estatais e não estatais, sendo que ambos podem usar da organização, técnicas, táticas e procedimentos operacionais (TTP) tanto da guerra regular, quanto da guerra irregular. Aqueles atores que recorrem ao uso da *Guerra Híbrida* têm como objetivo dominar o controle operacional sem restrições, podendo ultrapassar as fronteiras, as leis impostas e as leis morais da guerra. Nesse contexto, conforme **figura 2**, a *Guerra Híbrida* é definida como 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;

[2]"It is armed fighting between two or more countries or groups, or a particular example of this: First World War." Cambridge Dictionary. Disponível em: https://dictionary.cambridge.org/es/diccionario/ingles/war. Acesso em: 19 jul. 2021.

[3]"It is the activity of fighting a war, often including the weapons and methods that are used: guerrilla, naval, nuclear, trench warfare." Cambridge Dictionary. Disponível em: https://dictionary.cambridge.org/es/diccionario/ingles/warfare. Acesso em: 19 jul. 2021.

- propaganda com guerra de informação;
- apoio à manifestação local;
- operações psicológicas;
- Guerra Eletrônica;
- e outras.

Portanto, é importante frisar que a operacionalização da guerra híbrida demanda coordenação da estratégia militar com a estratégia nacional, em uma grande estratégia.

Figura 2: Alguns meios possíveis de combinação da Guerra Híbrida

Fonte: o autor.

A característica omnidimensional da guerra, fase anterior ao emprego de combates tradicionais, levanta a necessidade de que todos os poderes nacionais estejam em condições de atuar nos novos espaços criados por recentes dimensões do campo de batalha, o qual não é mais tradicional, conforme as Forças Armadas estavam habituadas a lutar. Além disso, o fenômeno demonstra necessidade de uma gestão unificada e integrada das inovações tecnológicas e não tecnológicas no setor de Defesa. Nesse caso, o Brasil precisará estar preparado para se defender em um ambiente de amplo espectro, pois os conflitos no futuro deverão acontecer em todas as dimensões do campo de batalha (Guerra Omnidimensional[4]). O avanço do conflito omnidimensional pode ser atribuído ao desgaste das instituições democráticas, pelas campanhas de desinformação, pela corrupção generalizada em todos os níveis de governo, e pela crescente perda de confiança na política.

Assim sendo, podemos aferir para a *Guerra Híbrida* uma forma real de compreensão da dinâmica dos conflitos. As tensões sociais e políticas tiveram um amplo impacto no desenvolvimento do modelo de guerra atual e no uso da força por diversos atores. Nesse caso, podemos afirmar, que é cada vez mais difícil definir e separar os atores, o modo de combater, os espaços do confronto e os instrumentos da guerra. No entanto, alguns princípios básicos podem ser usados para caracterizar a Guerra Híbrida: a sinergia de atores, a assimetria do conflito, a guerra omnidimensional anterior ao emprego de combates tradicionais, a segurança multidimensional, a criatividade, e os interesses políticos.

Como ilustra a **figura 3**, a *Guerra Híbrida* envolve operações que mesclam conflito convencional com conflito não convencional, guerra regular com guerra irregular, guerra eletrônica com guerra cibernética, dentre outras combinações possíveis. Assim, será cada vez mais necessário aprimorar o uso de operações de informações articuladas ao emprego de tropas de forças especiais contra ameaças difusas, associado ao emprego conjunto das Forças Armadas, o ambiente interagências e, se for o caso, às operações multinacionais.

[4]A análise da Guerra Omnidimensional é diacrônica, ou seja, deve ser realizada levando-se em consideração a evolução temporal do conflito: ataques financeiros; cibernéticos; batalhas baseadas em rede, com alvos estratégicos; suspensão temporária ou total da rede de internet ou de suas funcionalidades; ataques terroristas discretos ou de grande impacto. Todas essas ações fazem parte de uma escalada do conflito, que pode culminar num combate militar tradicional de segunda e terceira dimensão. (MOTA e AZEVEDO, 2012)

Figura 3: Princípios Básicos da *Guerra Híbrida*

Fonte: o autor.

Para Hoffman (2007), a guerra se caracteriza por diferentes tipos de conflitos, com diversidade de combatentes e de emprego de tecnologias, além de um amplo uso de forças, feito por adversários flexíveis e sofisticados. Sugere que os conflitos deverão incluir organizações híbridas - como a Força Paramilitar do *Hezbollah* contra Israel - empregando um amplo conjunto de habilidades. Para o autor, é possível que, exista a possibilidade dos Estados modificarem suas unidades convencionais em forças irregulares, com ênfase nas tropas especiais, contemplando o uso de diversas formas de guerra, inclusive de guerra híbrida estatal, com estruturas políticas funcionando em células descentralizadas e com o aparecimento de forças irregulares decisivas para o combate ou em condições de igualdade com as forças regulares

Pelo postulado de Frank Hoffman (2007), podemos aferir para a *Guerra Híbrida* uma forma real de compreensão da dinâmica dos conflitos. As tensões sociais e políticas tiveram um amplo impacto no desenvolvimento da guerra atual e no uso da força pelos diversos atores, tornando-se cada vez mais difícil definir e separar os atores, o modo de combater, os espaços do confronto e os instrumentos da guerra, os quais caminham para o campo da incerteza.

O futuro aponta, ainda, para a ampliação de conflitos de menor intensidade conduzidos por guerrilhas, milícias urbanas, facções criminosas, grupos terroristas, organizações político-partidárias extremistas e crime organizado. Cabe ressaltar que, além das ameaças híbridas, sempre haverá o risco de envolvimento em guerras regulares estatais definidas por combates em larga escala, para os quais o preparo da força não pode ser negligenciado.

Figura 4: Conflitos de menor intensidade no cenário futuro

Fonte: o autor.

Historicamente, após o fim da Guerra Fria e com a desintegração da antiga União das Repúblicas Socialistas Soviéticas (URSS), em 1991, o mundo saiu da divisão doutrinária e ideológica caracterizada pela bipolaridade (capitalistas x comunistas), para entrar na era "unimultipolar". De acordo com por Samuel Huntington, tratava-se da época em que ocorria a centralização de poder militar pelos Estados Unidos, porém, no campo econômico, havia várias outras potências. Atualmente, percebe-se uma tendência geopolítica caracterizada pela multipolaridade. Nesse novo cenário complexo, consolidado no século XXI, a preocupação contra as ameaças híbridas passou a ser um item importante na política de segurança dos Estados Nacionais.

Observa-se, na atualidade, a proliferação de ataques cibernéticos, como ferramenta da guerra de informação, articulada a outros meios, como: sistema de inteligência, de contrainteligência, de desativação do sistema de comunicações, de degradação do auxílio de navegação e de destruição da capacidade operacional dos computadores do inimigo. Exemplo disso foi a atuação de *hackers* russos na Guerra da Geórgia, em 2008, e na Guerra da Ucrânia, em 2014, ao atacarem diferentes alvos, desde partidos políticos a infraestruturas críticas, estabelecendo novos padrões para a guerra cibernética. Nesse contexto, em estudo sobre a guerra híbrida desencadeada pela Rússia contra a Ucrânia, entre 2014 e 2015, o questionamento de Marco Aurélio Guedes e Fernando Casalunga nos ajuda a entender como a tecnologia da informação ampliou a assimetria de poder entre os Estados contemporâneos. Os autores afirmam que, com o avanço das tecnologias de informação, o ciberespaço se tornou fulcral para projeção do poder russo no seu entorno regional:

> ao utilizar o ciberespaço para auxiliar as operações militares, a simbiose inovadora entre setores especiais das Forças Armadas russas e *hackers* civis produziu efeito sinérgico que resultou em vantagem considerável à Rússia durante o conflito com a anexação do território da península da Crimeia e apoio aos movimentos separatistas que ocuparam a região leste da Ucrânia (OLIVEIRA e CASALUNGA, 2020, p. 13).

Segundo Teixeira Júnior (2001, p. 20), as tendências da conduta da guerra no século XXI, que inclui a incorporação do espaço cibernético aos domínios terrestre, marítimo, aéreo e espacial, poderão evidenciar mudanças estruturais na condução das operações. Para o autor, será algo semelhante ao impacto que as "armas combinadas" tiveram na inovação militar no século XX. Nesse novo cenário, a capacidade das forças em operar em multidomínios reforçará a importância dos Estados-Maiores Conjuntos ou dos Comandos Unificados, a exemplo dos Estados Unidos.

Dialogando frente a esse complexo ambiente operacional, o *Manual de*

Operações de Informação do Exército (EB20-MC- 10.213) mostra como a dimensão informacional tornou-se essencial e como as capacidades relacionadas à Informação podem ser efetivamente integradas e exploradas nas operações militares.

> Diante do ambiente operacional em contínua transformação, onde a tecnologia infunde, na área da informação, junto à sociedade, mudanças cada vez mais rápidas, as Operações de Informação (Op Info) passam a ser uma aptidão essencial como instrumento integrador de capacidades relacionadas à informação, reunindo diversos vetores destinados a informar audiências amigas e influenciar públicos-alvo adversários e neutros, nas Operações no Amplo Espectro. Tais capacidades também se destinam a desgastar a tomada de decisão de potenciais oponentes, degradando a sua liberdade de ação, ao mesmo tempo protegendo o nosso processo decisório, visando, ainda, a evitar, impedir ou neutralizar os efeitos das ações adversárias na Dimensão Informacional (BRASIL; 2014, p. 2-7).

2. A Guerra de Informação no contexto da teoria da quarta geração

Entender o conceito de *Guerra de Informação* é condição indispensável para compreender o conceito de *Guerra Híbrida* no mundo Ocidental. Nesse contexto, um ponto importante é a análise evolutiva da teoria das gerações de conflito, proposta por William S. Lind, oficial do Exército norte-americano. Esse especialista assume como ponto de partida para seus debates o estabelecimento da *Paz de Westfália*, momento em que o Estado estabeleceu o monopólio da violência pela guerra e legitimou os direitos das nações em manterem e usarem força militar regular estatal. Apesar das limitações que restringem a construção teórica do autor à Era Moderna e da omissão dos componentes naval e aéreo, o trabalho de Lind pode ser uma escolha importante para os nossos estudos, por pensar na evolução da teoria geracional dos conflitos armados, acompanhada da transformação tecnológica militar, com seus efeitos táticos e estratégicos na diversidade de cenários dos conflitos (RODRIGUES, 2020, p. 24-25).

Para Lind (2004), a guerra de quarta geração surgiu após a 2ª Guerra Mundial, quando atores estatais e não estatais passaram a usar outros tipos de táticas, para compensar os diferentes níveis de capacidades tecnológicas. Pode ser observado no desenvolvimento dos conceitos da guerra de guerrilha, de insurgência e da guerra popular por descrever um tipo de conflito em que uma força com capacidades militares convencionais inferiores emprega meios de combate não convencionais ou irregulares, como forma de compensar as forças assimétricas no conflito.

Nesse sentido, a história indicava, ainda, que o Ocidente não teria mais o domínio cultural global, fato percebido quando aumentou consideravelmente a influência islâmica e asiática no mundo. Nesse novo momento, principalmente com o

fim da Guerra Fria, no contexto da Era da Informação, os conflitos migrariam para as cidades e a população sofreria diretamente as consequências dos embates; haveria o aumento de choques culturais e a geração de ações terroristas. A teoria indica o aumento da importância das tecnologias de alta precisão na obtenção de alvos, aprimoramento no armamento e proteção do combatente individual, meios de comunicação de difícil detecção, guerra cibernética, guerras psicológicas e guerras informacionais.

Nesse novo modelo de guerra, a população e sua cultura tornam-se alvos do ataque adversário. A guerra no Iraque e no Afeganistão, nos anos 1990, foi a base para o aperfeiçoamento da *teoria da guerra de quarta geração*. No entendimento de Lind (2004), o Estado perdeu o monopólio da violência e o mundo avançou no combate entre forças estatais e não estatais, como a *Al-Qaeda*, o *Hamas*, o *Hezbollah* e as *Forças Armadas Revolucionárias da Colômbia*.

O Coronel Visacro recupera o argumento de Lind (2004), reiterando que, na Era da Informação, diferentemente da Era Industrial, o monopólio da violência pelo Estado foi rompido, levando à fragmentação das ameaças e ao aparecimento de atores armados não estatais, tais como o *Hezbollah* e o *Hamas*, que empregam capacidades combinadas da guerra regular e da guerra irregular. Nesse cenário de incertezas e configuração difusa, temos o aumento da imprevisibilidade e a necessidade do preparo das forças armadas na composição por capacidades gerais, o que leva ao Ministério da Defesa a opção pelo planejamento baseado em capacidades da atualidade, focados na flexibilidade e mobilidade estratégica (VISACRO, 2018, p. 118).

Com a Era da Informação, têm-se a multiplicação dos meios militares e não militares empregados na condução de uma guerra, com prioridade de ações nos campos político, econômico e psicossocial, em detrimento dos esforços no campo militar. Atividades operacionais antes centralizadas no emprego militar passam a envolver a participação de outras agências estatais, ter influência de organizações internacionais, podendo ter a colaboração de organizações não-governamentais e a pressão da presença da mídia. Em um cenário como esse, é possível identificar uma grande quantidade de conflitos irregulares, assimétricos e intraestatais com potencialidade de internacionalização (VISACRO, 2019, p. 118).

A expressão *Guerra de Informação*[5] apareceu na literatura militar dos Estados Unidos da América, nos anos 1990, em consequência das duas grandes operações na

[5]Segundo o glossário de termos e expressões para o uso no Exército brasileiro, *guerra de informação* é o conjunto de ações destinadas a obter a superioridade das informações, afetando as redes de comunicação de um oponente e as informações que servem de base aos processos decisórios do adversário, ao mesmo tempo em que garante as informações e os processos amigos (BRASIL; 2018, p. 182).

Guerra do Golfo: *Desert Shield* (1990) e *Desert Storm* (1991). A Primeira Guerra do Golfo foi uma ação rápida, baseada no emprego da *Doutrina Powell*, cuja estratégia era dirigida às incertezas regionais, em substituição à guerra global contra a antiga URSS. Em apoio às operações de combate subsequentes, os EUA usaram o conceito DIME (*Diplomatic, Information, Military and Economic*), no denominado *soft power*, que gerou mudanças na doutrina de defesa do país. Alguns meses antes do início do conflito, foi realizada uma ampla campanha midiática contra a imagem de Saddam Hussein, o que contribuiu para a aplicação de sanções econômicas e militares, aprovadas por unanimidade pelo Conselho de Segurança da ONU e pela Liga dos Países Árabes.

Nesse contexto, a partir da Primeira Guerra do Golfo, a expressão *Guerra de Informação* passou a ser utilizada para classificar um novo modo de combate, em que a destruição física do oponente não ocupava mais o lugar principal da tática operacional. Segundo esse novo modelo, o uso de tecnologias serviria para coleta, processamento e difusão de informação no processo decisório do combate. A guerra de informação sairia dos bastidores e, articulada com a Revolução de Assuntos Militares (RMA), passaria a ser o principal elemento influenciador nas transformações da defesa baseada em tecnologia. O processo levou à exacerbação do fascínio pela RMA nos EUA e à transformação das Forças Armadas norte-americanas, que ocorreu também pela valorização do homem na dimensão da guerra, dividindo o protagonismo com a tecnologia. A centralidade pela tecnologia teria sido reflexo da própria imagem norte-americana espelhada em um desejo de ditar a conduta da guerra em seus próprios termos.

Nos EUA, o movimento de transformação levou ao estabelecimento da doutrina de Operações de Informações (Op Info) do Exército e à produção do Manual de Campanha 100-6, Operações de Informações (FM 100-6, *Information Operations*), de 1996, que dividiu as Op Info em cinco capacidades para apoio à destruição do oponente: (1) Operações Psicológicas (Op Psc); (2) Guerra Eletrônica (GE); (3) Operações de Redes Computacionais (Op R Compt); (4) Dissimulação Militar (Dsml Mil); e (5) Segurança das Operações (Seg Op) (RICHTER; 2009, p. 73).

Após os atentados de 11 de setembro de 2001 contra o *World Trade Center* e o Pentágono, as relações públicas e os assuntos civis (RP e As Civ) foram acrescidos como uma sexta capacidade. Primeiramente, em 2003, na revisão do *Information Operations* e, em 2006, na Publicação Conjunta 3-13, Operações de Informações (JP 3-13, *Information Operations*), do Departamento de Defesa (RICHTER; 2009, p. 72).

Para Correa (2012; p. 10), em 30 de outubro de 2003, o Secretário de Defesa dos

EUA, Donald H. Rumsfeld, aprovou o *Information Operations Roadmap* (IOR), um roteiro para as Op Info, que tornou esse modelo de operação uma competência militar primordial, estabelecendo diretrizes e metas para todos os sujeitos envolvidos com a Defesa, desde o nível político-estratégico até o nível tático operacional. Pelo IOR, o emprego das Op Info deve começar na paz, estender-se durante o conflito e só terminar após a restauração da paz e a conquista da instabilidade local.

Com relação ao Brasil, a doutrina militar do Exército define *ambiente operacional* como o conjunto de condições e circunstâncias que afetam o espaço de batalha onde as forças militares atuam e que interferem na forma como são empregadas, compreendendo três dimensões: física, humana e informacional, conforme **figura 5**. A dimensão física corresponde ao terreno do combate; a dimensão humana compreende os elementos relacionados às estruturas sociais, os comportamentos e interesses, normalmente geradores do conflito; e a dimensão informacional abrange os sistemas utilizados para obter, produzir, difundir e atuar sobre a informação (BRASIL; 2019, p. 2-1 e 2-2).

Figura 5: Ambiente Operacional

Fonte: o autor, com base em Manual de Doutrina Militar Terrestre, 2019.

Segundo o Manual de Operações de Informação do Exército, o conceito dessa operação consiste na atuação metodologicamente integrada de capacidade relacionada à informação, em conjunto com outros vetores, para informar e influenciar grupos ou indivíduos, bem como mudar a decisão do inimigo, ao mesmo tempo em que protege o seu processo decisório. As suas ações têm por objetivo evitar, impedir ou neutralizar os efeitos das atividades oponentes na dimensão informacional. As Op Info servem para obtenção de superioridade de informações e são integradas pelas capacidades relacionadas à informação, destacando-se a comunicação social, as operações de apoio à Informação, à Guerra Eletrônica, à Guerra Cibernética e à Inteligência (BRASIL; 2014, p. 3-1).

As Op Info podem ser utilizadas para modificar o ambiente operacional, por meio de um conjunto de atividades, predominantemente não militares, que são orientadas para a identificação de potenciais riscos e de fontes perenes de instabilidade; para a redução de antagonismos e erradicação de ameaças em sua origem; e para a interrupção da cadeia de eventos que possam levar ao agravamento de uma crise ou à deflagração de um conflito. As suas principais características são: prioridade para as dimensões informacional e humana do ambiente operacional; condicionada por diplomas legais; coesão em todos os níveis de planejamento; coordenação com todas as atividades e tarefas; flexibilidade na dosagem do esforço; importância da atividade de inteligência; ampla abrangência das operações de informação (pessoal e material); e adicionar poder de combate (BRASIL; 2014, p. 3-3). Com base nessa discussão, entraremos no próximo tópico que liga o espaço cibernético à arena informacional.

3. As novas ameaças do século XXI no contexto da guerra cibernética

O espaço cibernético é um domínio global dentro da dimensão informacional do ambiente operacional que consiste em uma rede independente de infraestruturas de Tecnologia da Informação e Comunicação e de dados residentes, incluindo a internet, rede de telecomunicações, controladores, sistemas de computador e processadores embarcados. As ações cibernéticas (exploração, ataque e proteção) materializam o emprego de recursos do espaço cibernético e têm por objetivo: proteger os próprios ativos de informações; explorar e atacar redes do inimigo, mantendo a capacidade de interferir no desenrolar das operações militares no espaço de batalha; bem como afetar as condições de normalidade em uma determinada área ou região, atingindo gravemente o funcionamento de estruturas estratégicas e serviços essenciais destinados à população (BRASIL; 2014, p. 4-8).

Nos EUA, a preocupação com o ciberespaço iniciou-se em 1988 e materializou-se com o lançamento da primeira *National Strategy to Secure Cyberspace*, em 2003 (SOESANTOS; 2019, p. 3). No mês de setembro de 2018 foi apresentada a atualização da *National Cyber Strategy of the United States of America*[6], como parte evolutiva da segurança cibernética norte-americana.

O ciberespaço ou espaço cibernético é reconhecido como a descrição do espaço não físico formado pela rede mundial de computadores, notadamente a internet, onde as pessoas podem interagir de diferentes maneiras, por meio de mensagens eletrônicas, salas de bate-papo, grupos de discussão e outros (CANONGIA e MANDARINO JUNIOR; 2009, p. 25). Na atualidade, achamos prudente acrescentar as redes sociais como forma de comunicação.

Em 2009, tanto o conceito de Segurança Cibernética quanto o de Defesa Cibernética ainda estavam em construção no Brasil. Naquele momento, de uma maneira bastante simplificada, entendia-se que a atuação da segurança cibernética compreendia aspectos e atitudes de prevenção e repressão (CANONGIA e MANDARINO JUNIOR; 2009, p. 25-26). O ano de 2009 é paradigmático, pois a primeira iniciativa governamental com relação ao setor cibernético ocorreu com a Diretriz Ministerial nº 014, do Ministério da Defesa, que atribuiu à Força Terrestre a responsabilidade pela coordenação e pela integração da atividade.

No caso brasileiro, somente em 2020 foi aprovada a primeira Estratégia Nacional de Segurança Cibernética, sob a responsabilidade do Gabinete de Segurança Institucional. No documento, constam os seguintes objetivos estratégicos: (a) tornar o Brasil mais próspero e confiável no ambiente digital; (b) aumentar a resiliência brasileira às ameaças cibernéticas; e (c) fortalecer a atuação brasileira em segurança cibernética no cenário internacional. Em 17 de novembro de 2020, o Ministério da Defesa criou o Sistema Militar de Defesa Cibernética (SMDC), por meio da Portaria nº 3.781/GM-MD, em cumprimento à Política Cibernética de Defesa, aprovada pela Portaria Normativa nº 3.389/MD, de 21 de dezembro de 2012, com o objetivo de ser aplicada nos grandes eventos que o Brasil sediaria: Copa das Confederações de 2013, Copa do Mundo de 2014 e Jogos Olímpicos de 2016. O SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional. O órgão central é o Comando de Defesa Cibernética, comando operacional conjunto permanentemente ativado.

[6]Disponível em: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Acesso em: 15 jan. 2021.

Em 2018, observando o *Glossário de Termos e Expressões para uso no Exército*, podemos perceber que, nove anos depois dos primeiros conceitos produzidos no Brasil, houve uma grande evolução no pensamento militar em relação ao espaço cibernético, pois o dicionário define o termo cibernético em referência a acesso, segurança, controle e fluxo de dados por redes de computadores (internet ou intranet). A Defesa Nacional inclui, no conceito, os recursos de tecnologia da informação e comunicações de cunho estratégico, tais como aqueles que compõem o Sistema Militar de Comando e Controle, os sistemas de armas e vigilâncias e os sistemas administrativos que possam afetar as atividades operacionais (BRASIL; 2018, p. 78).

No glossário do Exército, o conceito de *Defesa Cibernética* refere-se ao conjunto de ações relacionadas ao espaço cibernético, no contexto de um planejamento nacional de nível estratégico, coordenadas e integradas pelo Ministério da Defesa, com a finalidade de proteger os sistemas ativos de informação de interesse do MD, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente. A Defesa Cibernética engloba a execução de ações defensivas, exploratórias e ofensivas no espaço cibernético e as iniciativas para geração dessas capacidades no Comando do Exército e no Ministério da Defesa, de maneira que também possa atuar em grandes eventos. Já o conceito de *Segurança Cibernética* é definido como o conjunto de ações no nível político, coordenadas pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), a fim de viabilizar a proteção, no espaço cibernético, dos ativos e das infraestruturas críticas[7]. Nessas ações, incluem-se: a elaboração de marcos jurídicos, a criação de estruturas governamentais e a expedição de Políticas e Estratégias Nacionais relacionadas ao setor cibernético. Em síntese, a Segurança Cibernética é a arte de assegurar a existência e a continuidade da sociedade da informação de uma nação, garantindo e protegendo, no espaço cibernético, seus ativos de informação e suas infraestruturas críticas (BRASIL; 2018, p. 109 e 344).

Nesse contexto, o Comando de Defesa Cibernética coordena e integra operacionalmente, em ambiente interagências, as ações de Segurança e Defesa Cibernética contra ameaças hostis em todo território brasileiro. No caso o GSI, atua no campo da política nacional coordenando o planejamento da segurança da informação e a elaboração da Estratégia Nacional de Segurança Cibernética (BRASIL, 2020).

[7]De acordo com a Política Nacional de Segurança de Infraestruturas Críticas são instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade. (BRASIL, 2018)

Essa evolução doutrinária com relação aos conceitos pode ser percebida na Estratégia Nacional de Defesa (END) de 2012, que incorpora a ideia de Defesa com base na capacidade de monitorar/controlar o território nacional e o seu entorno estratégico, com intensificação do importante papel destinado às capacidades de informação em setores estratégicos, como o cibernético. No documento, o conceito de segurança foi ampliado, passando a abranger os campos políticos, militar, econômico, psicossocial, científico-tecnológico e ambiental.

Segundo o Manual de Operações de Informação do Exército, as capacidades relacionadas à informação são aptidões requeridas para afetar a capacidade inimiga ou potenciais adversários de orientar, obter, produzir ou difundir informações, em qualquer uma das três perspectivas da dimensão informacional: a física, formada por homens e instalações; a cognitiva, formada pelo nível mental e a lógica, formada pelos sistemas. Como parte dessas capacidades, o manual trabalha com a definição e o uso da *Guerra Cibernética*, como parte da revolução tecnológica que a elevou à condição de interesse dos assuntos relacionados à Defesa e à Segurança.

As capacidades relacionadas à área Cibernética, quando são empregadas em apoio às Operações de Informação, normalmente são focadas na integração de ações ofensivas e defensivas executadas dentro ou por meio do espaço cibernético, em sintonia com outras capacidades relacionadas à informação e em coordenação com várias Linhas de Operação (direção do emprego) e Linhas de Esforço (tarefas definidas das operações) da Força Terrestre (BRASIL; 2014, p. 4-9).

Com uma nova abordagem paradigmática sobre o uso da segurança cibernética, o Tenente-coronel do Exército dos EUA, David Beskon, e a professora de computação social na *School of Computer Science* da *Carnegie Mellon University,* Kathleen Carley, identificaram a segurança **cibernética** como um subdomínio emergente da Segurança Nacional, que afetará todos os níveis da guerra do futuro, seja ela convencional ou não convencional. Para os autores, 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 e 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 as ameaças cibernéticas sociais reais ou iminentes. E mais ainda, na atualidade, a tecnologia capacita atores estatais e não estatais a manipularem o mundo de crenças e ideias, à velocidade de algoritmos (BESKOW e CARLEY; 2019, p. 26).

> O enfraquecimento da confiança nas instituições nacionais pode levar a um ator oponente, estatal ou não estatal, a vencer uma guerra, antes do seu início.

Segundo os autores do artigo *Segurança Cibernética Social*, a guerra da informação, analisada pela ótica da *guerra híbrida*, está se tornando um fim em si mesmo. Na análise, registram que as guerras de informação são o principal tipo de guerra do mundo contemporâneo. A informação é empregada para fortalecer a narrativa do manipulador, enquanto faz seu ataque, interrompe, distorce e divide a sociedade, a cultura e os valores dos Estados e organizações oponentes. O enfraquecimento da confiança nas instituições nacionais pode levar a um ator oponente, estatal ou não estatal, a vencer uma guerra, antes do seu início (BESKOW e CARLEY; 2019, p. 26).

Tendo como plataforma de estudos o ambiente operacional em que as forças armadas dos EUA são empregadas, Beskon e Carley registram que o papel da informação dentro dos elementos da expressão do poder nacional está se tornando cada vez mais importante. Esse fato é perceptível, quando a *National Defense Strategy* (USA; 2018) define prioridades de investimento do ano fiscal de 2019-2023, para o espaço e ciberespaço como domínios de guerra; e para comando, controle, comunicações, computadores e inteligência, vigilância e reconhecimento, na defesa contra atores estatais e não estatais.

Na reflexão realizada, afirmam que a tecnologia permite que esses atores mencionados ampliem exacerbadamente seu poder no domínio informacional. E mais ainda, que, se não houver uma maior atenção para o fato, ocorrerá uma "*blitzkrieg informacional*", com os mesmos efeitos estratégicos do emprego da *blitzkrieg* alemã na Segunda Guerra Mundial (BESKOW e CARLEY; 2019, p. 26). Essa afirmação foi construída com base nas análises sobre a máquina de propaganda persuasiva russa que, durante muito tempo, foi empregada contra seu público interno e nas cidades satélites da antiga URSS, mudando para atacar alvos no exterior, cuja missão seria a disseminação de narrativas distorcidas para promover agitação e discordância entre os povos. Para além, legitima o debate, com a fala do General Valey Gerasimov, no artigo *O Valor da Ciência Está na Previsão*, de 2013, que definiu a *guerra de informação* como um instrumento importante da estratégia russa a

partir daquele momento, pois ela abria enormes possibilidades assimétricas para diminuir o potencial de combate do oponente.

O mais importante é que essas medidas estavam em consonância com as tradicionais operações da KGB (Comitê de Segurança do Estado) de medidas ativas para enfraquecer o Ocidente (BESKOW e CARLEY; 2019, p. 28). A KGB era uma organização de serviços secretos da antiga URSS, que, após sua dissolução, foi desmembrada em Serviço Federal de Segurança da Federação Russa (FSB) para segurança doméstica e Serviço de Inteligência Estrangeiro (SVR) para atividades no estrangeiro.

Pela teoria da "*blitzkrieg* informacional" russa, analisada por Beskon e Carley (2019, p. 28), a sua função seria abrir caminho entre todas as possíveis fissuras existentes em um Estado, fraturando a nação ou a coalizão, incluindo aí, medidas de exploração de dissidências entre partidos políticos, religiões, sociedades, forças armadas e alianças internacionais, para enfraquecer suas defesas contra um ataque externo.

Para Beskow e Carley, 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; e as ciências sociais[8] no emprego de operações de informação coordenadas com o objetivo de conseguir efeitos estratégicos (BESKOW e CARLEY; 2019, p. 26).

Segundo os autores, o domínio sociocibernético oferece diferentes formas de manobra da *Segurança Cibernética Social*. No domínio, o adversário tem a capacidade tanto de manipular a informação das redes de conhecimento, quanto de manipular as redes sociais[9]. Essas redes podem ser redes sociais (*Facebook* e *Instagram*), redes de conversa (*Whatsapp*), ou redes informacionais (#COVID19), que têm o objetivo de aumentar a agitação e reduzir a confiança interna, independente da narrativa, sendo destinada a criar fissuras na sociedade atacada (BESKOW e CARLEY; 2019, p. 32).

O ataque cibernético contra a Estônia, em 2007, com a interrupção de alguns

[8]Para Beskow e Carley (2019, p. 26-27), a *segurança cibernética social* é uma ciência social computacional multidisciplinar, cujas novas teorias se fundem a teorias da ciência política, sociologia, comunicação, ciência organizacional, marketing, linguística, antropologia, investigação forense, ciência da decisão, e psicologia social.

[9]Para maior detalhamento do assunto, sugere-se observar a tabela: o Modelo BEND de manobras informacionais, publicada em BESKON e CARLEY; 2028, p. 31. As formas de manobra BEND descrevem como um ator pode manipular o mercado de crenças, ideias e informações.

serviços e a remoção de outros, não deixa dúvidas a respeito da necessidade de se entender que: (a) as notícias falsas são importantes; (b) as pessoas podem ser manipuladas; (c) os nossos sistemas precisam de melhor proteção; e (d) o papel que as pessoas desempenham na dimensão humana da *guerra da informação* precisa ser melhor compreendido.

No contexto das operações de informação, os *bots* são cada vez mais utilizados como multiplicadores do poder de combate. Cerca de duas semanas antes dos bombardeios aéreos e da circulação de tropas russas em território georgiano, na guerra de 2008, a infraestrutura do país foi alvo de ofensiva cibernética, por meio de barragens coordenadas de milhões de pedidos – conhecidos como ataques de negação de serviço distribuídos (*Denial of Service – DDoS*) – que terminaram por sobrecarregar vários servidores oficiais da Geórgia. Dois dias mais tarde, as investidas de *DDoS* tornariam inoperante a maioria das páginas oficiais do país. Durante essa fase, os ataques foram particularmente levados a cabo por *botnets* (ARRAES, e NOGUEIRA; 2020, p. 9).

Conforme se pode visualizar na **figura 6**, os *botnets* são uma rede de computadores conectada com a Internet e infectada por um aplicativo malicioso (*malware*) que permite ao servidor o comando e o controle, isto é, permite o envio de comandos a esses *bots*, que servem para degradar um sistema. Eles podem ser usados para lançar mensagens eletrônicas de campanhas publicitárias (*spam*), mas também podem ser empregados para ataques de negação de serviço em larga escala.

Para Beskon e Carley, o *bot* pode ser definido como uma conta de mídia social que utiliza um computador para automatizar as tarefas do aplicativo, com efeito informacional. Como exemplo, uma conta *bot* no *Twitter*, pode automaticamente disparar mensagens, repassar *tuites*, acompanhar, adicionar amigos, replicar, citar e dar um "*like*". Esses *bots* são distribuídos em redes de *bots,* conhecidos com exércitos de *bots* ou *bots* coordenadores, que adicionam amigos, seguem uns aos outros e se promovem mutuamente para dar impressão de popularidade (2019, p. 33).

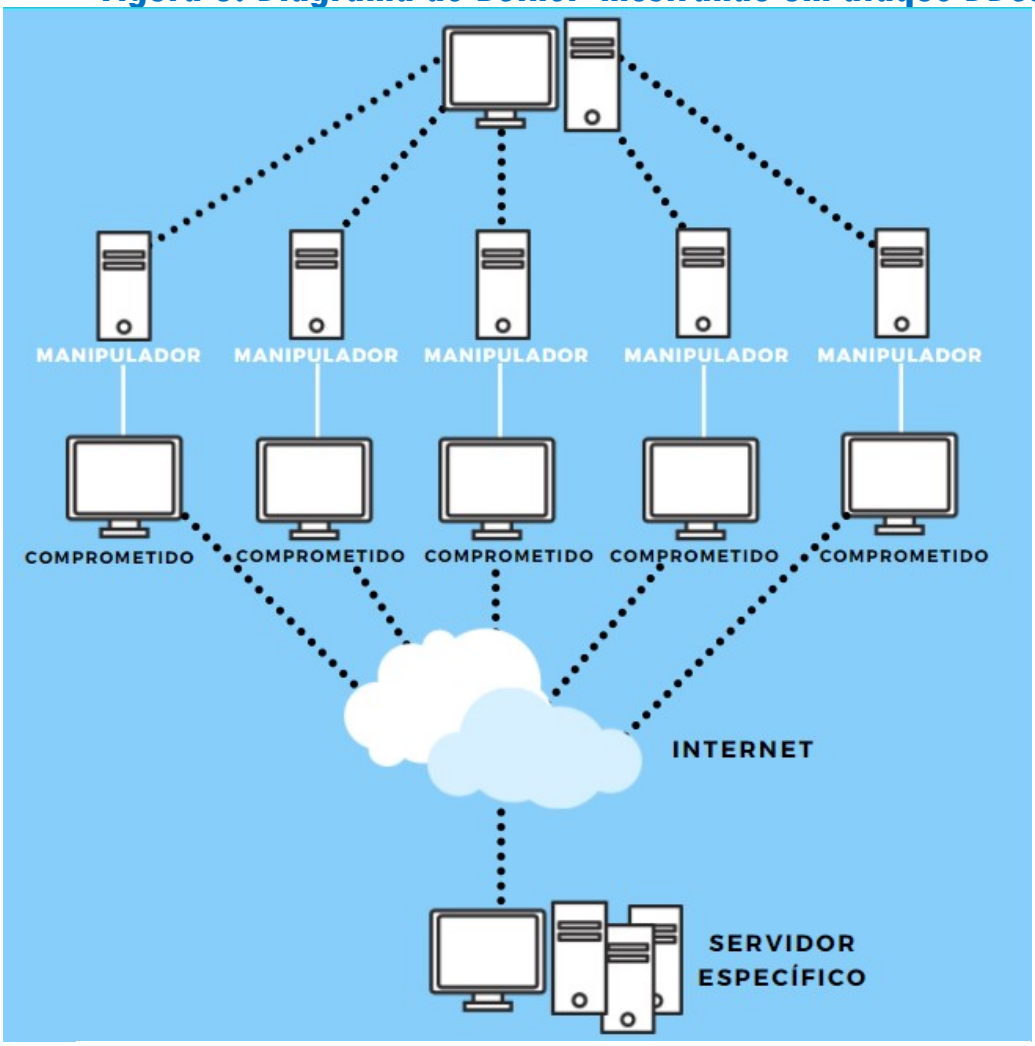
Em 2014, segundo o Relatório Anual sobre Ameaças à Segurança na Internet (*Internet Security Threat Report*, ou ISTR na sigla em inglês), o Brasil ocupava o 8º lugar no *ranking* de países que são origens de ataques cibernéticos por *hackers*. Ainda segundo o ISTR, os Estados Unidos da América lideravam a posição, seguidos da China, da Índia e da Holanda[10]. No entanto, desde 2014, os ataques promovidos por Estados mais que dobraram e os cometidos por *hackers*

[10] Disponível em: http://g1.globo.com/tecnologia/noticia/2014/04/brasil-e-8-pais-em-ranking-de-origem-de-ataques-ciberneticos.html. Acesso em: 11 MAI 2021.

independentes cresceram 83%. Os ataques planejados por grupos terroristas aumentaram 24% até o ano de 2017.

O estudo da PwC[11] mostra que as regiões mais afetadas por ataques cometidos por *hackers*, motivados por questões políticas e ideológicas, foram a Europa (21% dos incidentes), Ásia e Pacífico (21%); em seguida, aparecem Oriente Médio e África (18%), América do Norte (17%) e América do Sul (17%). O setor mais visado pelos *hackers* motivados por questões ideológicas foi o de Telecomunicações, que concentrou 24% dos ataques, seguido pela indústria automotiva (23%) e financeira (21%). Já os atores estatais tiveram como alvo prioritário indústrias do setor de mídia & entretenimento (17%) e 15% dos ataques de terroristas se concentraram no setor aeroespacial e defesa.

Figura 6: Diagrama de *Botnet* mostrando um ataque *DDoS*



Fonte: o autor, com base em https://pt.wikipedia.org/wiki/Botnet

[11] Disponível em: https://www.pwc.com.br/pt/sala-de-imprensa/noticias/ataques-ciberneticos-promovidos-governos-dobraram-ultimos-tres-anos-mostra-pesquisa-pwc.html. Acesso em: 11 maio 2021.

Em 2019, a *Cybersecurity Insiders* divulgou matéria com a lista dos países vulneráveis e os principais produtores de *cyber* ataques[12]. O Brasil (34,68%) figura na lista dos países com maiores taxas de infecção por *malware* em computadores junto com a China (49%) e a Rússia (38,95%), mas também faz parte da lista dos principais países com melhor preparo contra ataques cibernéticos, junto com o Canadá e os Estados Unidos da América. A lista dos países dos quais mais ataques de negação de serviço (*DDoS*) se originaram é liderada pela China (29,56%), EUA (21,59%) e Reino Unido (16,17%).

Em um contexto maior da *Guerra Híbrida*, a OTAN sinalizou, na reunião do Conselho em Bruxelas, ocorrida em 14 de junho de 2021, que passará a tratar os ataques cibernéticos contra infraestruturas críticas e instituições democráticas da mesma forma que uma agressão armada contra qualquer um de seus aliados. Reiterou também que irá considerar uma resposta militar contra Estados que patrocinem grupos *hackers* para perpetrarem esses ataques. A OTAN considerou o ciberespaço como um domínio militar legítimo, determinando o emprego de toda capacidade para dissuadir, defender e combater ativamente todo espectro de ameaças cibernéticas, incluindo aquelas conduzidas como parte de campanhas híbridas[13].

4. Reflexões finais e Implicações para o Exército

Conforme mencionado no início desse estudo, o conceito de *Guerra Híbrida* foi construído ao longo de diversas investigações (RODRIGUES, 2020, 2021a, 2021b) e demonstrou que a sua definição não é tão recente, ou seja, não foi fruto da interpretação do conflito da Rússia com a Ucrânia em 2014, mas teve sua origem na evolução complexa das teorias da guerra. Nesse caso, a *Guerra Híbrida* é entendida como forma de operacionalizar a guerra, quando falamos de uma atividade em si, referindo-nos aos tipos de armas, métodos, teorias, natureza da guerra e outros detalhes associados ao combate. A *guerra híbrida* representa a manifestação do fenômeno em formas de lutar, usado para analisar subsistemas, subdivisões de um todo que é a guerra. Assim sendo, acreditamos que a definição do conceito de *Guerra Híbrida*, do ponto de vista teórico, assume uma grande importância estratégica para o emprego militar do Exército Brasileiro, no contexto de mudanças paradigmáticas nos conflitos na atualidade, como foi o caráter híbrido da conduta da guerra russa na Ucrânia, em 2014.

[12] Disponível em: https://minutodaseguranca.blog.br/lista-de-paises-mais-vulneraveis-%E2%80%8B%E2%80%8Ba-ataques-cibernetico s/. Acesso em: 16 maio 2021.

[13] Disponível em: https://www.defesaemfoco.com.br/otan-adverte-que-considerara-resposta-militar-a-ciberataques/. Acesso em: 17 de junho de 2021.

Nesse contexto, a guerra de informações e a guerra cibernética tornaram-se ferramentas da *Guerra Híbrida*.

Com o passar do tempo, a sociedade tem se tornado cada vez mais conectada à rede mundial de computadores (internet) e às diversas redes de computadores internas (intranet). Nesse contexto, a informatização tem aumentado exponencialmente em todos os setores do Estado, tais como: segurança, defesa, infraestruturas críticas, educação, saúde, comunicação, mas também entre as instituições privadas e a sociedade civil.

Nos anos 1990, por exemplo, o uso da internet foi crucial para que o *Exército Zapatista de Libertação Nacional*, no México, atingisse um público mais amplo, com narrativas favoráveis e apoio a sua causa, naquilo que foi chamado por Tássio Franchi e Leonardo Vichi de militância cibernética ou guerra de internet. Nada diferente da forma de atuação, nos dias de hoje, de grupos como o *Hezbollah* e o *Estado Islâmico* (ISIS). O desafio do século XXI será prover uma segurança de qualidade que permita proteger as informações, os recursos, a privacidade, os organismos estatais e a sociedade (FRANCHI e VICHI, 2019, p. 131 e 133).

A Força Terrestre deve entender melhor o conceito de *segurança cibernética social*, para evitar que as vulnerabilidades internas do país sejam manipuladas por forças externas estatais ou não estatais. Na atualidade, uma das possíveis linhas de ação de uma "*blitzkrieg* informacional" é abrir caminho para criar desconfiança entre as forças armadas e a sociedade e, em alguns casos, aprofundar mais ainda o alto patamar de desconfiança da sociedade em relação aos políticos em geral, explorando muitas vezes a corrupção, agravada pelo cenário epidemiológico de COVID-19. Nesse caso, pode ocorrer uma zona de convergência entre a guerra cibernética e a guerra de informação, tendo a opinião pública como centro de gravidade.

Como sinaliza Visacro, diante das mudanças de realidade do combate, 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 (2018, p. 120-121).

Segundo Visacro (2018, p. 159), com relação às novas capacidades requeridas pelas forças armadas para atuar nos conflitos armados do século XXI, que envolvem as

chamadas "Guerras Híbridas", as organizações militares devem 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 das análises de antropólogos e profissionais das ciências humanas, com capacidade analítica etnográfica para atuar em ambientes multiculturais;
- interagir com a mídia, organismos de defesa dos direitos humanos, organizações não governamentais e outras agências estatais, presentes no interior da área de operações; e
- fazer uso habilidoso dos instrumentos jurídicos que lhe estão disponíveis, para assegurar a legitimidade do uso da força.

Cada vez mais, o Exército deve dar importância às Operações de Informação no mundo contemporâneo, marcado pelo desenvolvimento das *Guerras Híbridas*, incentivando a consolidação de uma cultura militar integradora no nível tático das capacidades, conforme explicitado no *Manual de Operações de Informação*: inteligência, guerra eletrônica, operações psicológicas, comunicação social, e guerra cibernética. Essas capacidades devem ser cada vez mais desenvolvidas, em um contexto amplo, de maneira que haja o desenvolvimento mais eficaz das operações de informação, no nível operacional.

No nosso entendimento, o que ficou evidente é que a grande variedade de tipos de conflitos modernos, somada à nova forma de fazer a guerra, tem uma relação direta tanto com os novos e avançados meios tecnológicos, como 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 que têm o objetivo de 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 em uma *Guerra Híbrida* é necessário obter sucesso nos campos de batalha convencional e assimétrico. Por isso, o planejamento das atividades operacionais e estratégicas não pode ser realizado como se estivéssemos travando duas guerras separadas, uma no campo de batalha convencional e outra com relação à segurança e estabilização da população.

Ao longo do estudo, ficou claro, ainda, que, na *Guerra Híbrida*, existe a necessidade de potencializar o uso de 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 atuais e criativas, com base no pensamento inovador para solução dos problemas militares contemporâneos, como o uso combinado do emprego de forças especiais com guerra cibernética, ou operações de informações e operações de dissimulação. No entanto, a utilização das forças especiais, nesse contexto, vai além do emprego tradicional e possui alcance político. Atingir objetivos, em cenários sem combates, é um exemplo de emprego desse tipo de tropa num 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.

Nesse sentido, é importante dizer que a definição da *Guerra Híbrida* não pode ser considerada apenas uma resposta assimétrica, empregada por um poder militar mais fraco, estatal ou não estatal. Uma nova forma de guerrear aparece nos conflitos da atualidade, com a capacidade de engajar de modo efetivo as diversas formas simultâneas de fazer a guerra. Seguindo uma proposta com melhor definição, esse novo 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.

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 Brasileiro, estão em intenso desenvolvimento, mas esbarram em problemas internos, de uso combinado das capacidades relacionadas à informação e externos, de adequação do seu planejamento estratégico com os interesses de outras forças na realização de operações conjuntas. Esses fatores dificultam a necessidade real de integração e sincronização das capacidades relacionadas à informação e aos recursos relacionados às operações de informação. No entanto, com relação à Defesa Cibernética e à Guerra Cibernética, essa capacidade parece apresentar o maior grau de integração no Ministério da Defesa, por conta da criação do Comando de Defesa Cibernética, tornando-se um importante agente integrador entre as Forças, apesar da dificuldade de realizar operações conjuntas.

Assim como a Estônia, que, após os ataques de 2007, mudou radicalmente sua defesa cibernética, adotando uma estratégia nacional de segurança cibernética, o Brasil deve ficar atento a algumas medidas que podem ser consideradas importantes para

adoção. Além disso, é necessário analisar a utilização de ferramentas híbridas no combate e/ou realizar operações de natureza híbrida. Fica evidente a necessidade de manter nossa estratégia nacional de segurança cibernética sempre atualizada na mesma proporção que ocorre a modernização dos sistemas de tecnologia da informação. Outra ação importante consiste na associação a empresas privadas para construir sistemas mais seguros. Uma medida adotada pelo país báltico, que pode servir de modelo para o Brasil, é a montagem de um *Data Center* de segurança máxima ("embaixada de dados" em Luxemburgo) que contenha *backups* de segurança para o caso de um ataque. Aquele país também se tornou um dos primeiros a usar a tecnologia *blockchain* (espécie de banco de dados à prova de violação) e estabeleceu uma nova unidade cibernética dentro de sua Liga de Defesa, uma organização formada por voluntários, além de pressionar a OTAN e outras organizações por mais cooperação internacional. Contudo, o ponto mais importante foi o investimento maciço em pessoal especializado, pois a tecnologia dá as ferramentas para proteger o sistema, mas o nível da segurança depende fundamentalmente dos usuários. É importante lembrar que alguns dos ataques cibernéticos mais danosos da atualidade não foram causados por um *hacker* sofisticado usando uma tecnologia avançada[14]. Pelo contrário, foram ocasionados por pessoas com acesso às informações privilegiadas nas empresas, após clicaram em um link de *phishing*.

O governo estoniano tem realizado, nos últimos anos, vultosos investimentos em programas de educação e treinamento. A política do Estado está garantindo que todos os cidadãos tenham acesso ao treinamento de que precisam para manter os sistemas de tecnologia da informação do país mais seguros, tais como campanhas de conscientização, oficinas especializadas para idosos e aulas de codificação para estudantes do jardim de infância (pré-escolar). Além de ensinar defesa, o governo está ensinando aos seus adolescentes a *hackear* em ambiente seguro e ético. Alguns ataques desses adolescentes ajudam as empresas a encontrarem vulnerabilidades em seus sistemas.

Cada vez mais, o Exército deve ficar atento à prospecção de novas tecnologias e ao funcionamento dos modernos sistemas com capacidade de proteção e vigilância do território nacional. Importante também não só dar continuidade, mas também intensificar 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

[14] Para mais informações ver: https://www.cnnbrasil.com.br/amp/business/2021/06/19/como-as-ameacas-russas-fizeram-da-estonia-um-pais-em-especialista-ciberseguranca?__twitter_impression=true. Acesso em: 19 jun. 2021.

dados entre diversos escalões da Força Terrestre.

Dessa forma, a prospecção de novas tecnologias civis brasileiras, mais simples e mais baratas, pode ajudar na proteção e na vigilância, como é o caso do *Atobá*[15], um veículo aéreo não tripulado (VANT) de grande porte, produzido pela *Stella Tecnologias*, empresa fluminense, com a participação de estudantes de engenharia da UFRJ, que cedeu também, laboratórios para realização de testes. O VANT foi projetado para aplicações militares e para a área de segurança pública. O seu primeiro voo de sucesso foi realizado em julho de 2020.

O *Atobá* foi idealizado para ser usado em operações de reconhecimento e de vigilância de fronteiras e da faixa oceânica pelas Forças Armadas. Também pode ser empregado em missões de busca e salvamento e no monitoramento de grandes eventos por forças policiais. O drone de 500 kg, 8 metros de comprimento e 11 metros de envergadura tem capacidade para levar 70 kg de equipamento, como radares, câmeras de vigilância e sensores multiespectrais. O aparelho desloca-se a 150 km/h e pode alcançar 5 mil metros de altitude, o que o torna imperceptível pelo simples olhar do homem. O *Atobá* pode ser adaptado, ainda, para carregar mísseis e bombas, desde que sejam respeitados seus limites de peso.

Figura 7: VANT Atobá

Fonte: https://revistapesquisa.fapesp.br/wp-content/uploads/2021/01/079-081_drone-atoba_299-1-1140.jpg

[15] Disponível em: https://revistapesquisa.fapesp.br/o-atoba-alca-voo/. Acesso em: 16 fev. 2021.

Para a proposta da nova Estratégia Nacional de Defesa (BRASIL; 2020a), a capacidade de proteção do território e da população brasileira exprime o mais relevante objetivo nacional: o de garantir a soberania, do patrimônio nacional e da integridade nacional. Segundo o documento, o que importa é dotar a Nação da capacidade de resposta em situações excepcionais, preservando-se o funcionamento normal das funções vitais do Estado.

No entanto, o Exército deve, cada vez mais, se preocupar com o desenvolvimento de dispositivos de proteção adequados para os seus sistemas de informação. É importante a adoção de mecanismos de defesa capazes de reduzir os riscos contra os nossos sistemas de informação e infraestrutura crítica, tornando-os menos vulneráveis contra ataques cibernéticos.

Os anos de 2020 e 2021, marcados pela Pandemia do COVID-19, tornam-se o momento exato para pensar em avaliações na segurança das condições de trabalho em *home office* e da segurança cibernética, pois, neste momento, a guerra cibernética e os crimes digitais tornaram-se as principais ameaças. A pandemia obrigou vários setores do governo, 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 cada vez mais ficar atentas aos possíveis ataques por parte de Estados oponentes ou de criminosos virtuais. Devemos aumentar a preocupação com a defesa cibernética brasileira e com a segurança nacional, contra potenciais ataques cibernéticos aos setores estratégicos e as infraestruturas críticas do país, como foi o caso do ataque *hacker* ao sistema de tecnologia da informação da EMBRAER[16], o ataque cibernético à Eletronuclear subsidiária da Eletrobrás[17], a tentativa de ataque ao sistema do Tribunal Superior Eleitoral, todos em 2020, e o vazamento[18] de dados telefônicos de mais de 100 milhões de brasileiros em 03 de fevereiro de 2021.

Apesar da Política Nacional de Defesa e da Estratégia Nacional de Defesa (BRASIL; 2020a), elaboradas no ano de 2020 e entregues ao Congresso Nacional no mês de julho, tratarem o Setor Cibernético como uma das três prioridades dos setores estratégicos da Defesa Nacional, o Brasil ainda possui muitas fragilidades e vulnerabilidades na internet, articuladas aos poucos recursos orçamentários para o setor e à pouca disponibilidade de mão de obra de qualidade

[16] Disponível em: https://g1.globo.com/sp/vale-do-paraiba-regiao/noticia/2020/12/09/embraer-investiga-volume-de-dados-vazados-apos-ter-sofrido-ataque-hacker.ghtml. Acesso em: 15 jan. 2021.
[17] Disponível em: https://oglobo.globo.com/economia/eletrobras-diz-que-eletronuclear-sofreu-ataque-cibernetico-mas-sem-risco-seguranca-das-operacoes-1-24868756. Acesso em: 16 fev. 2021.
[18] Disponível em: https://www.cnnbrasil.com.br/business/2021/02/10/novo-vazamento-expoe-dados-telefonicos-de-mais-de-100-milhoes-de-brasileiros. Acesso em: 16 fev. 2021.

para ser empregada na área de defesa cibernética.

Não obstante, estudos recentes analisando as Estratégias Nacionais de Defesa publicadas no período de 2008 a 2018, demonstram que o setor cibernético no Brasil, pode trazer a oportunidade de fornecimento de um bem público para a Defesa com transbordamento econômico-tecnológico para outros setores, com o fomento da pesquisa e da inovação, com a integração dos setores públicos e privados e a integração entre a Academia e a Indústria, dentro do binômio "Defesa e Desenvolvimento", no contexto da Segurança Nacional. Esse debate é bastante legítimo, pois o núcleo da defesa cibernética é baseado em ferramentas de tecnologia da informação e comunicação, o que permitiria a formação de um ciclo virtuoso entre coerção e riqueza e a possibilidade na composição de um complexo militar-universitário-industrial no formato do sistema tríplice hélice[19].

O mundo está se tornando cada vez mais refém da tecnologia e o espaço cibernético, no contexto da *Guerra Híbrida,* 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 cada vez mais necessário fortalecer o setor de defesa cibernética. Em relação ao 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, neste novo ambiente de conflito, possuirmos tecnologias nacionais, visando suavizar as nossas vulnerabilidades que poderão ser exploradas por um potencial oponente.

[19] FERREIRA NETO, 2020, p. 122-124.

Referências

ARRAES, Virgílio Caixeta, e NOGUEIRA, Michel Gomes. A Guerra Russo-Georgiana (2008): a inovação tecnológica em campo. *Meridiano 47*, Journal of Golbal Studies, 21: e21001, 2020. Publicado em: https://periodicos.unb.br/index.php/MED/article/view/29160/26174. Acesso em 16/01/2021.

BESKOW, David M., e CARLEY, Kathleen M.. Segurança Cibernética Social – Um requisito emergente de Segurança Nacional. *Military Review*. Terceiro Trimestre 2019. Disponível em: https://www.armyupress.army.mil/Portals/7/military-review/Archives/Portuguese/Beskow-Carley-Seguranca-Cibernetica-Social-POR-Q3-2019.pdf. Acesso em: 14 jan. 2021.

BRASIL. *Constituição da República Federativa do Brasil*. 1988.

BRASIL. Diretriz Ministerial nº 14: integração e coordenação dos setores estratégicos da defesa. Brasília: Ministério da Defesa, 2009.

BRASIL. *Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa, 2012a.

BRASIL. *Doutrina Militar de Defesa Cibernética*. Brasília: Ministério da Defesa, 2014. Disponível em: https://www.gov.br/defesa/pt-br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31a_ma_08a_defesaa_ciberneticaa_1a_2014.pdf. Acesso em: 17/ jan. 2021.

BRASIL. *Política Nacional de Segurança de Infraestruturas Críticas*. Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 19 jun. 2021.

BRASIL. *Estratégia Nacional de Defesa*. Brasília: Ministério da Defesa, 2020a. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 17 jan. 2021. **(Para Aprovação)**

BRASIL. *Estratégia Nacional de Segurança Cibernética*. Presidência da República, decreto nº 10.222, de 05 de fevereiro de 2020b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm#:~:text=A%20presente%20Estrat%C3%A9gia%20Nacional%20de,validade%20no%20quadri%C3%AAnio%202020%2D2023. Acesso em: 15 jan. 2021.

BRASIL. *Sistema Militar de Defesa Cibernética*. Brasília: Ministério da Defesa, 2020c. Disponível em: https://www.in.gov.br/web/dou/-/portaria-n-3.781/gm-md-de-17-de-novembro-de-2020-289248860. Acesso em: 17 jan. 201.

BRASIL. EXÉRCITO BRASILEIRO. Boletim do Exército nº 52. Portaria nº 3.405-MD, de 21 de dezembro de 2012b. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/1/1700/1/be52-12.pdf. Acesso em: 17 jan. 2021.

BRASIL. EXÉRCITO BRASILEIRO. *Manual de Campanha EB20-MC-10.213 Operações de Informação*. Brasília: Estado Maior do Exército, 2014.

BRASIL. EXÉRCITO BRASILEIRO. *Glossário de termos e expressões para uso no Exército*. 5ª Edição. Brasília: Estado-Maior do Exército, 2018.

BRASIL. EXÉRCITO BRASILEIRO. Manual de Fundamentos – *Doutrina Militar Terrestre*. 2ª Edição. Brasília: Estado Maior do Exército, 2019. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/4760/1/EB20-MF-10.102.pdf. Acesso em: 12 jan. 2021.

CANONGIA, Claudia, e MANDARINO JUNIOR, Raphael. Segurança cibernética: o desafio da nova Sociedade da Informação. *Parc. Estrat. Brasília*, v. 14, n. 29, jul-dez 2009, PP. 21-46. Disponível em: http://seer.cgee.org.br/index.php/parcerias_estrategicas/article/viewFile/349/342. Acesso em: 15 jan. 2021.

CHIRIO, Maud. *A política nos quartéis*: revoltas e protestos de oficiais na ditadura militar brasileira. Rio de Janeiro. Zahar, 2012.

COMBLIN, Joseph. *A ideologia da segurança nacional*: o poder militar na América Latina. Ed. Civilização Brasileira, 1978.

CORRÊA, A. J. Operações de informações: um antigo conceito com um novo paradigma. *Coleção Meira Mattos*, revista das ciências militares, nº 27,

3º quadrimestre 2012. Rio de Janeiro: ECEME, 2012. Disponível em: http://www.ebrevistas.eb.mil.br/RMM/article/view/123/211. Acesso em: 13 jan. 2021.

COSTA, Frederico Carlos de Sá. Sobre o conceito de "segurança nacional". *Tensões Mundiais*, v. 5, n. 9, p. 123-140, 22 nov. 2018. Disponível em: https://revistas.uece.br/index.php/tensoesmundiais/article/view/670/556. Acesso em: 05 jan. 2021.

ESCOLA SUPERIOR DE GUERRA. *Fundamentos do Poder Nacional*. Rio de Janeiro: ESG, 2019. Disponível em: https://www.esg.br/publi/FundamentosdoPoderNacional2019FINALFINAL.pdf. Acesso em 07 jan. 2021.

FERREIRA NETO, Walfredo Bento. *Uma Estratégia Nacional de Defesa para além da guerra*: geopolítica cibernética e seu transbordamento econômico-tecnológico no Brasil (2008-2018). Tese de Doutorado em Economia Política Internacional. Rio de Janeiro: Pepi/IE/UFRJ, 2020.

FOUCHER, Michel. *L'invention des frontières*. Paris: Fondation pour les Études de Défense Nationale, 1986. Disponível em: <https://gallica.bnf.fr/ark:/12148/bpt6k3322804w/f48.item>. Acesso em 17 junho de 20210.

FRANCHI, Tássio, e VICHI, Leonardo Perin. The beginning of warfare on the internet: zapatista strategic communications. *Defence Strategic Communications*. The official journal of the NATO Strategic Communications - Centre of Excellence, Volume 6, Spring 2019. DOI: 10.30966/2018. RIGA.6. Disponível em: https://stratcomcoe.org/t-franchi-l-perin-vichi-beginning-warfare-internet-zapatista-strategic-communications. Acesso em: 16 fev. 2021.

HEYDTE, Friedrich August Von der. *A Guerra Irregular Moderna*: em políticas de defesa e como fenômeno militar. Rio de Janeiro: Bibliex, 1990.
HERZ, M. Concepts of Security in South America. *Internacional Peacekeeping*, v. 17, n. 5, p. 598-612, 2010.
HOBBES, T. *Leviatã, ou Matéria, forma e poder de um estado eclesiástico e civil*. São Paulo: Abril Cultural, 1979.

HOFFMAN, Frank G. *Conflict in the 21ST century*: the rise of hybrid wars. Virgínia: Potomac Institute for Policy Studies, 2007.

HUBER, Thomas M. *Compound Warfare*: That Fatal Knot. General Editor. Kansas: US Army Command and General Staff College Press, 2002.

LIANG, Qiao and XIANGSUI, Wang. *Unrestricted Warfare*. Beijing: PLA Literature and Arts Publishing, 1999.

LIND, William S. Understanding Fourth Generation War. *Military Review*. Setembro-Outubro 2004.

MOTA, Rui Martins da; e AZEVEDO, Carlos E. Franco. A Guerra Omnidimensional: novas concepções do Pensamento Estratégico Militar. Revista da Escola Superior de Guerra, v. 27, n. 55, p. 55-68, jul./dez., 2012.

OLIVEIRA, Marco Aurélio Guedes de; e CASALUNGA, Fernando Henrique. Guerra Híbrida: o emprego da tecnologia da informação no conflito Rússia-Ucrânia (2014-2015). Rev. Bras. Est. Def., v. 7, nº. 2, jul./dez. 2020, p. 9-36. Disponível em: https://rbed.abedef.org/rbed/article/view/75208/42129. Acesso em: 21 jul. 2021.

RICHTER, Walter E. O futuro das Operações de Informações. *Militar Review*. Edição Brasileira. U.S. Army, Maio-junho, 2009. Disponível em: https://www.armyupress.army.mil/Journals/Edicao-Brasileira/Artigos-em-Destaque/2018/O-Futuro-das-Operacoes-de-Informacoes/. Acesso em: 13 jan. 2021.

RODRIGUES, Fernando da Silva. Guerra Híbrida: anexação da Crimeia e Crise da Ucrânia sob a perspectiva político-estratégica da OTAN. *Revista Análise Estratégica*. Vol 20 (2) Mar / Maio 2021a.

RODRIGUES, Fernando da Silva. Anexação da Crimeia e a Crise da Ucrânia sob a perspectiva político-estratégica da Rússia. *Revista Análise Estratégica*. Vol 19 (1) Dez 2020/Fev 2021b. Disponível em: http://www.ebrevistas.eb.mil.br/CEEExAE/article/view/7731/6700
RODRIGUES, Fernando da Silva. Guerra Híbrida: por uma discussão conceitual. *Revista Análise Estratégica*. Vol 18 (4) Set/Nov 2020. Disponível em: http://www.ebrevistas.eb.mil.br/CEEExAE/article/view/7012

SOESANTO, Stefan. *Trend Analysis*: the evolution of US deterrence strategy in cyberspace (1988-2019). Zurich: Center for Security Studies, 2019. Disponível em: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2019-08-The-Evolution-of-US-defense-strategy-in-cyberspace.pdf. Acesso em: 15 jan. 2021.

TEIXEIRA JÚNIOR, Augusto W. M. A guerra do futuro e suas implicações estratégicas: uma perspectiva Clausewitziana. *Análise Estratégica*, vol. 11 (1), Dez/Fev, 2019.

UNITED STATE OF AMERICA (USA). FM 100-16, *Information Operations.* Washington, DC: U.S. Government Printing Office, 27 August 1996.

UNITED STATE OF AMERICA (USA). *Information Operations Roadmap*. Department of Defense, 30 October 2003. Disponível em: http://www.iwar.org.uk/iwar/resources/io/io-roadmap.pdf. Acesso em: 13 jan. 2021.

UNITED STATE OF AMERICA (USA). JP 3-13, *Information Operations*. U.S. Joint Publication: 13 de fevereiro de 2006. Disponível em: https://fas.org/irp/doddir/dod/jp3_13.pdf. Acesso em: 13 jan. 2021.

UNITED STATE OF AMERICA (USA). *National Defense Strategy* 2018. Disponível em: https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf. Acesso em 16 jan. 2021.

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

WALKER, Márcio Saldanha. *A integração das capacidades relacionadas à informação nas Operações de Informação de Estado-Maior Conjunto*. Tese de Doutorado. Rio de Janeiro: Escola de Comando e Estado-Maior do Exército, 2017.